## CONTENTS

### Chapter 1
**Introduction to this guide**
- About this guide ........................................................................................................ 32
- Isilon scale-out NAS overview .................................................................................. 32
- IsilonSD Edge overview .............................................................................................. 32
- Where to go for support ........................................................................................... 32
  - Self-service support ............................................................................................... 33

### Chapter 2
**Isilon scale-out NAS**
- OneFS storage architecture ....................................................................................... 36
- Isilon node components ............................................................................................ 36
- Internal and external networks .................................................................................. 37
- Isilon cluster .............................................................................................................. 37
  - Cluster administration ............................................................................................ 37
  - Quorum .................................................................................................................. 38
  - Splitting and merging ............................................................................................ 39
  - Storage pools .......................................................................................................... 39
- The OneFS operating system ...................................................................................... 39
  - Data-access protocols ............................................................................................ 40
  - Identity management and access control ............................................................... 40
- Structure of the file system ......................................................................................... 41
  - Data layout .............................................................................................................. 42
  - Writing files ............................................................................................................ 42
  - Reading files ........................................................................................................... 42
  - Metadata layout ..................................................................................................... 43
  - Locks and concurrency ......................................................................................... 43
  - Striping ................................................................................................................... 43
- Data protection overview ............................................................................................ 44
  - N+M data protection .............................................................................................. 45
  - Data mirroring ........................................................................................................ 45
  - The file system journal ......................................................................................... 45
  - Virtual hot spare (VHS) ....................................................................................... 46
  - Balancing protection with storage space .............................................................. 46
- VMware integration ................................................................................................... 46
- Software modules ...................................................................................................... 46

### Chapter 3
**Introduction to the OneFS command-line interface**
- OneFS command-line interface overview .................................................................. 50
  - IsilonSD Edge command-line interface overview ................................................ 50
- Syntax diagrams ........................................................................................................ 50
- Universal options ...................................................................................................... 51
- Command-line interface privileges ......................................................................... 52
- SmartLock compliance command permissions ....................................................... 52
- OneFS time values ................................................................................................... 54

### Chapter 4
**General cluster administration**
- General cluster administration overview ................................................................ 58
- User interfaces ......................................................................................................... 58
- Connecting to the cluster ......................................................................................... 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to the web administration interface</td>
<td>59</td>
</tr>
<tr>
<td>Open an SSH connection to a cluster</td>
<td>60</td>
</tr>
<tr>
<td>Licensing</td>
<td>60</td>
</tr>
<tr>
<td>License status</td>
<td>61</td>
</tr>
<tr>
<td>License configuration</td>
<td>64</td>
</tr>
<tr>
<td>Activate a license</td>
<td>64</td>
</tr>
<tr>
<td>View license information</td>
<td>65</td>
</tr>
<tr>
<td>Certificates</td>
<td>65</td>
</tr>
<tr>
<td>Replace or renew the SSL certificate</td>
<td>65</td>
</tr>
<tr>
<td>Verify an SSL certificate</td>
<td>67</td>
</tr>
<tr>
<td>Self-signed SSL certificate data example</td>
<td>67</td>
</tr>
<tr>
<td>Cluster identity</td>
<td>67</td>
</tr>
<tr>
<td>Set the cluster name</td>
<td>68</td>
</tr>
<tr>
<td>Cluster contact information</td>
<td>68</td>
</tr>
<tr>
<td>Specify contact information</td>
<td>69</td>
</tr>
<tr>
<td>Cluster date and time</td>
<td>69</td>
</tr>
<tr>
<td>Set the cluster date and time</td>
<td>70</td>
</tr>
<tr>
<td>Specify an NTP time server</td>
<td>71</td>
</tr>
<tr>
<td>SMTP email settings</td>
<td>71</td>
</tr>
<tr>
<td>Configure SMTP email settings</td>
<td>71</td>
</tr>
<tr>
<td>View SMTP email settings</td>
<td>71</td>
</tr>
<tr>
<td>Configuring the cluster join mode</td>
<td>72</td>
</tr>
<tr>
<td>Specify the cluster join mode</td>
<td>72</td>
</tr>
<tr>
<td>File system settings</td>
<td>73</td>
</tr>
<tr>
<td>Specify the cluster character encoding</td>
<td>73</td>
</tr>
<tr>
<td>Enable or disable access time tracking</td>
<td>74</td>
</tr>
<tr>
<td>Security hardening</td>
<td>74</td>
</tr>
<tr>
<td>STIG hardening profile</td>
<td>75</td>
</tr>
<tr>
<td>Apply a security hardening policy</td>
<td>76</td>
</tr>
<tr>
<td>Revert a security hardening policy</td>
<td>77</td>
</tr>
<tr>
<td>View the security hardening status</td>
<td>78</td>
</tr>
<tr>
<td>Cluster monitoring</td>
<td>79</td>
</tr>
<tr>
<td>Monitor the cluster</td>
<td>79</td>
</tr>
<tr>
<td>View node status</td>
<td>79</td>
</tr>
<tr>
<td>Monitoring cluster hardware</td>
<td>80</td>
</tr>
<tr>
<td>View node hardware status</td>
<td>80</td>
</tr>
<tr>
<td>Chassis and drive states</td>
<td>80</td>
</tr>
<tr>
<td>Check battery status</td>
<td>83</td>
</tr>
<tr>
<td>SNMP monitoring</td>
<td>84</td>
</tr>
<tr>
<td>Events and alerts</td>
<td>87</td>
</tr>
<tr>
<td>Events overview</td>
<td>88</td>
</tr>
<tr>
<td>Event groups overview</td>
<td>88</td>
</tr>
<tr>
<td>Alerts overview</td>
<td>88</td>
</tr>
<tr>
<td>Channels overview</td>
<td>89</td>
</tr>
<tr>
<td>Viewing and modifying event groups</td>
<td>89</td>
</tr>
<tr>
<td>Managing alerts</td>
<td>91</td>
</tr>
<tr>
<td>Managing channels</td>
<td>92</td>
</tr>
<tr>
<td>Maintenance and testing</td>
<td>95</td>
</tr>
<tr>
<td>Cluster maintenance</td>
<td>97</td>
</tr>
<tr>
<td>Replacing node components</td>
<td>97</td>
</tr>
<tr>
<td>Upgrading node components</td>
<td>97</td>
</tr>
<tr>
<td>Managing drive firmware</td>
<td>98</td>
</tr>
<tr>
<td>Managing cluster nodes</td>
<td>104</td>
</tr>
<tr>
<td>Upgrading OneFS</td>
<td>106</td>
</tr>
<tr>
<td>Remote support</td>
<td>107</td>
</tr>
<tr>
<td>Configuring ESRS support</td>
<td>107</td>
</tr>
<tr>
<td>isi_phone_home</td>
<td>172</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td><strong>Event commands</strong></td>
<td></td>
</tr>
<tr>
<td>isi event alerts create</td>
<td>173</td>
</tr>
<tr>
<td>isi event alerts delete</td>
<td>176</td>
</tr>
<tr>
<td>isi event alerts list</td>
<td>176</td>
</tr>
<tr>
<td>isi event alerts modify</td>
<td>177</td>
</tr>
<tr>
<td>isi event alerts view</td>
<td>179</td>
</tr>
<tr>
<td>isi event channels create</td>
<td>180</td>
</tr>
<tr>
<td>isi event channels delete</td>
<td>182</td>
</tr>
<tr>
<td>isi event channels list</td>
<td>182</td>
</tr>
<tr>
<td>isi event channels modify</td>
<td>182</td>
</tr>
<tr>
<td>isi event channels view</td>
<td>187</td>
</tr>
<tr>
<td>isi event events list</td>
<td>187</td>
</tr>
<tr>
<td>isi event events view</td>
<td>187</td>
</tr>
<tr>
<td>isi event groups bulk</td>
<td>188</td>
</tr>
<tr>
<td>isi event groups list</td>
<td>188</td>
</tr>
<tr>
<td>isi event groups modify</td>
<td>191</td>
</tr>
<tr>
<td>isi event groups view</td>
<td>191</td>
</tr>
<tr>
<td>isi event settings modify</td>
<td>191</td>
</tr>
<tr>
<td>isi event settings view</td>
<td>192</td>
</tr>
<tr>
<td>isi event test create</td>
<td>192</td>
</tr>
<tr>
<td><strong>Hardware commands</strong></td>
<td></td>
</tr>
<tr>
<td>isi batterystatus list</td>
<td>193</td>
</tr>
<tr>
<td>isi batterystatus view</td>
<td>193</td>
</tr>
<tr>
<td>isi devices add</td>
<td>193</td>
</tr>
<tr>
<td>isi devices drive add</td>
<td>193</td>
</tr>
<tr>
<td>isi devices drive firmware list</td>
<td>195</td>
</tr>
<tr>
<td>isi devices drive firmware update list</td>
<td>195</td>
</tr>
<tr>
<td>isi devices drive firmware update start</td>
<td>196</td>
</tr>
<tr>
<td>isi devices drive firmware update view</td>
<td>196</td>
</tr>
<tr>
<td>isi devices drive firmware view</td>
<td>196</td>
</tr>
<tr>
<td>isi devices drive format</td>
<td>196</td>
</tr>
<tr>
<td>isi devices drive list</td>
<td>198</td>
</tr>
<tr>
<td>isi devices drive purpose</td>
<td>198</td>
</tr>
<tr>
<td>isi devices drive purposelist</td>
<td>199</td>
</tr>
<tr>
<td>isi devices drive smartfail</td>
<td>199</td>
</tr>
<tr>
<td>isi devices drive stopfail</td>
<td>200</td>
</tr>
<tr>
<td>isi devices drive suspend</td>
<td>201</td>
</tr>
<tr>
<td>isi devices drive suspend</td>
<td>201</td>
</tr>
<tr>
<td>isi devices firmware list</td>
<td>201</td>
</tr>
<tr>
<td>isi devices firmware update list</td>
<td>202</td>
</tr>
<tr>
<td>isi devices firmware update start</td>
<td>203</td>
</tr>
<tr>
<td>isi devices firmware update view</td>
<td>203</td>
</tr>
<tr>
<td>isi devices firmware view</td>
<td>205</td>
</tr>
<tr>
<td>isi devices format</td>
<td>205</td>
</tr>
<tr>
<td>isi devices list</td>
<td>205</td>
</tr>
<tr>
<td>isi devices node add</td>
<td>205</td>
</tr>
<tr>
<td>isi devices node list</td>
<td>206</td>
</tr>
<tr>
<td>isi devices node smartfail</td>
<td>206</td>
</tr>
<tr>
<td>isi devices node stopfail</td>
<td>207</td>
</tr>
<tr>
<td>isi devices purpose</td>
<td>207</td>
</tr>
<tr>
<td>isi devices purposelist</td>
<td>208</td>
</tr>
<tr>
<td>isi devices smartfail</td>
<td>208</td>
</tr>
<tr>
<td>isi devices stopfail</td>
<td>209</td>
</tr>
<tr>
<td>isi devices suspend</td>
<td>209</td>
</tr>
<tr>
<td>isi devices view</td>
<td>210</td>
</tr>
</tbody>
</table>
Chapter 5  Access zones 215
Access zones overview .......................................................... 216
Base directory guidelines...................................................... 216
Access zones best practices................................................... 217
Access zone limits............................................................... 218
Quality of service............................................................... 218
Managing access zones....................................................... 219
Create an access zone......................................................... 219
Assign an overlapping base directory................................. 220
Manage authentication providers in an access zone............. 220
Associate an IP address pool with an access zone.............. 221
Modify an access zone....................................................... 221
Delete an access zone....................................................... 221
View a list of access zones.................................................. 222
Access zone commands..................................................... 222
isi zone restrictions create.................................................. 222
isi zone restrictions delete............................................... 223
isi zone restrictions list.................................................... 224
isi zone zones create....................................................... 225
isi zone zones delete....................................................... 226
isi zone zones list.......................................................... 226
isi zone zones modify..................................................... 227
isi zone zones view........................................................ 229

Chapter 6  Authentication 231
Authentication overview.......................................................... 232
Authentication provider features......................................... 232
Supported authentication providers.................................... 232
Active Directory................................................................. 233
LDAP........................................................................... 234
NIS............................................................................ 234
Kerberos authentication...................................................... 235
Keytabs and SPNs overview................................................. 235
MIT Kerberos protocol support.......................................... 236
File provider................................................................. 236
Local provider............................................................... 236
Managing Active Directory providers................................ 237
Configure an Active Directory provider............................. 237
Modify an Active Directory provider................................ 238
Delete an Active Directory provider................................. 238
Managing LDAP providers................................................. 238
Configure an LDAP provider.............................................. 238
Modify an LDAP provider................................................ 239
Delete an LDAP provider.................................................. 239
Managing NIS providers.................................................... 240
Configure an NIS provider................................................ 240
Modify an NIS provider..................................................... 240
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete an NIS provider</td>
<td>240</td>
</tr>
<tr>
<td>Managing MIT Kerberos authentication</td>
<td>240</td>
</tr>
<tr>
<td>Managing MIT Kerberos realms</td>
<td>241</td>
</tr>
<tr>
<td>Managing MIT Kerberos providers</td>
<td>243</td>
</tr>
<tr>
<td>Managing MIT Kerberos domains</td>
<td>245</td>
</tr>
<tr>
<td>Managing SPNs and keys</td>
<td>247</td>
</tr>
<tr>
<td>Managing file providers</td>
<td>249</td>
</tr>
<tr>
<td>Configure a file provider</td>
<td>250</td>
</tr>
<tr>
<td>Generate a password file</td>
<td>250</td>
</tr>
<tr>
<td>Modify a file provider</td>
<td>250</td>
</tr>
<tr>
<td>Delete a file provider</td>
<td>251</td>
</tr>
<tr>
<td>Password file format</td>
<td>251</td>
</tr>
<tr>
<td>Group file format</td>
<td>252</td>
</tr>
<tr>
<td>Netgroup file format</td>
<td>253</td>
</tr>
<tr>
<td>Managing local users and groups</td>
<td>253</td>
</tr>
<tr>
<td>View a list of users and groups by provider</td>
<td>253</td>
</tr>
<tr>
<td>Create a local user</td>
<td>254</td>
</tr>
<tr>
<td>Create a local group</td>
<td>254</td>
</tr>
<tr>
<td>Naming rules for local users and groups</td>
<td>254</td>
</tr>
<tr>
<td>Configure or modify a local password policy</td>
<td>255</td>
</tr>
<tr>
<td>Local password policy settings</td>
<td>255</td>
</tr>
<tr>
<td>Modify a local user</td>
<td>257</td>
</tr>
<tr>
<td>Modify a local group</td>
<td>257</td>
</tr>
<tr>
<td>Delete a local user</td>
<td>257</td>
</tr>
<tr>
<td>Delete a local group</td>
<td>258</td>
</tr>
<tr>
<td>Authentication and access control commands</td>
<td>258</td>
</tr>
<tr>
<td>isi auth access</td>
<td>258</td>
</tr>
<tr>
<td>isi auth ads create</td>
<td>259</td>
</tr>
<tr>
<td>isi auth ads delete</td>
<td>263</td>
</tr>
<tr>
<td>isi auth ads list</td>
<td>263</td>
</tr>
<tr>
<td>isi auth ads modify</td>
<td>264</td>
</tr>
<tr>
<td>isi auth ads view</td>
<td>270</td>
</tr>
<tr>
<td>isi auth ads spn check</td>
<td>270</td>
</tr>
<tr>
<td>isi auth ads spn create</td>
<td>270</td>
</tr>
<tr>
<td>isi auth ads spn delete</td>
<td>271</td>
</tr>
<tr>
<td>isi auth ads spn fix</td>
<td>271</td>
</tr>
<tr>
<td>isi auth ads spn list</td>
<td>272</td>
</tr>
<tr>
<td>isi auth ads trusts controllers list</td>
<td>272</td>
</tr>
<tr>
<td>isi auth ads trusts list</td>
<td>273</td>
</tr>
<tr>
<td>isi auth ads trusts view</td>
<td>273</td>
</tr>
<tr>
<td>isi auth error</td>
<td>274</td>
</tr>
<tr>
<td>isi auth file create</td>
<td>274</td>
</tr>
<tr>
<td>isi auth file delete</td>
<td>277</td>
</tr>
<tr>
<td>isi auth file list</td>
<td>278</td>
</tr>
<tr>
<td>isi auth file modify</td>
<td>278</td>
</tr>
<tr>
<td>isi auth file view</td>
<td>285</td>
</tr>
<tr>
<td>isi auth groups create</td>
<td>286</td>
</tr>
<tr>
<td>isi auth groups delete</td>
<td>287</td>
</tr>
<tr>
<td>isi auth groups flush</td>
<td>287</td>
</tr>
<tr>
<td>isi auth groups list</td>
<td>288</td>
</tr>
<tr>
<td>isi auth groups members list</td>
<td>289</td>
</tr>
<tr>
<td>isi auth groups modify</td>
<td>290</td>
</tr>
<tr>
<td>isi auth groups view</td>
<td>291</td>
</tr>
<tr>
<td>isi auth id</td>
<td>292</td>
</tr>
<tr>
<td>isi auth krb5 create</td>
<td>292</td>
</tr>
<tr>
<td>isi auth krb5 delete</td>
<td>293</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>isi auth krb5 list</td>
<td>293</td>
</tr>
<tr>
<td>isi auth krb5 view</td>
<td>294</td>
</tr>
<tr>
<td>isi auth krb5 domain create</td>
<td>294</td>
</tr>
<tr>
<td>isi auth krb5 domain delete</td>
<td>294</td>
</tr>
<tr>
<td>isi auth krb5 domain list</td>
<td>295</td>
</tr>
<tr>
<td>isi auth krb5 domain modify</td>
<td>295</td>
</tr>
<tr>
<td>isi auth krb5 domain view</td>
<td>295</td>
</tr>
<tr>
<td>isi auth krb5 realm create</td>
<td>296</td>
</tr>
<tr>
<td>isi auth krb5 realm delete</td>
<td>296</td>
</tr>
<tr>
<td>isi auth krb5 realm modify</td>
<td>297</td>
</tr>
<tr>
<td>isi auth krb5 realm list</td>
<td>297</td>
</tr>
<tr>
<td>isi auth krb5 realm view</td>
<td>298</td>
</tr>
<tr>
<td>isi auth krb5 spn create</td>
<td>298</td>
</tr>
<tr>
<td>isi auth krb5 spn delete</td>
<td>298</td>
</tr>
<tr>
<td>isi auth krb5 spn check</td>
<td>299</td>
</tr>
<tr>
<td>isi auth krb5 spn fix</td>
<td>299</td>
</tr>
<tr>
<td>isi auth krb5 spn import</td>
<td>300</td>
</tr>
<tr>
<td>isi auth krb5 spn list</td>
<td>300</td>
</tr>
<tr>
<td>isi auth krb5 spn list</td>
<td>300</td>
</tr>
<tr>
<td>isi auth ldap create</td>
<td>301</td>
</tr>
<tr>
<td>isi auth ldap delete</td>
<td>308</td>
</tr>
<tr>
<td>isi auth ldap list</td>
<td>308</td>
</tr>
<tr>
<td>isi auth ldap modify</td>
<td>309</td>
</tr>
<tr>
<td>isi auth ldap modify</td>
<td>309</td>
</tr>
<tr>
<td>isi auth local list</td>
<td>320</td>
</tr>
<tr>
<td>isi auth local modify</td>
<td>320</td>
</tr>
<tr>
<td>isi auth local view</td>
<td>322</td>
</tr>
<tr>
<td>isi auth log-level modify</td>
<td>322</td>
</tr>
<tr>
<td>isi auth log-level view</td>
<td>323</td>
</tr>
<tr>
<td>isi auth mapping create</td>
<td>323</td>
</tr>
<tr>
<td>isi auth mapping delete</td>
<td>324</td>
</tr>
<tr>
<td>isi auth mapping dump</td>
<td>326</td>
</tr>
<tr>
<td>isi auth mapping import</td>
<td>327</td>
</tr>
<tr>
<td>isi auth mapping list</td>
<td>327</td>
</tr>
<tr>
<td>isi auth mapping modify</td>
<td>328</td>
</tr>
<tr>
<td>isi auth mapping token</td>
<td>329</td>
</tr>
<tr>
<td>isi auth mapping view</td>
<td>329</td>
</tr>
<tr>
<td>isi auth netgroups view</td>
<td>330</td>
</tr>
<tr>
<td>isi auth nis create</td>
<td>331</td>
</tr>
<tr>
<td>isi auth nis delete</td>
<td>334</td>
</tr>
<tr>
<td>isi auth nis list</td>
<td>334</td>
</tr>
<tr>
<td>isi auth nis modify</td>
<td>335</td>
</tr>
<tr>
<td>isi auth nis view</td>
<td>341</td>
</tr>
<tr>
<td>isi auth privileges</td>
<td>341</td>
</tr>
<tr>
<td>isi auth refresh</td>
<td>342</td>
</tr>
<tr>
<td>isi auth roles create</td>
<td>342</td>
</tr>
<tr>
<td>isi auth roles delete</td>
<td>342</td>
</tr>
<tr>
<td>isi auth roles list</td>
<td>343</td>
</tr>
<tr>
<td>isi auth roles members list</td>
<td>343</td>
</tr>
<tr>
<td>isi auth roles modify</td>
<td>344</td>
</tr>
<tr>
<td>isi auth roles privileges list</td>
<td>346</td>
</tr>
<tr>
<td>isi auth roles view</td>
<td>347</td>
</tr>
<tr>
<td>isi auth settings acls modify</td>
<td>347</td>
</tr>
<tr>
<td>isi auth settings acls view</td>
<td>352</td>
</tr>
<tr>
<td>isi auth settings global modify</td>
<td>353</td>
</tr>
<tr>
<td>isi auth settings global view</td>
<td>355</td>
</tr>
</tbody>
</table>
Home directory permissions................................................................. 406
Authenticating SMB users.................................................................. 406
Home directory creation through SMB................................................. 406
  Create home directories with expansion variables....................... 407
  Create home directories with the --inheritable-path-acl option... 408
  Create special home directories with the SMB share %U variable.... 409
Home directory creation through SSH and FTP.................................... 410
  Set the SSH or FTP login shell ................................................... 410
  Set SSH/FTP home directory permissions................................... 411
  Set SSH/FTP home directory creation options.......................... 412
  Provision home directories with dot files.................................... 413
Home directory creation in a mixed environment................................. 414
Interactions between ACLs and mode bits......................................... 414
Default home directory settings in authentication providers.................. 414
Supported expansion variables......................................................... 415
Domain variables in home directory provisioning.................................. 417

Chapter 10  
Data access control 419
Data access control overview.......................................................... 420
ACLs............................................................................................. 420
UNIX permissions............................................................................ 421
Mixed-permission environments....................................................... 421
  NFS access of Windows-created files........................................ 421
  SMB access of UNIX-created files............................................. 421
Managing access permissions.......................................................... 422
  View expected user permissions................................................. 422
  Configure access management settings................................... 423
  Modify ACL policy settings...................................................... 424
  Run the PermissionsRepair job................................................ 424

Chapter 11  
File sharing 427
File sharing overview......................................................................... 428
  Mixed protocol environments.................................................... 428
  Write caching with SmartCache.................................................. 429
SMB............................................................................................... 430
  SMB shares in access zones....................................................... 431
  SMB Multichannel....................................................................... 431
  SMB share management through MMC.................................... 433
  SMB server-side copy............................................................... 434
  SMB continuous availability...................................................... 434
  SMB file filtering........................................................................ 435
  Symbolic links and SMB clients............................................... 436
  Anonymous access to SMB shares.......................................... 437
  Managing SMB settings............................................................ 437
  Managing SMB shares.............................................................. 440
  SMB commands.......................................................................... 447
NFS............................................................................................... 478
  NFS exports............................................................................... 478
  NFS aliases............................................................................... 478
  NFS log files.............................................................................. 479
  Managing the NFS service........................................................ 479
  Managing NFS exports.............................................................. 480
  Managing NFS aliases............................................................... 484
CONTENTS

NFS commands................................................................. 486
FTP......................................................................................... 534
  View FTP settings......................................................... 534
  Enable FTP file sharing............................................... 534
  Configure FTP file sharing......................................... 535
  FTP commands............................................................... 535
HTTP and HTTPS............................................................... 542
  Enable and configure HTTP........................................ 543
  Enable HTTPS through the Apache service............. 543
  Disable HTTPS through the Apache service........... 543
  isi http settings modify........................................... 544
  isi http settings view............................................... 545
File filtering.................................................................... 547
  File filtering in an access zone.............................. 548
  Enable and configure file filtering in an access zone  548
  Disable file filtering in an access zone.................. 548
  View file filtering settings......................................... 549
  File filtering commands........................................... 549
  isi file-filter settings modify.................................... 549
  isi file-filter settings view....................................... 550
Auditing......................................................................... 553
  Auditing overview...................................................... 554
  Syslog.......................................................................... 554
  Syslog forwarding...................................................... 554
  Protocol audit events............................................... 555
  Supported event types............................................... 555
  Supported audit tools................................................ 556
  Sample audit log.......................................................... 557
  Managing audit settings............................................. 558
    Enable protocol access auditing.......................... 558
    Forward protocol access events to syslog............ 558
    Enable system configuration auditing................ 559
    Forward system configuration changes to syslog... 560
    Configure protocol event filters........................... 560
  Integrating with the EMC Common Event Enabler.... 561
    Install CEE for Windows.................................... 561
    Configure CEE for Windows................................ 562
  Auditing commands..................................................... 563
    isi audit settings global modify........................ 563
    isi audit settings global view............................. 565
    isi audit settings modify..................................... 565
    isi audit settings view.......................................... 568
    isi audit topics list................................................ 569
    isi audit topics modify......................................... 569
    isi audit topics view............................................... 570
Snapshots.................................................................... 571
  Snapshots overview.................................................. 572
  Data protection with SnapshotIQ.............................. 572
  Snapshot disk-space usage......................................... 572
  Snapshot schedules.................................................... 573
  Snapshot aliases......................................................... 573

Chapter 12  File filtering 547
  File filtering in an access zone.............................. 548
  Enable and configure file filtering in an access zone  548
  Disable file filtering in an access zone.................. 548
  View file filtering settings......................................... 549
  File filtering commands........................................... 549
    isi file-filter settings modify.................................... 549
    isi file-filter settings view....................................... 550
Chapter 13  Auditing 553
  Auditing overview...................................................... 554
  Syslog.......................................................................... 554
  Syslog forwarding...................................................... 554
  Protocol audit events............................................... 555
  Supported event types............................................... 555
  Supported audit tools................................................ 556
  Sample audit log.......................................................... 557
  Managing audit settings............................................. 558
    Enable protocol access auditing.......................... 558
    Forward protocol access events to syslog............ 558
    Enable system configuration auditing................ 559
    Forward system configuration changes to syslog... 560
    Configure protocol event filters........................... 560
  Integrating with the EMC Common Event Enabler.... 561
    Install CEE for Windows.................................... 561
    Configure CEE for Windows................................ 562
  Auditing commands..................................................... 563
    isi audit settings global modify........................ 563
    isi audit settings global view............................. 565
    isi audit settings modify..................................... 565
    isi audit settings view.......................................... 568
    isi audit topics list................................................ 569
    isi audit topics modify......................................... 569
    isi audit topics view............................................... 570
Chapter 14  Snapshots 571
  Snapshots overview.................................................. 572
  Data protection with SnapshotIQ.............................. 572
  Snapshot disk-space usage......................................... 572
  Snapshot schedules.................................................... 573
  Snapshot aliases......................................................... 573
## Deduplication with SmartDedupe

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deduplication overview</td>
<td>624</td>
</tr>
<tr>
<td>Deduplication jobs</td>
<td>624</td>
</tr>
<tr>
<td>Data replication and backup with deduplication</td>
<td>625</td>
</tr>
<tr>
<td>Snapshots with deduplication</td>
<td>625</td>
</tr>
<tr>
<td>Deduplication considerations</td>
<td>626</td>
</tr>
<tr>
<td>Shadow-store considerations</td>
<td>626</td>
</tr>
<tr>
<td>SmartDedupe license functionality</td>
<td>627</td>
</tr>
<tr>
<td>Managing deduplication</td>
<td>627</td>
</tr>
<tr>
<td>Assess deduplication space savings</td>
<td>627</td>
</tr>
<tr>
<td>Specify deduplication settings</td>
<td>628</td>
</tr>
<tr>
<td>View deduplication space savings</td>
<td>628</td>
</tr>
<tr>
<td>View a deduplication report</td>
<td>629</td>
</tr>
<tr>
<td>Deduplication job report information</td>
<td>629</td>
</tr>
<tr>
<td>Deduplication information</td>
<td>630</td>
</tr>
<tr>
<td>Deduplication commands</td>
<td>631</td>
</tr>
<tr>
<td>isi dedupe settings modify</td>
<td>631</td>
</tr>
<tr>
<td>isi dedupe settings view</td>
<td>632</td>
</tr>
<tr>
<td>isi dedupe stats</td>
<td>632</td>
</tr>
<tr>
<td>isi dedupe reports list</td>
<td>633</td>
</tr>
<tr>
<td>isi dedupe reports view</td>
<td>634</td>
</tr>
</tbody>
</table>

## Data replication with SyncIQ

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyncIQ data replication overview</td>
<td>638</td>
</tr>
<tr>
<td>Accessing SyncIQ with IsilonSD Edge</td>
<td>638</td>
</tr>
<tr>
<td>Replication policies and jobs</td>
<td>638</td>
</tr>
<tr>
<td>Automated replication policies</td>
<td>639</td>
</tr>
<tr>
<td>Source and target cluster association</td>
<td>640</td>
</tr>
<tr>
<td>Configuring SyncIQ source and target clusters with NAT</td>
<td>641</td>
</tr>
<tr>
<td>Full and differential replication</td>
<td>642</td>
</tr>
<tr>
<td>Controlling replication job resource consumption</td>
<td>643</td>
</tr>
<tr>
<td>Replication policy priority</td>
<td>643</td>
</tr>
<tr>
<td>Replication reports</td>
<td>643</td>
</tr>
<tr>
<td>Replication snapshots</td>
<td>644</td>
</tr>
<tr>
<td>Source cluster snapshots</td>
<td>644</td>
</tr>
<tr>
<td>Target cluster snapshots</td>
<td>644</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Data failover and failback with SyncIQ</td>
<td>645</td>
</tr>
<tr>
<td>Reversion process</td>
<td>645</td>
</tr>
<tr>
<td>Data failback</td>
<td>646</td>
</tr>
<tr>
<td>Recovery times and objectives for SyncIQ</td>
<td>646</td>
</tr>
<tr>
<td>RPO Alerts</td>
<td>647</td>
</tr>
<tr>
<td>Replication policy priority</td>
<td>647</td>
</tr>
<tr>
<td>SyncIQ license functionality</td>
<td>647</td>
</tr>
<tr>
<td>Creating replication policies</td>
<td>647</td>
</tr>
<tr>
<td>Excluding directories in replication</td>
<td>648</td>
</tr>
<tr>
<td>Excluding files in replication</td>
<td>648</td>
</tr>
<tr>
<td>File criteria options</td>
<td>649</td>
</tr>
<tr>
<td>Configure default replication policy settings</td>
<td>651</td>
</tr>
<tr>
<td>Create a replication policy</td>
<td>651</td>
</tr>
<tr>
<td>Create a SyncIQ domain</td>
<td>652</td>
</tr>
<tr>
<td>Assess a replication policy</td>
<td>652</td>
</tr>
<tr>
<td>Managing replication to remote clusters</td>
<td>653</td>
</tr>
<tr>
<td>Start a replication job</td>
<td>653</td>
</tr>
<tr>
<td>Pause a replication job</td>
<td>653</td>
</tr>
<tr>
<td>Resume a replication job</td>
<td>654</td>
</tr>
<tr>
<td>Cancel a replication job</td>
<td>654</td>
</tr>
<tr>
<td>View active replication jobs</td>
<td>654</td>
</tr>
<tr>
<td>Replication job information</td>
<td>655</td>
</tr>
<tr>
<td>Initiating data failover and failback with SyncIQ</td>
<td>655</td>
</tr>
<tr>
<td>Fail over data to a secondary cluster</td>
<td>655</td>
</tr>
<tr>
<td>Revert a failover operation</td>
<td>656</td>
</tr>
<tr>
<td>Fail back data to a primary cluster</td>
<td>657</td>
</tr>
<tr>
<td>Performing disaster recovery for SmartLock directories</td>
<td>658</td>
</tr>
<tr>
<td>Recover SmartLock compliance directories on a target cluster</td>
<td>658</td>
</tr>
<tr>
<td>Migrate SmartLock compliance directories</td>
<td>659</td>
</tr>
<tr>
<td>Managing replication policies</td>
<td>660</td>
</tr>
<tr>
<td>Modify a replication policy</td>
<td>660</td>
</tr>
<tr>
<td>Delete a replication policy</td>
<td>661</td>
</tr>
<tr>
<td>Enable or disable a replication policy</td>
<td>662</td>
</tr>
<tr>
<td>View replication policies</td>
<td>662</td>
</tr>
<tr>
<td>Replication policy information</td>
<td>663</td>
</tr>
<tr>
<td>Managing replication to the local cluster</td>
<td>663</td>
</tr>
<tr>
<td>Cancel replication to the local cluster</td>
<td>664</td>
</tr>
<tr>
<td>Break local target association</td>
<td>664</td>
</tr>
<tr>
<td>View replication policies targeting the local cluster</td>
<td>664</td>
</tr>
<tr>
<td>Remote replication policy information</td>
<td>665</td>
</tr>
<tr>
<td>Managing replication performance rules</td>
<td>665</td>
</tr>
<tr>
<td>Create a network traffic rule</td>
<td>665</td>
</tr>
<tr>
<td>Create a file operations rule</td>
<td>666</td>
</tr>
<tr>
<td>Modify a performance rule</td>
<td>666</td>
</tr>
<tr>
<td>Delete a performance rule</td>
<td>666</td>
</tr>
<tr>
<td>Enable or disable a performance rule</td>
<td>667</td>
</tr>
<tr>
<td>View performance rules</td>
<td>667</td>
</tr>
<tr>
<td>Managing replication reports</td>
<td>668</td>
</tr>
<tr>
<td>Configure default replication report settings</td>
<td>668</td>
</tr>
<tr>
<td>Delete replication reports</td>
<td>668</td>
</tr>
<tr>
<td>View replication reports</td>
<td>668</td>
</tr>
<tr>
<td>Replication report information</td>
<td>670</td>
</tr>
<tr>
<td>Managing failed replication jobs</td>
<td>670</td>
</tr>
<tr>
<td>Resolve a replication policy</td>
<td>671</td>
</tr>
<tr>
<td>Reset a replication policy</td>
<td>671</td>
</tr>
<tr>
<td>Perform a full or differential replication</td>
<td>672</td>
</tr>
</tbody>
</table>
Data replication commands................................................................. 672
isi sync policies create..................................................................... 672
isi sync policies modify................................................................. 683
isi sync policies delete................................................................. 694
isi sync policies list....................................................................... 695
isi sync policies reset.................................................................... 697
isi sync policies resolve................................................................. 698
isi sync policies view..................................................................... 698
isi sync policies disable................................................................. 699
isi sync policies enable................................................................. 699
isi sync jobs start........................................................................ 699
isi sync jobs pause....................................................................... 700
isi sync jobs resume..................................................................... 701
isi sync jobs cancel..................................................................... 701
isi sync jobs list.......................................................................... 701
isi sync jobs view........................................................................ 702
isi sync jobs reports list............................................................... 703
isi sync jobs reports view............................................................. 703
isi sync settings modify............................................................... 704
isi sync settings view................................................................... 705
isi sync target cancel................................................................... 705
isi sync target list......................................................................... 706
isi sync target view....................................................................... 707
isi sync target break..................................................................... 707
isi sync target reports list............................................................ 708
isi sync target reports view.......................................................... 708
isi sync target reports subreports list........................................... 710
isi sync target reports subreports view........................................ 710
isi sync reports list....................................................................... 712
isi sync reports view..................................................................... 714
isi sync reports rotate.................................................................. 714
isi sync reports subreports list...................................................... 714
isi sync reports subreports view................................................... 716
isi sync recovery allow-write........................................................ 716
isi sync recovery resync-prep......................................................... 717
isi sync rules create...................................................................... 718
isi sync rules modify.................................................................... 719
isi sync rules delete..................................................................... 720
isi sync rules list.......................................................................... 721
isi sync rules view....................................................................... 722

Chapter 17  Data layout with FlexProtect 723
FlexProtect overview......................................................................... 724
File striping.................................................................................. 724
Requested data protection............................................................... 724
FlexProtect data recovery............................................................... 725
Smartfail..................................................................................... 725
Node failures............................................................................... 725
Requesting data protection............................................................. 726
Requested protection settings........................................................ 726
Requested protection disk space usage.......................................... 727

Chapter 18  NDMP backup and recovery overview 729
NDMP backup and recovery overview............................................. 730
NDMP backup and recovery for IsilonSD Edge ........................................ 730
NDMP two-way backup ......................................................................... 730
NDMP three-way backup ....................................................................... 731
NDMP multi-stream backup and recovery .............................................. 731
Snapshot-based incremental backups ..................................................... 731
NDMP protocol support ........................................................................ 732
Supported DMAs .................................................................................. 733
NDMP hardware support ....................................................................... 733
NDMP backup limitations ....................................................................... 733
NDMP performance recommendations .................................................. 734
Excluding files and directories from NDMP backups ............................. 735
Configuring basic NDMP backup settings ............................................. 736
Configure and enable NDMP backup ..................................................... 737
Disable NDMP backup .......................................................................... 737
NDMP backup settings .......................................................................... 737
View NDMP backup settings ............................................................... 737
Managing NDMP user accounts ............................................................ 738
Create an NDMP user account ............................................................ 738
Modify the password of an NDMP user account .................................. 738
Delete an NDMP user account ............................................................ 738
View NDMP user accounts ................................................................. 739
Managing NDMP backup devices .......................................................... 739
Detect NDMP backup devices ............................................................... 739
Modify an NDMP backup device entry name ...................................... 739
Delete a device entry for a disconnected NDMP backup device .......... 739
View NDMP backup devices ............................................................... 740
Managing NDMP Fibre Channel ports .................................................. 740
Modify NDMP backup port settings ...................................................... 740
Enable or disable an NDMP backup port ............................................. 740
View NDMP backup ports ................................................................. 741
NDMP backup port settings ............................................................... 741
Managing NDMP sessions ................................................................... 741
End an NDMP session ......................................................................... 742
View NDMP sessions ........................................................................ 742
NDMP session information ................................................................. 742
Managing NDMP restartable backups ................................................... 743
Configure NDMP restartable backups for EMC NetWorker ............... 744
View NDMP restartable backup contexts ........................................... 744
Delete an NDMP restartable backup context ..................................... 745
Configure NDMP restartable backup settings ..................................... 745
View NDMP restartable backup settings ............................................. 745
Managing file list backups ................................................................... 745
Format of a backup file list ................................................................. 746
Placement of the file list ...................................................................... 747
Start a file list backup ......................................................................... 747
NDMP restore operations ...................................................................... 748
NDMP parallel restore operation ......................................................... 748
NDMP serial restore operation ........................................................... 748
Specify a NDMP serial restore operation ........................................... 748
Sharing tape drives between clusters .................................................... 748
Managing default NDMP variables ....................................................... 749
Specify the default NDMP variable settings for a path ....................... 749
Modify the default NDMP variable settings for a path ....................... 749
View the default NDMP settings for a path ......................................... 750
NDMP environment variables ............................................................. 750
Setting environment variables for backup operations ....................... 755
Managing snapshot based incremental backups

- Enable snapshot-based incremental backups for a directory
- Delete snapshots for snapshot-based incremental backups
- View snapshots for snapshot-based incremental backups

View NDMP backup logs

NDMP backup commands
- isi ndmp users create
- isi ndmp users delete
- isi ndmp users list
- isi ndmp users modify
- isi ndmp users view
- isi ndmp contexts delete
- isi ndmp contexts list
- isi ndmp contexts view
- isi ndmp dumpdates delete
- isi ndmp dumpdates list
- isi ndmp sessions delete
- isi ndmp sessions list
- isi ndmp sessions view
- isi ndmp settings diagnostics modify
- isi ndmp settings diagnostics view
- isi ndmp settings global modify
- isi ndmp settings global view
- isi ndmp settings variables create
- isi ndmp settings variables delete
- isi ndmp settings variables list
- isi ndmp settings variables modify
- isi fc settings list
- isi fc settings modify
- isi fc settings view
- isi tape delete
- isi tape list
- isi tape modify
- isi tape rescan
- isi tape view

Chapter 19  File retention with SmartLock

SmartLock overview

Compliance mode

SmartLock directories

Accessing SmartLock with IsilonSD Edge

Replication and backup with SmartLock

SmartLock replication and backup limitations

SmartLock license functionality

SmartLock considerations

Set the compliance clock

View the compliance clock

Creating a SmartLock directory

Retention periods

Autocommit time periods

Create an enterprise directory for a non-empty directory

Create a SmartLock directory

Managing SmartLock directories

Modify a SmartLock directory

View SmartLock directory settings
Chapter 23  Storage Pools  879
Storage pools overview......................................................... 880
Storage pool functions.......................................................... 880
    Storage pool functions supported with IsilonSD Edge........ 882
Autoprovisioning................................................................. 882
Node pools........................................................................... 883
    Node class compatibilities............................................. 883
    SSD compatibilities................................................... 884
    Manual node pools.................................................... 885
Virtual hot spare................................................................. 885
Spillover............................................................................. 886
Suggested protection............................................................ 886
Protection policies............................................................... 887
SSD strategies..................................................................... 887
Global namespace acceleration............................................ 888
L3 cache overview.............................................................. 889
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration to L3 cache</td>
<td>890</td>
</tr>
<tr>
<td>L3 cache on NL-series and HD-series node pools</td>
<td>890</td>
</tr>
<tr>
<td>Tiers</td>
<td>891</td>
</tr>
<tr>
<td>File pool policies</td>
<td>891</td>
</tr>
<tr>
<td>Managing node pools through the command-line interface</td>
<td>892</td>
</tr>
<tr>
<td>Create a node class compatibility</td>
<td>892</td>
</tr>
<tr>
<td>Merge compatible node pools</td>
<td>893</td>
</tr>
<tr>
<td>Delete a node class compatibility</td>
<td>894</td>
</tr>
<tr>
<td>Create an SSD compatibility</td>
<td>894</td>
</tr>
<tr>
<td>Delete an SSD compatibility</td>
<td>895</td>
</tr>
<tr>
<td>Create a node pool manually</td>
<td>896</td>
</tr>
<tr>
<td>Add a node to a manually managed node pool</td>
<td>897</td>
</tr>
<tr>
<td>Change the name or protection policy of a node pool</td>
<td>897</td>
</tr>
<tr>
<td>Remove a node from a manually managed node pool</td>
<td>897</td>
</tr>
<tr>
<td>Modify default storage pool settings</td>
<td>898</td>
</tr>
<tr>
<td>SmartPools settings</td>
<td>898</td>
</tr>
<tr>
<td>Managing L3 cache from the command-line interface</td>
<td>901</td>
</tr>
<tr>
<td>Set L3 cache as the default for new node pools</td>
<td>901</td>
</tr>
<tr>
<td>Enable L3 cache on a specific node pool</td>
<td>901</td>
</tr>
<tr>
<td>Restore SSDs to storage drives for a node pool</td>
<td>902</td>
</tr>
<tr>
<td>Managing tiers</td>
<td>902</td>
</tr>
<tr>
<td>Create a tier</td>
<td>902</td>
</tr>
<tr>
<td>Add or move node pools in a tier</td>
<td>903</td>
</tr>
<tr>
<td>Rename a tier</td>
<td>903</td>
</tr>
<tr>
<td>Delete a tier</td>
<td>903</td>
</tr>
<tr>
<td>Creating file pool policies</td>
<td>903</td>
</tr>
<tr>
<td>Create a file pool policy</td>
<td>904</td>
</tr>
<tr>
<td>Valid wildcard characters</td>
<td>905</td>
</tr>
<tr>
<td>Default file pool requested protection settings</td>
<td>905</td>
</tr>
<tr>
<td>Default file pool I/O optimization settings</td>
<td>907</td>
</tr>
<tr>
<td>Managing file pool policies</td>
<td>907</td>
</tr>
<tr>
<td>Modify a file pool policy</td>
<td>908</td>
</tr>
<tr>
<td>Configure default file pool policy settings</td>
<td>908</td>
</tr>
<tr>
<td>Prioritize a file pool policy</td>
<td>909</td>
</tr>
<tr>
<td>Delete a file pool policy</td>
<td>910</td>
</tr>
<tr>
<td>Monitoring storage pools</td>
<td>910</td>
</tr>
<tr>
<td>Monitor storage pools</td>
<td>910</td>
</tr>
<tr>
<td>View the health of storage pools</td>
<td>911</td>
</tr>
<tr>
<td>View results of a SmartPools job</td>
<td>911</td>
</tr>
<tr>
<td>Storage pool commands</td>
<td>912</td>
</tr>
<tr>
<td>isi filepool apply</td>
<td>912</td>
</tr>
<tr>
<td>isi filepool default-policy modify</td>
<td>914</td>
</tr>
<tr>
<td>isi filepool default-policy view</td>
<td>917</td>
</tr>
<tr>
<td>isi filepool policies create</td>
<td>917</td>
</tr>
<tr>
<td>isi filepool policies delete</td>
<td>922</td>
</tr>
<tr>
<td>isi filepool policies list</td>
<td>923</td>
</tr>
<tr>
<td>isi filepool policies modify</td>
<td>923</td>
</tr>
<tr>
<td>isi filepool policies view</td>
<td>928</td>
</tr>
<tr>
<td>isi filepool templates list</td>
<td>929</td>
</tr>
<tr>
<td>isi filepool templates view</td>
<td>930</td>
</tr>
<tr>
<td>isi storagepool compatibilities class active create</td>
<td>930</td>
</tr>
<tr>
<td>isi storagepool compatibilities class active delete</td>
<td>931</td>
</tr>
<tr>
<td>isi storagepool compatibilities class active list</td>
<td>932</td>
</tr>
<tr>
<td>isi storagepool compatibilities class active view</td>
<td>933</td>
</tr>
<tr>
<td>isi storagepool compatibilities class available list</td>
<td>933</td>
</tr>
<tr>
<td>isi storagepool compatibilities ssd active create</td>
<td>934</td>
</tr>
</tbody>
</table>
CloudPools 949

CloudPools overview ................................................................. 950
Accessing CloudPools with IsilonSD Edge ................................. 951
Supported cloud providers .......................................................... 951
  EMC Isilon ............................................................................. 951
  EMC ECS Appliance ............................................................... 951
  Virtustream Storage Cloud ...................................................... 952
  Amazon S3 ............................................................................ 952
  Microsoft Azure .................................................................... 952
CloudPools concepts ................................................................. 953
CloudPools file processing .......................................................... 954
Archiving files with file pool policies ........................................... 955
  Sample policies with CloudPools actions ................................. 955
  About file pool policy order ................................................... 956
  File pool policy cloud archive parameters ............................... 956
  File matching options for cloud archival policies .................... 960
Combining cloud and local storage policy actions ......................... 962
Retrieving file data from the cloud .............................................. 962
  Inline access of cloud data ................................................... 962
  Recalling files from the cloud ................................................. 962
CloudPools interoperability with other OneFS functions ................. 963
  Compression and encryption of cloud data ............................... 963
  NFS inline access .................................................................. 963
  SMB inline access .................................................................. 964
  Other protocols supporting inline access ................................. 964
SyncIQ interoperability .............................................................. 964
  SnapshotIQ integration .......................................................... 966
  NDMP backup and restore of cloud data ................................. 967
CloudPools best practices ........................................................... 967
  Use time stamps for cloud data archival and recall .................... 968
  CloudPools archiving and file size ........................................... 968
  Create exclusive accounts for CloudPools purposes .................. 968
CloudPools troubleshooting ....................................................... 968
  CloudPools expected behaviors .............................................. 969
  CloudPools logs .................................................................. 971
  Troubleshooting CloudPools .................................................. 971
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing cloud accounts</td>
<td>972</td>
</tr>
<tr>
<td>Create a cloud storage account</td>
<td>972</td>
</tr>
<tr>
<td>List cloud storage accounts</td>
<td>973</td>
</tr>
<tr>
<td>View a cloud storage account</td>
<td>973</td>
</tr>
<tr>
<td>Modify a cloud storage account</td>
<td>973</td>
</tr>
<tr>
<td>Delete a cloud storage account</td>
<td>974</td>
</tr>
<tr>
<td>Managing CloudPools</td>
<td>974</td>
</tr>
<tr>
<td>Create a CloudPool</td>
<td>974</td>
</tr>
<tr>
<td>List CloudPools</td>
<td>975</td>
</tr>
<tr>
<td>View CloudPool information</td>
<td>975</td>
</tr>
<tr>
<td>Modify a CloudPool</td>
<td>976</td>
</tr>
<tr>
<td>Delete a CloudPool</td>
<td>976</td>
</tr>
<tr>
<td>Archiving files with file pool policies</td>
<td>977</td>
</tr>
<tr>
<td>Create a file pool policy</td>
<td>977</td>
</tr>
<tr>
<td>List file pool policies</td>
<td>977</td>
</tr>
<tr>
<td>View a file pool policy</td>
<td>978</td>
</tr>
<tr>
<td>Modify a file pool policy</td>
<td>978</td>
</tr>
<tr>
<td>Delete a file pool policy</td>
<td>979</td>
</tr>
<tr>
<td>Apply a file pool policy to a specified file or path</td>
<td>979</td>
</tr>
<tr>
<td>Archive files directly to the cloud</td>
<td>979</td>
</tr>
<tr>
<td>Configuring access to cloud data from a secondary cluster</td>
<td>980</td>
</tr>
<tr>
<td>List available clusters</td>
<td>980</td>
</tr>
<tr>
<td>Allow access to cloud data on a secondary cluster</td>
<td>981</td>
</tr>
<tr>
<td>Remove access to data from a source cluster</td>
<td>982</td>
</tr>
<tr>
<td>Managing cloud jobs</td>
<td>982</td>
</tr>
<tr>
<td>View a list of cloud jobs</td>
<td>982</td>
</tr>
<tr>
<td>View a cloud job</td>
<td>983</td>
</tr>
<tr>
<td>Pause a cloud job</td>
<td>984</td>
</tr>
<tr>
<td>Resume a paused cloud job</td>
<td>984</td>
</tr>
<tr>
<td>Cancel a cloud job</td>
<td>984</td>
</tr>
<tr>
<td>Managing CloudPools settings</td>
<td>985</td>
</tr>
<tr>
<td>View cloud settings</td>
<td>985</td>
</tr>
<tr>
<td>Modify default cloud settings</td>
<td>985</td>
</tr>
<tr>
<td>Generate a new master encryption key</td>
<td>986</td>
</tr>
<tr>
<td>CloudPools command reference</td>
<td>986</td>
</tr>
<tr>
<td>isi cloud access add</td>
<td>986</td>
</tr>
<tr>
<td>isi cloud access list</td>
<td>987</td>
</tr>
<tr>
<td>isi cloud access remove</td>
<td>988</td>
</tr>
<tr>
<td>isi cloud access view</td>
<td>989</td>
</tr>
<tr>
<td>isi cloud accounts create</td>
<td>989</td>
</tr>
<tr>
<td>isi cloud accounts delete</td>
<td>990</td>
</tr>
<tr>
<td>isi cloud accounts list</td>
<td>991</td>
</tr>
<tr>
<td>isi cloud accounts modify</td>
<td>992</td>
</tr>
<tr>
<td>isi cloud accounts view</td>
<td>994</td>
</tr>
<tr>
<td>isi cloud archive</td>
<td>994</td>
</tr>
<tr>
<td>isi cloud jobs cancel</td>
<td>995</td>
</tr>
<tr>
<td>isi cloud jobs files list</td>
<td>996</td>
</tr>
<tr>
<td>isi cloud jobs list</td>
<td>997</td>
</tr>
<tr>
<td>isi cloud jobs pause</td>
<td>998</td>
</tr>
<tr>
<td>isi cloud jobs resume</td>
<td>999</td>
</tr>
<tr>
<td>isi cloud jobs view</td>
<td>999</td>
</tr>
<tr>
<td>isi cloud pools create</td>
<td>1000</td>
</tr>
<tr>
<td>isi cloud pools delete</td>
<td>1001</td>
</tr>
<tr>
<td>isi cloud pools list</td>
<td>1001</td>
</tr>
<tr>
<td>isi cloud pools modify</td>
<td>1002</td>
</tr>
<tr>
<td>isi cloud pools view</td>
<td>1004</td>
</tr>
</tbody>
</table>
Managing the HDFS service..........................................................1127
  Enable or disable the HDFS service.............................................1127
  Configure HDFS service settings................................................ 1127
  HDFS service settings..................................................................1128
  View HDFS settings......................................................................1128
  Modify HDFS log levels...............................................................1128
  View HDFS log levels..................................................................1129

Set the HDFS root directory..........................................................1129

Configuring HDFS authentication methods............................................1129
  Set the HDFS authentication method......................................... 1130
  Supported HDFS authentication methods.................................1130
  Configure HDFS authentication properties on the Hadoop client.1131

Create a local Hadoop user..............................................................1131

Enable or disable WebHDFS within an access zone................................. 1132

Configuring secure impersonation......................................................1132
  Create a proxy user...............................................................1132
  Modify a proxy user.............................................................1133
  Delete a proxy user.............................................................1133
  List the members of a proxy user........................................... 1133
  View proxy users....................................................................1134

Configure Ambari agent settings........................................................1134

Managing virtual HDFS racks..........................................................1135
  Create a virtual HDFS rack.........................................................1135
  Modify a virtual HDFS rack.......................................................1135
  Delete a virtual HDFS rack........................................................1136
  View virtual HDFS racks............................................................1136

HDFS commands.............................................................................1137
  isi hdfs log-level modify..........................................................1137
  isi hdfs log-level view..............................................................1138
  isi hdfs proxyusers create.........................................................1138
  isi hdfs proxyusers modify.......................................................1139
  isi hdfs proxyusers delete........................................................1141
  isi hdfs proxyusers members list................................................1142
  isi hdfs proxyusers list..............................................................1143
  isi hdfs proxyusers view............................................................1144
  isi hdfs racks create...............................................................1144
  isi hdfs racks modify.............................................................1145
  isi hdfs racks delete...............................................................1146
  isi hdfs racks list.................................................................1146
  isi hdfs racks view.................................................................1147
  isi hdfs settings modify..........................................................1147
  isi hdfs settings view..............................................................1148

Antivirus.........................................................................................1151
  Antivirus overview.......................................................................1152
  On-access scanning.......................................................................1152
  Antivirus policy scanning............................................................1153
  Individual file scanning..............................................................1153
  Antivirus scan reports.................................................................1153
  ICAP servers.................................................................................1153
  Supported ICAP servers................................................................1154
  Antivirus threat responses............................................................1154
  Configuring global antivirus settings.............................................1155
    Include specific files in antivirus scans ...................................1155
    Configure on-access scanning settings ...................................1155
Configure antivirus threat response settings ........................................ 1156
Configure antivirus report retention settings ...................................... 1156
Enable or disable antivirus scanning .............................................. 1156

Managing ICAP servers ........................................................................ 1156
Add and connect to an ICAP server ............................................... 1157
Temporarily disconnect from an ICAP server ................................. 1157
Reconnect to an ICAP server ..................................................... 1157
Remove an ICAP server ............................................................. 1157

Create an antivirus policy ................................................................. 1158
Managing antivirus policies ................................................................ 1158
Modify an antivirus policy ............................................................ 1158
Delete an antivirus policy ............................................................. 1158
Enable or disable an antivirus policy ............................................. 1158
View antivirus policies ................................................................ 1159

Managing antivirus scans .................................................................... 1159
Scan a file ................................................................................... 1159
Manually run an antivirus policy .................................................. 1159
Stop a running antivirus scan ..................................................... 1159

Managing antivirus threats ................................................................ 1160
Manually quarantine a file .......................................................... 1160
Rescan a file ................................................................................. 1160
Remove a file from quarantine .................................................... 1160
Manually truncate a file .............................................................. 1160
View threats ............................................................................... 1161
Antivirus threat information .......................................................... 1161

Managing antivirus reports .............................................................. 1161
View antivirus reports ................................................................. 1162
View antivirus events ................................................................. 1162

Antivirus commands ......................................................................... 1162
isi antivirus policies create.......................................................... 1162
isi antivirus policies delete.......................................................... 1164
isi antivirus policies list.............................................................. 1165
isi antivirus policies start............................................................. 1166
isi antivirus policies modify......................................................... 1166
isi antivirus policies view............................................................. 1168
isi antivirus release....................................................................... 1169
isi antivirus scan.......................................................................... 1169
isi antivirus settings modify......................................................... 1169
isi antivirus settings view............................................................. 1173
isi antivirus quarantine................................................................. 1173
isi antivirus reports scans list....................................................... 1173
isi antivirus reports scans view.................................................... 1175
isi antivirus reports threats list.................................................... 1175
isi antivirus reports threats view.................................................. 1176
isi antivirus reports delete........................................................... 1177
isi antivirus servers create........................................................... 1178
isi antivirus servers delete........................................................... 1178
isi antivirus servers list................................................................. 1179
isi antivirus servers modify.......................................................... 1180
isi antivirus servers view............................................................. 1180
isi antivirus status ........................................................................ 1180

Chapter 29 IsilonSD Edge ................................................................. 1181
IsilonSD Edge storage and architecture ........................................... 1182
IsilonSD cluster overview ............................................................. 1183
CHAPTER 1
Introduction to this guide

This section contains the following topics:

- About this guide ............................................................... 32
- Isilon scale-out NAS overview ........................................... 32
- IsilonSD Edge overview .................................................. 32
- Where to go for support .................................................. 32
About this guide

This guide describes how the Isilon OneFS command-line interface provides access to cluster configuration, management, and monitoring functionality. This guide also lists and describes all OneFS-specific commands that extend the standard UNIX command set.

Most of the information in this guide is also applicable for IsilonSD Edge, a software-defined version of OneFS running on the VMware ESXi hypervisor. Differences, if any, are highlighted in the respective sections of this guide.

Your suggestions help us to improve the accuracy, organization, and overall quality of the documentation. Send your feedback to https://www.research.net/s/isidocfeedback. If you cannot provide feedback through the URL, send an email message to docfeedback@isilon.com.

Isilon scale-out NAS overview

The EMC Isilon scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. Powered by the OneFS operating system, an EMC Isilon cluster delivers a scalable pool of storage with a global namespace.

The platform's unified software provides centralized web-based and command-line administration to manage the following features:

- A cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

IsilonSD Edge overview

IsilonSD Edge is a software-defined version of OneFS that runs on the VMware ESXi hypervisor and provides scale-out NAS capabilities on commodity hardware.

You can create OneFS nodes as virtual machines within OneFS clusters that are deployed on VMware ESXi hosts using the hardware resources available on those hosts. The virtual OneFS clusters and nodes are called IsilonSD clusters and IsilonSD nodes.

IsilonSD Edge supports most of the features and software modules that are supported by OneFS. It also provides centralized web-based and command-line administration, which is the same as OneFS, to manage the cluster and node management tasks. For more information, see the IsilonSD Edge Installation and Administration Guide.

Where to go for support

Contact EMC Isilon Technical Support for any questions about EMC Isilon products.
Support for IsilonSD Edge
If you are running a free version of IsilonSD Edge, community support is available through the EMC Isilon Community Network. However, if you have purchased one or more licenses of IsilonSD Edge, you can contact EMC Isilon Technical Support for assistance, provided you have a valid support contract for the product.

Self-service support

EMC provides the Isilon Advisor (IA), a free application that enables customers to self-support common Isilon issues.

The Isilon Advisor is the same application that is used by EMC Isilon Technical Support Engineers and Field Representatives to resolve service requests. You can use it to diagnose and troubleshoot issues. You can also use it to analyze the current health of your cluster and identify items that require attention. This can help you avoid issues that might arise in the future.

For more information about Isilon Advisor, and to download the latest version, see https://help.psapps.emc.com/pages/viewpage.action?pageId=2853972.
Introduction to this guide
CHAPTER 2
Isilon scale-out NAS

This section contains the following topics:

- OneFS storage architecture
- Isilon node components
- Internal and external networks
- Isilon cluster
- The OneFS operating system
- Structure of the file system
- Data protection overview
- VMware integration
- Software modules
OneFS storage architecture

EMC Isilon takes a scale-out approach to storage by creating a cluster of nodes that runs a distributed file system. OneFS combines the three layers of storage architecture—file system, volume manager, and data protection—into a scale-out NAS cluster.

Each node adds resources to the cluster. Because each node contains globally coherent RAM, as a cluster becomes larger, it becomes faster. Meanwhile, the file system expands dynamically and redistributes content, which eliminates the work of partitioning disks and creating volumes.

Nodes work as peers to spread data across the cluster. Segmenting and distributing data—a process known as striping—not only protects data, but also enables a user connecting to any node to take advantage of the entire cluster's performance.

OneFS uses distributed software to scale data across commodity hardware. Each node helps control data requests, boosts performance, and expands the cluster's capacity. No master device controls the cluster; no slaves invoke dependencies. Instead, each node helps control data requests, boosts performance, and expands the cluster's capacity.

Isilon node components

As a rack-mountable appliance, a storage node includes the following components in a 2U or 4U rack-mountable chassis with an LCD front panel: CPUs, RAM, NVRAM, network interfaces, InfiniBand adapters, disk controllers, and storage media. An Isilon cluster comprises three or more nodes, up to 144.

When you add a node to a cluster, you increase the cluster's aggregate disk, cache, CPU, RAM, and network capacity. OneFS groups RAM into a single coherent cache so that a data request on a node benefits from data that is cached anywhere. NVRAM is grouped to write data with high throughput and to protect write operations from power failures. As the cluster expands, spindles and CPU combine to increase throughput, capacity, and input-output operations per second (IOPS).

EMC Isilon makes several types of nodes, all of which can be added to a cluster to balance capacity and performance with throughput or IOPS:

<table>
<thead>
<tr>
<th>Node</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-Series</td>
<td>IOPS-intensive applications</td>
</tr>
<tr>
<td>X-Series</td>
<td>High-concurrency and throughput-driven workflows</td>
</tr>
<tr>
<td>NL-Series</td>
<td>Near-primary accessibility, with near-tape value</td>
</tr>
<tr>
<td>HD-Series</td>
<td>Maximum capacity</td>
</tr>
</tbody>
</table>

The following EMC Isilon nodes improve performance:

<table>
<thead>
<tr>
<th>Node</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-Series Performance Accelerator</td>
<td>Independent scaling for high performance</td>
</tr>
</tbody>
</table>
### Internal and external networks

A cluster includes two networks: an internal network to exchange data between nodes and an external network to handle client connections.

Nodes exchange data through the internal network with a proprietary, unicast protocol over InfiniBand. Each node includes redundant InfiniBand ports so you can add a second internal network in case the first one fails.

**Note**

In the case of IsilonSD Edge, nodes exchange data through the Ethernet switch. For more information on the internal and external network requirements for IsilonSD Edge, see the *IsilonSD Edge Installation and Administration Guide*.

Clients reach the cluster with 1 GigE or 10 GigE Ethernet. Since every node includes Ethernet ports, the cluster's bandwidth scales with performance and capacity as you add nodes.

**CAUTION**

Only Isilon nodes should be connected to your InfiniBand switch. Information exchanged on the back-end network is not encrypted. Connecting anything other than Isilon nodes to the InfiniBand switch creates a security risk.

### Isilon cluster

An Isilon cluster consists of three or more hardware nodes, up to 144. Each node runs the Isilon OneFS operating system, the distributed file-system software that unites the nodes into a cluster. A cluster’s storage capacity ranges from a minimum of 18 TB to a maximum of 50 PB.

If you are running IsilonSD Edge, see the *IsilonSD cluster* section in this guide for the IsilonSD cluster requirements.

### Cluster administration

OneFS centralizes cluster management through a web administration interface and a command-line interface. Both interfaces provide methods to activate licenses, check the status of nodes, configure the cluster, upgrade the system, generate alerts, view client connections, track performance, and change various settings.

In addition, OneFS simplifies administration by automating maintenance with a Job Engine. You can schedule jobs that scan for viruses, inspect disks for errors, reclaim disk space, and check the integrity of the file system. The engine manages the jobs to minimize impact on the cluster’s performance.

With SNMP versions 2c and 3, you can remotely monitor hardware components, CPU usage, switches, and network interfaces. EMC Isilon supplies management information bases (MIBs) and traps for the OneFS operating system.
OneFS also includes an application programming interface (API) that is divided into two functional areas: One area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster. You can send requests to the OneFS API through a Representational State Transfer (REST) interface, which is accessed through resource URLs and standard HTTP methods. The API integrates with OneFS role-based access control (RBAC) to increase security. See the Isilon Platform API Reference.

**Quorum**

An Isilon cluster must have a quorum to work properly. A quorum prevents data conflicts—for example, conflicting versions of the same file—in case two groups of nodes become unsynchronized. If a cluster loses its quorum for read and write requests, you cannot access the OneFS file system.

For a quorum, more than half the nodes must be available over the internal network. A seven-node cluster, for example, requires a four-node quorum. A 10-node cluster requires a six-node quorum. If a node is unreachable over the internal network, OneFS separates the node from the cluster, an action referred to as splitting. After a cluster is split, cluster operations continue as long as enough nodes remain connected to have a quorum.

In a split cluster, the nodes that remain in the cluster are referred to as the majority group. Nodes that are split from the cluster are referred to as the minority group.

When split nodes can reconnect with the cluster and resynchronize with the other nodes, the nodes rejoin the cluster’s majority group, an action referred to as merging.

A OneFS cluster contains two quorum properties:
- read quorum (efs.gmp.has_quorum)
- write quorum (efs.gmp.has_super_block_quorum)

By connecting to a node with SSH and running the `sysctl` command-line tool as root, you can view the status of both types of quorum. Here is an example for a cluster that has a quorum for both read and write operations, as the command’s output indicates with a 1, for true:

```
sysctl efs.gmp.has_quorum
  efs.gmp.has_quorum: 1
sysctl efs.gmp.has_super_block_quorum
  efs.gmp.has_super_block_quorum: 1
```

The degraded states of nodes—such as smartfail, read-only, offline, and so on—affect quorum in different ways. A node in a smartfail or read-only state affects only write quorum. A node in an offline state, however, affects both read and write quorum. In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work.

A cluster can lose write quorum but keep read quorum. Consider a four-node cluster in which nodes 1 and 2 are working normally. Node 3 is in a read-only state, and node 4 is in a smartfail state. In such a case, read requests to the cluster succeed. Write requests, however, receive an input-output error because the states of nodes 3 and 4 break the write quorum.

A cluster can also lose both its read and write quorum. If nodes 3 and 4 in a four-node cluster are in an offline state, both write requests and read requests receive an input-output error, and you cannot access the file system. When OneFS can reconnect with the nodes, OneFS merges them back into the cluster. Unlike a RAID system, an Isilon node can rejoin the cluster without being rebuilt and reconfigured.
Splitting and merging

Splitting and merging optimize the use of nodes without your intervention. OneFS monitors every node in a cluster. If a node is unreachable over the internal network, OneFS separates the node from the cluster, an action referred to as splitting. When the cluster can reconnect to the node, OneFS adds the node back into the cluster, an action referred to as merging.

When a node is split from a cluster, it will continue to capture event information locally. You can connect to a split node with SSH and run the `isi events list` command to view the local event log for the node. The local event log can help you troubleshoot the connection issue that resulted in the split. When the split node rejoins the cluster, local events gathered during the split are deleted. You can still view events generated by a split node in the node's event log file located at `/var/log/isi_celog_events.log`.

If a cluster splits during a write operation, OneFS might need to re-allocate blocks for the file on the side with the quorum, which leads allocated blocks on the side without a quorum to become orphans. When the split nodes reconnect with the cluster, the OneFS Collect system job reclaims the orphaned blocks.

Meanwhile, as nodes split and merge with the cluster, the OneFS AutoBalance job redistributes data evenly among the nodes in the cluster, optimizing protection and conserving space.

Storage pools

Storage pools segment nodes and files into logical divisions to simplify the management and storage of data.

A storage pool comprises node pools and tiers. Node pools group equivalent nodes to protect data and ensure reliability. Tiers combine node pools to optimize storage by need, such as a frequently used high-speed tier or a rarely accessed archive.

The SmartPools module groups nodes and files into pools. If you do not activate a SmartPools license, the module provisions node pools and creates one file pool. If you activate the SmartPools license, you receive more features. You can, for example, create multiple file pools and govern them with policies. The policies move files, directories, and file pools among node pools or tiers. You can also define how OneFS handles write operations when a node pool or tier is full. SmartPools reserves a virtual hot spare to reprotect data if a drive fails regardless of whether the SmartPools license is activated.

The OneFS operating system

A distributed operating system based on FreeBSD, OneFS presents an Isilon cluster's file system as a single share or export with a central point of administration.

The OneFS operating system does the following:

- Supports common data-access protocols, such as SMB and NFS.
- Connects to multiple identity management systems, such as Active Directory and LDAP.
- Authenticates users and groups.
- Controls access to directories and files.
Data-access protocols

With the OneFS operating system, you can access data with multiple file-sharing and transfer protocols. As a result, Microsoft Windows, UNIX, Linux, and Mac OS X clients can share the same directories and files.

OneFS supports the following protocols.

**SMB**

The Server Message Block (SMB) protocol enables Windows users to access the cluster. OneFS works with SMB 1, SMB 2, and SMB 2.1, as well as SMB 3.0 for Multichannel only. With SMB 2.1, OneFS supports client opportunity locks (oplocks) and large (1 MB) MTU sizes. The default file share is /ifs.

**NFS**

The Network File System (NFS) protocol enables UNIX, Linux, and Mac OS X systems to remotely mount any subdirectory, including subdirectories created by Windows users. OneFS works with NFS versions 3 and 4. The default export is /ifs.

**HDFS**

The Hadoop Distributed File System (HDFS) protocol enables a cluster to work with Apache Hadoop, a framework for data-intensive distributed applications. HDFS integration requires you to activate a separate license.

**FTP**

FTP allows systems with an FTP client to connect to the cluster and exchange files.

**HTTP and HTTPS**

HTTP and its secure variant, HTTPS, give systems browser-based access to resources. OneFS includes limited support for WebDAV.

**Swift**

Isilon Swift enables you to access file-based data stored on your EMC Isilon cluster as objects. The Swift API is implemented as a set of Representational State Transfer (REST) web services over HTTP or secure HTTP (HTTPS). Content and metadata can be ingested as objects and concurrently accessed through other supported EMC Isilon protocols. For more information, see the *Isilon Swift Technical Note*.

Identity management and access control

OneFS works with multiple identity management systems to authenticate users and control access to files. In addition, OneFS features access zones that allow users from different directory services to access different resources based on their IP address. Meanwhile, role-based access control (RBAC) segments administrative access by role.

OneFS authenticates users with the following identity management systems:

- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Network Information Service (NIS)
- Local users and local groups
A file provider for accounts in /etc/spwd.db and /etc/group files. With the file provider, you can add an authoritative third-party source of user and group information.

You can manage users with different identity management systems; OneFS maps the accounts so that Windows and UNIX identities can coexist. A Windows user account managed in Active Directory, for example, is mapped to a corresponding UNIX account in NIS or LDAP.

To control access, an Isilon cluster works with both the access control lists (ACLs) of Windows systems and the POSIX mode bits of UNIX systems. When OneFS must transform a file’s permissions from ACLs to mode bits or from mode bits to ACLs, OneFS merges the permissions to maintain consistent security settings.

OneFS presents protocol-specific views of permissions so that NFS exports display mode bits and SMB shares show ACLs. You can, however, manage not only mode bits but also ACLs with standard UNIX tools, such as the chmod and chown commands. In addition, ACL policies enable you to configure how OneFS manages permissions for networks that mix Windows and UNIX systems.

**Access zones**

OneFS includes an access zones feature. Access zones allow users from different authentication providers, such as two untrusted Active Directory domains, to access different OneFS resources based on an incoming IP address. An access zone can contain multiple authentication providers and SMB namespaces.

**RBAC for administration**

OneFS includes role-based access control for administration. In place of a root or administrator account, RBAC lets you manage administrative access by role. A role limits privileges to an area of administration. For example, you can create separate administrator roles for security, auditing, storage, and backup.

**Structure of the file system**

OneFS presents all the nodes in a cluster as a global namespace—that is, as the default file share, /ifs.

In the file system, directories are inode number links. An inode contains file metadata and an inode number, which identifies a file’s location. OneFS dynamically allocates inodes, and there is no limit on the number of inodes.

To distribute data among nodes, OneFS sends messages with a globally routable block address through the cluster’s internal network. The block address identifies the node and the drive storing the block of data.

---

**Note**

We recommend that you do not save data to the root /ifs file path but in directories below /ifs. The design of your data storage structure should be planned carefully. A well-designed directory optimizes cluster performance and cluster administration.
Data layout

OneFS evenly distributes data among a cluster's nodes with layout algorithms that maximize storage efficiency and performance. The system continuously reallocates data to conserve space.

OneFS breaks data down into smaller sections called blocks, and then the system places the blocks in a stripe unit. By referencing either file data or erasure codes, a stripe unit helps safeguard a file from a hardware failure. The size of a stripe unit depends on the file size, the number of nodes, and the protection setting. After OneFS divides the data into stripe units, OneFS allocates, or stripes, the stripe units across nodes in the cluster.

When a client connects to a node, the client's read and write operations take place on multiple nodes. For example, when a client connects to a node and requests a file, the node retrieves the data from multiple nodes and rebuilds the file. You can optimize how OneFS lays out data to match your dominant access pattern—concurrent, streaming, or random.

Writing files

On a node, the input-output operations of the OneFS software stack split into two functional layers: A top layer, or initiator, and a bottom layer, or participant. In read and write operations, the initiator and the participant play different roles.

When a client writes a file to a node, the initiator on the node manages the layout of the file on the cluster. First, the initiator divides the file into blocks of 8 KB each. Second, the initiator places the blocks in one or more stripe units. At 128 KB, a stripe unit consists of 16 blocks. Third, the initiator spreads the stripe units across the cluster until they span a width of the cluster, creating a stripe. The width of the stripe depends on the number of nodes and the protection setting.

After dividing a file into stripe units, the initiator writes the data first to non-volatile random-access memory (NVRAM) and then to disk. NVRAM retains the information when the power is off.

During the write transaction, NVRAM guards against failed nodes with journaling. If a node fails mid-transaction, the transaction restarts without the failed node. When the node returns, it replays the journal from NVRAM to finish the transaction. The node also runs the AutoBalance job to check the file's on-disk striping. Meanwhile, uncommitted writes waiting in the cache are protected with mirroring. As a result, OneFS eliminates multiple points of failure.

Reading files

In a read operation, a node acts as a manager to gather data from the other nodes and present it to the requesting client.

Because an Isilon cluster's coherent cache spans all the nodes, OneFS can store different data in each node's RAM. By using the internal InfiniBand network, a node can retrieve file data from another node's cache faster than from its own local disk. If a read operation requests data that is cached on any node, OneFS pulls the cached data to serve it quickly.

In addition, for files with an access pattern of concurrent or streaming, OneFS pre-fetches in-demand data into a managing node's local cache to further improve sequential-read performance.
Metadata layout

OneFS protects metadata by spreading it across nodes and drives. Metadata—which includes information about where a file is stored, how it is protected, and who can access it—is stored in inodes and protected with locks in a B+ tree, a standard structure for organizing data blocks in a file system to provide instant lookups. OneFS replicates file metadata across the cluster so that there is no single point of failure.

Working together as peers, all the nodes help manage metadata access and locking. If a node detects an error in metadata, the node looks up the metadata in an alternate location and then corrects the error.

Locks and concurrency

OneFS includes a distributed lock manager that orchestrates locks on data across all the nodes in a cluster.

The lock manager grants locks for the file system, byte ranges, and protocols, including SMB share-mode locks and NFS advisory locks. OneFS also supports SMB opportunistic locks.

Because OneFS distributes the lock manager across all the nodes, any node can act as a lock coordinator. When a thread from a node requests a lock, the lock manager’s hashing algorithm typically assigns the coordinator role to a different node. The coordinator allocates a shared lock or an exclusive lock, depending on the type of request. A shared lock allows users to share a file simultaneously, typically for read operations. An exclusive lock allows only one user to access a file, typically for write operations.

Striping

In a process known as striping, OneFS segments files into units of data and then distributes the units across nodes in a cluster. Striping protects your data and improves cluster performance.

To distribute a file, OneFS reduces it to blocks of data, arranges the blocks into stripe units, and then allocates the stripe units to nodes over the internal network. At the same time, OneFS distributes erasure codes that protect the file. The erasure codes encode the file’s data in a distributed set of symbols, adding space-efficient redundancy. With only a part of the symbol set, OneFS can recover the original file data.

Taken together, the data and its redundancy form a protection group for a region of file data. OneFS places the protection groups on different drives on different nodes—creating data stripes.

Because OneFS stripes data across nodes that work together as peers, a user connecting to any node can take advantage of the entire cluster’s performance.

By default, OneFS optimizes striping for concurrent access. If your dominant access pattern is streaming—that is, lower concurrency, higher single-stream workloads, such as with video—you can change how OneFS lays out data to increase sequential-read performance. To better handle streaming access, OneFS stripes data across more drives. Streaming is most effective on clusters or subpools serving large files.
Data protection overview

An Isilon cluster is designed to serve data even when components fail. By default, OneFS protects data with erasure codes, enabling you to retrieve files when a node or disk fails. As an alternative to erasure codes, you can protect data with two to eight mirrors.

When you create a cluster with five or more nodes, erasure codes deliver as much as 80 percent efficiency. On larger clusters, erasure codes provide as much as four levels of redundancy.

In addition to erasure codes and mirroring, OneFS includes the following features to help protect the integrity, availability, and confidentiality of data:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>OneFS can send files to servers running the Internet Content Adaptation Protocol (ICAP) to scan for viruses and other threats.</td>
</tr>
<tr>
<td>Clones</td>
<td>OneFS enables you to create clones that share blocks with other files to save space.</td>
</tr>
<tr>
<td>NDMP backup and restore</td>
<td>OneFS can back up data to tape and other devices through the Network Data Management Protocol. Although OneFS supports both three-way and two-way backup, two-way backup requires an Isilon Backup Accelerator Node.</td>
</tr>
</tbody>
</table>

**Note**

IsilonSD Edge supports only the three-way NDMP backup.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection domains</td>
<td>You can apply protection domains to files and directories to prevent changes.</td>
</tr>
</tbody>
</table>

The following software modules also help protect data, but they require you to activate a separate license:

<table>
<thead>
<tr>
<th>Licensed Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyncIQ</td>
<td>SyncIQ replicates data on another Isilon cluster and automates failover and failback operations between clusters. If a cluster becomes unusable, you can fail over to another Isilon cluster.</td>
</tr>
<tr>
<td>SnapshotIQ</td>
<td>You can protect data with a snapshot—a logical copy of data stored on a cluster.</td>
</tr>
<tr>
<td>SmartLock</td>
<td>The SmartLock tool prevents users from modifying and deleting files. You can commit files to a write-once, read-many state: The file can never be modified and cannot be deleted until after a set retention period. SmartLock</td>
</tr>
</tbody>
</table>
### N+M data protection

OneFS supports N+M erasure code levels of N+1, N+2, N+3, and N+4.

In the N+M data model, N represents the number of nodes, and M represents the number of simultaneous failures of nodes or drives that the cluster can handle without losing data. For example, with N+2 the cluster can lose two drives on different nodes or lose two nodes.

To protect drives and nodes separately, OneFS also supports N+M:B. In the N+M:B notation, M is the number of disk failures, and B is the number of node failures. With N+3:1 protection, for example, the cluster can lose three drives or one node without losing data.

The default protection level for clusters larger than 18 TB is N+2:1. The default for clusters smaller than 18 TB is N+1.

The quorum rule dictates the number of nodes required to support a protection level. For example, N+3 requires at least seven nodes so you can maintain a quorum if three nodes fail.

You can, however, set a protection level that is higher than the cluster can support. In a four-node cluster, for example, you can set the protection level at 5x. OneFS protects the data at 4x until a fifth node is added, after which OneFS automatically reprotects the data at 5x.

### Data mirroring

You can protect on-disk data with mirroring, which copies data to multiple locations. OneFS supports two to eight mirrors. You can use mirroring instead of erasure codes, or you can combine erasure codes with mirroring.

Mirroring, however, consumes more space than erasure codes. Mirroring data three times, for example, duplicates the data three times, which requires more space than erasure codes. As a result, mirroring suits transactions that require high performance.

You can also mix erasure codes with mirroring. During a write operation, OneFS divides data into redundant protection groups. For files protected by erasure codes, a protection group consists of data blocks and their erasure codes. For mirrored files, a protection group contains all the mirrors of a set of blocks. OneFS can switch the type of protection group as it writes a file to disk. By changing the protection group dynamically, OneFS can continue writing data despite a node failure that prevents the cluster from applying erasure codes. After the node is restored, OneFS automatically converts the mirrored protection groups to erasure codes.

### The file system journal

A journal, which records file-system changes in a battery-backed NVRAM card, recovers the file system after failures, such as a power loss. When a node restarts, the journal replays file transactions to restore the file system.
Virtual hot spare (VHS)

When a drive fails, OneFS uses space reserved in a subpool instead of a hot spare drive. The reserved space is known as a virtual hot spare.

In contrast to a spare drive, a virtual hot spare automatically resolves drive failures and continues writing data. If a drive fails, OneFS migrates data to the virtual hot spare to reprotect it. You can reserve as many as four disk drives as a virtual hot spare.

Balancing protection with storage space

You can set protection levels to balance protection requirements with storage space. Higher protection levels typically consume more space than lower levels because you lose an amount of disk space to storing erasure codes. The overhead for the erasure codes depends on the protection level, the file size, and the number of nodes in the cluster. Since OneFS stripes both data and erasure codes across nodes, the overhead declines as you add nodes.

VMware integration

OneFS integrates with several VMware products, including vSphere, vCenter, and ESXi.

For example, OneFS works with the VMware vSphere API for Storage Awareness (VASA) so that you can view information about an Isilon cluster in vSphere. OneFS also works with the VMware vSphere API for Array Integration (VAAI) to support the following features for block storage: hardware-assisted locking, full copy, and block zeroing. VAAI for NFS requires an ESXi plug-in.

With the Isilon Storage Replication Adapter, OneFS integrates with the VMware vCenter Site Recovery Manager to recover virtual machines that are replicated between Isilon clusters.

Software modules

You can access advanced features by activating licenses for EMC Isilon software modules.

Note

If you are running IsilonSD Edge, the supported list of software modules varies, depending on whether you have configured the free or purchased version of this product. For more information on the software modules available with IsilonSD Edge, see the IsilonSD Edge licensing overview section in this guide.

SmartLock

SmartLock protects critical data from malicious, accidental, or premature alteration or deletion to help you comply with SEC 17a-4 regulations. You can automatically commit data to a tamper-proof state and then retain it with a compliance clock.
HDFS
OneFS works with the Hadoop Distributed File System protocol to help clients running Apache Hadoop, a framework for data-intensive distributed applications, analyze big data.

SyncIQ automated failover and failback
SyncIQ replicates data on another Isilon cluster and automates failover and failback between clusters. If a cluster becomes unusable, you can fail over to another Isilon cluster. Failback restores the original source data after the primary cluster becomes available again.

Security hardening
Security hardening is the process of configuring your system to reduce or eliminate as many security risks as possible. You can apply a hardening policy that secures the configuration of OneFS, according to policy guidelines.

SnapshotIQ
SnapshotIQ protects data with a snapshot—a logical copy of data stored on a cluster. A snapshot can be restored to its top-level directory.

SmartDedupe
You can reduce redundancy on a cluster by running SmartDedupe. Deduplication creates links that can impact the speed at which you can read from and write to files.

SmartPools
SmartPools enables you to create multiple file pools governed by file-pool policies. The policies move files and directories among node pools or tiers. You can also define how OneFS handles write operations when a node pool or tier is full.

CloudPools
Built on the SmartPools policy framework, CloudPools enables you to archive data to cloud storage, effectively defining the cloud as another tier of storage. CloudPools supports EMC Isilon, EMC ECS Appliance, Virtustream Storage Cloud, Amazon S3, and Microsoft Azure as cloud storage providers.

SmartConnect Advanced
If you activate a SmartConnect Advanced license, you can balance policies to evenly distribute CPU usage, client connections, or throughput. You can also define IP address pools to support multiple DNS zones in a subnet. In addition, SmartConnect supports IP failover, also known as NFS failover.

InsightIQ
The InsightIQ virtual appliance monitors and analyzes the performance of your Isilon cluster to help you optimize storage resources and forecast capacity.

SmartQuotas
The SmartQuotas module tracks disk usage with reports and enforces storage limits with alerts.

Isilon Swift
Isilon Swift is an object storage gateway compatible with the OpenStack Swift 1.0 API. Through Isilon Swift, you can access existing file-based data stored on your EMC Isilon cluster as objects. The Swift API is implemented as a set of RESTful web services over HTTP or HTTPS. Since the Swift API is considered as a

Software modules
protocol, content and metadata can be ingested as objects and concurrently accessed through other supported EMC Isilon protocols.
CHAPTER 3

Introduction to the OneFS command-line interface

This section contains the following topics:

- OneFS command-line interface overview ........................................................... 50
- Syntax diagrams ................................................................................................ 50
- Universal options ................................................................................................ 51
- Command-line interface privileges .................................................................... 52
- SmartLock compliance command permissions .................................................. 52
- OneFS time values ............................................................................................. 54
OneFS command-line interface overview

The OneFS command-line interface extends the standard UNIX command set to include commands that enable you to manage an Isilon cluster outside of the web administration interface or LCD panel. You can access the command-line interface by opening a secure shell (SSH) connection to any node in the cluster.

You can run isi commands to configure, monitor, and manage Isilon clusters and the individual nodes in a cluster. Brief descriptions, usage information, and examples are provided for each command.

IsilonSD Edge command-line interface overview

The IsilonSD Edge command-line interface supports most of the OneFS commands. Some commands might not be applicable for IsilonSD Edge either because they are not supported by clusters running on a virtual infrastructure or because you have not purchased a license of IsilonSD Edge. Such commands are called out in the respective sections.

Syntax diagrams

The format of each command is described in a syntax diagram.

The following conventions apply for syntax diagrams:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Square brackets indicate an optional element. If you omit the contents of the square brackets when specifying a command, the command still runs successfully.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets indicate a placeholder value. You must replace the contents of the angle brackets with a valid value, otherwise the command fails.</td>
</tr>
<tr>
<td>{}</td>
<td>Braces indicate a group of elements. If the contents of the braces are separated by a vertical bar, the contents are mutually exclusive. If the contents of the braces are not separated by a bar, the contents must be specified together.</td>
</tr>
<tr>
<td></td>
<td>Vertical bars separate mutually exclusive elements within the braces.</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate that the preceding element can be repeated more than once. If ellipses follow a brace or bracket, the contents of the braces or brackets can be repeated more than once.</td>
</tr>
</tbody>
</table>

Each isi command is broken into three parts: command, required options, and optional options. Required options are positional, meaning that you must specify them...
in the order that they appear in the syntax diagram. However, you can specify a 
required option in an alternative order by preceding the text displayed in angle 
brackets with a double dash. For example, consider isi snapshot snapshots 
create.

```bash
isi snapshot snapshots create <name> <path>
    [--expires <timestamp>]
    [--alias <string>]
    [--verbose]
```

If the `<name>` and `<path>` options are prefixed with double dashes, the options can 
be moved around in the command. For example, the following command is valid:

```bash
isi snapshot snapshots create --verbose --path /ifs/data --alias 
newSnap_alias --name newSnap
```

Shortened versions of commands are accepted as long as the command is 
unambiguous and does not apply to multiple commands. For example, isi snap 
snap c newSnap /ifs/data is equivalent to isi snapshot snapshots 
create newSnap /ifs/data because the root of each word belongs to one 
command exclusively. If a word belongs to more than one command, the command 
fails. For example, isi sn snap c newSnap /ifs/data is not equivalent to isi 
snapshot snapshots create newSnap /ifs/data because the root of isi 
sn could belong to either isi snapshot or isi snmp.

If you begin typing a word and then press TAB, the rest of the word automatically 
appears as long as the word is unambiguous and applies to only one command. For 
example, isi snap completes to isi snapshot because that is the only valid 
possibility. However, isi sn does not complete, because it is the root of both isi 
snapshot and isi snmp.

**Universal options**

Some options are valid for all commands.

**Syntax**

```bash
isi [--timeout <integer>] [--debug] <command> [--help]
```

**--timeout <integer>**

Specifies the number of seconds before the command times out.

**--debug**

Displays all calls to the Isilon OneFS Platform API. If a traceback occurs, displays 
traceback in addition to error message.

**--help**

Displays a basic description of the command and all valid options for the 
command.
Examples

The following command causes the `isi sync policies list` command to timeout after 30 seconds:

```
isi --timeout 30 sync policies list
```

The following command displays help output for `isi sync policies list`:

```
isi sync policies list --help
```

Command-line interface privileges

You can perform most tasks granted by a privilege through the command-line interface (CLI). Some OneFS commands require root access.

SmartLock compliance command permissions

If a cluster is running in SmartLock compliance mode, root access is disabled on the cluster. Because of this, if a command requires root access, you can run the command only through the `sudo` program.

In compliance mode, you can run all `isi` commands that are followed by a space through `sudo`. For example, you can run `isi sync policies create` through `sudo`. In addition, you can also run the following `isi` commands through `sudo`; these commands are internal and are typically run only by Isilon Technical Support:

- `isi_auth_expert`
- `isi_bootdisk_finish`
- `isi_bootdisk_provider_dev`
- `isi_bootdisk_status`
- `isi_bootdisk_unlock`
- `isi_checkjournal`
- `isi_clean_idmap`
- `isi_client_stats`
- `isi_cpr`
- `isi_cto_update`
- `isi_disk_firmware_reboot`
- `isi_dmi_info`
- `isi_dmilog`
- `isi_dongle_sync`
- `isi_drivenum`
- `isi_dsp_install`
- `isi_dumpjournal`
- `isi_eth_mixer_d`
- `isi_evaluate_provision_drive`
Introduction to the OneFS command-line interface

- isi_fcb_vpd_tool
- isi_flexnet_info
- isi_flush
- isi_for_array
- isi_fputil
- isi_gather_info
- isi_gather_auth_info
- isi_gather_cluster_info
- isi_gconfig
- isi_get_itrace
- isi_get_profile
- isi_hangdump
- isi_hw_check
- isi_hw_status
- isi_ib_bug_info
- isi_ib_fw
- isi_ib_info
- isi_ilog
- isi_imdd_status
- isi_inventory_tool
- isi_ipmicmc
- isi_job_d
- isi_kill_busy
- isi_km_diag
- isi_lid_d
- isi_linmap_mod
- isi_logstore
- isi_lsiexputil
- isi_make_abr
- isi_mcp
- isi_mps_fw_status
- isi_netlogger
- isi_nodes
- isi_ntp_config
- isi_ovt_check
- isi_patch_d
- isi_phone_home
- isi_promptsupport
- isi_radish
- isi_rbm_ping
In addition to isi commands, you can run the following UNIX commands through sudo:

- date
- gcore
- ifconfig
- kill
- killall
- nfsstat
- ntpdate
- nvmecontrol
- pciconf
- pkill
- ps
- pwd_mkdb
- renice
- shutdown
- syslog
- tcpdump
- top

**OneFS time values**

OneFS uses different values for time depending on the application.

You can specify time periods, such as a month, for multiple OneFS applications.

However, because some time values have more than one meaning, OneFS defines time
values based on the application. The following table describes the time values for OneFS applications:

<table>
<thead>
<tr>
<th>Module</th>
<th>Month</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapshotIQ</td>
<td>30 days</td>
<td>365 days (does not account for leap year)</td>
</tr>
<tr>
<td>SmartLock</td>
<td>31 days</td>
<td>365 days (does not account for leap year)</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>30 days</td>
<td>365 days (does not account for leap year)</td>
</tr>
</tbody>
</table>
Introduction to the OneFS command-line interface
CHAPTER 4

General cluster administration

This section contains the following topics:

- General cluster administration overview ............................................................ 58
- User interfaces .................................................................................................. 58
- Connecting to the cluster ................................................................................ 59
- Licensing ............................................................................................................ 60
- Certificates ........................................................................................................ 65
- Cluster identity ................................................................................................... 67
- Cluster contact information ............................................................................... 68
- Cluster date and time .......................................................................................... 69
- SMTP email settings ........................................................................................... 71
- Configuring the cluster join mode ....................................................................... 72
- File system settings ............................................................................................ 73
- Security hardening ............................................................................................. 74
- Cluster monitoring .............................................................................................. 79
- Monitoring cluster hardware .............................................................................. 80
- Events and alerts ................................................................................................ 87
- Cluster maintenance ......................................................................................... 97
- Remote support ................................................................................................ 107
- Cluster administration commands .................................................................... 111
- Event commands .............................................................................................. 173
- Hardware commands ....................................................................................... 192
General cluster administration overview

You can manage general OneFS settings and module licenses for the EMC Isilon cluster.

General cluster administration covers several areas. You can:

- manage general settings such as cluster name, date and time, and email
- monitor the cluster status and performance, including hardware components
- configure how events and notifications are handled
- perform cluster maintenance such as adding, removing, and restarting nodes

Most management tasks are accomplished through both the web administration or command-line interface; however, you will occasionally encounter a task that can only be managed by one or the other.

User interfaces

OneFS and IsilonSD Edge provide several interfaces for managing the EMC Isilon clusters and IsilonSD clusters.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OneFS web administration</td>
<td>The browser-based OneFS web administration interface provides secure access with OneFS-supported browsers. Use this interface to view robust graphical monitoring displays and to perform cluster-management tasks.</td>
<td>The OneFS web administration interface uses port 8080 as its default port.</td>
</tr>
<tr>
<td>command-line interface</td>
<td>Run OneFS <em>isi</em> commands in the command-line interface to configure, monitor, and manage the cluster. Access to the command-line interface is through a secure shell (SSH) connection to any node in the cluster.</td>
<td>The OneFS command-line interface provides an extended standard UNIX command set for managing the cluster.</td>
</tr>
<tr>
<td>OneFS API</td>
<td>The OneFS application programming interface (API) is divided into two functional areas: one area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster. You can send requests to the OneFS API through a Representational State Transfer (REST) interface, which is accessed</td>
<td>You should have a solid understanding of HTTP/1.1 and experience writing HTTP-based client software before you implement client-based software through the OneFS API.</td>
</tr>
</tbody>
</table>
Connecting to the cluster

EMC Isilon cluster access is provided through the web administration interface or through SSH. You can use a serial connection to perform cluster administration tasks through the command-line interface.

You can also access the cluster through the node front panel to accomplish a subset of cluster management tasks. For information about connecting to the node front panel, see the installation documentation for your node.

**Note**
The node front panel is not available with IsilonSD Edge.

Log in to the web administration interface

You can monitor and manage your EMC Isilon cluster from the browser-based web administration interface.

**Procedure**

1. Open a browser window and type the URL for your cluster in the address field, replacing `<yourNodeIPaddress>` with the first IP address you provided when you configured ext-1 in the one of the following examples:

   **IPv4**
   
   ```
   https://<yourNodeIPaddress>:8080
   ```

   **IPv6**
   
   ```
   https://[<yourNodeIPaddress>]:8080
   ```

   **Note**
   IPv6 addresses are not supported with IsilonSD Edge.

   The system displays a message if your security certificates have not been configured. Resolve any certificate configurations and continue to the web site.
2. Log in to OneFS by typing your OneFS credentials in the **Username** and **Password** fields.

After you log into the web administration interface, there is a 4-hour login timeout.

**Open an SSH connection to a cluster**

You can use any SSH client such as OpenSSH or PuTTY to connect to an EMC Isilon cluster.

**Before you begin**

You must have valid OneFS credentials to log in to a cluster after the connection is open.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster, using the IP address of the node and port number 22.
2. Log in with your OneFS credentials.

At the OneFS command line prompt, you can use `isi` commands to monitor and manage your cluster.

**Licensing**

Advanced cluster features are available when you activate licenses for OneFS software modules. Each optional OneFS software module requires you to activate a separate license.

For more information about the following optional software modules, contact your EMC Isilon sales representative.

- CloudPools
- Security hardening
- HDFS
- InsightIQ
- Isilon Swift
- SmartConnect Advanced
- SmartDedupe
- SmartLock
- SmartPools
- SmartQuotas
- SnapshotIQ
- SyncIQ

**Note**

If you are running IsilonSD Edge, CloudPools, SmartLock, and SyncIQ are available only when you purchase an IsilonSD Edge license. All the other optional modules are available by default, with the free license of this product.
License status

The status of a OneFS module license indicates whether the functionality provided by a module is available on the cluster.

Licenses exist in one of the following states:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive</td>
<td>The license has not been activated on the cluster. You cannot access the features provided by the corresponding module.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>The license has been temporarily activated on the cluster. You can access the features provided by the corresponding module for a limited period of time. After the license expires, the features become unavailable unless the license is reactivated.</td>
</tr>
<tr>
<td>Activated</td>
<td>The license has been activated on the cluster. You can access the features provided by the corresponding module.</td>
</tr>
<tr>
<td>Expired</td>
<td>The evaluation license has expired on the cluster. You can no longer access the features provided by the corresponding module. The features will remain unavailable unless you reactivate the license.</td>
</tr>
</tbody>
</table>

**Note**

If you are running IsilonSD Edge, the licenses for the software modules depend on whether you have configured a free or purchased license of IsilonSD Edge and the corresponding license states.

The following table describes what functionality is available for each license depending on the license's status:

<table>
<thead>
<tr>
<th>License</th>
<th>Inactive</th>
<th>Evaluation/Activated</th>
<th>Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPools</td>
<td>Clients cannot connect to or store files in the cloud.</td>
<td>Clients may store, access, and modify files in the cloud. Cloud files may be accessed over common protocols such as NFS and SMB.</td>
<td>New connections may not be made to the cloud and new data may not be archived. Previously written cloud data can still be retrieved.</td>
</tr>
<tr>
<td>Security Hardening</td>
<td>Clients cannot apply or revert security hardening. Clients can apply and revert security hardening and view hardening status.</td>
<td>Clients cannot apply or revert security hardening. Clients can view hardening status.</td>
<td></td>
</tr>
</tbody>
</table>

Note
<table>
<thead>
<tr>
<th>License</th>
<th>Inactive</th>
<th>Evaluation/Activated</th>
<th>Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>Clients cannot access the cluster through HDFS.</td>
<td>You can configure HDFS settings and clients can access the cluster through HDFS.</td>
<td>You cannot configure HDFS settings. After the HDFS service restarts, clients can no longer access the cluster through HDFS.</td>
</tr>
<tr>
<td>InsightIQ</td>
<td>You cannot monitor the cluster with InsightIQ.</td>
<td>You can monitor the cluster with InsightIQ.</td>
<td>InsightIQ stops monitoring the cluster. Data previously collected by InsightIQ is still available on the InsightIQ instance.</td>
</tr>
<tr>
<td>Isilon Swift</td>
<td>Clients cannot access the cluster through Swift.</td>
<td>Clients can access existing file-based data stored on the cluster as objects through a Swift API client application over HTTP or HTTPS.</td>
<td>Clients can no longer access the cluster through Swift.</td>
</tr>
<tr>
<td>SmartConnect Advanced</td>
<td>Client connections are balanced by using a round-robin policy. IP address allocation is static. Each external network subnet can be assigned only one IP address pool.</td>
<td>You can access features such as CPU utilization, connection counting, and client connection policies in addition to the round-robin policy. You can also configure address pools to support multiple DNS zones within a single subnet, and support IP failover.</td>
<td>You can no longer specify SmartConnect Advanced settings.</td>
</tr>
<tr>
<td>SmartDedupe</td>
<td>You cannot deduplicate data with SmartDedupe.</td>
<td>You can deduplicate data with SmartDedupe.</td>
<td>You can no longer deduplicate data. Previously deduplicated data remains deduplicated.</td>
</tr>
<tr>
<td>SmartLock</td>
<td>You cannot enforce file retention with SmartLock.</td>
<td>You can enforce file retention with SmartLock.</td>
<td>You cannot create new SmartLock directories or modify SmartLock directory configuration settings for existing directories. You can still commit files to a write once read many (WORM) state, even after the SmartLock license is</td>
</tr>
<tr>
<td>License</td>
<td>Inactive</td>
<td>Evaluation/Activated</td>
<td>Expired</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SmartPools</td>
<td>All files belong to the default file pool and are governed by the default file pool policy. Virtual hot spare allocation, which reserves space for data repair if a drive fails, is also available.</td>
<td>You can create multiple file pools and file pool policies. You can also manage spillover which defines how write operations are handled when a storage pool is not writable.</td>
<td>You can no longer manage file pool policies, and the SmartPools job will no longer run. Newly added files will be governed by the default file pool policy, and the SetProtectPlus job will eventually apply the default file pool policy to all files in the cluster. If the SmartPools job is running when the license expires, the job completes before becoming disabled.</td>
</tr>
<tr>
<td>SmartQuotas</td>
<td>You cannot create quotas with SmartQuotas.</td>
<td>You can create quotas with SmartQuotas.</td>
<td>OneFS disables all quotas. Exceeding advisory and soft thresholds does not trigger events. Hard and soft thresholds are not enforced.</td>
</tr>
<tr>
<td>SnapshotIQ</td>
<td>You can view and manage snapshots generated by OneFS applications.</td>
<td>You can create, view, and manage snapshots. You can also configure snapshot settings.</td>
<td>You will no longer be able to generate snapshots. Existing snapshot schedules are not deleted; however, the schedules will not generate snapshots. You can still delete snapshots and access snapshot data.</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>You cannot replicate data with SyncIQ.</td>
<td>You can replicate data with SyncIQ</td>
<td>You will no longer be able to replicate data to remote clusters, and remote clusters will not be able to replicate data to the local cluster. Replication policies will still display a status of enabled; however, future replication jobs created by the policy will fail. If a replication job is in progress when the license expires, the job completes.</td>
</tr>
</tbody>
</table>
License configuration

You can configure some OneFS module licenses.

You can configure a license by performing specific operations through the corresponding module. Not all actions that require you to activate a license will configure the license. Also, not all licenses can be configured. Configuring a license does not add or remove access to any features provided by a module.

The following table describes the actions that cause each license to be configured:

<table>
<thead>
<tr>
<th>License</th>
<th>Cause of configuring</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPools</td>
<td>Create a cloud pool policy (other than the default pool policy).</td>
</tr>
<tr>
<td>Hardening</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>HDFS</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>InsightIQ</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>Isilon Swift</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>SmartConnect</td>
<td>Configure SmartConnect Advanced settings for at least one IP address pool.</td>
</tr>
<tr>
<td>SmartDedupe</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>SmartLock</td>
<td>Cannot configure this license.</td>
</tr>
<tr>
<td>SmartPools</td>
<td>Create a file pool policy (other than the default file pool policy).</td>
</tr>
<tr>
<td>SmartQuotas</td>
<td>Create a quota.</td>
</tr>
<tr>
<td>SnapshotIQ</td>
<td>Create a snapshot schedule.</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>Create a replication policy.</td>
</tr>
</tbody>
</table>

Note

In the case of IsilonSD Edge, the module licenses are bundled with the free and purchased licenses of IsilonSD Edge. You are not required to configure them separately.

Activate a license

To access a OneFS module, you must activate a license.

Before you begin

Before you can activate a license, you must obtain a valid license key, and you must have root user privileges on your cluster. To obtain a license key, contact your EMC Isilon sales representative.

Procedure

1. Run the `isi license activate` command.

The following command activates a license:

```
isi license activate <license key>
```
In the case of IsilonSD Edge, the software modules are bundled with the free and purchased licenses. You must configure and activate the IsilonSD Edge license to access the software modules.

## View license information

You can view information about the current status of any optional Isilon software modules.

**Procedure**

1. Run the following command:

   ```
   isi license licenses view
   ```

## Certificates

You can renew the Secure Sockets Layer (SSL) certificate for the Isilon web administration interface or replace it with a third-party SSL certificate.

All Platform API communication, which includes communication through the web administration interface, is over SSL. You can replace or renew the self-signed certificate with a certificate that you generate. To replace or renew an SSL certificate, you must be logged in as root.

### Replace or renew the SSL certificate

You can replace or renew the Secure Sockets Layer (SSL) certificate, which is used to access the EMC Isilon cluster through a browser.

**Before you begin**

When you renew or replace a self-signed SSL certificate, you must provide information for your organization in the format that is described in the self-signed SSL certificate data example.

The following folders are the default locations for the `server.crt` and `server.key` files in OneFS 6.0 and higher.

- **SSL certificate**: `/usr/local/apache2/conf/ssl.crt/server.crt`
- **SSL certificate key**: `/usr/local/apache2/conf/ssl.key/server.key`

**Procedure**

1. Establish an SSH connection to any node in the cluster.
2. To create the appropriate directory, run the following command:

   ```
   mkdir /ifs/local/
   ```

3. To change to the directory, run the following command:

   ```
   cd /ifs/local/
   ```
4. Choose the type of certificate you want to install.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Third-party (public or private) CA-issued certificate | a. To generate a new Certificate Signing Request (CSR) in addition to a new key, run the `openssl req` command. The following command generates a CSR where the hostname is `isilon.example.com`:<br>```bash
openssl req -new -nodes -newkey rsa:1024 -keyout <common name>.key -out <common-name>.csr
```<br>b. Send the contents of the `<common_name>.csr` file from the cluster to your Certificate Authority (CA) for signing. When you receive the signed certificate (now a `.crt` file) from the CA, copy the certificate to `/ifs/local/ <common-name>.crt`.
| Self-signed certificate based on the existing (stock) ssl.key | a. At the command prompt, run the following command to create a two-year certificate. Increase or decrease the value for `-days` to generate a certificate with a different expiration date.<br>```bash
cp /usr/local/apache2/conf/ssl.key/server.key . /
openssl req -new -days 730 -nodes -x509 -key server.key -out server.crt
```A renewal certificate is created, based on the existing (stock) `ssl.key` file. |

5. (Optional) To verify the attributes in an SSL certificate, run the `openssl req` command.<br>`openssl x509 -text -noout -in <common-name>.crt`

6. Run the following commands to install the certificate and key:<br>`isi services -a isi_webui disable chmod 640 <common name>.key \
isi_for_array -s 'cp /ifs/local/<common-name>.key /usr/local/apache2/conf/ssl.key/server.key' \
isi_for_array -s 'cp /ifs/local/<common-name>.crt /usr/local/apache2/conf/ssl.crt/server.crt' isi services -a isi_webui enable`

7. To remove files, run the `rm` command. The following command removes the files in `/ifs/local/folder1`:<br>`rm /ifs/local/folder1/*`
Verify an SSL certificate update

You can verify the details stored in a Secure Sockets Layer (SSL) certificate.

Procedure

1. Run the following command to open and verify the attributes in an SSL certificate:

   ```bash
   echo QUIT | openssl s_client -connect localhost:8080
   ```

Self-signed SSL certificate data example

Self-signed SSL certificate renewal or replacement requires you to provide data such as your fully qualified domain name and a contact email address.

When you renew or replace a self-signed SSL certificate, you are asked to provide data in the format shown in the following example. Some fields in the certificate file contain a default value. If you type `.`, the field is left blank when the certificate is generated.

- Country Name (2 letter code) [XX]:US
- State or Province Name (full name) [Some-State]:Washington
- Locality Name (for example, city) [default city]:Seattle
- Organization Name (for example, company) [Internet Widgits Pty Ltd]:Isilon
- Organizational Unit Name (for example, section) []:Support
- Common Name (for example, server FQDN or server name) [ ]:isilon.example.com
- Email Address []:support@example.com

In addition, you should add the following attributes to be sent with your certificate request:

- Challenge password [ ]:Isilon1
- Optional company name []:

Cluster identity

You can specify identity attributes for the EMC Isilon cluster.

Cluster name

The cluster name appears on the login page, and it makes the cluster and its nodes more easily recognizable on your network. Each node in the cluster is identified by the cluster name plus the node number. For example, the first node in a cluster named Images may be named Images-1.

Note

In the case of IsilonSD Edge, you can assign a cluster name only through the IsilonSD Management Plug-in. For more information, see the IsilonSD Edge Installation and Administration Guide.
Cluster description
The cluster description appears below the cluster name on the login page. The cluster description is useful if your environment has multiple clusters.

Login message
The login message appears as a separate box on the login page of the OneFS web administration interface, or as a line of text under the cluster name in the OneFS command-line interface. The login message can convey cluster information, login instructions, or warnings that a user should know before logging into the cluster. Set this information in the Cluster Identity page of the OneFS web administration interface.

Set the cluster name
You can specify a name, description, and login message to your EMC Isilon cluster. Cluster names must begin with a letter and can contain only numbers, letters, and hyphens. The cluster name is added to the node number to identify each node in the cluster. For example, the first node in a cluster named Images may be named Images-1.

Procedure
1. Open the isi config command prompt by running the following command:

   isi config

2. Run the name command.
   The following command sets the name of the cluster to NewName:

   name NewName

3. Save your changes by running the following command:

   commit

Cluster contact information
Isilon Technical Support personnel and event notification recipients will communicate with the specified contacts.

You can specify the following contact information for your EMC Isilon cluster:

- Company name and location
- Primary and secondary contact names
- Phone number and email address for each contact
Specify contact information

You can specify contact information so that Isilon Technical Support personnel and event notification recipients can contact you.

ESRS is the contact mechanism and must be enabled in order to specify contact information.

Procedure

1. Enable ESRS by running the following command:

   ```
   isi_promptesrs -e
   ```

   The system displays the following message:

   Would you like to enable ESRS? [yes]

2. Type `yes` and then press ENTER.

   The system displays the following message:

   Please enter company name:

3. Type your company name and then press ENTER.

4. Type your contact name and then press ENTER.

5. Type your contact phone and then press ENTER.

6. Type your contact email address and then press ENTER.

Cluster date and time

The Network Time Protocol (NTP) service is configurable manually, so you can ensure that all nodes in a cluster are synchronized to the same time source.

The NTP method automatically synchronizes cluster date and time settings through an NTP server. Alternatively, you can set the date and time reported by the cluster by manually configuring the service.

Windows domains provide a mechanism to synchronize members of the domain to a master clock running on the domain controllers, so OneFS adjusts the cluster time to that of Active Directory with a service. If there are no external NTP servers configured, OneFS uses the Windows domain controller as the NTP time server. When the cluster and domain time become out of sync by more than 4 minutes, OneFS generates an event notification.
If the cluster and Active Directory become out of sync by more than 5 minutes, authentication will not work.

**Set the cluster date and time**

You can set the date, time, and time zone that is used by the EMC Isilon cluster.

**Procedure**

1. Run the `isi config` command.
   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Specify the current date and time by running the `date` command.
   The following command sets the cluster time to 9:47 AM on July 22, 2015:
   
   ```
   date 2015/07/22 09:47:00
   ```

3. To verify your time zone setting, run the `timezone` command. The current time zone setting displays. For example:
   
   ```
   The current time zone is:  Pacific Time Zone
   ```

4. To view a list of valid time zones, run the `help timezone` command. The following options display:

   - Greenwich Mean Time
   - Eastern Time Zone
   - Central Time Zone
   - Mountain Time Zone
   - Pacific Time Zone
   - Arizona
   - Alaska
   - Hawaii
   - Japan
   - Advanced

5. To change the time zone, enter the `timezone` command followed by one of the displayed options.
   The following command changes the time zone to Hawaii:
   
   ```
   timezone Hawaii
   ```

   A message confirming the new time zone setting displays. If your desired time zone did not display when you ran the `help timezone` command, enter `timezone Advanced`. After a warning screen, you will proceed to a list of regions. When you select a region, a list of specific time zones for that region appears. Select the desired time zone (you may need to scroll), then enter `ok` or `cancel` until you return to the `isi config` prompt.

6. Run the `commit` command to save your changes and exit `isi config`. 
Specify an NTP time server

You can specify one or more Network Time Protocol (NTP) servers to synchronize the system time on the EMC Isilon cluster. The cluster periodically contacts the NTP servers and sets the date and time based on the information it receives.

Procedure

1. Run the `isi_ntp_config` command, specifying `add server`, followed by the host name, IPv4, or IPv6 address for the desired NTP server.

   The following command specifies ntp.time.server1.com:

   ```
   isi_ntp_config add server ntp.time.server1.com
   ```

SMTP email settings

If your network environment requires the use of an SMTP server or if you want to route EMC Isilon cluster event notifications with SMTP through a port, you can configure SMTP email settings.

SMTP settings include the SMTP relay address and port number that email is routed through. You can specify an origination email and subject line for all event notification emails sent from the cluster.

If your SMTP server is configured to support authentication, you can specify a username and password. You can also specify whether to apply encryption to the connection.

Configure SMTP email settings

You can send event notifications through the SMTP mail server. You can also enable SMTP authentication if your SMTP server is configured to use it.

You can configure SMTP email settings if your network environment requires the use of an SMTP server or if you want to route EMC Isilon cluster event notifications with SMTP through a port.

Procedure

1. Run the `isi email` command.

   The following example configures SMTP email settings:

   ```
   isi email settings modify --mail-relay 10.7.180.45 \ 
   --mail-sender isilon-cluster@company.com \ 
   --mail-subject "Isilon cluster event" --use-smtp-auth yes \ 
   --smtp-auth-username SMTPuser --smtp-auth-passwd Password123 \ 
   --use-encryption yes
   ```

View SMTP email settings

You can view SMTP email settings.

Procedure

1. Run the following command:

   ```
   isi email settings view
   ```
Configuring the cluster join mode

The cluster join mode specifies how a node is added to the EMC Isilon cluster and whether authentication is required. OneFS supports manual and secure join modes for adding nodes to the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Allows you to manually add a node to the cluster without requiring authorization.</td>
</tr>
<tr>
<td>Secure</td>
<td>Requires authorization of every node added to the cluster and the node must be added through the web administration interface or through the <code>isi devices -a add -d &lt;unconfigured_node_serial_no&gt;</code> command in the command-line interface.</td>
</tr>
</tbody>
</table>

**Note**
If you specify a secure join mode, you cannot join a node to the cluster through serial console wizard option [2] Join an existing cluster.

Specify the cluster join mode

You can specify a join mode that determines how nodes are added to the EMC Isilon cluster.

These instructions are not applicable for IsilonSD Edge.

**Procedure**

1. Open the `isi config` command prompt by running the following command:

   ```
isicfg
   ```

2. Run the `joinmode` command.
The following command prevents nodes from joining the cluster unless the join is initiated by the cluster:

```
joinmode secure
```

3. Save your changes by running the following command:

```
commit
```

## File system settings

You can configure global file system settings on an EMC Isilon cluster pertaining to access time tracking and character encoding.

You can enable or disable access time tracking, which monitors the time of access on each file. If necessary, you can also change the default character encoding on the cluster.

### Specify the cluster character encoding

You can modify the character encoding set for the EMC Isilon cluster after installation. Only OneFS-supported character sets are available for selection. UTF-8 is the default character set for OneFS nodes.

---

**Note**

If the cluster character encoding is not set to UTF-8, SMB share names are case-sensitive.

---

You must restart the cluster to apply character encoding changes.

---

**CAUTION**

Character encoding is typically established during installation of the cluster. Modifying the character encoding setting after installation may render files unreadable if done incorrectly. Modify settings only if necessary after consultation with Isilon Technical Support

---

**Procedure**

1. Run the `isi config` command.

   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Modify the character encoding by running the `encoding` command.

   The following command sets the encoding for the cluster to ISO-8859-1:

   ```
   encoding ISO-8859-1
   ```

3. Run the `commit` command to save your changes and exit the `isi config` subsystem.

4. Restart the cluster to apply character encoding modifications.
Enable or disable access time tracking

You can enable access time tracking to support features that require it.

By default, the EMC Isilon cluster does not track the timestamp when files are accessed. You can enable this feature to support OneFS features that use it. For example, access-time tracking must be enabled to configure SyncIQ policy criteria that match files based on when they were last accessed.

**Note**

Enabling access-time tracking may affect cluster performance.

**Procedure**

1. Enable or disable access time tracking by setting the `atime_enabled` system control.
   - To enable access time tracking, run the following command:
     ```bash
     sysctl efs.bam.atime_enabled=1
     ```
   - To disable access time tracking, run the following command:
     ```bash
     sysctl efs.bam.atime_enabled=0
     ```

2. To specify how often to update the last-accessed time, set the `atime_grace_period` system control.
   - Specify the amount of time as a number of seconds.
   - The following command configures OneFS to update the last-accessed time every two weeks:
     ```bash
     sysctl efs.bam.atime_grace_period=1209600
     ```

Security hardening

Security hardening is the process of configuring your system to reduce or eliminate as many security risks as possible. You can apply a hardening policy that secures the configuration of OneFS, according to policy guidelines.

Security hardening on OneFS is carried out by a hardening engine that reads a hardening profile and applies the profile guidelines. During this process, the hardening engine identifies configuration issues that will prevent hardening on the nodes. For example, the hardening engine might find that the file permissions set for a particular directory are not set to the expected value, or that the required directories are missing. When an issue is found, you can choose to allow the hardening engine to resolve the issue or to defer resolution and fix the issue manually.

**Note**

At this time, OneFS supports only Defense Information Systems Agency (DISA) Security Technology Security Guide (STIG) hardening. No other security profiles are available.
OneFS enables you to revert a security hardening policy if the hardening configuration is not right for your system. Reverting a policy returns OneFS to the configuration achieved by resolving issues, if any, prior to hardening.

OneFS also enables you to apply successive hardening. If a security hardening policy has already been applied to the system, you can apply a new policy with a new profile or with the same profile.

You must have an active security hardening license and be logged in to the EMC Isilon cluster as the root user to apply hardening to OneFS. To obtain a license, contact your EMC Isilon sales representative.

---

**Note**

Security hardening is not supported with IsilonSD Edge.

## STIG hardening profile

The STIG hardening profile contains configuration requirements set by the Department of Defense.

To meet federal Approved Products List (APL) requirements, the configuration of OneFS must comply with several Security Technology Implementation Guides (STIG) that contain hardening configuration requirements. STIGs are maintained by the Defense Information Systems Agency (DISA), which produces a STIG for several computing technologies referred to as assessment areas. The STIG hardening profile contains the requirements for all of the assessment areas that are applicable to OneFS.

After you apply the STIG hardening profile, the configuration of OneFS is modified to meet the STIG requirements. The following modifications are examples of the many system changes:

- After you log in through SSH or the web interface, the system will display a message that you are accessing a U.S. Government Information System and will display the terms and conditions of using the system.
- On each node, SSH and the web interface will listen only on the node's external IP address.
- Password complexity requirements for local user accounts will increase. Passwords must be at least 14 characters and contain at least one of each of the following character types: numeric, uppercase, lowercase, symbol.
- Root SSH will be disabled. To log in after hardening is applied, you can log in as root only through the web interface or through a serial console session.

### STIG profile assessment areas

The STIG hardening profile contains configuration requirements for several aspects of the system, which are referred to as areas of assessment.

The following table displays each area of assessment and the associated Security Technology Implementation Guide (STIG) that is enforced by the hardening profile:

<table>
<thead>
<tr>
<th>Area of assessment</th>
<th>STIG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>UNIX Manual SRG - Version 1, Release 3</td>
</tr>
<tr>
<td></td>
<td>UNIX Policy Manual SRG - Version 1, Release 2</td>
</tr>
<tr>
<td>Apache Web server</td>
<td>Apache 2.2 STIG UNIX - Version 1, Release 4</td>
</tr>
<tr>
<td>Web server</td>
<td>Web Server SRG - Version 1, Release 1</td>
</tr>
</tbody>
</table>
## Apply a security hardening policy

You can select a hardening profile and apply security hardening to the EMC Isilon cluster.

**Before you begin**

Security hardening requires root privileges and can be performed only through the command-line interface.

Once hardening has been successfully applied to the cluster, root SSH is not allowed on a hardened cluster. To log in as the root user on a hardened cluster, you must connect through a serial console session.

You must have an active security hardening license to apply hardening to OneFS. To obtain a license, contact your EMC Isilon sales representative.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in as root.
2. Run the `isi hardening apply` command.

The following command directs the hardening engine to apply the STIG hardening profile to the Isilon cluster.

```bash
isi hardening apply --profile=STIG
```

The hardening engine checks whether the system contains any configuration issues that must be resolved before hardening can be applied.

- If the hardening engine does not encounter any issues, the hardening policy is applied.
- If the hardening engine encounters issues, the system displays output similar to the following example:

```
Found the following Issue(s) on the cluster:
Issue #1 (Isilon Control_id:isi_GEN001200_01)
```
Node: test-cluster-2
1: /etc/syslog.conf: Actual permission 0664; Expected permission 0654

Issue #2 (Isilon Control_id:isi_GEN001200_02)
Node: test-cluster-3
1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555
Node: test-cluster-2
1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555

Total: 2 issue(s)
Do you want to resolve the issue(s)?[Y/N]:

3. Resolve any configuration issues. At the prompt Do you want to resolve the issue(s)?[Y/N], choose one of the following actions:
   a. To allow the hardening engine to resolve all issues, type Y.
      The system will fix the issues and then apply the hardening policy.
   b. To defer resolution and fix all found issues manually, type N.
      After you have fixed all deferred issues, run the isi hardening apply command again.

Note
If the hardening engine encounters an issue that is considered catastrophic, the system will prompt you to resolve the issue manually; the hardening engine cannot resolve a catastrophic issue.

Revert a security hardening policy

You can revert a security hardening policy that has been applied to the EMC Isilon cluster.

Before you begin
Reverting security hardening requires root privileges and can be performed only through the command-line interface. To log in as the root user on a hardened cluster, you must connect through a serial console session; root SSH is not allowed on a hardened cluster.
You must have an active security hardening license to revert a hardening policy on OneFS. To obtain a license, contact your EMC Isilon sales representative.

Procedure
1. Open a serial console session on any node in the cluster and log in as root.
2. Run the isi hardening revert command.
   The hardening engine checks whether the system is in an expected state.
   • If the hardening engine does not encounter any issues, the hardening policy is reverted.
   • If the hardening engine encounters any issues, the system displays output similar to the following example:

    Found the following Issue(s) on the cluster:
    Issue #1 (Isilon Control_id:isi_GEN001200_01)
Node: test-cluster-2
1: /etc/syslog.conf: Actual permission 0664; Expected permission 0645

Issue #2 (Isilon Control_id:isi_GEN001200_02)
Node: test-cluster-3
1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555

Node: test-cluster-2
1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555

Total: 2 issue(s)
Do you want to resolve the issue(s)? [Y/N]:

3. Resolve any configuration issues. At the prompt **do you want to resolve the issue(s)? [Y/N]**, choose one of the following actions:

   a. To allow the hardening engine to resolve all issues, type **Y**.

      The hardening engine will set the affected configurations to the expected state and then revert the hardening policy.

   b. To defer resolution and fix all found issues manually, type **N**.

      The hardening engine halts the revert process until all issues are fixed. After you have fixed all deferred issues, run the `isi hardening revert` command again.

---

**Note**

If the hardening engine encounters an issue that is considered catastrophic, the system will prompt you to resolve the issue manually; the hardening engine cannot resolve a catastrophic issue.

---

**View the security hardening status**

You can view the security hardening status of the EMC Isilon cluster and each cluster node.

**Before you begin**

Viewing the security hardening status of the cluster requires root privileges and can be performed only through the command-line interface. To log in as the root user on a hardened cluster, you must connect through a serial console session; root SSH is not allowed on a hardened cluster.

You do not need a security hardening license to view the hardening status of the cluster.

**Procedure**

1. Open a console session on any node in the cluster and log in as root.

2. Run the `isi hardening status` command to view the status of security hardening on the Isilon cluster.

   The system displays output similar to the following example:

   ```
   Cluster Name: test-cluster
   Hardening Status: Not Hardened
   ```
Cluster monitoring

You can view health and status information for the EMC Isilon cluster and monitor cluster and node performance.

Run the `isi status` command to review the following information:

- Cluster, node, and drive health
- Storage data such as size and amount used
- IP addresses
- Throughput
- Critical events
- Job status

Additional commands are available to review performance information for the following areas:

- General cluster statistics
- Statistics by protocol or by clients connected to the cluster
- Performance data by drive
- Historical performance data

Advanced performance monitoring and analytics are available through the InsightIQ module, which requires you to activate a separate license. For more information about optional software modules, contact your EMC Isilon sales representative.

Monitor the cluster

You can monitor the health and performance of a cluster with charts and tables.

Procedure

1. Run the following command:

   ```
   isi status
   ```

View node status

You can view the status of a node.

Procedure

1. (Optional) Run the `isi status` command:

   The following command displays information about a node with a logical node number (LNN) of 1:

   ```
   isi status -n 1
   ```
Monitoring cluster hardware

You can manually check the status of hardware on the EMC Isilon cluster as well as enable SNMP to remotely monitor components.

View node hardware status

You can view the hardware status of a node.

Procedure

1. Click Dashboard > Cluster Overview > Cluster Status.
2. (Optional) In the Status area, click the ID number for a node.
3. In the Chassis and drive status area, click Platform.

Chassis and drive states

You can view chassis and drive state details.

In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work. A cluster can lose write quorum but keep read quorum. OneFS provides details about the status of chassis and drives in your cluster. The following table describes all the possible states that you may encounter in your cluster.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHY</td>
<td>All drives in the node are functioning correctly.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td>A solid state drive (SSD) was deployed as level 3 (L3) cache to increase the size of cache memory and improve throughput speeds.</td>
<td>Command-line interface</td>
<td></td>
</tr>
<tr>
<td>SMARTFAIL or Smartfail or restripe in progress</td>
<td>The drive is in the process of being removed safely from the file system, either because of an I/O error or by user request. Nodes or drives in a smartfail or</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NOT AVAILABLE</td>
<td>A drive is unavailable for a variety of reasons. You can click the bay to view detailed information about this condition.</td>
<td>Command-line interface, web administration interface</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state includes the <strong>ERASE</strong> and <strong>SED_ERROR</strong> command-line interface states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSPENDED</td>
<td>This state indicates that drive activity is temporarily suspended and the drive is not in use. The state is manually initiated and does not occur during normal cluster activity.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>NOT IN USE</td>
<td>A node in an offline state affects both read and write quorum.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>REPLACE</td>
<td>The drive was smartfailed successfully and is ready to be replaced.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>STALLED</td>
<td>The drive is stalled and undergoing stall evaluation. Stall evaluation is the process of checking drives that are slow or having other issues. Depending on the outcome of the evaluation, the drive may return to service or be smartfailed. This is a transient state.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>NEW</td>
<td>The drive is new and blank. This is the</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>USED</td>
<td>The drive was added and contained an Isilon GUID but the drive is not from this node. This drive likely will be formatted into the cluster.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>PREPARING</td>
<td>The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>EMPTY</td>
<td>No drive is in this bay.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>WRONG_TYPE</td>
<td>The drive type is wrong for this node. For example, a non-SED drive in a SED node, SAS instead of the expected SATA drive type.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>BOOT_DRIVE</td>
<td>Unique to the A100 drive, which has boot drives in its bays.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>SED_ERROR</td>
<td>The drive cannot be acknowledged by the OneFS system.</td>
<td>Command-line interface, web administration interface</td>
<td>X</td>
</tr>
<tr>
<td>Note</td>
<td>In the web administration interface, this state is included in Not available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERASE</td>
<td>The drive is ready for removal but needs your attention because the data has not been erased. You can erase the drive manually to guarantee that data is removed.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
</tbody>
</table>
### Check battery status

You can monitor the status of NVRAM batteries and charging systems. This task may only be performed at the OneFS command-line interface on node hardware that supports the command.

These instructions are not applicable for IsilonSD Edge.

**Procedure**

1. Open an SSH connection to any node in the cluster.
2. Run the `isi batterystatus list` command to view the status of all NVRAM batteries and charging systems on the node.

The system displays output similar to the following example:

```
Lnn  Status1  Status2  Result1  Result2
----------------------------------------
1    Good     Good     -        -
2    Good     Good     -        -
3    Good     Good     -        -
----------------------------------------
```

**SNMP monitoring**

You can use SNMP to remotely monitor the EMC Isilon cluster hardware components, such as fans, hardware sensors, power supplies, and disks. Use the default Linux SNMP tools or a GUI-based SNMP tool of your choice for this purpose.

You can enable SNMP monitoring on individual nodes on your cluster, and you can also monitor cluster information from any node. Generated SNMP traps are sent to your SNMP network. You can configure an event notification rule that specifies the network station where you want to send SNMP traps for specific events, so that when an event occurs, the cluster sends the trap to that server. OneFS supports SNMP in read-only mode. OneFS supports SNMP version 2c, which is the default, and SNMP version 3.

**Note**

OneFS does not support SNMP version 1. Although an option for `--snmp-v1-v2-access` exists in the OneFS command-line interface (CLI) command `isi snmp settings modify`, if you turn on this feature, OneFS will only monitor through SNMP version 2c.

You can configure settings for SNMP version 3 alone or for both SNMP version 2c and version 3.

**Note**

If you configure SNMP version 3, OneFS requires the SNMP-specific security level of AuthNoPriv as the default value when querying the cluster. The security level AuthPriv is not supported.

Elements in an SNMP hierarchy are arranged in a tree structure, similar to a directory tree. As with directories, identifiers move from general to specific as the string progresses from left to right. Unlike a file hierarchy, however, each element is not only named, but also numbered.

For example, the SNMP `entity.iso.org.dod.internet.private.enterprises.isilon.oneFSss.s sLocalNodeId.0` maps to `1.3.6.1.4.1.12124.3.2.0`. The part of the name that refers to the OneFS SNMP namespace is the 12124 element. Anything further to the right of that number is related to OneFS-specific monitoring.

Management Information Base (MIB) documents define human-readable names for managed objects and specify their data types and other properties. You can download MIBs that are created for SNMP-monitoring of an Isilon cluster from the OneFS web administration interface or manage them using the command line interface (CLI).

MIBs are stored in `/usr/share/snmp/mibs/` on a OneFS node. The OneFS ISILON-MIBs serve two purposes:
- Augment the information available in standard MIBs
- Provide OneFS-specific information that is unavailable in standard MIBs

ISILON-MIB is a registered enterprise MIB. Isilon clusters have two separate MIBs:

**ISILON-MIB**
Defines a group of SNMP agents that respond to queries from a network monitoring system (NMS) called OneFS Statistics Snapshot agents. As the name implies, these agents snapshot the state of the OneFS file system at the time that it receives a request and reports this information back to the NMS.

**ISILON-TRAP-MIB**
Generates SNMP traps to send to an SNMP monitoring station when the circumstances occur that are defined in the trap protocol data units (PDUs).

The OneFS MIB files map the OneFS-specific object IDs with descriptions. Download or copy MIB files to a directory where your SNMP tool can find them, such as `/usr/share/snmp/mibs/`.

To enable Net-SNMP tools to read the MIBs to provide automatic name-to-OID mapping, add `-m All` to the command, as in the following example:

```
snmpwalk -v2c -c public -m All <node IP> isilon
```

If the MIB files are not in the default Net-SNMP MIB directory, you may need to specify the full path, as in the following example. Note that all three lines are a single command.

```
snmpwalk -m /usr/local/share/snmp/mibs/ISILON-MIB.txt:/usr/share/snmp/mibs /ONEFS-TRAP-MIB.txt -v2c -C c -c public <node IP> enterprises.onefs
```

**Note**
The previous examples are run from the `snmpwalk` command on a cluster. Your SNMP version may require different arguments.

**Managing SNMP settings**

You can use SNMP to monitor cluster hardware and system information. You can configure settings through either the web administration interface or the command-line interface.

You can enable SNMP monitoring on individual nodes in the cluster, and you can monitor information cluster-wide from any node when you enable SNMP on each node. When using SNMP on an Isilon cluster, you should use a fixed general username. A password for the general user can be configured in the web administration interface.

You should configure a network monitoring system (NMS) to query each node directly through a static IPv4 or IPv6 address. This approach allows you to confirm that all nodes have external IP addresses and therefore respond to SNMP queries. Because the SNMP proxy is enabled by default, the SNMP implementation on each node is configured automatically to proxy for all other nodes in the cluster except itself. This proxy configuration allows the Isilon Management Information Base (MIB) and standard MIBs to be exposed seamlessly through the use of context strings for supported SNMP versions. After you download and save the appropriate MIBs, you
can configure SNMP monitoring through either the web administration interface or though the command-line interface.

### Configure SNMP settings

You can configure SNMP monitoring settings

**Note**

When SNMP v3 is used, OneFS requires the SNMP-specific security level of AuthNoPriv as the default value when querying the EMC Isilon cluster. The security level AuthPriv is not supported.

**Procedure**

- Run the `isi snmp settings modify` command.

The following command enables SNMP v3 access:

```
isi snmp settings modify --snmp-v3-access=yes
```

### Configure the cluster for SNMP monitoring

You can configure your EMC Isilon cluster to remotely monitor hardware components using SNMP.

**Before you begin**

When SNMPv3 is used, OneFS requires the SNMP-specific security level of AuthNoPriv as the default value when querying the cluster. The security level AuthPriv is not supported.

You can enable or disable SNMP monitoring, allow SNMP access by version, and configure other settings, some of which are optional. All SNMP access is read-only.

**Note**

The Isilon cluster does not generate SNMP traps unless you configure an event notification rule to send events.

**Procedure**

1. Click **Cluster Management > General Settings > SNMP Monitoring**.
2. In the **SNMP Service Settings**, click the **Enable SNMP Service** check box. The SNMP service is enabled by default.
3. Download the MIB file you want to use (base or trap).

   Follow the download process that is specific to your browser.
4. Copy the MIB files to a directory where your SNMP tool can find them, such as `/usr/share/snmp/mibs/`

   To have Net-SNMP tools read the MIBs to provide automatic name-to-OID mapping, add `-m All` to the command, as in the following example:

```
snmpwalk -v2c -c public -m All <node IP> isilon
```
5. If your protocol is SNMPv2, ensure that the **Allow SNMPv2 Access** check box is selected. SNMPv2 is selected by default.
6. In the **SNMPv2 Read-Only Community Name** field, enter the appropriate community name. The default is `I$ilonpublic`.

7. To enable SNMPv3, click the **Allow SNMPv3 Access** check box.

8. Configure SNMP v3 Settings:
   a. In the **SNMPv3 Read-Only User Name** field, type the SNMPv3 security name to change the name of the user with read-only privileges.

      The default read-only user is `general`.

   b. In the **SNMPv3 Read-Only Password** field, type the new password for the read-only user to set a new SNMPv3 authentication password.

      The default password is `password`. We recommend that you change the password to improve security. The password must contain at least eight characters and no spaces.

   c. Type the new password in the **Confirm password** field to confirm the new password.

9. In the **SNMP Reporting** area, enter a cluster description in the **Cluster Description** field.

10. In the **System Contact Email** field, enter the contact email address.

11. Click **Save Changes**.

### View SNMP settings

You can review SNMP monitoring settings.

**Procedure**

- Run the following command:

```bash
isi snmp settings view
```

This is an example of the output generated by the command:

```
System Location: unset
System Contact: unset@unset.invalid
Snmp V1 V2C Access: Yes
Read Only Community: I$ilonpublic
Snmp V3 Access: No
Snmp V3 Read Only User: general
SNMP Service Enabled: Yes
```

### Events and alerts

OneFS continuously monitors the health and performance of your cluster and generates events when situations occur that might require your attention.

Events can be related to file system integrity, network connections, jobs, hardware, and other vital operations and components of your cluster. After events are captured, they are analyzed by OneFS. Events with similar root causes are organized into event groups.
Note

For descriptions of individual event types by event type ID, see the *Isilon OneFS Event Reference*. Certain events such as hardware events do not apply to IsilonSD Edge.

An event group is a single point of management for numerous events related to a particular situation. You can determine which event groups you want to monitor, ignore, or resolve.

An alert is the message that reports on a change that has occurred in an event group. You can control how alerts related to an event group are distributed. Alerts are distributed through channels. You can create and configure a channel to send alerts to a specific audience, control the content the channel distributes, and limit frequency of the alerts.

Events overview

Events are individual occurrences or conditions related to the data workflow, maintenance operations, and hardware components of your cluster.

Throughout OneFS there are processes that are constantly monitoring and collecting information on cluster operations.

When the status of a component or operation changes, the change is captured as an event and placed into a priority queue at the kernel level.

Every event has two ID numbers that help to establish the context of the event:

- The event type ID identifies the type of event that has occurred.
- The event instance ID is a unique number that is specific to a particular occurrence of an event type. When an event is submitted to the kernel queue, an event instance ID is assigned. You can reference the instance ID to determine the exact time that an event occurred.

You can view individual events. However, you manage events and alerts at the event group level.

Event groups overview

Event groups are collections of individual events that are related symptoms of a single situation on your cluster. Event groups provide a single point of management for multiple event instances that are generated in response to a situation on your cluster.

For example, if a chassis fan fails in a node, OneFS might capture multiple events related both to the failed fan itself, and to exceeded temperature thresholds within the node. All events related to the fan will be represented in a single event group. Because there is a single point of contact, you do not need to manage numerous individual events. You can handle the situation as a single, coherent issue.

All management of events is performed at the event group level. You can mark an event group as resolved or ignored. You can also configure how and when alerts are distributed for an event group.

Alerts overview

An alert is a message that describes a change that has occurred in an event group. At any point in time, you can view event groups to track situations occurring on your cluster. However, you can also create alerts that will proactively notify you if there is a change in an event group.
For example, you can generate an alert when a new event is added to an event group, when an event group is resolved, or when the severity of an event group changes. You can configure your cluster to only generate alerts for specific event groups, conditions, severity, or during limited time periods. Alerts are delivered through channels. You can configure a channel to determine who will receive the alert and when.

Channels overview

Channels are pathways by which event groups send alerts. When an alert is generated, the channel associated with the alert determines how the alert is distributed and who receives the alert. You can configure a channel to deliver alerts with one of the following mechanisms: SMTP, SNMP, or ConnectEMC. You can also specify routing and labeling information that is required by the delivery mechanism.

Viewing and modifying event groups

You can view event and modify the status of event groups.

View an event group

You can view the details of an event group.

Procedure

1. (Optional) To identify the group ID of the event group that you want to view, run the following command:

   ```
   isi event groups list
   ```

2. To view the details of a specific event group, run the `isi event groups view` command and specify the event group ID.

   The following example command displays the details for an event group with the event group ID of 65686:

   ```
   isi event groups view 65686
   ```

   The system displays output similar to the following example:

   | ID: 65686 |
   | Started: 08/15 02:12 |
   | Causes Long: Node 2 offline |
   | Last Event: 2015-08-15T03:01:17 |
   | Ignore: No |
   | Ignore Time: Never |
   | Resolved: Yes |
   | Ended: 08/15 02:46 |
   | Events: 6 |
   | Severity: critical |
Change the status of an event group

You can ignore or resolve an event group.

Procedure

1. (Optional) To identify the group ID of the event group that you want modify, run the following command:

   isi event groups list

2. To change the status of an event group, run the `isi event groups modify` command. To change the status of all event groups at once, run the `isi event groups bulk` command.

   The following example command modifies an event group with the event group ID of 7 to a status of ignored:

   ```
   isi event groups modify 7 --ignored true
   ```

   The following example command changes the status of all event groups to resolved:

   ```
   isi event groups bulk --resolved true
   ```

View an event

You can view the details of a specific event.

Procedure

1. (Optional) To identify the instance ID of the event that you want to view, run the following command:

   ```
   isi event events list
   ```

2. To view the details of a specific event, run the `isi event events view` command and specify the event instance ID.

   The following example command displays the details for an event with the instance ID of 3.121:

   ```
   isi event events view 3.121
   ```

   The system displays output similar to the following example:

   ```
   ID: 3.121
   Eventgroup ID: 7
   Event Type: 200020001
   Message: Gigabit Ethernet link ext-1 (vmx1) running below capacity
   DevId: 3
   Lnn: 3
   Time: 2015-08-04T16:02:10
   ```
Managing alerts

You can view, create, modify, or delete alerts to determine the information you deliver about event groups.

View an alert

You can view the details of a specific alert.

Procedure

1. (Optional) To identify the alert ID of the alert that you want to view, run the following command:

   isi event alerts list

2. To view the details of a specific alert, run the isi event alerts view command and specify the name of the alert.

   The following example command displays the details for an event with the name NewExternal:

   isi event alerts view NewExternal

   The name of the alert is case-sensitive.

   The system displays output similar to the following example:

   Name: NewExternal
   Eventgroup: 3
   Category: 200000000, 700000000, 900000000
   Channel: RemoteSupport
   Condition: NEW

Create a new alert

You can create new alerts to provide specific updates on event groups.

Procedure

1. Run the isi event alerts create command.

   The following command creates an alert named Hardware, sets the alert condition to NEW_EVENTS, and sets the channel that will broadcast the event as RemoteSupport:

   isi event alerts create Hardware NEW-EVENTS --channel RemoteSupport

   The following command creates an alert named ExternalNetwork, sets the alert condition to NEW, sets the source event group to the event group with the ID

...
number 3, sets the channel that will broadcast the event as RemoteSupport, sets the severity level to critical, and sets the maximum alert limit to 10:

```
isi event alerts create ExternalNetwork NEW --eventgroup 3 --channel RemoteSupport --severity critical --limit 10
```

Modify an alert

You can modify an alert that you created.

**Procedure**

1. (Optional) To identify the name of the alert that you want to modify, run the following command:

   ```
   isi event alerts list
   ```

2. Modify an alert by running the `isi event alerts modify` command.

   The following example command modifies the alert named ExternalNetwork by changing the name of the alert to ExtNetwork, adding the event group with an event group ID number of 131091, and filtering so that alerts will only be sent for event groups with a severity value of critical:

   ```
   isi event alerts modify ExternalNetwork --name ExtNetwork --add-eventgroup 131091 --severity critical
   ```

Delete an alert

You can delete alerts that you created.

**Procedure**

1. (Optional) To identify the name of the alert that you want to delete, run the following command:

   ```
   isi event alerts list
   ```

2. Delete an alert by running the `isi event alerts delete` command.

   The following example command deletes the alert named ExtNetwork:

   ```
   isi event alerts delete ExtNetwork
   ```

   The name of the alert is case-sensitive.

3. Type `yes` to confirm deletion.

Managing channels

You can view, create, modify, or delete channels to determine how you deliver information about event groups.
View a channel

You can view the details of a specific channel.

Procedure

1. (Optional) To identify the name of the channel that you want to view, run the following command:

   ```bash
   isi event channels list
   ```

2. To view the details of a channel, run the `isi event channels view` command and specify the name of the channel.

   The following example command displays the details for a channel with the name Support:

   ```bash
   isi event channels view Support
   ```

   The name of the channel is case-sensitive.

   The system displays output similar to the following example:

   ```
   ID: 3
   Name: Support
   Type: smtp
   Enabled: Yes
   Excluded Nodes: 2
   Address: email@support.com
   Send As: email@support2.com
   Subject: Support Request
   SMTP Host: -
   SMTP Port: 25
   SMTP Use Auth: No
   SMTP Username: -
   SMTP Password: -
   SMTP Security: -
   Batch: NONE
   Enabled: Yes
   Allowed Nodes: 1
   ```

Create a new channel

You can create and configure new channels to send out alert information.

Procedure

1. Run the `isi event channels create` command.

   The following command creates a channel named Support and sets the type to EMCConnect.

   ```bash
   isi event channels create Support connectemc
   ```
The following command creates a channel named Meeting, sets the type to SNMP, sets the SNMP host to hostname, and the SNMP community string to public.

```
isi event channels create Meeting snmp --host hostname --community public
```

**Modify a channel**

You can modify a channel that you created.

**Procedure**

1. (Optional) To identify the name of the channel that you want to modify, run the following command:

   ```
   isi event channels list
   ```

2. Modify a channel by running the `isi event channels modify` command.

   The following example command modifies the channel named Support by changing the send-from email address to email@support3.com:

   ```
   isi event channels modify Support --send-as email@support3.com
   ```

   The following example command modifies the channel named Support by changing the SMTP username to admin, and the SMTP password to p@ssword:

   ```
   isi event channels modify Support --smtp-username admin --smtp-password p@ssword
   ```

**Delete a channel**

You can delete channels that you created.

**Before you begin**

You will not be able to delete a channel that is currently in use by an alert. Remove a channel from an alert by running the `isi event alerts modify` command.

**Procedure**

1. (Optional) To identify the name of the channel that you want to delete, run the following command:

   ```
   isi event channels list
   ```

2. Delete a channel by running the `isi event channels delete` command.

   The following example command deletes the alert named Support:

   ```
   isi event channels delete Support
   ```

   The name of the channel is case-sensitive.
3. Type yes to confirm deletion.

**Maintenance and testing**

You can modify event settings to specify retention and storage limits for event data, schedule maintenance windows, and send test events.

**Event data retention and storage limits**

You can modify settings to determine how event data is handled on your cluster.

By default, data related to resolved event groups is retained indefinitely. You can set a retention limit to make the system automatically delete resolved event group data after a certain number of days.

You can also limit the amount of memory that event data can occupy on your cluster. By default, the limit is 1 megabyte of memory for every 1 terabyte of total memory on the cluster. You can adjust this limit to be between 1 and 100 megabytes of memory. For smaller clusters, the minimum amount of memory that will be set aside is 1 gigabyte.

When your cluster reaches a storage limit, the system will begin deleting the oldest event group data to accommodate new data.

**View event storage settings**

You can view your storage and maintenance settings.

**Procedure**

1. To view, run the `isi event settings view` command.

   The system displays output similar to the following example:

   ```
   Retention Days: 90
   Storage Limit: 1
   Maintenance Start: 2015-08-05T08:00:00
   Maintenance Duration: 4H
   Heartbeat Interval: daily
   ```

**Modify event storage settings**

You can modify your storage and maintenance settings.

**Procedure**

1. Modify your settings by running the `isi event settings modify` command.

   The following example command changes the number of days that resolved event groups are saved to 120:

   ```
   isi event settings modify --retention-days 120
   ```

   The following example command changes the storage limit for event data to 5 MB for every 1 TB of total cluster storage:

   ```
   isi event settings modify --storage-limit 5
   ```
Maintenance windows

You can schedule a maintenance window by setting a maintenance start time and duration.

During a scheduled maintenance window, the system will continue to log events, but no alerts will be generated. Scheduling a maintenance window will keep channels from being flooded by benign alerts associated with cluster maintenance procedures.

Active event groups will automatically resume generating alerts when the scheduled maintenance period ends.

Schedule a maintenance window

You can schedule a maintenance window to discontinue alerts while you are performing maintenance on your cluster.

Procedure

1. Schedule a maintenance window by running the `isi event settings modify` command.

   The following example command schedules a maintenance window that begins on September 1, 2015 at 11:00pm and lasts for two days:

   ```
   isil event settings modify --maintenance-start 2015-09-01T23:00:00 --maintenance-duration 2D
   ```

Test events and alerts

Test events called heartbeat events are automatically generated. You can also manually generate test alerts.

In order to confirm that the system is operating correctly, test events are automatically sent every day, one event from each node in your cluster. These are referred to as heartbeat events and are reported to an event group named Heartbeat Event.

To test the configuration of channels, you can manually send a test alert through the system.

Create a test alert

You can manually generate a test alert.

Procedure

1. Manually generate a test alert by running the `isi event test create` command.

   The following example command creates a test alert with the message Test message:

   ```
   isil event test create "Test message"
   ```

Modify the heartbeat event

You can change the frequency that a heartbeat event is generated.

This procedure is available only through the command-line interface.
Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Modify the heartbeat event interval by running the `isi event settings modify` command.

   The following example command modifies the heartbeat event so that it is sent on a weekly basis:

   ```bash
   isi event settings modify --heartbeat-interval weekly
   ```

Cluster maintenance

Trained service personnel can replace or upgrade components in Isilon nodes. Isilon Technical Support can assist you with replacing node components or upgrading components to increase performance.

Replacing node components

If a node component fails, Isilon Technical Support will work with you to quickly replace the component and return the node to a healthy status.

Trained service personnel can replace the following field replaceable units (FRUs):

- battery
- boot flash drive
- SATA/SAS Drive
- memory (DIMM)
- fan
- front panel
- intrusion switch
- network interface card (NIC)
- InfiniBand card
- NVRAM card
- SAS controller
- power supply

*Note*

These components are not applicable for an IsilonSD node.

If you configure your cluster to send alerts to Isilon, Isilon Technical Support will contact you if a component needs to be replaced. If you do not configure your cluster to send alerts to Isilon, you must initiate a service request.

Upgrading node components

You can upgrade node components to gain additional capacity or performance.

Trained service personnel can upgrade the following components in the field:
These node components are not applicable for IsilonSD Edge.

- drive
- memory (DIMM)
- network interface card (NIC)

If you want to upgrade components in your nodes, contact Isilon Technical Support.

Managing drive firmware

If the firmware of any drive in a cluster becomes obsolete, the cluster performance or hardware reliability might get affected. To ensure overall data integrity, you may update the drive firmware to the latest revision by installing the drive support package or the drive firmware package.

Drive firmware and its related features and functions are not applicable for IsilonSD Edge.

You can determine whether the drive firmware on your cluster is of the latest revision by viewing the status of the drive firmware.

We recommend that you contact EMC Isilon Technical Support before updating the drive firmware.

Drive firmware update overview

You can update the drive firmware through drive support packages or drive firmware packages.

Download and install either of these packages from http://support.emc.com depending on the OneFS version running on your cluster and the type of drives on the nodes.

Drive Support Package

For clusters running OneFS 7.1.1 and later, install a drive support package to update the drive firmware. You do not need to reboot the affected nodes to complete the firmware update. A drive support package provides the following additional capabilities:

- Updates the following drive configuration information:
  - List of supported drives
  - Drive firmware metadata
  - SSD wear monitoring data
  - SAS and SATA settings and attributes
- Automatically updates the drive firmware for new and replacement drives to the latest revision before those drives are formatted and used in a cluster. This is applicable only for clusters running OneFS 7.2 and later.
Note
Firmware of drives in use cannot be updated automatically.

Drive Firmware Package
For clusters running OneFS versions earlier than 7.1.1, or for clusters with non-bootflash nodes, install a cluster-wide drive firmware package to update the drive firmware. You must reboot the affected nodes to complete the firmware update.

Install a drive support package
For clusters running OneFS 7.1.1 and later, install the latest drive support package to update your drive firmware to the latest supported revision.

Before you begin
See the Considerations for installing the latest drive support package section before you begin the installation.

Procedure
1. Go to the EMC Support page that lists all the available versions of the drive support package.
2. Click the latest version of the drive support package and download the file.
   
   Note
   See the Considerations for installing the latest drive support package section in order to select the appropriate variant of the package. If you are unable to download the package, contact EMC Isilon Technical Support for assistance.
   
3. Open a secure shell (SSH) connection to any node in the cluster and log in.
4. Create or check for the availability of the directory structure /ifs/data/Isilon_Support/dsp.
5. Copy the downloaded file to the dsp directory through SCP, FTP, SMB, NFS, or any other supported data-access protocols.
6. Unpack the file by running the tar command.
   For example, based on the variant selected for the drive support package, unpack the package by running one of the following commands:

   
   ```
   tar -zxvf Drive_Support_<version>.tgz
   tar –zxvf Drive_Support_<version>_No_SSD.tgz
   ```

7. Install the package by running the isi_dsp_install command.
   For example, based on the variant selected for the drive support package, install the package by running one of the following commands:

   ```
   isi_dsp_install Drive_Support_<version>.tar
   isi_dsp_install Drive_Support_<version>_No_SSD.tar
   ```
You must run the `isi_dsp_install` command to install the drive support package. Do not use the `isi pkg` command.

- Running `isi_dsp_install` will install the drive support package on the entire cluster.
- The installation process takes care of installing all the necessary files from the drive support package followed by the uninstallation of the package. You do not need to delete the package after its installation or prior to installing a later version.

View drive firmware status

You can view the status of the drive firmware on the cluster to determine whether you need to update the firmware.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Perform one of the following tasks:
   - View the drive firmware status of all the nodes. Depending on your version of OneFS, run one of the following commands:
     - OneFS 8.0 or later
       ```bash
       isi devices drive firmware list --node-1nn all
       ```
     - Earlier than OneFS 8.0
       ```bash
       isi drivefirmware status
       ```
   - To view the drive firmware status of drives on a specific node, run one of the following commands:
     - OneFS 8.0 or later
       ```bash
       isi devices drive firmware list --node-1nn <node-number>
       ```
     - Earlier than OneFS 8.0
       ```bash
       isi drivefirmware status -n <node-number>
       ```
     If a drive firmware update is not required, the Desired FW column is empty.

Update drive firmware

If the firmware for a drive becomes obsolete, you must update the drive firmware.

This procedure explains how to update the drive firmware on nodes that contain bootflash drives. To update drive firmware on nodes that do not contain bootflash drives, you must download and install the latest drive firmware package. For more information, see the latest drive firmware package release notes available on [https://support.emc.com/](https://support.emc.com/).

Note

- Do not restart or power off nodes while drive firmware is being updated on the cluster.
Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.

2. Depending on your version of OneFS, run one of the following commands to update the drive firmware for your cluster:

   **OneFS 8.0 or later**
   
   To update the drive firmware for your entire cluster, run the following command:
   
   ```bash
   isi devices drive firmware update start all --node-1nn all
   ```
   
   To update the drive firmware for a specific node only, run the following command:
   
   ```bash
   isi devices drive firmware update start all --node-1nn <node-number>
   ```

   **OneFS 7.1.1 - OneFS 8.0**
   
   For OneFS versions between 7.1.1 - 8.0 you will need to run the following command on each node that requires drive firmware:
   
   ```bash
   isi devices -a fwupdate
   ```

   **CAUTION**

   You must wait for one node to finish updating before you initiate an update on the next node. To confirm that a node has finished updating, run the following command:
   
   ```bash
   isi devices -d <node-number>
   ```
   
   A drive that is still updating will display a status of FWUPDATE.

   Updating the drive firmware of a single drive takes approximately 15 seconds, depending on the drive model. OneFS updates drives sequentially.

**Verify a drive firmware update**

After you update the drive firmware in a node, confirm that the firmware is updated properly and that the affected drives are operating correctly.

**Procedure**

1. Ensure that no drive firmware updates are currently in progress by running one of the following commands:

   **OneFS 8.0 or later**

   ```bash
   isi devices drive firmware update list
   ```

   **Earlier than OneFS 8.0**

   ```bash
   isi devices
   ```

   If a drive is currently being updated, [FW_UPDATE] appears in the status column.
2. Verify that all drives have been updated by running the following command:

OneFS 8.0 or later

```bash
isi devices drive firmware list
```

Earlier than OneFS 8.0

```bash
isi drivefirmware status
```

If all drives have been updated, the Desired FW column is empty.

3. Verify that all affected drives are operating in a healthy state by running the following command:

OneFS 8.0 or later

```bash
isi devices drive list --node-1nn all
```

Earlier than OneFS 8.0

```bash
isi devices
```

If a drive is operating in a healthy state, [HEALTHY] appears in the status column.

**Drive firmware status information**

You can view information about the status of the drive firmware through the OneFS command-line interface.

The following example shows the output of the `isi drivefirmware status` command:

<table>
<thead>
<tr>
<th>Model</th>
<th>FW</th>
<th>Desired FW</th>
<th>Count</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HGST HUS724030ALA640</td>
<td>MF80AAC0</td>
<td>30</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Where:

**Model**
Displays the name of the drive model.

**FW**
Displays the version number of the firmware currently running on the drives.

**Desired FW**
If the drive firmware should be upgraded, displays the version number of the drive firmware that the firmware should be updated to.

**Count**
Displays the number of drives of this model that are currently running the specified drive firmware.
Nodes
Displays the LNNs of nodes that the specified drives exist in.

The following example shows the output of the isi devices command with the -a fwstatus option:

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Model</th>
<th>FW</th>
<th>Desired FW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td>HGST HUS724030ALA640</td>
<td>MF80AAC0</td>
<td></td>
</tr>
<tr>
<td>Bay 2</td>
<td>HGST HUS724030ALA640</td>
<td>MF80AAC0</td>
<td></td>
</tr>
<tr>
<td>Bay 3</td>
<td>HGST HUS724030ALA640</td>
<td>MF80AAC0</td>
<td></td>
</tr>
</tbody>
</table>

Where:
Drive
Displays the number of the bay that the drive is in.

Note
This column is not labeled in the output. The information appears under the node number.

Model
Displays the name of the drive model.

FW
Displays the version number of the firmware currently running on the drive.

Desired FW
Displays the version number of the drive firmware that the drive should be updated to. If a drive firmware update is not required, the Desired FW column is empty.

Automatic update of drive firmware
For clusters running OneFS 7.2 or later, install the latest drive support package on a node to automatically update the firmware for a new or replacement drive.

The information within the drive support package determines whether the firmware of a drive must be updated before the drive is formatted and used. If an update is available, the drive is automatically updated with the latest firmware.

Note
New and replacement drives added to a cluster are formatted regardless of the status of their firmware revision. You can identify a firmware update failure by viewing the firmware status for the drives on a specific node. In case of a failure, run the isi devices command with the fwupdate action on the node to update the firmware manually. For example, run the following command to manually update the firmware on node 1:

```bash
isi devices -a fwupdate -d 1
```
Managing cluster nodes

You can add and remove nodes from a cluster. You can also shut down or restart the entire cluster.

Add a node to a cluster

You can add a new node to an existing EMC Isilon cluster.

Before you begin

Before you add a node to a cluster, verify that an internal IP address is available. Add IP addresses as necessary before you add a new node.

If a new node is running a different version of OneFS than a cluster, the system changes the node version of OneFS to match the cluster.

Note

- For specific information about version compatibility between OneFS and EMC Isilon hardware, refer to the Isilon Supportability and Compatibility Guide.
- If you are running IsilonSD Edge, follow the instructions in the IsilonSD Edge Installation and Administration Guide to add a node to an IsilonSD cluster through the IsilonSD Management Plug-in.

Procedure

1. To identify the serial number of the node to be added, run the following command:
   ```
   isi devices node list
   ```

2. To join the node to the cluster, run the following command:
   ```
   isi devices node add <serial-number>
   ```
   For example, the following command joins a node to the cluster with a serial number of 43252:
   ```
   isi devices node add 43252
   ```

Remove a node from the cluster

You can remove a node from a cluster. When you remove a node, the system smartfails the node to ensure that data on the node is transferred to other nodes in the cluster.

Removing a storage node from a cluster deletes the data from that node. Before the system deletes the data, the FlexProtect job safely redistributes data across the nodes remaining in the cluster.

Procedure

1. Run the `isi devices` command.
The following command removes a node with a logical node number (LNN) of 2 from the cluster:

```bash
isi devices --action smartfail --device 2
```

**Note**

If you are running IsilonSD Edge, follow the instructions in the *IsilonSD Edge Installation and Administration Guide* to remove a node from the IsilonSD cluster.

### Modify the LNN of a node

You can modify the logical node number (LNN) of a node. This procedure is available only through the command-line interface (CLI).

The nodes within your cluster can be renamed to any name/integer between 1 and 144. By changing the name of your node, you are resetting the LNN.

**Note**

- Although you can specify any integer as an LNN, we recommend that you do not specify an integer greater than 144. Specifying LNNs above 144 can result in significant performance degradation.
- Ignore these instructions if you are running IsilonSD Edge because you cannot modify the LNN of an IsilonSD node.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Open the isi config command prompt by running the following command:

```bash
isi config
```
3. Run the `lnnset` command.

The following command switches the LNN of a node from 12 to 73:

```bash
lnnset 12 73
```
4. Enter `commit`.

**Results**

You might need to reconnect to your SSH session before the new node name is automatically changed.

### Restart or shut down the cluster

You can restart or shut down the EMC Isilon cluster.

**Procedure**

1. Run the `isi config` command.

   The command-line prompt changes to indicate that you are in the `isi config` subsystem.
2. Restart or shutdown nodes on the cluster.
   - To restart a single node or all nodes on the cluster, run the `reboot` command.
     
     The following command restarts a single node by specifying the LNN (logical node number):
     
     ```
     reboot 7
     ```
   - To shut down a single node or all nodes on the cluster, run the `shutdown` command.
     
     The following command shuts down all nodes on the cluster:
     
     ```
     shutdown all
     ```

### Upgrading OneFS

Two options are available for upgrading the OneFS operating system: a rolling upgrade or a simultaneous upgrade. Before upgrading OneFS software, a pre-upgrade check must be performed.

A rolling upgrade individually upgrades and restarts each node in the EMC Isilon cluster sequentially. During a rolling upgrade, the cluster remains online and continues serving clients with no interruption in service, although some connection resets may occur on SMB clients. Rolling upgrades are performed sequentially by node number, so a rolling upgrade takes longer to complete than a simultaneous upgrade. The final node in the upgrade process is the node that you used to start the upgrade process.

Note

Rolling upgrades are not available for all clusters. For instructions on how to plan an upgrade, prepare the cluster for upgrade, and perform an upgrade of the operating system, see the OneFS Upgrades – Isilon Info Hub

A simultaneous upgrade installs the new operating system and restarts all nodes in the cluster at the same time. Simultaneous upgrades are faster than rolling upgrades but require a temporary interruption of service during the upgrade process. Your data is inaccessible during the time that it takes to complete the upgrade process.

Before beginning either a simultaneous or rolling upgrade, OneFS compares the current cluster and operating system with the new version to ensure that the cluster meets certain criteria, such as configuration compatibility (SMB, LDAP, SmartPools), disk availability, and the absence of critical cluster events. If upgrading puts the cluster at risk, OneFS warns you, provides information about the risks, and prompts you to confirm whether to continue the upgrade.

If the cluster does not meet the pre-upgrade criteria, the upgrade does not proceed, and the unsupported statuses are listed.

Note

EMC Isilon Technical Support recommends that you run the optional pre-upgrade checks. Before starting an upgrade, OneFS checks that your cluster is healthy enough to complete the upgrade process. Some of the pre-upgrade checks are mandatory, and will be performed even if you choose to skip the optional checks. All pre-upgrade checks contribute to a safer upgrade.
Remote support

OneFS allows remote support through EMC Secure Remote Services (ESRS) which monitors your EMC Isilon cluster, and with your permission, allows remote access to Isilon Technical Support personnel to gather cluster data and troubleshoot issues.

ESRS is a secure, IP-based customer service support system. ESRS features include 24x7 remote monitoring and secure authentication with AES 256-bit encryption and RSA digital certificates.

When configured, ESRS monitors your Isilon cluster on a node-by-node basis and sends alerts regarding the health of your devices. Isilon Technical Support personnel can establish remote sessions through SSH or the web administration interface. During remote sessions, support personnel can run scripts that gather diagnostic data about cluster settings and operations, which is sent to a secure FTP site, and troubleshoot open support cases on your cluster.

If you enable remote support, you must share cluster login credentials with Isilon Technical Support personnel. Isilon Technical Support personnel will request remote access to your cluster only in the context of an open support case, and you can allow or deny the remote session request.

ESRS is included with the OneFS operating system and does not require you to activate a separate license. You must enable and configure ESRS before it can run scripts to gather data. The feature may have been enabled when the cluster was first set up, but you can enable or disable ESRS at any time.

For a complete description of ESRS features and functionality, see the most recent version of the document titled *EMC Secure Remote Services Technical Description*. Additional documentation about ESRS can be found on the EMC Online Support site.

Configuring ESRS support

You can configure support for EMC Secure Remote Services (ESRS) on your Isilon cluster.

Before configuring ESRS, at least one ESRS gateway server must be installed and configured. The gateway server acts as the single point of entry and exit for IP-based remote support activities and monitoring notifications. You can also set up a secondary gateway server as a failover.

ESRS does not support IPv6 communications. To support ESRS transmissions and remote connections, at least one subnet on the EMC Isilon cluster must be configured for IPv4 addresses. All nodes that you want managed by ESRS must have at least one network interface that is a member of an IPv4 address pool.

You must designate one or more IP address pools that will handle remote gateway connections by support personnel. The IP address pool must belong to a subnet under groupnet0, which is the default system groupnet and is referenced by the System access zone. We recommend that you designate pools with static IP addresses that are dedicated to remote connections through ESRS.

If ESRS transmissions fail, you can direct ESRS to send event notifications to a failover SMTP address. You can also specify whether an email should be sent upon transmission failure. The SMTP address and email address are specified in OneFS general cluster settings.

When you enable support for ESRS on a cluster, the serial number and IP address of each node is sent to the gateway server. Once node information is received, you can:
Select which nodes you want managed through ESRS with the ESRS Configuration Tool.

Create rules for remote support connections to Isilon nodes with the ESRS Policy Manager.

See the most recent version of the document titled *EMC Secure Remote Services Site Planning Guide* for a complete description the gateway server requirements, installation, and configuration.

See the most recent version of the document titled *EMC Secure Remote Services Installation and Operations Guide* for a complete description of the ESRS Configuration Tool.

See the most recent version of the document titled *EMC Secure Remote Services Policy Manager Operations Guide* for a complete description of the ESRS Policy Manger.

Additional documentation about ESRS can be found on the EMC Online Support site.

**Remote support scripts**

After you enable remote support through ESRS, Isilon Technical Support personnel can request logs with scripts that gather EMC Isilon cluster data and then upload the data.

The remote support scripts based on the Isilon isi_gather_info log-gathering tool are located in the /ifs/data/Isilon_Support/ directory on each node.

Additionally, isi_phone_home, a tool that focuses on cluster- and node-specific data, is enabled once you enable ESRS. This tool is pre-set to send information about your cluster to Isilon Technical Support on a weekly basis. You can disable or enable isi_phone_home from the OneFS command-line interface.

The following table lists the data-gathering activities that remote support scripts perform. At the request of an Isilon Technical Support representative, these scripts can be run automatically to collect information about your cluster's configuration settings and operations. ESRS then uploads the information to a secure Isilon FTP site, so that it is available for Isilon Technical Support personnel to analyze. The remote support scripts do not affect cluster services or the availability of your data.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean watch folder</td>
<td>Clears the contents of /var/crash.</td>
</tr>
<tr>
<td>Get application data</td>
<td>Collects and uploads information about OneFS application programs.</td>
</tr>
<tr>
<td>Generate dashboard file daily</td>
<td>Generates daily dashboard information.</td>
</tr>
<tr>
<td>Generate dashboard file sequence</td>
<td>Generates dashboard information in the sequence that it occurred.</td>
</tr>
<tr>
<td>Get ABR data (as built record)</td>
<td>Collects as-built information about hardware.</td>
</tr>
<tr>
<td>Get ATA control and GMirror status</td>
<td>Collects system output and invokes a script when it receives an event that corresponds to a predetermined eventid.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get cluster data</td>
<td>Collects and uploads information about overall cluster configuration and operations.</td>
</tr>
<tr>
<td>Get cluster events</td>
<td>Gets the output of existing critical events and uploads the information.</td>
</tr>
<tr>
<td>Get cluster status</td>
<td>Collects and uploads cluster status details.</td>
</tr>
<tr>
<td>Get contact info</td>
<td>Extracts contact information and uploads a text file that contains it.</td>
</tr>
<tr>
<td>Get contents (var/crash)</td>
<td>Uploads the contents of /var/crash.</td>
</tr>
<tr>
<td>Get job status</td>
<td>Collects and uploads details on a job that is being monitored.</td>
</tr>
<tr>
<td>Get domain data</td>
<td>Collects and uploads information about the cluster’s Active Directory Services (ADS) domain membership.</td>
</tr>
<tr>
<td>Get file system data</td>
<td>Collects and uploads information about the state and health of the OneFS / ifs/ file system.</td>
</tr>
<tr>
<td>Get IB data</td>
<td>Collects and uploads information about the configuration and operation of the InfiniBand back-end network.</td>
</tr>
<tr>
<td>Get logs data</td>
<td>Collects and uploads only the most recent cluster log information.</td>
</tr>
<tr>
<td>Get messages</td>
<td>Collects and uploads active /var/log/messages files.</td>
</tr>
<tr>
<td>Get network data</td>
<td>Collects and uploads information about cluster-wide and node-specific network configuration settings and operations.</td>
</tr>
<tr>
<td>Get NFS clients</td>
<td>Runs a command to check if nodes are being used as NFS clients.</td>
</tr>
<tr>
<td>Get node data</td>
<td>Collects and uploads node-specific configuration, status, and operational information.</td>
</tr>
<tr>
<td>Get protocol data</td>
<td>Collects and uploads network status information and configuration settings for the NFS, SMB, HDFS, FTP, and HTTP protocols.</td>
</tr>
<tr>
<td>Get Pcap client stats</td>
<td>Collects and uploads client statistics.</td>
</tr>
<tr>
<td>Get readonly status</td>
<td>Warns if the chassis is open and uploads a text file of the event information.</td>
</tr>
<tr>
<td>Get usage data</td>
<td>Collects and uploads current and historical information about node performance and resource usage.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>isi_gather_info</td>
<td>Collects and uploads all recent cluster log information.</td>
</tr>
<tr>
<td>isi_gather_info --incremental</td>
<td>Collects and uploads changes to cluster log information that have occurred since the most recent full operation.</td>
</tr>
<tr>
<td>isi_gather_info --incremental single node</td>
<td>Collects and uploads changes to cluster log information that have occurred since the most recent full operation. Prompts you for the node number.</td>
</tr>
<tr>
<td>isi_gather_info single node</td>
<td>Collects and uploads details for a single node. Prompts you for the node number.</td>
</tr>
<tr>
<td>isi_phone_home --script-file</td>
<td>Collects and uploads recent cluster- and node-specific information.</td>
</tr>
<tr>
<td>Upload the dashboard file</td>
<td>Uploads dashboard information to the secure Isilon Technical Support FTP site.</td>
</tr>
</tbody>
</table>

### Enable and configure ESRS support

You can enable support for EMC Secure Remote Services (ESRS) on an Isilon cluster.

**Before you begin**

You must install and configure an ESRS gateway server before you can enable ESRS on an Isilon cluster. The IP address pools that will handle gateway connections must already exist in the system and must belong to a subnet under groupnet0, which is the default system groupnet.

Ignore this procedure if you are running IsilonSD Edge.

**Procedure**

- Run the `isi remotesupport connectemc modify` command to enable and configure ESRS.

  The following command enables ESRS, specifies an IPv4 address as the primary gateway, directs OneFS to use SMTP if ESRS fails to transmit, and specifies two IP address pools to handle gateway connections:

  ```
  isi remotesupport connectemc modify --enabled=yes 
  --primary-esrs-gateway=192.0.2.1 --use-smtp-failover=yes 
  --gateway-access-pools=subnet0.pool2,subnet3.pool1
  ```

  The following command enables ESRS, specifies gw-serv-esrs1 as the primary gateway server, and adds an IP address pool to the list of pools that handle gateway connections:

  ```
  isi remotesupport connectemc modify --enabled=yes 
  --primary-esrs-gateway=gw-serv-esrs1 --add-gateway-access-pools=subnet0.pool3
  ```
Disable ESRS support

You can disable support for EMC Secure Remote Services (ESRS) on the Isilon cluster.

Ignore this procedure if you are running IsilonSD Edge.

Procedure

- Disable ESRS on an Isilon cluster by running the following command:

  ```
  isi remotesupport connectemc modify --enabled=no
  ```

View ESRS configuration settings

You can view EMC Secure Remote Services (ESRS) settings specified on an EMC Isilon cluster.

Ignore this procedure if you are running IsilonSD Edge.

Procedure

- Run the `isi remotesupport connectemc view` command.

  The system displays output similar to the following example:

  ```
  Enabled: yes
  Primary Esrs Gateway: 198.51.100.12
  Secondary Esrs Gateway: 198.51.100.14
  Use SMTP Failover: yes
  Email Customer On Failure: no
  Gateway Access Pools: subnet0.pool2, subnet3.pool1
  ```

Cluster administration commands

You can configure, monitor, and manage the Isilon cluster using cluster administration commands.

If you are running IsilonSD Edge, the commands specific to security hardening, remote support, upgrading cluster firmware, and adding new or remaining nodes to a running upgrade process, do not apply.

**isi config**

Opens a new prompt where node and cluster settings can be altered.

The command-line prompt changes to indicate that you are in the `isi config` subsystem. While you are in the `isi config` subsystem, other OneFS commands are unavailable and only `isi config` commands are valid.

**Syntax**

```
isi config
```
Note

- The following commands are not recognized unless you are currently at the isi config command prompt.
- Changes are not applied until you run the commit command.
- Some commands require you to restart the cluster.

Commands

changes
Displays a list of changes to the configuration that have not been committed.

commit
Commits configuration settings and then exits isi config.

date <time-and-date>
Displays or sets the current date and time on the cluster.

<time-and-date>
Sets cluster time to the time specified.
Specify <time-and-date> in the following format:

<YYYY>-<MM>-<DD>[T<hh>:<mm>[:<ss>]]

Specify <time> as one of the following values.

Y
  Specifies years

M
  Specifies months

W
  Specifies weeks

D
  Specifies days

h
  Specifies hours

s
  Specifies seconds

deliprange [ <interface-name> [ <ip-range> ] ]
Displays a list of internal network IP addresses that can be assigned to nodes or removes specified addresses from the list.

<interface-name>
  Specifies the name of the interface as one of the following values:
  int-a
failover

Specifies the range of IP addresses that can no longer be assigned to nodes. Specify in the form `<lowest-ip>-<highest-ip>`.

encoding [list] [encoding]

Sets the default encoding character set for the cluster.

CAUTION

Character encoding is typically established during installation of the cluster. Incorrectly modifying character encoding settings may render files unreadable. Modify settings only if necessary and after consultation with Isilon Technical Support.

list

Displays the list of supported character sets.

exit

Exits the `isi config` subsystem.

help

Displays a list of all `isi config` commands. For information about specific commands, the syntax is `help [<command>]`.

interface <interface-name>{enable | disable}

The interface command displays the IP ranges, netmask, and MTU and enables or disables internal interfaces. When issued with no argument, this command displays IP ranges, netmask, and MTU of all interfaces. When issued with an `<interface-name>` argument, this command displays IP ranges, netmask, and MTU for only the specified interface.

{enable | disable}

Enables or disables the specified interface.

<interface-name>

 Specifies the name of the interface as `int-a` or `int-b`.

iprange [<interface-name> [<lowest-ip>-<highest-ip>]]

Displays a list of internal IP addresses that can be assigned to nodes, or adds addresses to the list.

<interface-name>

 Specifies the name of the interface as `int-a`, `int-b`, or `failover`.

<lowest-ip>-<highest-ip>

Specifies the range of IP addresses that can be assigned to nodes.
Obsolete. Use `lnnset` to renumber cluster nodes. The IP address cannot be set manually.

`joinmode [mode]`
Displays the setting for how nodes are added to the current cluster. Options `mode` specifies the cluster add node setting as one of the following values.

- `manual`  
  Configures the cluster so that joins can be initiated by either the node or the cluster.

- `secure`  
  Configures the cluster so that joins can be initiated by only the cluster.

`lnnset [old-lnn new-lnn]`
Displays a table of logical node number (LNN), device ID, and internal IP address for each node in the cluster when run without arguments. Changes the LNN when specified.

- `<old-lnn>`  
  Specifies the old LNN that is to be changed.

- `<new-lnn>`  
  Specifies the new LNN that is replacing the old LNN value for that node.

**Note**

The new LNN must not be currently assigned to another node. Users logged in to the shell or web administration interface of a node whose LNN is changed must log in again to view the new LNN.

`migrate [interface-name] [old-range] [new-range] [-n netmask]`
Displays a list of IP address ranges that can be assigned to nodes or both adds and removes IP ranges from that list.

- `<interface-name>`  
  Specifies the name of the interface as `int-a`, `int-b`, and `failover`.

- `<old-range>`  
  Specifies the range of IP addresses that can no longer be assigned to nodes. If unspecified, all existing IP ranges are removed before the new IP range is added. Specify in the form of `<lowest-ip>-<highest-ip>`.

- `<new-range>`  
  Specifies the range of IP addresses that can be assigned to nodes. Specify in the form of `<lowest-ip>-<highest-ip>`.

- `-n netmask`  
  Specifies a new netmask for the interface.
Note
If more than one node is given a new IP address, the cluster reboots when the change is committed. If only one node is given a new IP address, only that node is rebooted.

mtu [<value>]
Displays the size of the maximum transmission unit (MTU) that the cluster uses for internal network communications when run with no arguments. Sets a new size of the MTU value, when specified. This command is for the internal network only.

Note
This command is not valid for clusters with an InfiniBand back end.

<value>
Specifies the new size of the MTU value. Any value is valid, but not all values may be compatible with your network. The most common settings are 1500 for standard frames and 9000 for jumbo frames.

name [<new_name>]
Displays the names currently assigned to clusters when run with no arguments. Assigns new names to clusters, as specified.

<new name>
Specifies a new name for the cluster.

netmask [<interface-name> [ <ip-mask> ]]
Displays the subnet IP mask that the cluster is currently using or sets new subnet IP masks, as specified. Specifies the interface name as int-a and int-b.

<interface-name>
Specifies the name of the interface. Valid names are int-a and int-b.

<ip-mask>
Specifies the new IP mask for the interface.

quit
Exits the isi config subsystem.

reboot [{<node_lnn> | all}]
Reboots one or more nodes, specified by LNN. If no nodes are specified, reboots the node from which the command is run. To reboot the cluster, specify all.

Note
If run on an unconfigured node, this command does not accept any arguments.

remove
Deprecated. Instead, run the isi devices -a smartfail command.

shutdown [{<node_lnn> | all}]

Shuts down one or more nodes, specified by LNN. If no nodes are specified, shuts down the node from which the command is run. To shut down the cluster, specify all.

**Note**

If run on an unconfigured node, this command does not accept any arguments.

`status [advanced]`

Displays current information on the status of the cluster. To display additional information, including device health, specify `advanced`.

`timezone [<timezone identifier>]`

Displays the current time zone or specifies new time zones. Specifies the new timezone for the cluster as one of the following values:

- Greenwich Mean Time
- Eastern Time Zone
- Central Time Zone
- Mountain Time Zone
- Pacific Time Zone
- Arizona
- Alaska
- Hawaii
- Japan

Advanced. Opens a prompt with more time zone options.

`version`

Displays information about the current OneFS version.

`wizard`

Activates a wizard on unconfigured nodes and reactivates the wizard if you exit it during the initial node configuration process. The wizard prompts you through the node-configuration steps.

**isi email settings modify**

Modify email settings for the cluster.

**Syntax**

```
isi email settings modify
[--mail-relay <string>]
[--smtp-port <integer>]
[--mail-sender <string>]
[--mail-subject <string>]
[--use-smtp-auth {yes | no}]
```
Options

--mail-relay <string>
  Sets the SMTP relay address.

--smtp-port <integer>
  Sets the SMTP port. The default is 25.

--mail-sender <string>
  Sets the originator email address.

mail-subject <string>
  Set the prefix string for the email subject.

--use-smtp-auth {yes | no}
  Use SMTP authentication.

{--smtp-auth-username | -u} <string>
  Sets the SMTP user name.

--use-encryption {yes | no}
  Use encryption (TLS) for SMTP authentication.

--batch-mode {all | severity | category | none}
  Sets the method that notifications are batched together to be sent by email.

--user-template <string>
  Specifies the path to access a custom email template.

--clear-user-template
  Clears the path specified to access a custom email template.

{--smtp-auth-passwd | -p} <string>
  Sets the SMTP authentication password.

--clear-smtp-auth-passwd
  Clears the specified SMTP authentication password.

--set-smtp-auth-passwd
  Specifies --smtp-auth-passwd interactively.

{--verbose | -v}
  Displays more detailed information.
isi email settings view

View cluster email settings.

Syntax

```bash
isi email settings view
```

Example

To view the currently-configured email settings, run the following command:

```bash
isi email settings view
```

The system displays output similar to the following example:

```plaintext
Mail Relay: -
SMTP Port: 25
Mail Sender: -
Mail Subject: -
Use SMTP Auth: No
SMTP Auth Username: -
Use Encryption: No
Batch Mode: none
User Template: -
SMTP Auth Password Set: False
```

isi hardening apply

Applies security hardening to the EMC Isilon cluster.

Syntax

```bash
isi hardening apply <profile> [--report {yes | no}] [--verbose]
```

Options

 `<profile>`

Specifies the hardening profile that will be applied to the Isilon cluster. Currently, OneFS supports only the DISA (Defense Information Systems Agency) STIG (Security Technology Implementation Guide) profile for security hardening on the cluster.

`--report {yes | no}`

Specifies whether to check the state of the Isilon cluster and report the results without actually applying the hardening profile. The system displays any issues it finds, which can be resolved by the hardening engine or deferred to be fixed manually.

`{--verbose | -v}`

Displays more detailed information.
isi hardening revert

Reverts all security hardening that has been applied to the EMC Isilon cluster.

Syntax

```
isi hardening revert
[--verbose]
[--force]
```

Options

|--verbose | -v  
  Displays more detailed information.

|--force | -f  
  Suppresses command-line prompts and messages to revert hardening.

isi hardening status

Displays the status of security hardening for the EMC Isilon cluster and each cluster node, and indicates the hardening profile applied to the cluster.

Syntax

```
isi hardening status
```

Options

There are no options for this command.

isi license licenses activate

Activate a new licensable product by entering a license key.

Syntax

```
isi license licenses activate <key>
[--verbose]
```

Options

|--verbose | -v  
  License key.

Displays more detailed information.
isi license licenses list

Retrieve license information for all licensable products.

Syntax

```
isi license licenses list
    [--limit <integer>]
    [--sort {name | status | expiration}]
    [--descending]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

```
{--limit | -l} <integer>
    The number of licenses to display.

--sort {name | status | expiration}
    Sort data by the specified field.

{--descending | -d}
    Sort data in descending order.

--format {table | json | csv | list}
    Display licenses in table, JSON, CSV, or list format.

{--no-header | -a}
    Do not display headers in table or CSV formats.

{--no-footer | -z}
    Do not display table summary footer information.

{--verbose | -v}
    Displays more detailed information.
```

isi license licenses view

Retrieve license information for any licensable product.

Syntax

```
isi license licenses view <name>
```

Options

```
<name>
    Product name for the license to view.
```
Example
To view the license information for SmartQuotas, run the following command:

`isi email settings view SmartQuotas`

The system displays output similar to the following example:

```
Name: SmartQuotas
Status: Evaluation
Expiration: 2016-10-04T14:08:26
```

**isi remotesupport connectemc modify**

Enables or disables support for EMC Secure Remote Services (ESRS) on an Isilon node.

**Syntax**

```
isi remotesupport connectemc modify
[--enabled {yes|no}]
[--primary-esrs-gateway <string>]
[--secondary-esrs-gateway <string>]
[--use-smtp-failover {yes|no}]
[--email-customer-on-failure {yes|no}]
[--gateway-access-pools <string>]
[--clear-gateway-access-pools]
[--add-gateway-access-pools <string>]
[--remove-gateway-access-pools <string>]
```

**Options**

**--enabled {yes|no}**

Specifies whether support ESRS is enabled on the Isilon cluster.

**--primary-esrs-gateway <string>**

Specifies the primary ESRS gateway server. The gateway server acts as the single point of entry and exit for IP-based remote support activities and monitoring notifications. You can specify the gateway as an IPv4 address or the gateway name.

**--secondary-esrs-gateway <string>**

Specifies an optional secondary ESRS gateway server that acts as a failover server. You can specify the gateway as an IPv4 address or the gateway name.

**--use-smtp-failover {yes|no}**

Specifies whether to send event notifications to a failover SMTP address upon ESRS transmission failure. The SMTP email address is specified through the `isi email settings modify` command.

**--email-customer-on-failure {yes|no}**

Specifies whether to send an alert to a customer email address upon failure of other notification methods. The customer email address is specified through the `isi_promptesrs -e` command.

**--gateway-access-pools <string>**
Specifies the IP address pools on the Isilon cluster that will handle remote support connections through the ESRS gateway. The IP address pools must belong to a subnet under `groupnet0`, which is the default system groupnet.

**Note**
We recommend that you designate pools with static IP addresses that are dedicated to remote connections through ESRS.

```
--clear-gateway-access-pools
```
Deletes the list of IP address pools that handle remote support connections.

```
--add-gateway-access-pools <string>...  
```
Adds one or more IP address pools to the list of pools that will handle remote support connections through the ESRS gateway.

```
--remove-gateway-access-pools <string>...  
```
Deletes one or more IP address pools from the list of pools that will handle remote support connections through the ESRS gateway.

**Examples**
The following command enables ESRS, specifies an IPv4 address as the primary gateway, directs OneFS to email the customer if all transmission methods fail, and removes an IP address pool from the list of pools that handle gateway connections:

```
isi remotesupport connectemc modify --enabled=yes \  
--primary-esrs-gateway=192.0.2.1 --email-customer-on-failure=yes \  
--remove-gateway-access-pools=subnet3.pool1
```

**isi remotesupport connectemc view**
Displays EMC Secure Remote Services (ESRS) settings on an Isilon node.

**Syntax**
```
isi remotesupport connectemc view
```

**Options**
This command has no options.

**isi services**
Displays a list of available services. The `-l` and `-a` options can be used separately or together.

**Syntax**
```
isi services  
[-l | -a]  
[<service> [{enable | disable}]]]
```
Options

-l
Lists all available services and the current status of each. This is the default value for this command.

-a
Lists all services, including hidden services, and the current status of each.

<service>{enable|disable}
Enables or disables the specified service.

Examples
The following example shows the command to enable a specified hidden service.

isi services -a <hidden-service> enable

isi set

Works similar to chmod, providing a mechanism to adjust OneFS-specific file attributes, such as the requested protection, or to explicitly restripe files. Files can be specified by path or LIN.

Syntax

isi set
[-f -F -L -n -v -r -R]
[-p <policy>]
[-w <width>]
[-c (on | off)]
[-g <restripe_goal>]
[-e <encoding>]
[-d <@r drives>]
[-a {<default> | <streaming> | <random> | <custom{1..5}> | <disabled>}]]
[-l {<concurrency> | <streaming> | <random>}]]
[--diskpool {<id> | <name>}]]
[-s (on | off)]
[-p (on | off)]
[{--strategy | -s} {<avoid> | <metadata> | <metadata-write> | <data>}
[<file> {<path> | <lin>}]

Options

-f
Suppresses warnings on failures to change a file.

-F
Includes the /ifs/.ifsvar directory content and any of its subdirectories. Without -F, the /ifs/.ifsvar directory content and any of its subdirectories are skipped. This setting allows the specification of potentially dangerous, unsupported protection policies.

-L
Specifies file arguments by LIN instead of path.

-n
Displays the list of files that would be changed without taking any action.

-v
Displays each file as it is reached.

-r
Runs a restripe.

-R
Sets protection recursively on files.

-p <policy>
Specifies protection policies in the following forms:
+M
Where M is the number of node failures that can be tolerated without loss of data. +M must be a number from, where numbers 1 through 4 are valid.

+D:M
Where D indicates the number of drive failures and M indicates number of node failures that can be tolerated without loss of data. D must be a number from 1 through 4 and M must be any value that divides into D evenly. For example, +2:2 and +4:2 are valid, but +1:2 and +3:2 are not.

Nx
Where N is the number of independent mirrored copies of the data that will be stored. N must be a number, with 1 through 8 being valid choices.

-w <width>
Specifies the number of nodes across which a file is striped. Typically, w = N + M, but width can also mean the total of the number of nodes that are used.
You can set a maximum width policy of 32, but the actual protection is still subject to the limitations on N and M.

-c {on | off}
Specifies whether write-coalescing is turned on.

-g <restripe goal>
Specifies the restripe goal. The following values are valid:
repair
reprotect
rebalance
retune

-e <encoding>
Specifies the encoding of the filename. The following values are valid:

- EUC-JP
- EUC-JP-MS
- EUC-KR
- ISO-8859-1
- ISO-8859-10
- ISO-8859-13
- ISO-8859-14
- ISO-8859-15
- ISO-8859-160
- ISO-8859-2
- ISO-8859-3
- ISO-8859-4
- ISO-8859-5
- ISO-8859-6
- ISO-8859-7
- ISO-8859-8
- ISO-8859-9
- UTF-8
- UTF-8-MAC
- Windows-1252
- Windows-949
- Windows-SJIS

\(-d \text{ <@r drives>}\)

Specifies the minimum number of drives that the file is spread across.

\(-a \text{ <value>}\)

Specifies the file access pattern optimization setting. The following values are valid:

- default
- streaming
- random
- custom1
- custom2
- custom3
- custom4
- custom5
- disabled

\(-l \text{ <value>}\)
Specifies the file layout optimization setting. This is equivalent to setting both the
-a and -d flags.

- concurrency
- streaming
- random

--diskpool <id | name>
Sets the preferred diskpool for a file.

-A {on | off}
Specifies whether file access and protections settings should be managed
manually.

-P {on | off}
Specifies whether the file inherits values from the applicable file pool policy.

{--strategy | -s} <value>
Sets the SSD strategy for a file. The following values are valid:

If the value is metadata-write, all copies of the file's metadata are laid out on SSD
storage if possible, and user data still avoids SSDs. If the value is data, Both the
file's meta-data and user data (one copy if using mirrored protection, all blocks if
FEC) are laid out on SSD storage if possible.

avoid
Writes all associated file data and metadata to HDDs only. The data and
metadata of the file are stored so that SSD storage is avoided, unless doing
so would result in an out-of-space condition.

metadata
Writes both file data and metadata to HDDs. One mirror of the metadata for
the file is on SSD storage if possible, but the strategy for data is to avoid
SSD storage.

metadata-write
Writes file data to HDDs and metadata to SSDs, when available. All copies of
metadata for the file are on SSD storage if possible, and the strategy for data
is to avoid SSD storage.

data
Uses SSD node pools for both data and metadata. Both the metadata for the
file and user data, one copy if using mirrored protection and all blocks if FEC,
are on SSD storage if possible.

<file> {<path> | <lin>}
Specifies a file by path or LIN.
isi snmp settings modify

Modify SNMP settings for a cluster.

Syntax

```bash
isi snmp settings modify
  [--service {yes | no}]
  [--system-location <string>]
  [--revert-system-location]
  [--system-contact <string>]
  [--revert-system-contact]
  [--snmp-v1-v2c-access {yes | no}]
  [--revert-snmp-v1-v2c-access]
  [--read-only-community <string>]
  [--revert-read-only-community]
  [--snmp-v3-access {yes | no}]
  [--revert-snmp-v3-access]
  [--snmp-v3-read-only-user <string>]
  [--revert-snmp-v3-read-only-user]
  [--snmp-v3-password <string>]
  [--revert-snmp-v3-password]
  [--set-snmp-v3-password]
  [--verbose]
```

Options

---service {yes | no}
Enables or disables the SNMP service.

---system-location <string>
The location of the SNMP system.

--revert-system-location
Sets --system-location to the system default.

---system-contact <string>
A valid email address for the system owner.

--revert-system-contact
Sets --system-contact to the system default.

---snmp-v1-v2c-access {yes | no}
Enables or disables the SNMP v1 and v2c protocols.

--revert-snmp-v1-v2c-access
Sets --snmp-v1-v2c-access to the system default.

{--read-only-community | -c} <string>
The name of the read-only community.

--revert-read-only-community
Sets --read-only-community to the system default.

---snmp-v3-access {yes | no}
Enables or disables SNMP v3.

--revert-snmp-v3-access
Sets --snmp-v3-access to the system default.

{--snmp-v3-read-only-user | -u} <string>
The read-only user for SNMP v3 read requests.

--revert-snmp-v3-read-only-user
Sets --snmp-v3-read-only-user to the system default.

{--snmp-v3-password | -p} <string>
Modify the SNMP v3 password.

--revert-snmp-v3-password
Sets --snmp-v3-password to the system default.

--set-snmp-v3-password
Specify --snmp-v3-password interactively.

**isi snmp settings view**

View SNMP settings for the cluster.

**Syntax**

```
isi snmp settings view
```

**Example**

To view the currently-configured SNMP settings, run the following command:

```
isi snmp settings view
```

The system displays output similar to the following example:

```
System Location: unset
System Contact: unset@unset.invalid
Snmp V1 V2C Access: Yes
Read Only Community: I$ilonpublic
Snmp V3 Access: No
Snmp V3 Read Only User: general
SNMP Service Enabled: No
```

**isi statistics client**

Displays the most active, by throughput, clients accessing the cluster for each supported protocol. You can specify options to track access by user, for example, more than one user on the same client host access the cluster.

**Syntax**

```
isi statistics client
    [--numeric]
    [--local-addresses <string>]
    [--local-names <string>]
    [--remote-addresses <integer>]
    [--remote-names <string>]
    [--user-ids <integer>]
```
Options

--numeric
If text identifiers of local hosts, remote clients, or users are in the list of columns
to display (the default setting is for them to be displayed), display the unresolved
numeric equivalent of these columns.

--local-addresses <string>
Specifies local IP addresses for which statistics will be reported.

--local-names <string>
Specifies local host names for which statistics will be reported.

--remote-addresses <string>
Specifies remote IP addresses for which statistics will be reported.

--remote-names <string>
Specifies remote client names for which statistics will be reported.

--user-ids <string>
Specifies user ids for which statistics will be reported. The default setting is all
users.

--user-names <string>
Specifies user names for which statistics will be reported. The default setting is all
users.

--protocols <value>
Specifies which protocols to report statistics on. Multiple values can be specified
in a comma-separated list, for example --protocols http,papi. The
following values are valid:

- all
- external
- ftp
- hdfs
- http
- internal
irp
jobd
lsass_in
lsass_out
nlm
nfs3
nfs4
papi
siq
smb1
smb2

--classes <string>
Specify which operation classes to report statistics on. The default setting is all classes. The following values are valid:

other
File-system information for other uncategorized operations
write
File and stream writing
read
File and stream reading
namespace_read
Attribute stat and ACL reads; lookup directory reading
namespace_write
Renames; attribute setting; permission time and ACL writes

{--nodes | -n} <node>
Specifies which nodes to report statistics on. Multiple values can be specified in a comma-separated list, for example, --nodes 1,2. The default value is all. The following values are valid:

all

{--degraded | -d}
Causes the report to continue if some nodes do not respond.

--nohumanize
Displays all data in base quantities, without dynamic conversion. If set, this option also disables the display of units within the data table.

{--interval | -i}<float>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.
Note

To run the report to run indefinitely, specify -1.

```
{--limit | -l} <integer>
  Limits the number of statistics to display.

--long
  Displays all possible columns.

--totalby <column>
  Aggregates results according to specified fields. The following values are valid:
  * Node
  * {Proto | protocol}
  * Class
  * {UserId | user.id}
  * {UserName | user.name}
  * {LocalAddr | local_addr}
  * {LocalName | local_name}
  * {RemoteAddr | remote_addr}
  * {RemoteName | remote_name}

--output <column>
  Specifies which columns to display. The following values are valid:
  * {NumOps | num_operations}
    Displays the number of times an operation has been performed.
  * {Ops | operation_rate}
    Displays the rate at which an operation has been performed. Displayed in operations per second.
  * {InMax | in_max}
    Displays the maximum input (received) bytes for an operation.
  * {InMin | in_min}
    Displays the minimum input (received) bytes for an operation.
  * In
    Displays the rate of input for an operation since the last time isi statistics collected the data. Displayed in bytes per second.
  * {InAvg | in_avg}
    Displays the average input (received) bytes for an operation.
  * {OutMax | out_max}
    Displays the maximum output (sent) bytes for an operation.
  * {OutMin | out_min}
    Displays the minimum output (sent) bytes for an operation.
```
Out
Displays the rate of output for an operation since the last time isi
statistics collected the data. Displayed in bytes per second.

{OutAvg | out_avg}
Displays the average output (sent) bytes for an operation.

{TimeMax | time_max}
Displays the maximum elapsed time taken to complete an operation.
Displayed in microseconds.

{TimeMin | time_min}
Displays the minimum elapsed time taken to complete an operation.
Displayed in microseconds.

{TimeAvg | time_avg}
Displays the average elapsed time taken to complete an operation. Displayed
in microseconds.

Node
Displays the node on which the operation was performed.

{Proto | protocol}
Displays the protocol of the operation.

Class
Displays the class of the operation.

{UserID | user.id}
Displays the numeric UID of the user issuing the operation request.

{UserName | user.name}
Displays the resolved text name of the UserID. If resolution cannot be
performed, UNKNOWN is displayed.

{LocalAddr | local_addr}
Displays the local IP address of the user issuing the operation request.

{LocalName | local_name}
Displays the local host name of the user issuing the operation request.

{RemoteAddr | remote_addr}
Displays the remote IP address of the user issuing the operation request.

{RemoteName | remote_name}
Displays the remote client name of the user issuing the operation request.

--sort <column>
Specifies how rows are ordered. The following values are valid:

- {NumOps | num_operations}
- {Ops | operation_rate}
- {InMax | in_max}
- {InMin | in_min}
• In
  • {InAvg | in_avg}
  • {OutMax | out_max}
  • {OutMin | out_min}
• Out
  • {OutAvg | out_avg}
  • {TimeMax | time_max}
  • {TimeMin | time_min}
  • {TimeAvg | time_avg}
• Node
  • {Proto | protocol}
• Class
  • {UserID | user.id}
  • {UserName | user.name}
  • {LocalAddr | local_addr}
  • {LocalName | local_name}
  • {RemoteAddr | remote_addr}
  • {RemoteName | remote_name}

```bash
--format {table | json | csv | list | top}
```
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

---

**Note**

If you specify `--top` without `--repeat`, the report runs indefinitely.

```bash
{--noheader | -a}
```
Displays data without column headings.

```bash
{--no-footer | -z}
```
Displays data without footers.

```bash
{--verbose | -v}
```
Displays more detailed information.

## isi statistics drive

Displays performance information by drive.

**Syntax**

```bash
isi statistics drive
[--type <value>]
[--nodes <value>]
[--degraded]
```
Options

--type <string>
Specifies the drive types for which statistics will be reported. The default setting is all drives. The following values are valid:

- sata
- sas
- ssd

{ --nodes | -n} <node>
Specifies which nodes to report statistics on. Multiple values can be specified in a comma-separated list, for example, --nodes 1,2. The default value is all. The following values are valid:

- all
- <int>

{--degraded | -d}
Sets the report to continue running if some nodes do not respond.

--nohumanize
Displays all data in base quantities, without dynamic conversion. If set, this parameter also disables the display of units within the data table.

{--interval | -I} <integer>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.

Note
To set the report to run indefinitely, specify -1.

{--limit | -l} <integer>
Limits the number of statistics to display.

--long
Displays all possible columns.

--output <column>
Specifies which columns to display. The following values are valid:
--sort <column>
Specifies how the rows are ordered. The following values are valid:

- {Timestamp | time}
- {Drive | drive_id}
- {Type | }
- {BytesIn | bytes_in}
- {SizeIn | xfer_size_in}
- {OpsOut | xfers_out}
- {BytesOut | bytes_out}
- {SizeOut | xfer_size_out}
- {TimeAvg | access_latency}
- {Slow | access_slow}
- {TimeInQ | iosched_latency}
- {Queued | iosched_queue}
- {Busy | used_bytes_percent}
- {Inodes | used_inodes}

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

Note
If you specify --top without --repeat, the report runs indefinitely.

{--noheader | -a}
Displays data without column headings.

\{ --no-footer \ | -z \}

Displays data without footers.

\{--verbose \ | -v\}

Displays more detailed information.

isi statistics heat

Displays the most active /ifs paths for various metrics.

Syntax

```
isi statistics heat
   [ --events <string> ]
   [ --pathdepth <integer> ]
   [ --maxpath <integer> ]
   [ --classes <string> ]
   [ --numeric ]
   [ --nodes <value> ]
   [ --degraded ]
   [ --nohumanize ]
   [ --interval <integer> ]
   [ --repeat <integer> ]
   [ --limit <integer> ]
   [ --long ]
   [ --totalby <column> ]
   [ --output <column> ]
   [ --sort <column> ]
   [ --format ]
   [ --no-header ]
   [ --no-footer ]
   [ --verbose ]
```

Options

--events <string>

Specifies which event types for the specified information are reported. The following values are valid:

blocked

Access to the LIN was blocked waiting for a resource to be released by another operation. Class is other.

contended

A LIN is experiencing cross-node contention; it is being accessed simultaneously through multiple nodes. Class is other.

deadlocked

The attempt to lock the LIN resulted in deadlock. Class is other.

getattr

A file or directory attribute has been read. Class is namespace_read.

link

The LIN has been linked into the file system; the LIN associated with this event is the parent directory and not the linked LIN. Class is namespace_write.
lock
   The LIN is locked. Class is other.

lookup
   A name is looked up in a directory; the LIN for the directory searched is the
   one associated with the event. Class is namespace_read.

read
   A read was performed. Class is read.

rename
   A file or directory was renamed. The LIN associated with this event is the
   directory where the rename took place for either the source directory or the
   destination directory, if they differ. Class is namespace_write.

setattr
   A file or directory attribute has been added, modified, or deleted. Class is
   namespace_write.

unlink
   A file or directory has been unlinked from the file system, the LIN associated
   with this event is the parent directory of the removed item. Class is
   namespace_write.

write
   A write was performed. Class is write.

-pathdepth <integer>
   Reduces paths to the specified depth.

--maxpath <integer>
   Specifies the maximum path length to look up in the file system.

--classes <string>
   Specifies which classes for the specified information will be reported. The default
   setting is all classes. The following values are valid:

   write
      File and stream writing

   read
      File and stream reading

   namespace_write
      Renames; attribute setting; permission, time, and ACL writes

   namespace_read
      Attribute, stat, and ACL reads; lookup, directory reading

   other
      File-system information

   --numeric
If text identifiers of local hosts, remote clients, or users are in the list of columns to display (the default setting is for them to be displayed), display the unresolved numeric equivalent of these columns.

{ --nodes | -n} <value>
Specifies which nodes to report statistics on. Multiple values can be specified in a comma-separated list—for example, --nodes 1,2. The default value is all. The following values are valid:
- all
- <int>

{--degraded | -d}
Sets the report to continue running if some nodes do not respond.

--nohumanize
Displays all data in base quantities, without dynamic conversion. If set, this option also disables the display of units within the data table.

{--interval | -I} <integer>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.

Note
To set the report to run indefinitely, specify -1.

--limit <integer>
Displays only the specified number of entries after totaling and ordering.

--long
Displays all possible columns.

--totalby <column>
Aggregates results according to specified fields. The following values are valid:
- Node
- {Event | event_name}
- {Class | class_name}
- LIN
- Path

--output <column>
Specifies the columns to display. The following values are valid:

{Ops | operation_rate}
Displays the rate at which an operation has been performed. Displayed in operations per second.

Node
Displays the node on which the operation was performed.
Event | event_name
Displays the name of the event.

Class | class_name
Displays the class of the operation.

LIN
Displays the LIN for the file or directory associated with the event.

Path
Displays the path associated with the event LIN.

--sort <column>
Specifies how rows are ordered. The following values are valid:
- {Ops | operation_rate}
- Node
- {Event | event_name}
- {Class | class_name}
- LIN
- Path

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

Note
If you specify --top without --repeat, the report runs indefinitely.

--noheader | -a
Displays data without column headings.

--no-footer | -z
Displays data without footers.

--verbose | -v
Displays more detailed information.

isi statistics query current
Displays current statistics.

Syntax

isi statistics query current
[--keys <string>]
[--substr]
[--raw]
[--nodes <value>]
[--degraded]
[--interval <number>]
Options

--keys <string>...
Specify which statistics should be reported for requested nodes, where the value for <string> is a statistics key. Use the isi statistics list keys command for a complete listing of statistics keys.

--substr
Matches the statistics for '.*<key>.*' for every key specified with --keys.

--raw
Outputs complex objects as hex.

{--nodes | -n} <node>
Specify which nodes to report statistics on. Multiple values can be specified in a comma-separated list, for example, --nodes 1,2. The default value is all. The following values are valid:
- all
- <int>

{--degraded | -d}
Sets the report to continue running if some nodes do not respond.

{--interval | -i} <float>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.

Note
To set the report to run indefinitely, specify -1.

{--limit | -l} <integer>
Limits the number of statistics to display.

--long
Displays all possible columns.

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.
Note
If you specify --top without --repeat, the report runs indefinitely.

|--noheader | -a
    Displays data without column headings.

|--no-footer | -z
    Displays data without footers.

|--verbose | -v
    Displays more detailed information.

isi statistics query history
Displays available historical statistics. Not all statistics are configured to support a historical query.

Syntax

isi statistics query history
    |--keys <string>
    |--substr
    |--begin <integer>
    |--end <integer>
    |--resolution <number>
    |--memory-only
    |--raw
    |--nodes <value>
    |--degraded
    |--nohumanize
    |--interval <number>
    |--repeat <number>
    |--limit
    |--format
    |--no-header
    |--no-footer
    |--verbose

Options

|--keys <string>...
    Specifies which statistics should be reported for requested nodes, where the value for <string> is a statistics key. Use the isi statistics list keys command for a complete listing of statistics keys.

|--substr
    Matches the statistics for ‘.*<key>.*’ for every key specified with --keys.

|--begin <time>
    Specifies begin time in UNIX Epoch timestamp format.

|--end <time>
    Specifies end time in UNIX Epoch timestamp format.

|--resolution <integer>
    Specifies the minimum interval between series data points in seconds.
--memory-only
Retrieves only the statistics in memory, not those persisted to disk.

--raw
Outputs complex objects as hex.

{ --nodes | -n} <node>
Specifies which nodes to report statistics on. Multiple values can be specified in a comma-separated list, for example, --nodes 1,2. The default value is all. The following values are valid:
• all
• <int>

{--degraded | -d}
Sets the report to continue running if some nodes do not respond.

--nohumanize
Displays all data in base quantities, without dynamic conversion. If set, this option also disables the display of units within the data table.

{--interval | -i} <float>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.

Note
To set the report to run indefinitely, specify -1.

{--limit | -l} <integer>
Limits the number of statistics to display.

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

Note
If you specify --top without --repeat, the report runs indefinitely.

{--noheader | -a}
Displays data without column headings.

{--no-footer | -z}
Displays data without footers.

{--verbose | -v}
Displays more detailed information.
isi statistics list keys

Displays a list of all available keys.

Syntax

```
isi statistics list operations
 [--limit]
 [--format]
 [--no-header]
 [--no-footer]
 [--verbose]
```

Options

`{--limit | -l}<integer>`
Limits the number of statistics to display.

`--format {table | json | csv | list | top}`
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

**Note**

If you specify `--top` without `--repeat`, the report runs indefinitely.

`{--noheader | -a}`
Displays data without column headings.

`{ --no-footer | -z}`
Displays data without footers.

`{--verbose | -v}`
Displays more detailed information.

isi statistics list operations

Displays a list of valid arguments for the `--operations` option.

Syntax

```
isi statistics list operations
 [--protocols <value>]
 [--limit]
 [--format]
 [--no-header]
 [--no-footer]
 [--verbose]
```

Options

`--protocols <value>`
Specifies which protocols to report statistics on. Multiple values can be specified in a comma-separated list, for example `--protocols http,papi`. The following values are valid:

- nfs3
- smb1
- nlm
- ftp
- http
- siq
- smb2
- nfs4
- papi
- jobd
- irp
- lsass_in
- lsass_out
- hdfs
- console
- ssh

```
|--limit | -l|<integer>
```
Limits the number of statistics to display.

```
--format {table | json | csv | list | top}
```
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

**Note**
If you specify `--top` without `--repeat`, the report runs indefinitely.

```
|--noheader | -a
```
Displays data without column headings.

```
|--no-footer | -z
```
Displays data without footers.

```
|--verbose | -v
```
Displays more detailed information.

**isi statistics protocol**

Displays statistics by protocol, such as NFSv3 and HTTP.

**Syntax**

```
isi statistics protocol
```
Options

**--classes <class>**

Specifies which operation classes to report statistics on. The following values are valid:

- **other**
  File-system information. Multiple values can be specified in a comma-separated list.

- **write**
  File and stream writing

- **read**
  File and stream reading

- **create**
  File link node stream and directory creation

- **delete**
  File link node stream and directory deletion

- **namespace_read**
  Attribute stat and ACL reading; lookup directory reading

- **namespace_write**
  Renames; attribute setting; permission time and ACL writes

- **file_state**
  Open, close; locking: acquire, release, break, check; notification

- **session_state**
  Negotiation inquiry or manipulation of protocol connection or session state

**--protocols <value>**

Specifies which protocols to report statistics on. Multiple values can be specified in a comma-separated list, for example **--protocols http, papi**. The following values are valid:
• nfs3
• smb1
• nlm
• ftp
• http
• siq
• smb2
• nfs4
• papi
• jobd
• irp
• lsass_in
• lsass_out
• hdfs
• all
• internal
• external

--operations <operation>
Specifies the operations on which statistics are reported. To view a list of valid
values, run the isi statistics list operations command. Multiple
values can be specified in a comma-separated list.

--zero
Shows table entries with no values.

{--nodes | -n} <node>
Specifies which nodes to report statistics on. Multiple values can be specified in a
comma-separated list, for example, --nodes 1,2. The default value is all. The
following values are valid:
• all
• <int>

{--degraded | -d}
Causes the report to continue running if some nodes do not respond.

--nohumanize
Displays all data in base quantities, without dynamic conversion. If set, this option
also disables the display of units in the data table.

{--interval | -i} <float>
Reports data at the interval specified in seconds.

{--repeat | -r} <integer>
Specifies how many times to run the report before quitting.
Note

To set the report to run indefinitely, specify -1.

`{--limit | -l}<integer>`
Limits the number of statistics to display.

`--long`
Displays all possible columns.

`--totalby <column>`
Aggregates results according to specified fields. The following values are valid:
- Node
- {Proto | protocol}
- Class
- {Op | operation}

`--output <column>`
Specifies which columns to display. The following values are valid:

`{timestamp | time}`
Displays the time at which the isi statistics tool last gathered data. Displayed in POSIX time (number of seconds elapsed since January 1, 1970). Specify `<time-and-date>` in the following format:

```
<YYYY>-<MM>-<DD>[T<hh>:<mm>[:<ss>]]
```

Specify `<time>` as one of the following values.

- **Y**
  Specifies years
- **M**
  Specifies months
- **W**
  Specifies weeks
- **D**
  Specifies days
- **h**
  Specifies hours
- **s**
  Specifies seconds

`{NumOps | operation_count}`
Displays the number of times an operation has been performed.
{Ops | operation_rate}
  Displays the rate at which an operation has been performed. Displayed in operations per second.

{InMax | in_max}
  Displays the maximum input (received) bytes for an operation.

{InMin | in_min}
  Displays the minimum input (received) bytes for an operation.

In
  Displays the rate of input for an operation since the last time isi statistics collected the data. Displayed in bytes per second.

{InAvg | in_avg}
  Displays the average input (received) bytes for an operation.

{InStdDev | in_standard_dev}
  Displays the standard deviation of the input (received) bytes for an operation. Displayed in bytes.

{OutMax | out_max}
  Displays the maximum output (sent) bytes for an operation.

{OutMin | out_min}
  Displays the minimum output (sent) bytes for an operation.

Out
  Displays the rate of output for an operation since the last time isi statistics collected the data. Displayed in bytes per second.

{OutAvg | out_avg}
  Displays the average output (sent) bytes for an operation.

{OutStdDev | out_standard_dev}
  Displays the standard deviation of the output (sent) bytes for an operation. Displayed in bytes.

{TimeMax | time_max}
  Displays the maximum elapsed time taken to complete an operation. Displayed in microseconds.

{TimeMin | time_min}
  Displays the minimum elapsed time taken to complete an operation. Displayed in microseconds.

{TimeAvg | time_avg}
  Displays the average elapsed time taken to complete an operation. Displayed in microseconds.

{TimeStdDev | time_standard_dev}
  Displays the elapsed time taken to complete an operation as a standard deviation from the mean elapsed time.
Node
Displays the node on which the operation was performed.

{Proto | protocol}
Displays the protocol of the operation.

Class
Displays the class of the operation.

{Op | operation}
Displays the name of the operation

--sort <column>
Specifies how rows are ordered. The following values are valid:
- Class
- In
- InAvg | in_avg
- InMax | in_max
- InMin | in_min
- InStdDev | in_standard_dev
- Node
- NumOps | operation_count
- Op | operation
- Ops | operation_rate
- Out
- OutAvg | out_avg
- OutMax | out_max
- OutMin | out_min
- OutStdDev | out_standard_dev
- Proto | protocol
- TimeAvg | time_avg
- TimeMax | time_max
- TimeMin | time_min
- TimeStamp | time
- TimeStdDev | time_standard_dev

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

Note
If you specify --top without --repeat, the report runs indefinitely.
Displays data without column headings.

Displays data without footers.

Displays more detailed information.

isi statistics pstat

Displays a selection of cluster-wide and protocol data.

Syntax

```bash
isi statistics pstat
   [--protocol <protocol>]
   [--degraded]
   [--interval <integer>]
   [--repeat <integer>]
   [--format]
   [--verbose]
```

Options

```
--protocols <value>
   Specifies which protocols to report statistics on. Multiple values can be specified in a comma-separated list, for example `--protocols http,papi`. The following values are valid:
   * nfs3
   * smb1
   * nlm
   * ftp
   * http
   * siq
   * smb2
   * nfs4
   * papi
   * jobd
   * irp
   * lsass_in
   * lsass_out
   * hdfs
```

```
--degraded | -d
   Sets the report to continue running if some nodes do not respond.
```

```
--interval | -i <float>
   Reports data at the interval specified in seconds.
```
```bash
{--repeat | -r} <integer>
   Specifies how many times to run the report before quitting.

   Note
   To set the report to run indefinitely, specify -1.

--format {table | json | csv | list | top}
   Displays output in table, JavaScript Object Notation (JSON), comma-separated
   value (CSV), list format, or top-style display where data is continuously
   overwritten in a single table.

   Note
   If you specify --top without --repeat, the report runs indefinitely.

{--verbose | -v}
   Displays more detailed information.
```

### isi statistics system

Displays general cluster statistics, including op rates for all supported protocols and
network and disk traffic.

#### Syntax

```bash
isi statistics system
   [--oprates]
   [--nodes]
   [--degraded]
   [--nohumanize]
   [--interval <integer>]
   [--repeat <integer>]
   [--limit]
   [--long]
   [--output <column>]
   [--sort <column>]
   [--format]
   [--no-header]
   [--no-footer]
   [--verbose]
```

#### Options

- **--oprates**
  Displays the protocol operation rate statistics instead of the default throughput
  statistics.

- **{ --nodes | -n} <node>**
  Specifies which nodes to report statistics on. Multiple values can be specified in a
  comma-separated list, for example, --nodes 1,2. The default value is all. The
  following values are valid:
  - all
  - <int>

- **{--degraded | -d}**
Sets the report to continue running if some nodes do not respond.

```
--nohumanize
```
Displays all data in base quantities, without dynamic conversion. If set, this option also disables the display of units within the data table.

```
{--interval | -I} <integer>
```
Reports data at the interval specified in seconds.

```
{--repeat | -r} <integer>
```
Specifies how many times to run the report before quitting.

### Note
To set the report to run indefinitely, specify `-1`.

```
{--limit | -l} <integer>
```
Limits the number of statistics to display.

```
--long
```
Displays all possible columns.

```
--output <column>
```
Specifies which columns to display. The following values are valid:

- `{Timestamp | time}
- Node
- CPU
- SMB
- FTP
- HTTP
- NFS
- HDFS
- Total
- `{NetIn | net_in}
- `{NetOut | net_out}
- `{DiskIn | disk_in}
- `{DiskOut | disk_out}

```
--sort <column>
```
Specifies how rows are ordered. The following values are valid:

- `{Timestamp | time}
- Node
- CPU
- SMB
- FTP
- HTTP
- NFS
- HDFS
- Total
- {NetIn | net_in}
- {NetOut | net_out}
- {DiskIn | disk_in}
- {DiskOut | disk_out}

--format {table | json | csv | list | top}
Displays output in table, JavaScript Object Notation (JSON), comma-separated value (CSV), list format, or top-style display where data is continuously overwritten in a single table.

Note
If you specify --top without --repeat, the report runs indefinitely.

{--noheader | -a}
Displays data without column headings.

{--no-footer | -z}
Displays data without footers.

{--verbose | -v}
Displays more detailed information.

isi status
Displays information about the current status of the nodes on the cluster.

Syntax

```bash
isi status
 [--all-nodes | -a]
[ --node | -n <integer>]
[ --all-nodepools | -p]
[ --nodepool | -l <string>]
[ --quiet | -q]
[ --verbose | -v]
```

Options

--all-nodes | -a
Display node-specific status for all nodes on a cluster.

--node | -n <integer>
Display node-specific status for the node specified by its logical node number (LNN).

--all-nodepools | -p
Display node pool status for all node pools in the cluster.

--nodepool | -l <string>
Display node pool status for the specified node pool.

--quiet | -q
Display less detailed information.

--verbose | -v
Display more detailed information for the --nodepool or --all-nodepools options.

isi upgrade cluster add-nodes
Add new nodes to a running upgrade process.

Syntax

```
isi upgrade cluster add-nodes <nodes> [--yes]
```

Options

**<nodes>**
List of comma-separated (1,3,7) or dash-separated (1-7) specified logical node numbers (LNNs) to mark for upgrade.

--yes
Automatically answer yes at the prompt.

isi upgrade cluster add-remaining-nodes
Let the system include any remaining or new nodes inside an existing upgrade.

Syntax

```
isi upgrade cluster add-remaining-nodes [--yes]
```

Options

--yes
Automatically answer yes at the prompt.

isi upgrade cluster archive
Start an archive of the upgrade framework.

Syntax

```
isi upgrade cluster archive [--clear]
```

Options

--clear
Clear the upgrade after an archive is complete.
**isi upgrade cluster assess**

Runs upgrade checks without starting an upgrade.

**Syntax**

\`isi upgrade cluster assess <install-image-path>\`

**Options**

\`<install-image-path>`

The path of the upgrade install image. Must be within an /ifs or http:// source.

**isi upgrade cluster commit**

Commits the upgrade to the new version. Rollback is not possible after you run this command.

**Syntax**

\`isi upgrade cluster commit [--yes]\`

**Options**

\`--yes\`

Automatically answers yes at the upgrade commitment prompt.

**isi upgrade cluster firmware**

This is the command-line interface for firmware upgrades.

**Syntax**

\`isi upgrade cluster firmware <action> [--timeout <integer>]\`

**Options**

\`<action>`

Specifies actions you can take against the firmware upgrade.

- **package**
  
  Lists all the nodes on the cluster and shows detailed firmware package information on the given node.

- **devices**
  
  Lists all the nodes on the cluster and shows detailed status of the current firmware for each node.

- **assess**
  
  Runs upgrade checks without starting a firmware upgrade.
view
  Shows overview status of the current firmware upgrade activity.

start
  Starts upgrade processes.

---

**Note**

All upgrade processes take a long time to run. The return status of a command only relates to the issuing of the command itself, not the successful completion of it.

--timeout `<integer>`

Number of seconds for a command timeout.

**Example**

The following command runs upgrade checks without starting the firmware upgrade.

```
isi upgrade cluster firmware assess
```

**isi upgrade cluster from-version**

Displays the version of the cluster you are upgrading from.

**Syntax**

```
isi upgrade cluster from-version
```

**Example**

To view information about the cluster version you are upgrading from, run the following command:

```
isi upgrade cluster from-version
```

The system displays output similar to the following example:

```
Upgrading Current OS Version: 7.2.1.1
  Major: 7
Minor: 0
  Maintenance: 0
Bugfix: 0
```
isi upgrade cluster nodes firmware

This is the command-line interface for the non-disruptive upgrade firmware upgrade framework.

Syntax

```
isi upgrade cluster nodes firmware <action>
   [--timeout <integer>]
```

Options

`<action>`

Specifies reporting actions you can take regarding node firmware updates.

- `devices`
  Reports devices on the nodes which are supported in the installed firmware package.

- `package`
  Reports the contents of the installed firmware package.

- `progress`
  Reports, in list or view format, status information regarding the firmware upgrade.

`--timeout <integer>`

Number of seconds for a command timeout.

Example

The following command displays the contents of the installed firmware package:

```
isi upgrade cluster nodes firmware package
```

isi upgrade cluster nodes list

List all nodes on the cluster and show detailed status of their upgrade activity.

Syntax

```
isi upgrade cluster nodes list
```

Example

To list upgrade status for all nodes on the cluster, run the following command:

```
isi upgrade cluster nodes list
```

The system displays output similar to the following example:

```
Node LNN: 1
Node Upgrade State: committed
   Error Details: None
```
isi upgrade cluster nodes view

Show detailed status of the current upgrade activity on a specified node.

Syntax

```
isi upgrade cluster nodes view <lnn>
```

Options

`<lnn>`

The logical node number (LNN) of the node for which you want to view upgrade status.

Example

To view the upgrade status for a node with the LNN 1, run the following command:

```
isi upgrade cluster nodes view 1
```

The system displays output similar to the following example:

```
Node LNN: 1
Node Upgrade State: committed
Error Details: None
Last Upgrade Action: -
Last Action Result: -
Node Upgrade Progress: None
Node OS Version: 8.0.0.0
```

isi upgrade cluster retry-last-action

Retry the last upgrade action on a node, in case the previous action failed.

Syntax

```
isi upgrade cluster retry-last-action <nodes>
```
Options

\texttt{<nodes>}

A list of comma-separated (1,3,7) or dash-separated (1-7) logical node numbers to select. You can also use \texttt{all} to select all the cluster's nodes at any given time.

\textbf{isi upgrade cluster rollback}

Stop upgrading a cluster, and return to the previous version. This causes a disruptive rollback of the upgrade.

\textbf{Syntax}

\begin{verbatim}
isi upgrade cluster rollback
    [--yes]
\end{verbatim}

Options

\texttt{--yes}

Automatically answer yes to the confirmation prompt.

\textbf{isi upgrade cluster settings}

Show the settings of the currently running upgrade.

\textbf{Syntax}

\begin{verbatim}
isi upgrade cluster settings
\end{verbatim}

Options

There are no options for this command.

\textbf{isi upgrade cluster start}

Start an upgrade process.

\textbf{Syntax}

\begin{verbatim}
isi upgrade cluster start \texttt{<install-image-path>}
    [--skip-optional]
    [--yes]
    [--simultaneous]
    [--nodes \texttt{<integer_range_list>}]\end{verbatim}

Options

\texttt{\textless install-image-path\textgreater}

The file path of the location of the upgrade install image. The file path must be accessible in a /ifs directory or by an https:// URL.

\texttt{--skip-optional}

Skips the optional pre-upgrade checks.

\texttt{--yes}

Automatically answer yes to the confirmation prompt.
--simultaneous
Start a simultaneous upgrade.

--nodes integer_range_list
List of comma-separated (1,3,7) or dash-separated (1-7) logical node numbers (LNNs) to select for upgrade.

**isi upgrade cluster to-version**

Show the version of the cluster to which you are upgrading.

**Syntax**

```bash
isi upgrade cluster to-version
```

**Options**
There are no options for this command.

**isi upgrade cluster view**

Show status of the current upgrade activity on the cluster.

**Syntax**

```bash
isi upgrade cluster view
```

**Options**
There are no options for this command.

**isi upgrade patches abort**

Repairs the patch system by attempting to discontinue the most recent failed action.

**Syntax**

```bash
isi upgrade patches abort
    [--force]
```

**Options**

```bash
    [--force | -f]
```

Skips the confirmation prompt for this command.

**isi upgrade patches install**

Installs a system patch.

**Syntax**

```bash
isi upgrade patches install <patch>
    [--rolling {yes | no}]
    [--override]
```
Options

<patch>
  The file path location of the patch to install. This must be an absolute path within the /ifs file system.

{--rolling | -r}{yes | no}
  Performs a rolling patch install. A value of no will install simultaneously on all nodes.

{--override | -o}
  Overrides the patch system validation, and forces the patch installation.

**isi upgrade patches list**

Lists all system patches.

**Syntax**

```bash
isi upgrade patches list
    [--local]
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

--local
  Lists patch information only on the local node.

{--limit | -l} <integer>
  The number of upgrade patches to display.

--format {table | json | csv | list}
  Displays upgrade patches in table, JSON, CSV or list format.

{--no-header | -a}
  Does not display headers in CSV or table formats.

{--no-footer | -z}
  Does not display table summary footer information.

{--verbose | -v}
  Displays more detailed information.

**isi upgrade patches uninstall**

Uninstalls a system patch.

**Syntax**

```bash
isi upgrade patches uninstall <patch>
    [--rolling {yes | no}]
```
## isi upgrade patches view

Shows details of a system patch.

**Syntax**

\[
\text{isi upgrade patches view <patch> [--local]}
\]

**Options**

**<patch>**

The name or ID of the patch to view.

**--local**

Shows patch information only for the local node.

## isi version

Displays cluster version information.

**Syntax**

\[
\text{isi version [--format \{list | json\}] [--verbose]}
\]

**Options**

**--format \{list | json\}**

Displays the cluster version information in list or JSON format.

**--verbose | -v**

Displays more detailed cluster version information.
isi_for_array

Runs commands on multiple nodes in an array, either in parallel or in serial.
When options conflict, the one specified last takes precedence.

Note
The -k, -u, -p, and -q options are valid only for SSH transport.

Syntax

isi_for_array
   [--array-name <array>]
   [--array-file <filename>]
   [--directory <directory>]
   [--diskless]
   [--ignore-errors]
   [--known-hosts-file <filename>]
   [--user <user>]
   [--nodes <nodes>]
   [--password <password>]
   [--pre-command <command>]
   [--query-password]
   [--quiet]
   [--serial]
   [--storage]
   [--transport <transport-type>]
   [--throttle <setting>]
   [--exclude-nodes <nodes>]
   [--exclude-down-nodes]

Options

{--array-name | -a} <array>
   Uses <array>.

{--array-file | -A} <filename>
   Reads array information from <filename>. The default looks first for
   $HOME/.array.xml, then for /etc/ifs/array.xml.

{--directory | -d} <directory>
   Runs commands from the specified directory on remote computers. The current
   working directory is the default directory. An empty <directory> results in
   commands being run in the user's home directory on the remote computer.

{--diskless | -D}
   Runs commands from diskless nodes.

{--ignore | -I}
   Suppresses the printing of error messages for nodes that return non-zero exit
   status. Returns the maximum exit status from all nodes.

{--known-hosts-file | -k} <filename>
   Uses <filename> for SSH known hosts file instead of the default /dev/null
   directory.

{--user | -u | -l} <user>
Logs in as `<user>` instead of as the default root user.

`{--nodes | -n} <nodes>`

Runs commands on the specified nodes, which can be specified multiple times. Must be a list of either node names or ranges of node IDs; for example, 1,3-5,neal8,10. If no nodes are explicitly listed, the whole array is used.

`{--password | -p | --pw} <password>`

Uses the specified password instead of the default password.

`{--pre-command | -P} <command>`

Runs the specified command before any other commands. This is useful for setting up the environment and it can be specified multiple times. You can specify -- to reset the list of pre-commands.

`{--query-password | -q}`

Prompts the user for a password.

`{--quiet | -Q}`

Suppresses printing of the host prefix for each output line.

`{--serial | -s}`

Runs commands in serial instead of parallel.

`{--storage | -S}`

Run commands from storage nodes.

`{--transport | -t} <transport-type>`

Specifies the network transport type. The default value is rpc. Valid transports values are rpc or ssh.

`{--throttle | -T} <setting>`

Adjusts throttling. To disable throttling, specify 0. The default value is 24.

`{--exclude-nodes | -x} <nodes>`

Excludes specified nodes from the command. This argument is specified in the same manner as the -n option.

`{--exclude-down-nodes | -X}`

Excludes offline nodes from the command. This command is limited to cluster local use only.

**Example**

In SmartLock compliance mode, to run `isi_for_array` for a command that requires root privileges, you must specify `sudo` twice. For example, the following command runs `isi statistics client list` on each node in a compliance cluster.

```
sudo isi_for_array -u compadmin sudo isi statistics client list
```
isi get

Displays information about a set of files, including the requested protection, current actual protection, and whether write-coalescing is enabled.

Requested protection appears in one of three colors: green, yellow, or red. Green indicates full protection. Yellow indicates degraded protection under a mirroring policy. Red indicates a loss of one or more data blocks under a parity policy.

Syntax

```
isi get {{[-a] [-d] [-g] [-s] [(-D | -DD | -DDC)] [-R] <path>}
| {{[-g] [-s] [(-D | -DD | -DDC)] [-R] -L <lin>}}
```

Options

- **-a**
  Displays the hidden "." and ".." entries of each directory.

- **-d**
  Displays the attributes of a directory instead of the contents.

- **-g**
  Displays detailed information, including snapshot governance lists.

- **-s**
  Displays the protection status using words instead of colors.

- **-D**
  Displays more detailed information.

- **-DD**
  Includes information about protection groups and security descriptor owners and groups.

- **-DDC**
  Includes cyclic redundancy check (CRC) information.

- **-R**
  Displays information about the subdirectories and files of the specified directories.

- **<path>**
  Displays information about the specified file or directory.
  Specify as a file or directory path.

- **-L <lin>**
  Displays information about the specified file or directory.
  Specify as a file or directory LIN.
Examples
The following command displays information on /ifs/home/ and all of its subdirectories:

```
isiget -R /ifs/home
```

The system displays output similar to the following example:

```
<table>
<thead>
<tr>
<th>POLICY</th>
<th>LEVEL</th>
<th>PERFORMANCE</th>
<th>COAL</th>
<th>FILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>4x/2</td>
<td>concurrency on</td>
<td>./</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>8x/3</td>
<td>concurrency on</td>
<td>../</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>4x/2</td>
<td>concurrency on</td>
<td>admin/</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>4x/2</td>
<td>concurrency on</td>
<td>ftp/</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>4x/2</td>
<td>concurrency on</td>
<td>newUser1/</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>4x/2</td>
<td>concurrency on</td>
<td>newUser2/</td>
<td></td>
</tr>
</tbody>
</table>

/ifs/home/admin:

```
default 4+2/2 concurrency on .zshrc
```

/ifs/home/ftp:

```
default 4x/2 concurrency on incoming/
default 4x/2 concurrency on pub/
```

/ifs/home/ftp/incoming:

/ifs/home/ftp/pub:

/ifs/home/newUser1:

```
default 4+2/2 concurrency on .cshrc
default 4+2/2 concurrency on .login
default 4+2/2 concurrency on .login_conf
default 4+2/2 concurrency on .mail_aliases
default 4+2/2 concurrency on .mailrc
default 4+2/2 concurrency on .profile
default 4+2/2 concurrency on .rhosts
default 4+2/2 concurrency on .shrc
default 4+2/2 concurrency on .zshrc
```

/ifs/home/newUser2:

```
default 4+2/2 concurrency on .cshrc
default 4+2/2 concurrency on .login
default 4+2/2 concurrency on .login_conf
default 4+2/2 concurrency on .mailAliases
default 4+2/2 concurrency on .mailrc
default 4+2/2 concurrency on .profile
default 4+2/2 concurrency on .rhosts
default 4+2/2 concurrency on .shrc
default 4+2/2 concurrency on .zshrc
```

**isi_gather_info**

Collects and uploads the most recent cluster log information to EMC Secure Remote Services (ESRS).

Multiple instances of \(-i, -f, -s, -S, \) and \(-l\) are allowed.

`gather_expr` and `analysis_expr` can be quoted.

The default temporary directory is `/ifs/data/Isilon_Support/` (change with \(-L\) or \(-T\).
Syntax

```bash
isi_gather_info
  [-h]
  [-v]
  [-u <user>]
  [-p <password>]
  [-i]
  [--incremental]
  [-l]
  [-f <filename>]
  [-n <nodes>]
  [--local-only]
  [--skip-node-check]
  [-s gather-script]
  [-S gather-expr]
  [-l gather-expr]
  [-a analysis-script]
  [-A analysis-expr]
  [-t <tarfile>]
  [-x exclude_tool]
  [-I]
  [-L]
  [-T <temp-dir>]
  [--tardir <dir>]
  [--symlinkdir <dir>]
  [--varlog_recent]
  [--varlog_all]
  [--nologs]
  [--group <name>]
  [--clean-cores]
  [--clean-all]
  [--no-dumps]
  [--dumps]
  [--no-cores]
  [--cores]
  [--upgrade-archive]
  [--debug]
  [--verbose]
  [--noconfig]
  [--save-only]
  [--save]
  [--upload]
  [--noupload]
  [--re-upload <filename>]
  [--verify-upload]
  [--http]
  [--nohttp]
  [--http-host <host>]
  [--http-path <dir>]
  [--http-proxy <host>]
  [--http-proxy-port <port>]
  [--ftp]
  [--noftp]
  [--ftp-user <user>]
  [--ftp-pass <password>]
  [--ftp-host <host>]
  [--ftp-path <dir>]
  [--ftp-port <alt-port>]
  [--ftp-proxy <host>]
  [--ftp-proxy-port <port>]
  [--ftp-mode <mode>]
  [--esrs]
  [--email]
  [--noemail]
  [--email-addresses]
  [--email-from]
```
Options

- **h**
  Prints this message and exits.

- **v**
  Prints version info and exits.

- **u <user>**
  Specifies the login as <user> instead of as the default root user.

- **p <password>**
  Uses <password>.

- **i**
  Includes only the listed utility. See also the -l option for a list of utilities to include. The special value all may be used to include every known utility.

--**incremental**
  Gathers only those logs that changed since last log upload.

- **l**
  Lists utilities and groups that can be included. See -l and --group.

- **f <filename>**
  Gathers <filename> from each node. The value must be an absolute path.

- **n <nodes>**
  Gathers information from only the specified nodes. Nodes must be a list or range of LNNs, for example, 1,4-10,12,14. If no nodes are specified, the whole array is used. Note that nodes are automatically excluded if they are down.

--**local-only**
  Gathers information only from only the local node. Run this option when gathering files from the /ifs filesystem.

--**skip-node-check**
  Skips the check for node availability.

- **s gather-script**
  Runs <gather-script> on every node.

- **S gather-expr**
  Runs <gather-expr> on every node.

- **l gather-expr**
Runs `<gather-expr>` on the local node.

- `-a analysis-script`
  Runs `<analysis-script>` on results.

- `-A analysis-expr`
  Runs `<analysis-expr>` on every node.

- `-t <tarfile>`
  Saves all results to the specified `<tarfile>` rather than to the default tar file.

- `-x exclude_tool`
  Excludes the specified tool or tools from being gathered from each node. Multiple tools can be listed as comma-separated values.

- `-I`
  Saves results to `/ifs`. This is the default setting.

- `-L`
  Save all results to local storage `/var/crash/support/`.

- `-T <temp-dir>`
  Saves all results to `<temp-dir>` instead of the default directory. `-T` overrides `-L` and `-l`.

--`--tardir <dir>`
Places the final package directly into the specified directory.

--`--symlinkdir <dir>`
Creates a symlink to the final package in the specified directory.

--`--varlog_recent`
Gathers all logs in `/var/log`, with the exception of the compressed and rotated old logs. The default setting is all logs.

--`--varlog_all`
Gathers all logs in `/var/log`, including compressed and rotated old logs. This is the default setting.

--`--nologs`
Does not gather the required minimum number of logs.

--`--group <name>`
Adds a specific group of utilities to the tar file.

--`--clean-cores`
Deletes cores from `/var/crash` after successful compression of the package.

--`--clean-dumps`
Deletes dumps from `/var/crash` after successful compression of the package.
--clean-all
   Deletes cores and dumps from /var/crash after successful compression of the package.

--no-dumps
   Does not gather hang dumps for the package.

--dumps
   Adds cores to the package.

--no-cores
   Does not gather cores for the package.

--cores
   Adds dumps to the package.

--upgrade-archive
   Adds the upgrade archive to the package.

--debug
   Displays debugging messages.

--verbose
   Displays more detailed information.

--noconfig
   Uses built-in default values and bypasses the configuration file.

--save-only
   Saves the CLI-specified configuration to file and exits.

--save
   Saves the CLI-specified configuration to file and runs it.

--upload
   Uploads logs to Isilon Technical Support automatically. This is the default setting.

--noupload
   Specifies no automatic upload to Isilon Technical Support.

--re-upload <filename>
   Re-uploads the specified <filename>.

--verify-upload
   Creates a tar file and uploads to test connectivity.

--http
   Attempts HTTP upload. This is the default setting.

--nohttp
   Specifies no HTTP upload attempt.

--http-host <host>
Specifies an alternate HTTP site for upload.

\textbf{--http-path <dir>}
Specifies an alternate HTTP upload directory.

\textbf{--http-proxy <host>}
Specifies the proxy server to use.

\textbf{--http-proxy-port <port>}
Specifies the proxy port to use.

\textbf{--ftp}
Attempts FTP upload. This setting is the default value.

\textbf{--noftp}
Specifies no FTP upload attempt.

\textbf{--ftp-user <user>}
Specifies an alternate user for FTP (default: anonymous).

\textbf{--ftp-pass <password>}
Specifies an alternate password for FTP.

\textbf{--ftp-host <host>}
Specifies an alternate FTP site for upload.

\textbf{--ftp-path DIR}
Specifies an alternate FTP upload directory.

\textbf{--ftp-port <alt-port>}
Specifies an alternate FTP port for upload.

\textbf{--ftp-proxy <host>}
Specifies the proxy server to use.

\textbf{--ftp-proxy-port <port>}
Specifies the proxy port to use.

\textbf{--ftp-mode <mode>}
Specifies the mode of FTP file transfer. The following values are valid: \texttt{both}, \texttt{active}, \texttt{passive}. \texttt{The default value is both.}

\textbf{--esrs}
Attempts ESRS upload.

\textbf{--email}
Attempts SMTP upload. If set, SMTP is tried first.

\textbf{--noemail}
Specifies no SMTP upload attempt. This is the default value.

--email-addresses
Specifies email addresses as comma-separated strings.

--email-from
Specifies the sender's email address.

--email-subject
Specifies an alternative email subject.

--email-body
Specifies alternative email text shown on head of body.

--skip-size-check
Does not check the size of the gathered file.

isi_phone_home

Modify the settings for the isi_phone_home feature, which gathers specific node- and cluster-related information to send to Isilon Technical Support on a weekly basis. This feature is enabled by default if you have EMC Secure Remote Services (ESRS) enabled.

Syntax

```bash
isi_phone_home
[--enable]
[--disable]
[--logging-level {debug | info | warning | error | critical}]
[--list-file <string>]
[--script-file <string>]
[--create-package]
[--send-data]
[--delete-data]
```

Options

**Note**

We recommend that you run only the `--enable` or `--disable` options from the OneFS command-line interface. All others are run automatically when the tool is enabled, and are provided here for reference in case Isilon Technical Support asks you for a specific type of information.

`{--enable | -e}`

Enables `isi_phone_home`, providing that ESRS is configured and enabled. If you enabled ESRS when configuring the Isilon cluster, this feature is automatically enabled.

`{--disable | -d}`

Disables `isi_phone_home`.

`{--logging-level | -o}{debug | info | warning | error | critical}`
Emits logs specific to a log state, as well as all logs of higher priority. The default is error, which means all logs of condition error and critical are emitted. If you select a lower level log such as warning, all logs of level warning, error, and critical are emitted. We recommend that you do not change the default setting.

\{--list-file | -l\} <string>
Receives the name of a list file that contains isi commands to be run against the cluster. These list files are located in /usr/local/isi_phone_home/list.

\{--script-file | -r\} <string>
Receives the name of a Python script file to be run against the cluster. These script files are located in /usr/local/isi_phone_home/script.

\{--create-package | -c\}
Groups all the files in the /ifs/data/Isilon_Support/phone_home/data directory into a gzip file that is copied to /ifs/data/Isilon_Support/phone_home/pkg.

\{--send-data | -s\}
Scans /ifs/data/Isilon_Support/phone_home/pkg and uploads any unsent gzip files to Isilon Technical Support through ESRS.

\{--delete-data | -t\}
Deletes all gzip files older than 30 days from the /ifs/data/Isilon_Support/phone_home/pkg directory.

## Event commands

You can access and configure OneFS events and notification rules settings using the event commands. Running isi events without subcommands is equivalent to running isi events list.

### isi event alerts create

Creates a new alert.

**Syntax**

```
isi event alerts create <name> <condition>  
[ --category <string> ]  
[ --eventgroup <string> ]  
[ --severity { emergency | critical | warning | information } ]  
[ --channel <string> ]  
[ --limit <integer> ]  
[ --interval <duration> ]  
[ --transient <duration> ]  
[ --description <string> ]  
[ --verbose ]
```

**Options**

- `<name>`
  Specifies the alert name.
<condition>
Specifications the condition under which alert is sent. Condition values are case sensitive. The following values are valid:

NEW
Reports on event group occurrences that have never been reported on before.

NEW_EVENTS
Reports on event group occurrences that are new since the event group was last reported on.

ONGOING
Provides periodic reports on event group occurrences that have not been resolved.

SEVERITY_INCREASE
Reports on event group occurrences whose severity has increased since the event group was last reported on.

SEVERITY_DECREASE
Reports on event group occurrences whose severity has decreased since the event group was last reported on.

RESOLVED
Reports on event group occurrences that have been resolved since the event group was last reported on.

--category <string>...
Specifies the name of one or more event group categories to alert on.

--eventgroup <string>...
Specifies the name of one or more event groups to alert on.

--severity {emergency | critical | warning | information}
Specifies the event severity that the alert will report on. Severity values are case sensitive. Repeat --severity to make the alert report on additional severity levels.

{--channel | -c} <string>...
Specifies the name of one or more channels to deliver the alert over.

--limit <integer>
Sets the maximum number of alerts that can be sent. Applies only to the NEW_EVENTS alert condition.

--interval <integer> <time>
Sets the time period between reports for ongoing alerts. Applies only to the ONGOING alert condition.
The following <time> values are valid:

Y
Specifies years.
M
    Specifies months
W
    Specifies weeks
D
    Specifies days
H
    Specifies hours
m
    Specifies minutes
s
    Specifies seconds

--transient <integer> <time>
    Sets a minimum time that an event group occurrence must exist before it is
    reported on. Any occurrence lasting less than the time period is considered
    transient and will not be reported.
    The following <time> values are valid:
Y
    Specifies years
M
    Specifies months
W
    Specifies weeks
D
    Specifies days
H
    Specifies hours
m
    Specifies minutes
s
    Specifies seconds

--description <string>
    Specifies a description of the alert.

{--verbose | -v}
    Displays more detailed information.
**isi event alerts delete**

Deletes an alert.

**Syntax**

```bash
isi event alerts delete <id>
   [--force]
   [--verbose]
```

**Options**

- `<id>`
  Specifies the ID of the alert you want to delete.

- `|--force | -f`
  Deletes the alert without asking for confirmation.

- `|--verbose | -v`
  Displays more detailed information.

**isi event alerts list**

Displays a list of alerts.

**Syntax**

```bash
isi event alerts list
   [--channel <string>]
   [--limit <integer>]
   [--sort {name | eventgroup | category | channel | condition | limit | interval | transient}]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

- `|--channel | -c <string>...`
  Displays alerts for the specified channel only.

- `|--limit | -l <integer>`
  Sets the maximum number of alerts to display.

- `|--sort {name | eventgroup | category | channel | condition | limit | interval | transient}`
  Specifies the field to sort items by.

- `|--descending | -d`
  Sorts the data in descending order.

- `|--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a }
Displays table and CSV output without headers.

{ --no-footer | -z }
Displays table output without footers.

{ --verbose | -v }
Displays more detailed information.

isi event alerts modify
Modifies an alert.

Syntax

isi event alerts modify <id>
    [--name <string>]
    [--eventgroup <string>]
    [--clear-eventgroup]
    [--add-eventgroup <string>]
    [--remove-eventgroup <string>]
    [--category <string>]
    [--clear-category]
    [--add-category <string>]
    [--remove-category <string>]
    [--channel <string>]
    [--clear-channel]
    [--add-channel <string>]
    [--remove-channel <string>]
    [--severity {emergency | critical | warning | information}]
    [--clear-severity]
    [--add-severity {emergency | critical | warning | information}]
    [--remove-severity {emergency | critical | warning | information}]
    [--condition {NEW | NEW_EVENTS | ONGOING | SEVERITY_INCREASE | SEVERITY_DECREASE | RESOLVED}]
    [--limit <integer>]
    [--interval <integer> <time>]
    [--transient <integer> <time>]
    [--verbose]

Options

<iid>
Specifies the ID of the alert you want to modify.

{ --name | -n } <string>
Specifies the alert condition name.

--eventgroup <string>...
Specifies the name of one or more event groups to alert on.

--clear-eventgroup
Clears the value for an event group to alert on.

--add-eventgroup <string>...
Adds the name of one or more event groups to alert on.

--remove-eventgroup <string>...
Removes the name of one or more event groups to alert on.

--category <string>...
Specifies the name of one or more event group categories to alert on.

--clear-category
Clears the value for an event group category to alert on.

--add-category <string>...
Adds the name of one or more event group categories to alert on.

--remove-category <string>...
Removes the name of one or more event group categories to alert on.

{- --channel | -c} <string>...
Specifies the name of one or more channels to deliver the alert over.

--clear-channel
Clears the value for a channel to deliver the alert over.

--add-channel <string>...
Adds the name of one or more channels to deliver the alert over.

--remove-channel <string>...
Removes the name of one or more channels to deliver the alert over.

--severity {emergency | critical | warning | information}
Specifies the event severity that the alert will report on. Severity values are case sensitive. Repeat --severity to make the alert report on additional severity levels.

--clear-severity
Clears all severity filters for an alert.

--add-severity {emergency | critical | warning | information}
Adds another severity value for an alert to report on. Repeat --add-severity to make the alert report on additional severity levels.

--remove-severity {emergency | critical | warning | information}
Removes a severity value that an alert is reporting on. Repeat --remove-severity to remove an additional severity level that an alert is reporting on.

--condition {NEW | NEW_EVENTS | ONGOING | SEVERITY_INCREASE | SEVERITY_DECREASE | RESOLVED}
Specifies the condition under which alert is sent.
Condition values are case sensitive. The following values are valid:

NEW
Reports on event group occurrences that have never been reported on before.
NEW_EVENTS
Reports on event group occurrences that are new since the event group was last reported on.

ONGOING
Provides periodic reports on event group occurrences that have not been resolved.

SEVERITY_INCREASE
Reports on event group occurrences whose severity has increased since the event group was last reported on.

SEVERITY_DECREASE
Reports on event group occurrences whose severity has decreased since the event group was last reported on.

RESOLVED
Reports on event group occurrences that have been resolved since the event group was last reported on.

--limit <integer>
Sets the maximum number of alerts that can be sent. Applies only to the NEW_EVENTS alert condition.

--interval <integer> <time>
Sets the time period between reports for ongoing alerts. Applies only to the ONGOING alert condition.
The following <time> values are valid:

Y
Specifies years

M
Specifies months

W
Specifies weeks

D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds

--transient <integer> <time>
Sets a minimum time that an event group occurrence must exist before it is reported on. Any occurrence lasting less than the time period is considered transient and will not be reported.
The following `<time>` values are valid:

Y
  Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours
m
  Specifies minutes
s
  Specifies seconds

`{--verbose | -v}`
  Displays more detailed information.

**isi event alerts view**

Displays the details of an alert.

**Syntax**

```
isi event alerts view <id>
```

**Options**

**<id>**
  Specifies the alert ID.

**isi event channels create**

Creates a new channel.

**Syntax**

```
isi event channels create <name> <type>  
  [--enabled {true | false}]  
  [--allowed-nodes <integer>]  
  [--excluded-nodes <integer>]  
  [--address <string>]  
  [--send-as <string>]  
  [--subject <string>]  
  [--smtp-host <string>]  
  [--smtp-port <integer>]  
  [--smtp-use-auth <boolean>]  
  [--smtp-username <string>]  
```
Options

**<name>**

Specifies the channel name.

**<type>**

Specifies the mechanism by which alerts are sent.
Type values are case sensitive. The following values are valid:

- **smtp**
  
  Alerts are sent as emails through an SMTP server.

- **snmp**
  
  Alerts are sent through SNMP.

- **connectemc**
  
  Alerts are sent through ConnectEMC.

**--enabled {true | false}**

Specifies whether the channel is enabled.

**--allowed-nodes <integer>...**

Specifies one or more nodes that are allowed to send alerts through the channel.
If you do not specify any allowed nodes, all nodes in the cluster will be allowed to send alerts. The value of <integer> is the node number you want to allow.

**--excluded-nodes <integer>...**

Specifies one or more nodes that are not allowed to send alerts through the channel. The value of <integer> is the node number you want to exclude.

**--address <string>...**

For SMTP channels only. Specifies one or more email addresses you want to receive alerts on this channel. The value of <string> is an email address.

**--send-as <string>**

For SMTP channels only. Specifies the email address you want to send alerts from on this channel. The value of <string> is an email address.

**--subject <string>**

For SMTP channels only. Specifies the subject line for emails sent on this channel.

**--smtp-host <string>**

For SMTP channels only. Specifies the SMTP relay host.

**--smtp-port <integer>**

For SMTP channels only. Specifies the SMTP relay port.
--smtp-use-auth {true | false}
For SMTP channels only. Enables or disables SMTP authentication.

--smtp-username <string>
For SMTP channels only. Specifies the username for SMTP authentication.

--smtp-password <string>
For SMTP channels only. Specifies the password for SMTP authentication.

--smtp-security {STARTTLS | NONE}
For SMTP channels only. Enables or disables SMTP encryption.

--batch {NONE | ALL | CATEGORY | SEVERITY}
For SMTP channels only. Specifies how SMTP alerts will be batched.

--batch-period <integer> <time>
For SMTP channels only. Specifies the interval between batched alerts. The following <time> values are valid:
Y
  Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours
m
  Specifies minutes
s
  Specifies seconds

--host <string>
For SNMP channels only. Specifies the host name or address

--community <string>
For SNMP channels only. Specifies the community string.

{--verbose | -v}
Displays more detailed information.
isi event channels delete

Deletes a channel.

Syntax

```
isi event channels delete <name>
    [--force]
    [--verbose]
```

Options

- `<name>`
  Specifies the name of the channel you want to delete.

- `[--force | -f]`
  Deletes the channel without asking for confirmation.

- `[--verbose | -v]`
  Displays more detailed information.

isi event channels list

Displays a list of channels.

Syntax

```
isi event channels list <id>
    [--limit <integer>]
    [-l]
    [-d]
    [--sort id | name | type | enabled | allowed_nodes | excluded_nodes | address | send_as | subject | smtp_host | smtp_port | smtp_use_auth | smtp_username | smtp_password | smtp_security | batch | batch_period | host | community]
    [--descending]
    [--format table | json | csv | list]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

- `--limit | -l <integer>`
  Sets the maximum number of channels to display.

- `--sort id | name | type | enabled | allowed_nodes | excluded_nodes | address | send_as | subject | smtp_host | smtp_port | smtp_use_auth | smtp_username | smtp_password | smtp_security | batch | batch_period | host | community`
  Specifies the field to sort items by.

- `--descending | -d`
  Sorts the data in descending order.

- `--format table | json | csv | list`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a }  
Displays table and CSV output without headers.

{ --no-footer | -z }  
Displays table output without footers.

{ --verbose | -v }  
Displays more detailed information.

**isi event channels modify**

Modifies a channel.

**Syntax**

```
isi event channels <name>
   [--type {smtp | snmp | connectemc}]
   [--enabled {true | false}]
   [--allowed-nodes <integer>]
   [--clear-allowed-nodes]
   [--add-allowed-nodes <integer>]
   [--remove-allowed-nodes <integer>]
   [--excluded-nodes <integer>]
   [--clear-excluded-nodes]
   [--add-excluded-nodes <integer>]
   [--remove-excluded-nodes <integer>]
   [--address <string>]
   [--clear-address]
   [--add-address <string>]
   [--remove-address <string>]
   [--send-as <string>]
   [--subject <string>]
   [--smtp-host <string>]
   [--smtp-port <integer>]
   [--smtp-use-auth <boolean>]
   [--smtp-username <string>]
   [--smtp-password <string>]
   [--smtp-security {STARTTLS | NONE}]
   [--batch {NONE | ALL | CATEGORY | SEVERITY}]
   [--batch-period <integer> <time>]
   [--host <string>]
   [--community <string>]
   [--verbose]
```

**Options**

**<name>**

Specifies the name of the channel you want to modify.

**<type>**

Specifies the mechanism by which alerts are sent. Type values are case sensitive. The following values are valid:

- **smtp**
  
  Alerts are sent as emails through an SMTP server.

- **snmp**
  
  Alerts are sent through SNMP.
connectemc
   Alerts are sent through ConnectEMC.

--enabled {true | false}
   Specifies whether the channel is enabled.

--allowed-nodes <integer>...
   Specifies one or more nodes that are allowed to send alerts through the channel.
   If you do not specify any allowed nodes, all nodes in the cluster will be allowed to
   send alerts. The value of <integer> is the node number you want to allow.

--clear-allowed-nodes
   Clears all values for allowed nodes.

--add-allowed-nodes <integer>...
   Adds one or more nodes to the allowed nodes list. The value of <integer> is the
   node number you want to allow.

--remove-allowed-nodes <integer>...
   Removes one or more nodes from the allowed nodes list. The value of
   <integer> is the node number you want to remove.

--excluded-nodes <integer>...
   Specifies one or more nodes that are not allowed to send alerts through the
   channel. The value of <integer> is the node number you want to exclude.

--clear-excluded-nodes
   Clears all values for excluded nodes.

--add-excluded-nodes <integer>...
   Adds one or more nodes to the excluded nodes list. The value of <integer> is
   the node number you want to exclude.

--remove-excluded-nodes <integer>...
   Removes one or more nodes from the excluded nodes list. The value of
   <integer> is the node number you want to remove.

--address <string>...
   For SMTP channels only. Specifies one or more email addresses you want to
   receive alerts on this channel. The value of <string> is an email address.

--clear-address
   For SMTP channels only. Clears all values for email addresses.

--add-address <string>...
   For SMTP channels only. Specifies one or more email addresses you want to add
   to the alert distribution list for this channel. The value of <string> is an email
   address.

--remove-address <string>...
   For SMTP channels only. Specifies one or more email addresses you want to
   remove from the alert distribution list for this channel. The value of <string> is
   an email address.
--send-as <string>
For SMTP channels only. Specifies the email address you want to send alerts from on this channel. The value of <string> is an email address.

--subject <string>
For SMTP channels only. Specifies the subject line for emails sent on this channel.

--smtp-host <string>
For SMTP channels only. Specifies the SMTP relay host.

--smtp-port <integer>
For SMTP channels only. Specifies the SMTP relay port.

--smtp-use-auth {true | false}
For SMTP channels only. Enables or disables SMTP authentication.

--smtp-username <string>
For SMTP channels only. Specifies the username for SMTP authentication.

--smtp-password <string>
For SMTP channels only. Specifies the password for SMTP authentication.

--smtp-security {STARTTLS | NONE}
For SMTP channels only. Enables or disables SMTP encryption.

--batch {NONE | ALL | CATEGORY | SEVERITY}
For SMTP channels only. Specifies how SMTP alerts will be batched.

--batch-period <integer> <time>
For SMTP channels only. Specifies the interval between batched alerts. The following <time> values are valid:

Y
  Specifies years

M
  Specifies months

W
  Specifies weeks

D
  Specifies days

H
  Specifies hours

m
  Specifies minutes

s
  Specifies seconds

--host <string>
For SNMP channels only. Specifies the host name or address.

--community <string>
For SNMP channels only. Specifies the community string.

{--verbose | -v}
Displays more detailed information.

isi event channels view
Displays the details of a channel.

Syntax

isi event channels view <name>

Options

<name>
Specifies the name of the channel you want to view.

isi event events list
Displays all events.

Syntax

isi event events list
  [--eventgroup-id <name>]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]

Options

--eventgroup-id <name>
Displays events that are included in the specified event group.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
Displays table and CSV output without headers.

{ --no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.
**isi event events view**

Displays the details of an event.

**Syntax**

`isi event events view <id>`

**Options**

<id>

Specifies the instance ID of the event you want to view.

**isi event groups bulk**

Changes the status of all event groups.

**Syntax**

`isi event groups bulk`

```
[--ignore {true | false}]
[--resolved {true | false}]
[--verbose]
```

**Options**

--ignore {true | false}

Specifies whether all event groups have a status of ignored.

--resolved {true | false}

Specifies whether all event groups have a status of resolved.

After you resolve an event group, you cannot reverse that action. Any new events that would have been added to the resolved event group will be added to a new event group.

{--verbose | -v}

Displays more detailed information.

**isi event groups list**

Displays a list of all event groups.

**Syntax**

`isi event groups list`

```
[--begin <timestamp>]
[--end <timestamp>]
[--resolved {true | false}]
[--ignore {true | false}]
[--events <integer>]
[--cause <string>]
[--limit <integer>]
[--sort {id | started | causes_long | last_event | ignore | ignore_time | resolved | ended | events | severity}]
```
Options

{--begin | -b} <timestamp>
Filters the list to only show event groups that were created after the specified date and time.
Specify <timestamp> in the following format:

{--end | -e} <timestamp>
Filters the list to only show event groups that were created before the specified date and time.
Specify <timestamp> in the following format:

--resolved {true | false}
Specifies whether the list will show only event groups that are resolved, or not resolved.

--ignore {true | false}
Specifies whether the list will show only event groups that are ignored, or not ignored.

--events <integer>
Filters the list to only show event groups with the specified number of events recorded against the event group.

--cause <string>
Filters the list to only show event groups with the specified cause.

{--limit | -l} <integer>
Sets the maximum number of event groups to display.

--sort {id | started | causes_long | last_event | ignore | ignore_time | resolved | ended | events | severity}
Specifies the field to sort items by.

{--descending | -d}
Sorts the data in descending order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

**isi event groups modify**

Changes the status of an event group.

**Syntax**

```bash
isi event <id>
  [--ignore {true | false}]
  [--resolved {true | false}]
  [--verbose]
```

**Options**

<id>
Specifies the ID number of the event group you want to modify.

--ignore {true | false}
Specifies whether the event group has a status of ignored.

--resolved {true | false}
Specifies whether the event group has a status of resolved.
After you resolve an event group, you cannot reverse that action. Any new events that would have been added to the resolved event group will be added to a new event group.

{--verbose | -v}
Displays more detailed information.

**isi event groups view**

View the details of an event group.

**Syntax**

```bash
isi event groups view <id>
```

**Options**

<id>
Specifies the ID number of the event group you want to view.
isi event settings modify

Configures event storage settings.

Syntax

```
isiclass event settings modify
  [--retention-days <integer>]
  [--storage-limit <integer>]
  [--maintenance-start <timestamp>]
  [--clear-maintenance-start]
  [--maintenance-duration <duration>]
  [--heartbeat-interval <string>]
  [--verbose]
```

Options

```
{--retention-days | -r}<integer>
  Retention of resolved event group data in days.

{--storage-limit | -s}<integer>
  Sets the amount of memory that event data can occupy on your cluster. You can set this limit to be between 1 and 100 megabytes of memory. For smaller clusters, the minimum amount of memory that will be set aside is 1 gigabyte.

--maintenance-start <timestamp>
  Sets the start date and time of a maintenance window.
  Specify <timestamp> in the following format:

      <yyyy>-<mm>-<dd>[T<HH>:<MM>:<SS>]]

--clear-maintenance-start
  Clears the value for the start date and time of a maintenance window.

--maintenance-duration <integer> <time>
  Sets the duration of a maintenance window.
  The following <time> values are valid:

      Y
        Specifies years

      M
        Specifies months

      W
        Specifies weeks

      D
        Specifies days

      H
        Specifies hours

      m
        Specifies minutes
```
Specifies seconds

--heartbeat-interval <string>
  Sets the interval between heartbeat events.
  The following <time> values are valid:
  - daily
  - weekly
  - monthly

{--verbose | -v}
  Displays more detailed information.

**isi event settings view**

Displays event storage settings.

**Syntax**

```
isi event settings view
```

**isi event test create**

Creates a test alert.

**Syntax**

```
isi event test create <message>
  [--verbose]
```

**Options**

**<message>**

Specifies the message text of the test alert.

{--verbose | -v}

Displays more detailed information.

**Hardware commands**

You can check the status of your cluster hardware, including specific node components, through the hardware commands.

Most of the hardware commands are not applicable for IsilonSD Edge.
isi batterystatus list

Displays a list of batteries in the cluster by node, along with the status of each battery.

Syntax

```bash
isi batterystatus list
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
   Displays table and CSV output without headers.

{ --no-footer | -z}
   Displays table output without footers.

{ --verbose | -v}
   Displays more detailed information.

isi batterystatus view

Displays the status of a node's batteries.

Syntax

```bash
isi batterystatus view <id>
```

Options

--node-1nn <integer>
   Specifies the node you want to view. If omitted, battery status for the local node is displayed.

isi devices add

Defaults to isi devices drive add. Scans for available drives and adds the drives to the node.

Note

You can add available nodes to a cluster by running the command isi devices node add.
Syntax

isi devices add <bay>
    [--node-lnn <integer>]
    [--force]
    [--verbose]

Options

{<bay> | all}
    Specifies the bay number that contains the drive to be added to the node. You can specify all to scan the entire node.

--node-lnn <integer>
    Specifies the node number to scan for new drives. If omitted, the local node will be scanned.

{--force | -f}
    Adds the drive or drives without asking for confirmation.

{--verbose | -v}
    Displays more detailed information.

isi devices drive add

Scans for available drives and adds the drives to the node.

Syntax

isi devices drive add <bay>
    [--node-lnn <integer>]
    [--force]
    [--verbose]

Options

{<bay> | all}
    Specifies the bay number that contains the drive to be added to the node. You can specify all to scan the entire node.

--node-lnn <integer>
    Specifies the node number to scan for new drives. If omitted, the local node will be scanned.

{--force | -f}
    Adds the drive or drives without asking for confirmation.

{--verbose | -v}
    Displays more detailed information.
**isi devices drive firmware list**

Displays a list of firmware details for the data drives in a node.

**Syntax**

```
isi devices drive firmware list
   [--node-1nn <string>]
   [--summary]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

--node-1nn {all | <integer>}
   Specifies the node number of the drives you would like to display firmware information for. You may specify all nodes. If omitted, only the drive firmware information for the local node will be displayed.

{ --summary | -s}
   Displays a summary of drive firmware counts by model and revision.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
   Displays table and CSV output without headers.

{ --no-footer | -z}
   Displays table output without footers.

{--verbose | -v}
   Displays more detailed information.

**isi devices drive firmware update list**

Displays the status of firmware updates on the cluster.

**Syntax**

```
isi devices drive firmware update list
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
Displays table and CSV output without headers.

```
--no-footer | -z
```
Displays table output without footers.

```
--verbose | -v
```
Displays more detailed information.

**isi devices drive firmware update start**

Updates firmware on one or more drives in a node.

**Syntax**

```
isi devices drive firmware update start <bay>
    [--node-lnn <integer>]
    [--force]
    [--verbose]
```

**Options**

```
{<bay> | all}
```
Specifies the bay number that contains the drive to be updated. You can specify all to update every drive in the node.

```
--node-lnn <integer>
```
Specifies the node number on which to update drives. If omitted, drives will be updated in the local node.

```
{--force | -f}
```
Updates the drive or drives without asking for confirmation.

```
{--verbose | -v}
```
Displays more detailed information.

**isi devices drive firmware update view**

Displays information about a drive firmware update for a node.

**Syntax**

```
isi devices drive firmware update view
    [--node-lnn <integer>]
```

**Options**

```
--node-lnn <integer>
```
Specifies the LNN (logical node number) of the node that is running the firmware update you want to view. If omitted, firmware update status for the local node will be displayed.
isi devices drive firmware view

Displays information about the firmware on a single drive.

Syntax

```bash
isi devices drive firmware view {<bay> | --lnum <integer>}
   [--node-lnn <integer>]
```

Options

```
{<bay> | --lnum <integer>}
   Specifies the bay number or LNUM (logical drive number) of the drive to view.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you
   want to view. If omitted, the drive in the local node will be displayed.
```

isi devices drive format

Formats a drive so you can add it to a node.

Syntax

```bash
isi devices drive format <bay>
   [--node-lnn <integer>]
   [--purpose <string>]
   [--force]
   [--verbose]
```

Options

```
<bay>
   Specifies the bay number that contains the drive to be formatted.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you
   want to format. If omitted, the specified drive in the local node will be formatted.

--purpose <string>
   Specifies the purpose to assign to the new drive. You can view a list of the
   possible drive purposes by running isi devices drive purposelist. If
   omitted, OneFS will automatically assign the drive purpose.

{--force | -f}
   Formats the drive without asking for confirmation.

{--verbose | -v}
   Displays more detailed information.
```
**isi devices drive list**

Displays a list of data drives in a node.

**Syntax**

```bash
isi devices drive list
    [--node-lnn <string>]
    [--override]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

--node-lnn {all | <integer>}
  Specifies the node number of the drives you would like to display. You may specify all nodes. If omitted, only the drives in the local node will be displayed.

{--override | -V}
  Displays legacy bay numbers instead of grid values.

--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
  Displays table and CSV output without headers.

{--no-footer | -z}
  Displays table output without footers.

{--verbose | -v}
  Displays more detailed information.

**isi devices drive purpose**

Assigns a use case to a drive. For example, you can designate a drive for normal data storage operations, or you can designate the drive for L3 caching instead of storage.

**Syntax**

```bash
isi devices drive purpose {<bay> | --lnum <integer>} --purpose <string>
    [--node-lnn <integer>]
    [--force]
    [--verbose]
```

**Options**

{<bay> | --lnum <integer>}
  Specifies the bay number or LNUM (logical drive number) of the drive to assign.

--purpose <string>
Specifies the purpose to assign to the drive. You can view a list of the possible drive purposes by running `isi devices drive purposelist`.

`--node-lnn <integer>`
Specifies the LNN (logical node number) of the node that contains the drive you want to assign. If omitted, the specified drive in the local node will be assigned.

`{--force | -f}`
Forms the drive without asking for confirmation.

`{--verbose | -v}`
Displays more detailed information.

### isi devices drive purposelist

Displays a list of possible use cases for drives. For example, you may be able to designate a drive for normal data storage operations, or you can designate the drive for L3 caching instead of storage.

**Syntax**

```bash
isi devices drive purposelist
    [--node-lnn <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
```

**Options**

`--node-lnn <integer>`
Specifies the LNN (logical node number) of the node that you want to view the purpose list for. If omitted, the purpose list of the local node will display.

`--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{ --no-header | -a}`
Displays table and CSV output without headers.

`{ --no-footer | -z}`
Displays table output without footers.

### isi devices drive smartfail

Smartfails a drive so you can remove it from a node.

**Syntax**

```bash
isi devices drive smartfail {<bay> | --lnum <integer>}
    [--node-lnn <integer>]
    [--force]
    [--verbose]
```
Options

{<bay> | --lnum <integer>}
   Specifies the bay number or LNUM (logical drive number) of the drive to smartfail.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you want to smartfail. If omitted, the specified drive in the local node will be smartfailed.

{--force | -f}
   Smartfails the drive without asking for confirmation.

{--verbose | -v}
   Displays more detailed information.

**isi devices drive stopfail**

Discontinues the smartfail process on a drive.

**Syntax**

```
isi devices drive stopfail {<bay> | --lnum <integer>}
   [--node-lnn <integer>]
   [--force]
   [--verbose]
```

Options

{<bay> | --lnum <integer>}
   Specifies the bay number or LNUM (logical drive number) of the drive to discontinue smartfailing.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you want to discontinue smartfailing. If omitted, the specified drive in the local node will be discontinue smartfailing.

{--force | -f}
   Discontinues smartfailing the drive without asking for confirmation.

{--verbose | -v}
   Displays more detailed information.

**isi devices drive suspend**

Temporarily suspends all activities for a drive.

**Syntax**

```
isi devices drive suspend {<bay> | --lnum <integer>}
   [--node-lnn <integer>]
   [--force]
   [--verbose]
```
Options

{<bay> | --lnum <integer>}
   Specifies the bay number or LNUM (logical drive number) of the drive to suspend.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you want to suspend. If omitted, the specified drive in the local node will be suspended.

{--force | -f}
   Smartfails the drive without asking for confirmation.

{--verbose | -v}
   Displays more detailed information.

isi devices drive view

Displays information about a single drive.

Syntax

    isi devices drive view {<bay> | --lnum <integer>}
      [--node-lnn <integer>]

Options

{<bay> | --lnum <integer>}
   Specifies the bay number or LNUM (logical drive number) of the drive to view.

--node-lnn <integer>
   Specifies the LNN (logical node number) of the node that contains the drive you want to view. If omitted, the drive in the local node will be displayed.

isi devices firmware list

Defaults to isi devices drive firmware list. Displays a list of firmware details for the data drives in a node.

Syntax

    isi devices firmware list
      [--node-lnn <string>]
      [--summary]
      [--format {table | json | csv | list}]
      [--no-header]
      [--no-footer]
      [--verbose]

Options

--node-lnn {all | <integer>}
Specifies the node number of the drives you would like to display firmware information for. You may specify all nodes. If omitted, only the drive firmware information for the local node will be displayed.

```{--summary | -s}
  Displays a summary of drive firmware counts by model and revision.
```

```--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
```

```{--no-header | -a}
  Displays table and CSV output without headers.
```

```{--no-footer | -z}
  Displays table output without footers.
```

```{--verbose | -v}
  Displays more detailed information.
```

**isi devices firmware update list**

Defaults to **isi devices drive firmware update list**. Displays the status of drive firmware updates on the cluster.

**Syntax**

```
isi devices firmware update list
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]
```

**Options**

```--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
```

```{--no-header | -a}
  Displays table and CSV output without headers.
```

```{--no-footer | -z}
  Displays table output without footers.
```

```{--verbose | -v}
  Displays more detailed information.
```
isi devices firmware update start

Defaults to isi devices drive firmware update start. Updates firmware on one or more drives in a node.

Syntax

```bash
isi devices firmware update start <bay>
    [--node-lnn <integer>]
    [--force]
    [--verbose]
```

Options

```
{<bay> | all}
  Specifies the bay number that contains the drive to be updated. You can specify all to update every drive in the node.

--node-lnn <integer>
  Specifies the node number on which to update drives. If omitted, drives will be updated in the local node.

{--force | -f}
  Updates the drive or drives without asking for confirmation.

{--verbose | -v}
  Displays more detailed information.
```

isi devices firmware update view

Defaults to isi devices drive firmware update view. Displays information about a drive firmware update for a node.

Syntax

```bash
isi devices firmware update view
    [--node-lnn <integer>]
```

Options

```
--node-lnn <integer>
  Specifies the LNN (logical node number) of the node that is running the firmware update you want to view. If omitted, firmware update status for the local node will be displayed.
```
### isi devices firmware view

Defaults to `isi devices drive firmware view`. Displays information about the firmware on a single drive.

**Syntax**

```bash
isi devices firmware view {<bay> | --lnum <integer>}
[--node-lnn <integer>]
```

**Options**

```
{<bay> | --lnum <integer>}
```

Specifies the bay number or LNUM (logical drive number) of the drive to view.

```
--node-lnn <integer>
```

Specifies the LNN (logical node number) of the node that contains the drive you want to view. If omitted, the drive in the local node will be displayed.

### isi devices format

Defaults to `isi devices drive format`. Formats a drive so you can add it to a node.

**Syntax**

```bash
isi devices format <bay>
[--node-lnn <integer>]
[--purpose <string>]
[--force]
[--verbose]
```

**Options**

```
<bay>
```

Specifies the bay number that contains the drive to be formatted.

```
--node-lnn <integer>
```

Specifies the LNN (logical node number) of the node that contains the drive you want to format. If omitted, the specified drive in the local node will be formatted.

```
--purpose <string>
```

Specifies the purpose to assign to the new drive. You can view a list of the possible drive purposes by running `isi devices drive purposelist`. If omitted, OneFS will automatically assign the drive purpose.

```
{--force | -f}
```

Formats the drive without asking for confirmation.

```
{--verbose | -v}
```

Displays more detailed information.
isi devices list

Defaults to isi devices drive list. Displays a list of data drives in a node.

Note

You can display nodes that are available to join the cluster by running the command isi devices node list.

Syntax

```
isi devices list
    [--node-lnn <string>]
    [--override]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

```
--node-lnn {all | <integer>}
    Specifies the node number of the drives you would like to display. You may specify all nodes. If omitted, only the drives in the local node will be displayed.

{ --override | -V }
    Displays legacy bay numbers instead of grid values.

--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a }
    Displays table and CSV output without headers.

{ --no-footer | -z }
    Displays table output without footers.

{ --verbose | -v }
    Displays more detailed information.
```

isi devices node add

Joins an available node to the cluster.

Syntax

```
isi devices node add <serial-number>
    [--force]
    [--verbose]
```

Options

```
<serial-number>
    Specifies the serial number of the node you want to add to the cluster.
```
### isi devices node list

Displays a list of nodes that are available to join the cluster.

**Syntax**

```
isi devices node list
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

- **--format** `{table | json | csv | list}`
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

- **--no-header | -a**
  Displays table and CSV output without headers.

- **--no-footer | -z**
  Displays table output without footers.

- **--verbose | -v**
  Displays more detailed information.

### isi devices node smartfail

Smartfails a node and removes it from the cluster.

**Syntax**

```
isi devices node smartfail
   [--node-lln <integer>]
   [--force]
   [--verbose]
```

**Options**

- **--node-lln <integer>**
  Specifies the LNN (logical node number) of the node that you want to smartfail. If omitted, the local node will be smartfailed.

- **--force | -f**
  Smartfails the drive without asking for confirmation.

- **--verbose | -v**
  Displays more detailed information.
isi devices node stopfail

Discontinues the smartfail process on a node.

Syntax

```
isi devices node stopfail
  [--node-lnn <integer>]
  [--force]
  [--verbose]
```

Options

```
--node-lnn <integer>
  Specifies the LNN (logical node number) of the node that you want to
discontinue smartfailing. If omitted, the local node will discontinue smartfailing.
```

```
{--force | -f}
  Discontinues smartfailing the drive without asking for confirmation.
```

```
{--verbose | -v}
  Displays more detailed information.
```

isi devices purpose

Defaults to `isi devices drive purpose`. Assigns a use case to a drive. For example, you can designate a drive for normal data storage operations, or you can designate the drive for L3 caching instead of storage.

Syntax

```
isi devices purpose {<bay> | --lnum <integer>} --purpose <string>
  [--node-lnn <integer>]
  [--force]
  [--verbose]
```

Options

```
{<bay> | --lnum <integer>}
  Specifies the bay number or LNUM (logical drive number) of the drive to assign.
```

```
--purpose <string>
  Specifies the purpose to assign to the drive. You can view a list of the possible
drive purposes by running `isi devices drive purposelist`.
```

```
--node-lnn <integer>
  Specifies the LNN (logical node number) of the node that contains the drive you
want to assign. If omitted, the specified drive in the local node will be assigned.
```

```
{--force | -f}
  Formats the drive without asking for confirmation.
```

```
{--verbose | -v}
  Displays more detailed information.
```
isi devices purposelist

Defaults to `isi devices drive purposelist`. Displays a list of possible use cases for drives. For example, you may be able to designate a drive for normal data storage operations, or you can designate the drive for L3 caching instead of storage.

**Syntax**

```
isi devices purposelist
    [--node-lnn <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
```

**Options**

`--node-lnn <integer>`

Specifies the LNN (logical node number) of the node that you want to view the purpose list for. If omitted, the purpose list of the local node will display.

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{ --no-header | -a }`

Displays table and CSV output without headers.

`{ --no-footer | -z }`

Displays table output without footers.

isi devices smartfail

Defaults to `isi devices drive smartfail`. Smartfails a drive so you can remove it from a node.

**Note**

You can smartfail a node by running the command `isi devices node smartfail`.

**Syntax**

```
isi devices smartfail {[bay] | --lnum <integer>}
    [--node-lnn <integer>]
    [--force]
    [--verbose]
```

**Options**

`{[bay] | --lnum <integer>}`

Specifies the bay number or LNUM (logical drive number) of the drive to smartfail.

`--node-lnn <integer>`
Specifies the LNN (logical node number) of the node that contains the drive you want to smartfail. If omitted, the specified drive in the local node will be smartfailed.

`|--force | -f`
Smartfails the drive without asking for confirmation.

`|--verbose | -v`
Displays more detailed information.

isi devices stopfail

Defaults to `isi devices drive stopfail`. Discontinues the smartfail process on a drive.

**Note**

You can discontinue the smartfail process on a node by running the command `isi devices node stopfail`.

**Syntax**

```
isi devices stopfail {<bay> | --lnum <integer>}
[--node-lnn <integer>]
[--force]
[--verbose]
```

**Options**

`{<bay> | --lnum <integer>}`

Specifies the bay number or LNUM (logical drive number) of the drive to discontinue smartfailing.

`--node-lnn <integer>`

Specifies the LNN (logical node number) of the node that contains the drive you want to discontinue smartfailing. If omitted, the specified drive in the local node will be discontinue smartfailing.

`|--force | -f`

Discontinues smartfailing the drive without asking for confirmation.

`|--verbose | -v`

Displays more detailed information.

isi devices suspend

Defaults to `isi devices drive suspend`. Temporarily suspends all activities for a drive.

**Syntax**

```
isi devices suspend {<bay> | --lnum <integer>}
[--node-lnn <integer>]
```
Options

\{<bay> | --lnum <integer>\}
Specifies the bay number or LNUM (logical drive number) of the drive to suspend.

--node-lnn <integer>
Specifies the LNN (logical node number) of the node that contains the drive you want to suspend. If omitted, the specified drive in the local node will be suspended.

\{--force | -f\}
Smartfails the drive without asking for confirmation.

\{--verbose | -v\}
Displays more detailed information.

**isi devices view**

Defaults to isi devices drive view. Displays information about a single drive.

**Syntax**

```
isi devices view {<bay> | --lnum <integer>}
     [--node-lnn <integer>]
```

**Options**

\{<bay> | --lnum <integer>\}
Specifies the bay number or LNUM (logical drive number) of the drive to view.

--node-lnn <integer>
Specifies the LNN (logical node number) of the node that contains the drive you want to view. If omitted, the drive in the local node will be displayed.

**isi readonly list**

Displays a list of read-only status by node.

**Syntax**

```
isir readonly list
[--format {table | json | csv | list}]
     [--no-header]
     [--no-footer]
     [--verbose]
```

**Options**

--format \{table | json | csv | list\}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}
  Displays table and CSV output without headers.

{ --no-footer | -z}
  Displays table output without footers.

{--verbose | -v}
  Displays more detailed information.

**isi readonly modify**

Modifies a node's read-only status.

**Syntax**

isi readonly modify
  [--allowed <boolean>]
  [--enabled <boolean>]
  [--node-lnn <string>]
  [--verbose]

**Options**

--allowed <boolean>
  Changes the current read-only mode allowed status for a node.

--enabled <boolean>
  Changes the current read-only user mode status for a node.

---

**Note**

This parameter only sets user-specified requests for read-only mode. If read-only mode is not allowed, the node remains in read/write until read-only mode is allowed. If the node has been placed in read-only mode by OneFS, it will remain in read-only mode until the conditions that triggered read-only mode have cleared.

--node-lnn {all | <integer>}
  Specifies the node on which you want to modify read-only status. You may specify all nodes. If omitted, only the local node will be modified.

{--verbose | -v}
  Displays more detailed information.

**isi readonly view**

Displays the read-only status of a node.

**Syntax**

isi readonly view
  [--node-lnn <integer>]

---
**Options**

`--node-lnn <integer>`

Specifies the node you want to view. If omitted, read-only status for the local node is displayed.

**isi servicelight list**

Displays a list of service LEDs in the cluster by node, along with the status of each service LED.

**Syntax**

```
isi servicelight list
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{- --no-header | -a}`

Displays table and CSV output without headers.

`{- --no-footer | -z}`

Displays table output without footers.

`{--verbose | -v}`

Displays more detailed information.

**isi servicelight modify**

Turns a node's service LED on or off.

**Syntax**

```
isi servicelight modify
    [--enabled <boolean>]
    [--node-lnn <integer>]
    [--verbose]
```

**Options**

`--enabled <boolean>`

Enables or disables a node's service LED.

`--node-lnn <integer>`

Specifies the node on which you want to modify the service light status. If omitted, the local node will be used.

`{--verbose | -v}`
Displays more detailed information.

**isi servicelight view**

Displays the status of a node's service LED.

**Syntax**

`isi servicelight view
[--node-lnn <integer>]`

**Options**

`--node-lnn <integer>`

Specifies the node you want to view. If omitted, service LED status for the local node is displayed.
CHAPTER 5

Access zones

This section contains the following topics:

- Access zones overview ................................................................. 216
- Base directory guidelines ............................................................. 216
- Access zones best practices ........................................................ 217
- Access zone limits ........................................................................ 218
- Quality of service ........................................................................ 218
- Managing access zones ............................................................... 219
- Access zone commands ............................................................... 222
Access zones overview

Although the default view of an EMC Isilon cluster is that of one physical machine, you can partition a cluster into multiple virtual containers called access zones. Access zones allow you to isolate data and control who can access data in each zone.

Access zones support configuration settings for authentication and identity management services on a cluster, so you can configure authentication providers and provision protocol directories such as SMB shares and NFS exports on a zone-by-zone basis. When you create an access zone, a local provider is automatically created, which allows you to configure each access zone with a list of local users and groups. You can also authenticate through a different authentication provider in each access zone.

To control data access, you associate the access zone with a groupnet, which is a top-level networking container that manages DNS client connection settings and contains subnets and IP address pools. When you create an access zone, you must specify a groupnet. If a groupnet is not specified, the access zone will reference the default groupnet. Multiple access zones can reference a single groupnet. You can direct incoming connections to the access zone through a specific IP address pool in the groupnet. Associating an access zone with an IP address pool restricts authentication to the associated access zone and reduces the number of available and accessible SMB shares and NFS exports.

An advantage to multiple access zones is the ability to configure audit protocol access for individual access zones. You can modify the default list of successful and failed protocol audit events and then generate reports through a third-party tool for an individual access zone.

A cluster includes a built-in access zone named System where you manage all aspects of a cluster and other access zones. By default, all cluster IP addresses connect to the System zone. Role-based access, which primarily allows configuration actions, is available through only the System zone. All administrators, including those given privileges by a role, must connect to the System zone to configure a cluster. The System zone is automatically configured to reference the default groupnet on the cluster, which is groupnet0.

Configuration management of a non-System access zone is not permitted through SSH, the OneFS Platform API, or the web administration interface. However, you can create and delete SMB shares in an access zone through the Microsoft Management Console (MMC).

Base directory guidelines

A base directory defines the file system tree exposed by an access zone. The access zone cannot grant access to any files outside of the base directory. You must assign a base directory to each access zone.

Base directories restrict path options for several features such as SMB shares, NFS exports, the HDFS root directory, and the local provider home directory template. The base directory of the default System access zone is /ifs and cannot be modified.

To achieve data isolation within an access zone, EMC recommends creating a unique base directory path that is not identical to or does not overlap another base directory, with the exception of the System access zone. For example, do not specify /ifs/data/hr as the base directory for both the zone2 and zone3 access zones, or
if /ifs/data/hr is assigned to zone2, do not assign /ifs/data/hr/personnel to zone3.

OneFS supports overlapping data between access zones for cases where your workflows require shared data; however, this adds complexity to the access zone configuration that might lead to future issues with client access. For the best results from overlapping data between access zones, EMC recommends that the access zones also share the same authentication providers. Shared providers ensures that users will have consistent identity information when accessing the same data through different access zones.

If you cannot configure the same authentication providers for access zones with shared data, EMC recommends the following best practices:

- Select Active Directory as the authentication provider in each access zone. This causes files to store globally unique SIDs as the on-disk identity, eliminating the chance of users from different zones gaining access to each other's data.
- Avoid selecting local, LDAP, and NIS as the authentication providers in the access zones. These authentication providers use UIDs and GIDs, which are not guaranteed to be globally unique. This results in a high probability that users from different zones will be able to access each other's data.
- Set the on-disk identity to native, or preferably, to SID. When user mappings exist between Active Directory and UNIX users or if the Services for Unix option is enabled for the Active Directory provider, OneFS stores SIDs as the on-disk identity instead of UIDs.

### Access zones best practices

You can avoid configuration problems on the EMC Isilon cluster when creating access zones by following best practices guidelines.

<table>
<thead>
<tr>
<th>Best practice</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create unique base directories.</td>
<td>To achieve data isolation, the base directory path of each access zone should be unique and should not overlap or be nested inside the base directory of another access zone. Overlapping is allowed, but should only be used if your workflows require shared data.</td>
</tr>
<tr>
<td>Separate the function of the System zone from other access zones.</td>
<td>Reserve the System zone for configuration access, and create additional zones for data access. Move current data out of the System zone and into a new access zone.</td>
</tr>
<tr>
<td>Create access zones to isolate data access for different clients or users.</td>
<td>Do not create access zones if a workflow requires data sharing between different classes of clients or users.</td>
</tr>
<tr>
<td>Assign only one authentication provider of each type to each access zone.</td>
<td>An access zone is limited to a single Active Directory provider; however, OneFS allows multiple LDAP, NIS, and file authentication providers in each access zone. It is recommended that you assign only one type of each provider per access zone in order to simplify administration.</td>
</tr>
</tbody>
</table>
Avoid overlapping UID or GID ranges for authentication providers in the same access zone.
The potential for zone access conflicts is slight but possible if overlapping UIDs/GIDs are present in the same access zone.

### Access zone limits

You can follow access zone limits guidelines to help size the workloads on the OneFS system.

If you configure multiple access zones on an EMC Isilon cluster, limits guidelines are recommended for optimal system performance. The limits described in the *EMC Isilon Guidelines for Large Workloads* publication are recommended for heavy enterprise workflows on a cluster, treating each access zone as a separate physical machine.

### Quality of service

You can set upper bounds on quality of service by assigning specific physical resources to each access zone.

Quality of service addresses physical hardware performance characteristics that can be measured, improved, and sometimes guaranteed. Characteristics measured for quality of service include but are not limited to throughput rates, CPU usage, and disk capacity. When you share physical hardware in an EMC Isilon cluster across multiple virtual instances, competition exists for the following services:

- CPU
- Memory
- Network bandwidth
- Disk I/O
- Disk capacity

Access zones do not provide logical quality of service guarantees to these resources, but you can partition these resources between access zones on a single cluster. The following table describes a few ways to partition resources to improve quality of service:

<table>
<thead>
<tr>
<th>Use</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICs</td>
<td>You can assign specific NICs on specific nodes to an IP address pool that is associated with an access zone. By assigning these NICs, you can determine the nodes and interfaces that are associated with an access zone. This enables the separation of CPU, memory, and network bandwidth. If you are running IsilonSD Edge, the port group manages the NICs on the IsilonSD nodes. For more information on port group configuration, see the <em>IsilonSD Edge Installation and Administration Guide</em>.</td>
</tr>
<tr>
<td>Use</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SmartPools</td>
<td>SmartPools are separated by node hardware equivalence classes, usually into multiple tiers of high, medium, and low performance. The data written to a SmartPool is written only to the disks in the nodes of that pool. Associating an IP address pool with only the nodes of a single SmartPool enables partitioning of disk I/O resources.</td>
</tr>
<tr>
<td>SmartQuotas</td>
<td>Through SmartQuotas, you can limit disk capacity by a user or a group or in a directory. By applying a quota to an access zone's base directory, you can limit disk capacity used in that access zone.</td>
</tr>
</tbody>
</table>

**Managing access zones**

You can create access zones on the EMC Isilon cluster, view and modify access zone settings, and delete access zones.

**Create an access zone**

You can create an access zone to isolate data and restrict which users can access the data.

**Procedure**

1. Run the `isi zone zones create` command.

   The following command creates an access zone named `zone3` and sets the base directory to `/ifs/hr/data`:

   ```
   isi zone zones create zone3 /ifs/hr/data
   ```

   The following command creates an access zone named `zone3`, sets the base directory to `/ifs/hr/data` and creates the directory on the EMC Isilon cluster if it does not already exist:

   ```
   isi zone zones create zone3 /ifs/hr/data --create-path
   ```

   The following command creates an access zone named `zone3`, sets the base directory to `/ifs/hr/data`, and associates the access zone with `groupnet2`:

   ```
   isi zone zones create zone3 /ifs/hr/data --groupnet=groupnet2
   ```
Assign an overlapping base directory

You can create overlapping base directories between access zones for cases where your workflows require shared data.

Procedure

1. Run the `isi zone zones create` command.

   The following command creates an access zone named `zone5` and sets the base directory to `/ifs/hr/data` even though the same base directory was set for `zone3`:

   ```
   isi zone zones create zone5 --path=/ifs/hr/data --force-overlap
   ```

Manage authentication providers in an access zone

You modify an access zone to add and remove authentication providers. When you add an authentication provider, it must belong to the same groupnet referenced by the access zone. When you remove an authentication provider from an access zone, the provider is not removed from the system and remains available for future use.

The order in which authentication providers are added to access zone designates the order in which providers are searched during authentication and user lookup.

Procedure

1. To add an authentication provider, run the `isi zone zones modify` command with the `--add-auth-providers` option.

   You must specify the name of the authentication provider in the following format: `<provider-type>:<provider-name>`.

   The following command adds a file authentication provider named `HR-Users` to the `zone3` access zone:

   ```
   isi zone zones modify zone3 --add-auth-providers=file:hr-users
   ```

2. To remove an authentication provider, run the `isi zone zones modify` command with the `--remove-auth-providers` option.

   You must specify the name of the authentication provider in the following format: `<provider-type>:<provider-name>`.

   The following command removes the file authentication provider named `HR-Users` from the `zone3` access zone:

   ```
   isi zone zones modify zone3 --remove-auth-providers=file:hr-users
   ```

   The following command removes all authentication providers from the `zone3` access zone:

   ```
   isi zone zones modify zone3 --clear-auth-providers
   ```
Associate an IP address pool with an access zone

You can associate an IP address pool with an access zone to ensure that clients can connect to the access zone only through the range of IP addresses assigned to the pool.

Before you begin

The IP address pool must belong to the same groupnet referenced by the access zone.

Procedure

1. Run the `isi network pools modify` command.
   
   Specify the pool ID you want to modify in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>`

   The following command associates zone3 with pool1 which is under groupnet1 and subnet1:

   ```
   isi network pools modify groupnet1.subnet1.pool1 --access-zone=zone3
   ```

Modify an access zone

You can modify the properties of any access zone except the name of the built-in System zone.

Procedure

1. Run the `isi zone zones modify` command.

   The following command renames the zone3 access zone to zone5 and removes all current authentication providers from the access zone:

   ```
   isi zone zones modify zone3 --name=zone5 --clear-auth-providers
   ```

Delete an access zone

You can delete any access zone except the built-in System zone. When you delete an access zone, all associated authentication providers remain available to other access zones, but IP addresses are not reassigned to other access zones. SMB shares, NFS exports, and HDFS data paths are deleted when you delete an access zone; however, the directories and data still exist, and you can map new shares, exports, or paths in another access zone.

Procedure

1. Run the `isi zone zones delete` command.

   The following command deletes the zone3 access zone:

   ```
   isi zone zones delete zone3
   ```
View a list of access zones

You can view a list of all access zones on the EMC Isilon cluster, or you can view details for a specific access zone.

Procedure

1. To view a list of all access zones on the cluster, run the `isi zone zones list` command.

   The system displays output similar to the following example:

   ```
   Name   Path
   ------------------------
   System /ifs
   zone3  /ifs/hr/benefits
   zone5  /ifs/marketing/collateral
   ------------------------
   ```

2. To view the details of a specific access zone, run the `isi zone zones view` command and specify the zone name.

   The following command displays the setting details of zone5:

   ```
   isi zone zones view zone5
   ```

   The system displays output similar to the following example:

   ```
   Name: zone5
   Path: /ifs/marketing/collateral
   Groupnet: groupnet0
   Map Untrusted: -
   Auth Providers: lsa-local-provider:zone5
   NetBIOS Name: -
   User Mapping Rules: -
   Home Directory Umask: 0077
   Skeleton Directory: /usr/share/skel
   Cache Entry Expiry: 4H
   Zone ID: 3
   ```

Access zone commands

You can configure and manage access zones through access zone commands.

isi zone restrictions create

Prohibits user or group access to the `/ifs` directory. Attempts to read or write files by restricted users or groups return ACCESS DENIED errors.

Syntax

```
isi zone restrictions create <zone> {<user> | --uid <integer> |
| --group <string> | --gid <integer> | --sid <string> |
| --wellknown <string>}
[--verbose]
```
Options
<zone>
   Specifies an access zone by name.

<user>
   Specifies a user by name.

--uid <integer>
   Specifies a user by UID.

--group <string>
   Specifies a group by name.

--gid <integer>
   Specifies a group by GID.

--sid <string>
   Specifies an object by user or group SID.

--wellknown <name>
   Specifies a well-known user, group, machine, or account name.

{---verbose | -v}
   Returns a success or fail message after running the command.

isi zone restrictions delete

Removes a restriction that prohibits user or group access to the /ifs directory.

Syntax

isi zone restrictions delete <zone> {<user> | --uid <integer>
   | --group <string> | --gid <integer> | --sid <string>
   | --wellknown <string>} --force
   [+--verbose]
Specifies an object by user or group SID.

--wellknown <string>
Specifies an object by well-known SID.

{--force | -f}
Suppresses command-line prompts and messages.

{--verbose | -v}
Returns a success or fail message after running the command.

isi zone restrictions list
Displays a list of users or groups that are prohibited from accessing the /ifs directory.

Syntax

```bash
isi zone restrictions list <zone>
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

Options

<zone>
Specifies an access zone by name.

{--limit | -l} <integer>
Displays no more than the specified number of items.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

Examples

To display a list of restricted users for the built-in System zone, run the following command:

```bash
isi zone restrictions list system
```
isi zone zones create

Creates an access zone.

Syntax

```
isi zone zones create <name> <path>
  [--map-untrusted <workgroup>]
  [--auth-providers <provider-type>:<provider-name>]
  [--netbios-name <string>]
  [--user-mapping-rules <string>]
  [--home-directory-umask <integer>]
  [--skeleton-directory <string>]
  [--cache-entry-expiry <duration>]
  [--create-path]
  [--force-overlap]
  [--groupnet <groupnet>]
  [--verbose]
```

Options

`<name>`
  Specifies the name of the access zone.

`<path>`
  Specifies the base directory path for the zone.

`--map-untrusted <workgroup>`
  Maps untrusted domains to the specified NetBIOS workgroup during authentication.

`--auth-providers <provider-type>:<provider-name>`
  Specifies one or more authentication providers, separated by commas, for authentication to the access zone. Authentication providers are checked in the order specified. You must specify the name of the authentication provider in the following format: <provider-type>:<provider-name>.

`--netbios-name <string>`
  Specifies the NetBIOS name.

`--user-mapping-rules <string>`
  Specifies one or more user mapping rules, separated by commas, for the access zone.

`--home-directory-umask <integer>`
  Specifies the permissions to set on auto-created user home directories.

`--skeleton-directory <string>`
  Sets the skeleton directory for user home directories.

`--cache-entry-expiry <duration>`
  Specifies duration of time to cache a user/group.

`--create-path`
  Specifies that the value entered as the access zone path is to be created if it does not already exist.
--force-overlap
Allows the base directory to overlap with the base directory of another access zone.

--groupnet <string>
Specifies the groupnet referenced by the access zone.

{--verbose | -v}
Displays the results of running the command.

isi zone zones delete
Deletes an access zone. All authentication providers that are associated with the access zone remain available to other zones, but IP addresses are not reassigned. You cannot delete the built-in System zone.

Syntax

isi zone zones delete <zone>
    [--force]
    [--verbose]

Options

<zone>
    Specifies the name of the access zone to delete.

{--force | -f}
    Suppresses command-line prompts and messages.

{--verbose | -v}
    Displays the results of running the command.

isi zone zones list
Displays a list of access zones in the cluster.

Syntax

isi zone zones list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]

Options

{--limit | -l} <integer>
    Displays no more than the specified number of items.

--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
Displays table and CSV output without headers.

Displays table output without footers.

Displays more detailed information.

Examples
To view a list of all access zones in the cluster, run the following command:

```bash
isi zone zones list
```

**isi zone zones modify**

Modifies an access zone.

**Syntax**

```
isi zone zones modify <zone>
  [--name <string>]
  [--path <path>]
  [--map-untrusted <string>]
  [--auth-providers <provider-type>:<provider-name>]
  [--clear-auth-providers]
  [--remove-auth-providers <provider-type>:<provider-name>]
  [--netbios-name <string>]
  [--user-mapping-rules <string>]
  [--clear-user-mapping-rules]
  [--add-user-mapping-rules <string>]
  [--remove-user-mapping-rules <string>]
  [--skeleton-directory <string>]
  [--cache-entry-expiry <duration>]
  [--revert-cache-entry-expiry]
  [--create-path]
  [--force-overlap]
  [--verbose]
```

**Options**

- **<zone>**
  Specifies the name of the access zone to modify.

- **--name <string>**
  Specifies a new name for the access zone. You cannot change the name of the built-in System access zone.

- **--path <path>**
  Specifies the base directory path for the zone.

- **--map-untrusted <string>**
  Specifies the NetBIOS workgroup to map untrusted domains to during authentication.

- **--auth-providers <provider-type>:<provider-name>**
  Specifies the authentication providers for the access zone.

- **--clear-auth-providers**
  Clears all authentication providers for the access zone.

- **--remove-auth-providers <provider-type>:<provider-name>**
  Removes an authentication provider from the access zone.

- **--netbios-name <string>**
  Specifies the NetBIOS workgroup name for the access zone.

- **--user-mapping-rules <string>**
  Specifies the user mapping rules for the access zone.

- **--clear-user-mapping-rules**
  Clears all user mapping rules for the access zone.

- **--add-user-mapping-rules <string>**
  Adds user mapping rules to the access zone.

- **--remove-user-mapping-rules <string>**
  Removes user mapping rules from the access zone.

- **--skeleton-directory <string>**
  Specifies the skeleton directory for the access zone.

- **--cache-entry-expiry <duration>**
  Specifies the cache entry expiration duration for the access zone.

- **--revert-cache-entry-expiry**
  Reverts the cache entry expiration for the access zone.

- **--create-path**
  Creates the specified path for the access zone.

- **--force-overlap**
  Forces the zone to overlap with other zones.

- **--verbose**
  Displays more detailed information.
Specifies one or more authentication providers, separated by commas, for authentication to the access zone. This option overwrites any existing entries in the authentication providers list. To add or remove providers without affecting the current entries, configure settings for --add-auth-providers or --remove-auth-providers.

--clear-auth-providers
Removes all authentication providers from the access zone.

--add-auth-providers <provider-type>:<provider-name>
Adds one or more authentication providers, separated by commas, to the access zone.

--remove-auth-providers <provider-type>:<provider-name>
Removes one or more authentication providers, separated by commas, from the access zone.

--netbios-name <string>
Specifies the NetBIOS name.

--user-mapping-rules <string>
Specifies one or more user mapping rules, separated by commas, for the access zone. This option overwrites all entries in the user mapping rules list. To add or remove mapping rules without overwriting the current entries, configure settings with --add-user-mapping-rules or --remove-user-mapping-rules.

--clear-user-mapping-rules
Removes all user mapping rules from the access zone.

--add-user-mapping-rules <string>
Adds one or more user mapping rules, separated by commas, to the access zone.

--remove-user-mapping-rules <string>
Removes one or more user mapping rules, separated by commas, from the access zone.

--home-directory-umask <integer>
Specifies the permissions to set on auto-created user home directories.

--skeleton-directory <string>
Sets the skeleton directory for user home directories.

--cache-entry-expiry <duration>
Specifies duration of time to cache a user/group.

--cache-entry-expiry
Sets the value of --cache-entry-expiry to the system default.

--create-path
Specifies that the zone path is to be created if it doesn't already exist.

--force-overlap
Allows the base directory to overlap with the base directory of another access zone.

{--verbose | -v}
Displays the results of running the command.

**isi zone zones view**

Displays the properties of an access zone.

**Syntax**

```bash
isi zone zones view <zone>
```

**Options**

`<zone>`

Specifies the name of the access zone to view.
Access zones
CHAPTER 6
Authentication

This section contains the following topics:

- Authentication overview ................................................................. 232
- Authentication provider features .................................................. 232
- Supported authentication providers ............................................. 232
- Active Directory ................................................................. 233
- LDAP .................................................................................... 234
- NIS ............................................................................... 234
- Kerberos authentication ............................................................. 235
- File provider ........................................................................ 236
- Local provider ........................................................................ 236
- Managing Active Directory providers ........................................ 237
- Managing LDAP providers .......................................................... 238
- Managing NIS providers .............................................................. 240
- Managing MIT Kerberos authentication ..................................... 240
- Managing file providers .............................................................. 249
- Managing local users and groups ................................................ 253
- Authentication and access control commands ........................... 258
Authentication overview

OneFS supports local and remote authentication providers to verify that users attempting to access an EMC Isilon cluster are who they claim to be. Anonymous access, which does not require authentication, is supported for protocols that allow it.

OneFS supports concurrent multiple authentication provider types, which are analogous to directory services. For example, OneFS is often configured to authenticate Windows clients with Active Directory and to authenticate UNIX clients with LDAP. You can also configure NIS, designed by Sun Microsystems, to authenticate users and groups when they access a cluster.

Note

OneFS is RFC 2307-compliant.

Authentication provider features

You can configure authentication providers for your environment.

Authentication providers support a mix of the features described in the following table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>All authentication providers support plain-text authentication. You can configure some providers to support NTLM or Kerberos authentication also.</td>
</tr>
<tr>
<td>Users and groups</td>
<td>OneFS provides the ability to manage users and groups directly on the cluster.</td>
</tr>
<tr>
<td>Netgroups</td>
<td>Specific to NFS, netgroups restrict access to NFS exports.</td>
</tr>
<tr>
<td>UNIX-centric user and group properties</td>
<td>Login shell, home directory, UID, and GID. Missing information is supplemented by configuration templates or additional authentication providers.</td>
</tr>
<tr>
<td>Windows-centric user and group properties</td>
<td>NetBIOS domain and SID. Missing information is supplemented by configuration templates.</td>
</tr>
</tbody>
</table>

Supported authentication providers

You can configure local and remote authentication providers to authenticate or deny user access to an EMC Isilon cluster.

The following table compares features that are available with each of the authentication providers that OneFS supports. In the following table, an x indicates that a feature is fully supported by a provider; an asterisk (*) indicates that additional configuration or support from another provider is required.
Active Directory

Active Directory is a Microsoft implementation of Lightweight Directory Access Protocol (LDAP), Kerberos, and DNS technologies that can store information about network resources. Active Directory can serve many functions, but the primary reason for joining the cluster to an Active Directory domain is to perform user and group authentication.

You can join the EMC Isilon cluster to an Active Directory (AD) domain by specifying the fully qualified domain name, which can be resolved to an IPv4 or an IPv6 address, and a user name with join permission. When the cluster joins an AD domain, a single AD machine account is created. The machine account establishes a trust relationship with the domain and enables the cluster to authenticate and authorize users in the Active Directory forest. By default, the machine account is named the same as the cluster. If the cluster name is more than 15 characters long, the name is hashed and displayed after joining the domain.

OneFS supports NTLM and Microsoft Kerberos for authentication of Active Directory domain users. NTLM client credentials are obtained from the login process and then presented in an encrypted challenge/response format to authenticate. Microsoft Kerberos client credentials are obtained from a key distribution center (KDC) and then presented when establishing server connections. For greater security and performance, we recommend that you implement Kerberos, according to Microsoft guidelines, as the primary authentication protocol for Active Directory.

Each Active Directory provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the Active Directory provider will use when communicating with external servers. The groupnet associated with the Active Directory provider cannot be changed. Instead you must delete the Active Directory provider and create it again with the new groupnet association.

You can add an Active Directory provider to an access zone as an authentication method for clients connecting through the access zone. OneFS supports multiple instances of Active Directory on an Isilon cluster; however, you can assign only one Active Directory provider per access zone. The access zone and the Active Directory provider must reference the same groupnet. Configure multiple Active Directory instances only to grant access to multiple sets of mutually-untrusted domains. Otherwise, configure a single Active Directory instance if all domains have a trust

<table>
<thead>
<tr>
<th>Authentication provider</th>
<th>NTLM</th>
<th>Kerberos</th>
<th>User/group management</th>
<th>Netgroups</th>
<th>UNIX properties (RFC 2307)</th>
<th>Windows properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>x</td>
<td>x</td>
<td>*</td>
<td></td>
<td>*</td>
<td>x</td>
</tr>
<tr>
<td>LDAP</td>
<td>*</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>NIS</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIT Kerberos</td>
<td>x</td>
<td></td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
relationship. You can discontinue authentication through an Active Directory provider by removing the provider from associated access zones.

**LDAP**

The Lightweight Directory Access Protocol (LDAP) is a networking protocol that enables you to define, query, and modify directory services and resources.

OneFS can authenticate users and groups against an LDAP repository in order to grant them access to the cluster. OneFS supports Kerberos authentication for an LDAP provider.

The LDAP service supports the following features:

- Users, groups, and netgroups.
- Configurable LDAP schemas. For example, the ldapsam schema allows NTLM authentication over the SMB protocol for users with Windows-like attributes.
- Simple bind authentication, with and without SSL.
- Redundancy and load balancing across servers with identical directory data.
- Multiple LDAP provider instances for accessing servers with different user data.
- Encrypted passwords.
- IPv4 and IPv6 server URIs.

Each LDAP provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the LDAP provider will use when communicating with external servers. The groupnet associated with the LDAP provider cannot be changed. Instead you must delete the LDAP provider and create it again with the new groupnet association.

You can add an LDAP provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one LDAP provider. The access zone and the LDAP provider must reference the same groupnet. You can discontinue authentication through an LDAP provider by removing the provider from associated access zones.

**NIS**

The Network Information Service (NIS) provides authentication and identity uniformity across local area networks. OneFS includes an NIS authentication provider that enables you to integrate the cluster with your NIS infrastructure.

NIS, designed by Sun Microsystems, can authenticate users and groups when they access the cluster. The NIS provider exposes the passwd, group, and netgroup maps from an NIS server. Hostname lookups are also supported. You can specify multiple servers for redundancy and load balancing.

Each NIS provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the NIS provider will use when communicating with external servers. The groupnet associated with the NIS provider cannot be changed. Instead you must delete the NIS provider and create it again with the new groupnet association.

You can add an NIS provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one NIS provider. The access zone and the NIS provider must reference the same groupnet.
You can discontinue authentication through an NIS provider by removing the provider from associated access zones.

**Note**

NIS is different from NIS+, which OneFS does not support.

## Kerberos authentication

Kerberos is a network authentication provider that negotiates encryption tickets for securing a connection. OneFS supports Microsoft Kerberos and MIT Kerberos authentication providers on an EMC Isilon cluster. If you configure an Active Directory provider, support for Microsoft Kerberos authentication is provided automatically. MIT Kerberos works independently of Active Directory.

For MIT Kerberos authentication, you define an administrative domain known as a realm. Within this realm, an authentication server has the authority to authenticate a user, host, or service; the server can resolve to either IPv4 or IPv6 addresses. You can optionally define a Kerberos domain to allow additional domain extensions to be associated with a realm.

The authentication server in a Kerberos environment is called the Key Distribution Center (KDC) and distributes encrypted tickets. When a user authenticates with an MIT Kerberos provider within a realm, an encrypted ticket with the user's service principal name (SPN) is created and validated to securely pass the user's identification for the requested service.

Each MIT Kerberos provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the Kerberos provider will use when communicating with external servers. The groupnet associated with the Kerberos provider cannot be changed. Instead you must delete the Kerberos provider and create it again with the new groupnet association.

You can add an MIT Kerberos provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one MIT Kerberos provider. The access zone and the Kerberos provider must reference the same groupnet. You can discontinue authentication through an MIT Kerberos provider by removing the provider from associated access zones.

## Keytabs and SPNs overview

A Key Distribution Center (KDC) is an authentication server that stores accounts and keytabs for users connecting to a network service within an EMC Isilon cluster. A keytab is a key table that stores keys to validate and encrypt Kerberos tickets.

One of the fields in a keytab entry is a service principal name (SPN). An SPN identifies a unique service instance within a cluster. Each SPN is associated with a specific key in the KDC. Users can use the SPN and its associated keys to obtain Kerberos tickets that enable access to various services on the cluster. A member of the SecurityAdmin role can create new keys for the SPNs and modify them later as necessary. An SPN for a service typically appears as `<service>/<fqdn>@<realm>`. 

Authentication

Kerberos authentication

Keytabs and SPNs overview

235
SPNs must match the SmartConnect zone name and the FQDN hostname of the cluster. If the SmartConnect zone settings are changed, you must update the SPNs on the cluster to match the changes.

MIT Kerberos protocol support

MIT Kerberos supports certain standard network communication protocols such as HTTP, HDFS, and NFS. MIT Kerberos does not support SMB, SSH, and FTP protocols.

For the NFS protocol support, MIT Kerberos must be enabled for an export and also a Kerberos provider must be included within the access zone.

File provider

A file provider enables you to supply an authoritative third-party source of user and group information to an EMC Isilon cluster. A third-party source is useful in UNIX and Linux environments that synchronize /etc/passwd, /etc/group, and etc/netgroup files across multiple servers.

Standard BSD /etc/spwd.db and /etc/group database files serve as the file provider backing store on a cluster. You generate the spwd.db file by running the pwd_mkdb command in the OneFS command-line interface (CLI). You can script updates to the database files.

On an Isilon cluster, a file provider hashes passwords with libcrypt. For the best security, we recommend that you use the Modular Crypt Format in the source /etc/passwd file to determine the hashing algorithm. OneFS supports the following algorithms for the Modular Crypt Format:

- MD5
- NT-Hash
- SHA-256
- SHA-512

For information about other available password formats, run the man 3 crypt command in the CLI to view the crypt man pages.

Local provider

The local provider provides authentication and lookup facilities for user accounts added by an administrator.

Local authentication is useful when Active Directory, LDAP, or NIS directory services are not configured or when a specific user or application needs access to the cluster.

Local groups can include built-in groups and Active Directory groups as members.

In addition to configuring network-based authentication sources, you can manage local users and groups by configuring a local password policy for each node in the cluster.
OneFS settings specify password complexity, password age and re-use, and password-attempt lockout policies.

Managing Active Directory providers

You can view, configure, modify, and delete Active Directory providers. OneFS includes a Kerberos configuration file for Active Directory in addition to the global Kerberos configuration file, both of which you can configure through the command-line interface. You can discontinue authentication through an Active Directory provider by removing it from all access zones that are using it.

Configure an Active Directory provider

You can configure one or more Active Directory providers, each of which must be joined to a separate Active Directory domain. By default, when you configure an Active Directory provider, it is automatically added to the System access zone.

Note

Consider the following information when you configure an Active Directory (AD) provider:

- When you join Active Directory from OneFS, cluster time is updated from the Active Directory server, as long as an NTP server has not been configured for the cluster.
- If you migrate users to a new or different Active Directory domain, you must re-set the ACL domain information after you configure the new provider. You can reset the domain information with third-party tools, such as Microsoft SubInACL.
- The Active Directory provider must be associated with a groupnet.
- The Active Directory domain can be resolved to an IPv4 or an IPv6 address.

Procedure

1. Run the `isi auth ads create` command to create an Active Directory provider by specifying the domain name of the Active Directory server and the name of an AD user that has permission to join machines to the AD domain.

   The following command specifies adserver.company.com as the fully-qualified domain name of the Active Directory server to be created in the system, specifies "administrator" as the AD user that has permission to join the cluster to the AD domain, and associates the provider with groupnet3:

   ```bash
   isi auth ads create --name=adserver.company.com \   --user=administrator --groupnet=groupnet3
   ```
Modify an Active Directory provider

You can modify the advanced settings for an Active Directory provider.

Procedure

1. Run the following command to modify an Active Directory provider, where
   `<provider-name>` is a placeholder for the name of the provider that you want to modify.

   ```bash
   isi auth ads modify <provider-name>
   ```

Delete an Active Directory provider

When you delete an Active Directory provider, you disconnect the cluster from the
Active Directory domain that is associated with the provider, disrupting service for
users who are accessing it. After you leave an Active Directory domain, users can no
longer access the domain from the cluster.

Procedure

1. Run the following command to Delete an Active Directory provider, where
   `<name>` is a placeholder for the Active Directory name that you want to delete.

   ```bash
   isi auth ads delete <name>
   ```

Managing LDAP providers

You can view, configure, modify, and delete LDAP providers. You can discontinue
authentication through an LDAP provider by removing it from all access zones that are
using it.

Configure an LDAP provider

By default, when you configure an LDAP provider, it is automatically added to the
System access zone.

Procedure

1. Run the `isi auth ldap create` command to create an LDAP provider.

   The following command creates an LDAP provider called test-ldap and
   associates it with groupnet3. The command also sets a base distinguished
   name, which specifies the root of the tree in which to search for identities, and
   specifies ldap://2001:DB8:170:7cff::c001 as the server URI:

   ```bash
   isi auth ldap create test-ldap \
   --base-dn="dc=test-ldap,dc=example,dc=com" \
   --server-uris="ldap://[2001:DB8:170:7cff::c001]" \
   --groupnet=groupnet3
   ```
Note

The base distinguished name is specified as a sequence of relative distinguished name values, separated by commas. Specify a base distinguished name if the LDAP server allows anonymous queries.

The following command creates an LDAP provider called test-ldap and associates it with groupnet3. It also specifies a bind distinguished name and bind password, which are used to join the LDAP server, and specifies ldap:// test-ldap.example.com as the server URI:

```
isi auth ldap create test-ldap \
  --base-dn="dc=test-ldap,dc=example,dc=com" \ 
  --bind-dn="cn=test,ou=users,dc=test-ldap,dc=example,dc=com" \ 
  --bind-password="mypasswd" \ 
  --server-uris="ldap://test-ldap.example.com" \ 
  --groupnet=groupnet3
```

Note

The bind distinguished name is specified as a sequence of relative distinguished name values, separated by commas, and must have the proper permissions to join the LDAP server to the cluster. Specify a bind distinguished name if the LDAP server does not allow anonymous queries.

Modify an LDAP provider

You can modify any setting for an LDAP provider except its name. You must specify at least one server for the provider to be enabled.

Procedure

1. Run the following command to modify an LDAP provider, where `<provider-name>` is a placeholder for the name of the provider that you want to modify:

```
isi auth ldap modify <provider-name>
```

Delete an LDAP provider

When you delete an LDAP provider, it is removed from all access zones. As an alternative, you can stop using an LDAP provider by removing it from each access zone that contains it so that the provider remains available for future use.

For information about the parameters and options that are available for this procedure, run the `isi auth ldap delete --help` command.

Procedure

1. Run the following command to delete an LDAP provider, where `<name>` is a placeholder for the name of the LDAP provider that you want to delete.

```
isiauth ldap delete <name>
```
Managing NIS providers

You can view, configure, and modify NIS providers or delete providers that are no longer needed. You can discontinue authentication through an NIS provider by removing it from all access zones that are using it.

Configure an NIS provider

You can configure multiple NIS providers, each with its own settings, and add them to one or more access zones.

Procedure

1. Configure an NIS provider by running the `isi auth nis create` command.

   The following example creates an NIS provider called nistest that is associated with groupnet3, specifies nistest.company.com as the NIS server and company.com as the domain:

   ```
   isi auth nis create nistest --groupnet=groupnet3\n   --servers="nistest.example.com" --nis-domain="example.com"
   ```

Modify an NIS provider

You can modify any setting for an NIS provider except its name. You must specify at least one server for the provider to be enabled.

Procedure

1. Run the following command to modify an NIS provider, where `<provider-name>` is a placeholder for provider that you want to modify.

   ```
   isi auth nis modify <provider-name>
   ```

Delete an NIS provider

When you delete an NIS provider, it is removed from all access zones. As an alternative, you can stop using an NIS provider by removing it from each access zone that contains it, so that the provider remains available for future use.

Procedure

1. Run the following command to delete an NIS provider, where `<name>` is a placeholder for the name of the NIS provider that you want to delete.

   ```
   isi auth nis delete <name>
   ```

Managing MIT Kerberos authentication

You can configure an MIT Kerberos provider for authentication without Active Directory. Configuring an MIT Kerberos provider involves creating an MIT Kerberos realm, creating a provider, and joining a predefined realm. Optionally, you can configure an MIT Kerberos domain for the provider. You can also update the
encryption keys if there are any configuration changes to the Kerberos provider. You can include the provider in one or more access zones.

Managing MIT Kerberos realms

An MIT Kerberos realm is an administrative domain that defines the boundaries within which an authentication server has the authority to authenticate a user or service. You can create, view, edit, or delete a realm. As a best practice, specify a realm name using uppercase characters.

Create an MIT Kerberos realm

You can create an MIT Kerberos realm by defining a Key Distribution Center (KDC) and an administrative server.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to create an MIT Kerberos realm.

Procedure

1. Run the `isi auth krb5 realm create` command to create an MIT Kerberos realm.

   The following command creates an MIT Kerberos realm called TEST.COMPANY.COM, specifies admin.test.company.com as the administrative server, and specifies keys.test.company.com as a key distribution center:

   ```bash
   isi auth krb5 realm create --realm=TEST.COMPANY.COM --kdc=keys.test.company.com --admin-server=admin.test.company.com
   ```

   The realm name is case-sensitive and must be specified in uppercase letters. The administrative server and key distribution center can be specified as an IPv4 address, an IPv6 address, or a hostname.

Modify an MIT Kerberos realm

You can modify an MIT Kerberos realm by modifying the Key Distribution Center (KDC), the domain (optional), and the administrative server settings for that realm.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to delete an MIT Kerberos provider.

Procedure

1. Run the `isi auth krb5 realm modify` command to modify an MIT Kerberos realm.

   The following command modifies the MIT Kerberos realm called TEST.COMPANY.COM by adding a KDC specified as an IPv6 address:

   ```bash
   isi auth krb5 realm modify --realm=TEST.COMPANY.COM --kdc=2001:DB8:170:7cfd::c001
   ```
The realm name is case-sensitive and must be specified in uppercase letters. The key distribution center can be specified as an IPv4 address, an IPv6 address, or a host name.

**View an MIT Kerberos realm**

You can view details related to the name, Key Distribution Centers (KDCs), and the administrative server associated with an MIT Kerberos realm.

**Procedure**

1. To view a list of all Kerberos realms configured on the cluster, run the `isi auth krb5 realm list` command.
   
The system displays output similar to the following example:

   ```plaintext
   Realm
   -------------------
   TEST.COMPANY.COM
   ENGKERB.COMPANY.COM
   OPSKERB.COMPANY.COM
   -------------------
   Total: 3
   ```

2. To view the setting details for a specific Kerberos realm, run the `isi auth krb5 realm view` command followed by the realm name.
   
The specified realm name is case-sensitive.
   
The following command displays setting details for the realm called TEST.COMPANY.COM:

   ```plaintext
   isi auth krb realm view TEST.COMPANY.COM
   ```

   The systems displays output similar to the following example:

   ```plaintext
   Realm: TEST.COMPANY.COM
   Is Default Realm: Yes
   KDC: 2001:DB8:170:7cff::c001,
   keys.test.company.com
   Admin Server: admin.test.company.com
   ```

   **Note**

   The KDC and the admin server can be specified as an IPv4 or IPv6 address, or a hostname.

**Delete an MIT Kerberos realm**

You can delete one or more MIT Kerberos realms and all the associated MIT Kerberos domains.

**Before you begin**

Kerberos realms are referenced by Kerberos providers. Before you can delete a realm for which you have created a provider, you must first delete that provider.
You must be a member of a role that has ISI_PRIV_AUTH privileges to delete an MIT Kerberos realm.
Procedure

1. Run the `isi auth krb5 realm delete` command to delete an MIT Kerberos realm.

   For example, run the following command to delete a realm:

   ```
   isi auth krb5 realm delete <realm>
   ```

Managing MIT Kerberos providers

You can create view, delete, or modify an MIT Kerberos provider. You can also configure the Kerberos provider settings.

Creating an MIT Kerberos provider

You can create an MIT Kerberos provider by obtaining the credentials for accessing a cluster through the Key Distribution Center (KDC) of the Kerberos realm. This process is also known as joining a realm. Thus when you create a Kerberos provider you also join a realm that has been previously defined.

Depending on how OneFS manages your Kerberos environment, you can create a Kerberos provider through one of the following methods:

- Accessing the Kerberos administration server and creating keys for services on the OneFS cluster.
- Manually transferring the Kerberos key information in the form of keytabs.

Create an MIT Kerberos provider and join a realm with administrator credentials

You can create an MIT Kerberos provider and join an MIT Kerberos realm using the credentials authorized to access the Kerberos administration server. You can then create keys for the various services on the EMC Isilon cluster. This is the recommended method for creating a Kerberos provider and joining a Kerberos realm.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to access the Kerberos administration server.

Procedure

1. Run the `isi auth krb5 create` command to create a Kerberos provider and join a Kerberos realm; where `<realm>` is the name of the Kerberos realm which already exists or is created if it does not exist:

   The realm name is case-sensitive and must be specified in uppercase letters.

   In the following example command, the Kerberos realm TEST.COMPANY.COM is created and joined to the provider, which is associated with groupnet3. The command also specifies admin.test.company.com as the administrative server and keys.test.company.com as the KDC, and specifies a username and password that are authorized to access to the administration server:

   ```
   isi auth krb5 create --realm=TEST.COMPANY.COM \
   --user=administrator --password=secretcode \
   --kdc=keys.test.company.com
   ```
Create an MIT Kerberos provider and join a realm with a keytab file

You can create an MIT Kerberos provider and join an MIT Kerberos realm through a keytab file. Follow this method only if your Kerberos environment is managed by manually transferring the Kerberos key information through the keytab files.

Before you begin

Make sure that the following prerequisites are met:

- The Kerberos realm must already exist on the cluster
- A keytab file must exist on the cluster.
- You must be a member of a role that has ISI_PRIV_AUTH privileges to access the Kerberos administration server.

Procedure

1. Run the `isi auth krb5 create` command.

   The following command creates a Kerberos provider that is associated with groupnet3, joins the Kerberos realm called `cluster-name.company.com` and specifies a keytab file located at `/tmp/krb5.keytab`:

   ```bash
   isi auth krb5 create cluster-name.company.com \ 
   --keytab-file=/tmp/krb5.keytab --groupnet=groupnet3
   ```

View an MIT Kerberos provider

You can view the properties of an MIT Kerberos provider after creating it.

Procedure

1. Run the following command to view the properties of a Kerberos provider:

   ```bash
   isi auth krb5 view <provider-name>
   ```

List the MIT Kerberos providers

You can list one or more MIT Kerberos providers and display the list in a specific format. You can also specify a limit for the number of providers to be listed.

Procedure

1. Run the `isi auth krb5 list` command to list one or more Kerberos providers.
For example, run the following command to list the first five Kerberos providers in a tabular format without any headers or footers:

```
isi auth krb5 list -l 5 --format table --no-header --no-footer
```

Delete an MIT Kerberos provider

You can delete an MIT Kerberos provider and remove it from all the referenced access zones. When you delete a provider, you also leave an MIT Kerberos realm.

**Before you begin**

You must be a member of a role that has ISI_PRIV_AUTH privileges to delete a Kerberos provider.

**Procedure**

1. Run the `isi auth krb5 delete` command as follows to delete a Kerberos provider.

```
isi auth krb5 delete <provider-name>
```

Configure MIT Kerberos provider settings

You can configure the settings of a Kerberos provider to allow the DNS records to locate the Key Distribution Center (KDC), Kerberos realms, and the authentication servers associated with a Kerberos realm. These settings are global to all Kerberos users across all nodes, services, and zones. Some settings are applicable only to client-side Kerberos and are independent of the Kerberos provider.

**Before you begin**

You must be a member of a role that has ISI_PRIV_AUTH privileges to view or modify the settings of a Kerberos provider.

**Procedure**

1. Run the `isi auth settings krb5` command with the `view` or `modify` subcommand.
   2. Specify the settings to modify.

Managing MIT Kerberos domains

You can optionally define MIT Kerberos domains to allow additional domain extensions to be associated with an MIT Kerberos realm. You can always specify a default domain for a realm.

You can create, modify, delete, and view an MIT Kerberos domain. A Kerberos domain name is a DNS suffix that you specify typically using lowercase characters.

Add an MIT Kerberos domain to a realm

You can optionally add an MIT Kerberos domain to an MIT Kerberos realm to enable additional Kerberos domain extensions to be associated with a Kerberos realm.

**Before you begin**

You must be a member of a role that has ISI_PRIV_AUTH privileges to associate a Kerberos domain with a Kerberos realm.
Procedure

1. Add a Kerberos domain by running the `isi auth krb5 domain create` command.

   For example, run the following command to add a Kerberos domain to a Kerberos realm:

   ```
   isi auth krb5 domain create <domain>
   ```

Modify an MIT Kerberos domain

You can modify an MIT Kerberos domain by modifying the realm settings.

Before you begin

You must be a member of a role that has `ISI_PRIV_AUTH` privileges to modify an MIT Kerberos domain.

Procedure

1. Run the `isi auth krb5 domain modify` command to modify a Kerberos domain.

   For example, run the following command to modify a Kerberos domain by specifying an alternate Kerberos realm:

   ```
   isi auth krb5 domain modify <domain> --realm <realm>
   ```

View an MIT Kerberos domain mapping

You can view the properties of an MIT Kerberos domain mapping.

Procedure

1. Run the `isi auth krb5 domain view` command with a value specified for the `<domain>` variable to view the properties of a Kerberos domain mapping:

   ```
   isi auth krb5 domain view <domain>
   ```

List MIT Kerberos domains

You can list one or more MIT Kerberos domains and display the list in a tabular, JSON, CSV, or list format. You can also specify a limit for the number of domains to be listed.

Procedure

1. Run the `isi auth krb5 domain list` command to list one or more MIT Kerberos domains.

   For example, run the following command to list the first ten MIT Kerberos domains in a tabular format without any headers or footers:

   ```
   isi auth krb5 domain list -l=10 --format=table --no-header --no-footer
   ```
Delete an MIT Kerberos domain mapping

You can delete one or more MIT Kerberos domain mappings.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to delete an MIT Kerberos domain mapping.

Procedure

1. Run the `isi auth krb5 domain delete` command to delete an MIT Kerberos domain mapping.

   For example, run the following command to delete a domain mapping:

   ```bash
   isi auth krb5 domain delete <domain>
   ```

Managing SPNs and keys

A service principal name (SPN) is the name referenced by a client to identify an instance of a service on an EMC Isilon cluster. An MIT Kerberos provider authenticates services on a cluster through SPNs.

You can perform the following operations on SPNs and their associated keys:

- Update the SPNs if there are any changes to the SmartConnect zone settings that are based on those SPNs
- List the registered SPNs to compare them against a list of discovered SPNs
- Update keys associated with the SPNs either manually or automatically
- Import keys from a keytab table
- Delete specific key versions or delete all the keys associated with an SPN

View SPNs and keys

You can view the service principal names (SPNs) and their associated keys that are registered for an MIT Kerberos provider. Clients obtain Kerberos tickets and access services on EMC Isilon clusters through SPNs and their associated keys.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to view SPNs and keys.

Procedure

1. Run the `isi auth krb5 spn list` command to list one or more SPNs and their associated keys and the Key version numbers (Kvnos).

   For example, run the following command to list the first five SPNs for an MIT Kerberos provider in a tabular format without any headers or footers:

   ```bash
   isi auth krb5 list <provider-name> -l 5 --format table --no-header --no-footer <spn-list>
   ```
Delete keys

You can delete specific key versions or all the keys associated with a service principal name (SPN).

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to delete keys.

After creating new keys due to security reasons or to match configuration changes, follow this procedure to delete older version of the keys so that the keytab table is not populated with redundant keys.

Procedure

1. Run the `isi auth krb5 spn delete` command to delete all keys for a specified SPN or a specific version of a key.

   For example, run the following command to delete all the keys associated with an SPN for an MIT Kerberos provider:

   ```
   isi auth krb5 spn delete <provider-name> <spn> --all
   ```

   The `<provider-name>` is the name of the MIT Kerberos provider. You can delete a specific version of the key by specifying a key version number value for the `kvno` argument and including that value in the command syntax.

Manually add or update a key for an SPN

You can manually add or update keys for a service principal name (SPN). This process creates a new key for the specified SPN.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to add or update a key for an SPN.

Procedure

1. Run the `isi auth krb5 spn create` command to add or update keys for an SPN.

   For example, run the following command to add or update a key for an SPN by specifying the `<provider-name>`, `<user>`, and `<spn>` positional arguments:

   ```
   isi auth krb5 spn create <provider-name> <user> <spn>
   ```

Automatically update an SPN

You can automatically update or add a service principal name (SPN) if it is registered with an MIT Kerberos provider but does not appear in the list of discovered SPNs.

Before you begin

You must be a member of a role that has ISI_PRIV_AUTH privileges to automatically update an SPN.

Procedure

1. Run the `isi auth krb5 spn check` command to compare the list of registered SPNs against the list of discovered SPNs.
Proceed to the next step if the comparison does not show similar results.

2. Run the `isi auth krb5 spn fix` command to fix the missing SPNs.

   For example, run the following command to add missing SPNs for an MIT Kerberos service provider:

   ```
   isi auth krb5 spn fix <provider-name> <user>
   ```

   You can optionally specify a password for `<user>` which is the placeholder for a user who has the permission to join clients to the given domain.

**Import a keytab file**

An MIT Kerberos provider joined through a legacy keytab file might not have the ability to manage keys through the Kerberos admin credentials. In such a case, import a new keytab file and then add the keytab file keys to the provider.

**Before you begin**

Make sure that the following pre-requisites are met before you import a keytab file:

- You must create and copy a keytab file to a node on the cluster where you will perform this procedure.
- You must be a member of a role that has ISI_PRIV_AUTH privileges to import a keytab file.

**Procedure**

1. Import the keys of a keytab file by running the `isi auth krb5 spn import` command.

   For example, run the following command to import the keys of the `<keytab-file>` to the provider referenced as `<provider-name>`:

   ```
   isi auth krb5 spn import <provider-name> <keytab-file>
   ```

**Managing file providers**

You can configure one or more file providers, each with its own combination of replacement files, for each access zone. Password database files, which are also called user database files, must be in binary format.

Each file provider pulls directly from up to three replacement database files: a group file that has the same format as `/etc/group`; a netgroups file; and a binary password file, `spwd.db`, which provides fast access to the data in a file that has the `/etc/master.passwd` format. You must copy the replacement files to the cluster and reference them by their directory path.

**Note**

If the replacement files are located outside the `/ifs` directory tree, you must distribute them manually to every node in the cluster. Changes that are made to the system provider's files are automatically distributed across the cluster.
Configure a file provider

You can specify replacement files for any combination of users, groups, and netgroups.

Procedure

1. Run the following command to configure a file provider, where `<name>` is your name for the file provider.

   ```
   isi auth file create <name>
   ```

Generate a password file

Password database files, which are also called user database files, must be in binary format.

This procedure must be performed through the command-line interface (CLI). For command-usage guidelines, run the `man pwd_mkdb` command.

Procedure

1. Establish an SSH connection to any node in the cluster.
2. Run the `pwd_mkdb `<file>` command, where `<file>` is the location of the source password file.

   ```
   Note
   By default, the binary password file, `spwd.db`, is created in the `/etc` directory. You can override the location to store the `spwd.db` file by specifying the `-d` option with a different target directory.
   ```

   The following command generates an `spwd.db` file in the `/etc` directory from a password file that is located at `/ifs/test.passwd`:

   ```
   pwd_mkdb /ifs/test.passwd
   ```

   The following command generates an `spwd.db` file in the `/ifs` directory from a password file that is located at `/ifs/test.passwd`:

   ```
   pwd_mkdb -d /ifs /ifs/test.passwd
   ```

Modify a file provider

You can modify any setting for a file provider, including its name.

Note

Although you can rename a file provider, there are two caveats: you can rename a file provider through only the web administration interface and you cannot rename the System file provider.
**Procedure**

1. Run the following command to modify a file provider, where `<provider-name>` is a placeholder for the name that you supplied for the provider.

   ```bash
   isi auth file modify <provider-name>
   ```

**Delete a file provider**

To stop using a file provider, you can clear all of its replacement file settings or you can permanently delete the provider.

**Note**

You cannot delete the System file provider.

**Procedure**

1. Run the following command to delete a file provider, where `<name>` is a placeholder for the name of the provider that you want to delete.

   ```bash
   isi auth file delete <name>
   ```

**Password file format**

The file provider uses a binary password database file, `spwd.db`. You can generate a binary password file from a `master.passwd`-formatted file by running the `pwd_mkdb` command.

The `master.passwd` file contains ten colon-separated fields, as shown in the following example:

```
admin:*:10:10::0:0:Web UI Administrator:/ifs/home/admin:/bin/zsh
```

The fields are defined below in the order in which they appear in the file.

**Note**

UNIX systems often define the `passwd` format as a subset of these fields, omitting the Class, Change, and Expiry fields. To convert a file from `passwd` to `master.passwd` format, add `:0:0:` between the GID field and the Gecos field.

**Username**

The user name. This field is case-sensitive. OneFS does not limit the length; many applications truncate the name to 16 characters, however.

**Password**

The user’s encrypted password. If authentication is not required for the user, you can substitute an asterisk (*) for a password. The asterisk character is guaranteed to not match any password.

**UID**

The UNIX user identifier. This value must be a number in the range 0-4294967294 that is not reserved or already assigned to a user. Compatibility issues occur if this value conflicts with an existing account’s UID.
**GID**

The group identifier of the user’s primary group. All users are a member of at least one group, which is used for access checks and can also be used when creating files.

**Class**

This field is not supported by OneFS and should be left empty.

**Change**

OneFS does not support changing the passwords of users in the file provider. This field is ignored.

**Expiry**

OneFS does not support the expiration of user accounts in the file provider. This field is ignored.

**Gecos**

This field can store a variety of information but is usually used to store the user’s full name.

**Home**

The absolute path to the user’s home directory, beginning at /ifs.

**Shell**

The absolute path to the user’s shell. If this field is set to /sbin/nologin, the user is denied command-line access.

---

**Group file format**

The file provider uses a group file in the format of the /etc/group file that exists on most UNIX systems.

The group file consists of one or more lines containing four colon-separated fields, as shown in the following example:

```
admin:*:10:root,admin
```

The fields are defined below in the order in which they appear in the file.

**Group name**

The name of the group. This field is case-sensitive. Although OneFS does not limit the length of the group name, many applications truncate the name to 16 characters.

**Password**

This field is not supported by OneFS and should contain an asterisk (*).

**GID**

The UNIX group identifier. Valid values are any number in the range 0-4294967294 that is not reserved or already assigned to a group. Compatibility issues occur if this value conflicts with an existing group's GID.

**Group members**

A comma-delimited list of user names.
Netgroup file format

A netgroup file consists of one or more netgroups, each of which can contain members. Hosts, users, or domains, which are members of a netgroup, are specified in a member triple. A netgroup can also contain another netgroup.

Each entry in a netgroup file consists of the netgroup name, followed by a space-delimited set of member triples and nested netgroup names. If you specify a nested netgroup, it must be defined on a separate line in the file.

A member triple takes the following form:

\[
(\texttt{<host>}, \texttt{<user>}, \texttt{<domain>})
\]

Where \texttt{<host>} is a placeholder for a machine name, \texttt{<user>} is a placeholder for a user name, and \texttt{<domain>} is a placeholder for a domain name. Any combination is valid except an empty triple: \texttt{()},.

The following sample file contains two netgroups. The rootgrp netgroup contains four hosts: two hosts are defined in member triples and two hosts are contained in the nested othergrp netgroup, which is defined on the second line.

```bash
rootgrp (myserver, root, somedomain.com) (otherserver, root, somedomain.com)
othergrp
othergrp (other-win,, somedomain.com) (other-linux,, somedomain.com)
```

**Note**

A new line signifies a new netgroup. You can continue a long netgroup entry to the next line by typing a backslash character (\) in the right-most position of the first line.

Managing local users and groups

When you create an access zone, each zone includes a local provider that allows you to create and manage local users and groups. Although you can view the users and groups of any authentication provider, you can create, modify, and delete users and groups in the local provider only.

View a list of users and groups by provider

You can view users and groups by a provider type.

**Procedure**

1. Run the following command to view a list of users and groups for a specified provider, where \texttt{<provider-type>} is a placeholder for your provider-type string and \texttt{<provider-name>} is a placeholder for the name that you assigned the specific provider:

   ```bash
   isi auth users list --provider="<provider-type>:\<provider-name>"
   ```
2. To list users and groups for an LDAP provider type that is named Unix LDAP, run a command similar to the following example:

```bash
isi auth users list --provider="lsa-ldap-provider:Unix LDAP"
```

Create a local user

Each access zone includes a local provider that allows you to create and manage local users and groups. When creating a local user account, you can configure its name password, home directory, UNIX user identifier (UID), UNIX login shell, and group memberships.

Procedure

1. Run the following command to create a local user, where `<name>` is your name for the user, `<provider-name>` specifies the provider for this user, and `<string>` is the password for this user.

```bash
isi auth users create <name> --provider="local:<provider-name>" --password="<string>"
```

Note

A user account is disabled if no password is specified. If you do not create a password when you create the user account, you can add a password later by running the `isi auth users modify` command, specifying the appropriate user by username, UID, or SID.

Create a local group

In the local provider of an access zone, you can create groups and assign members to them.

Procedure

1. Run the following command to create a local group, where `<name>` and `<provider-name>` are values that you provide to define the group.

```bash
isi auth groups create <name> --provider "local:<provider-name>"
```

Naming rules for local users and groups

Local user and group names must follow naming rules in order to ensure proper authentication and access to the EMC Isilon cluster.

You must adhere to the following naming rules when creating and modifying local users and groups:

- The maximum name length is 104 characters. It is recommended that names do not exceed 64 characters.
- Names cannot contain the following invalid characters:
  " / \ [ ] ; : ; = , + * ? < >
Configure or modify a local password policy

You can configure and modify a local password policy for a local provider.

This procedure must be performed through the command-line interface (CLI).

Procedure

1. Establish an SSH connection to any node in the cluster.
2. (Optional) Run the following command to view the current password settings:
   
   isi auth local view system

3. Run the isi auth local modify command, choosing from the parameters described in Local password policy default settings.
   
   The --password-complexity parameter must be specified for each setting.

   isi auth local modify system --password-complexity=lowercase \  --password-complexity=uppercase --password-complexity=numeric \  --password-complexity=symbol

   The following command configures a local password policy for a local provider:

   isi auth local modify <provider-name> \  --min-password-length=20 \  --lockout-duration=20m \  --lockout-window=5m \  --lockout-threshold=5 \  --add-password-complexity=uppercase \  --add-password-complexity=numeric

Local password policy settings

You can configure local password policy settings and specify the default for each setting through the isi auth local modify command. Password complexity
increases the number of possible passwords that an attacker must check before the correct password is guessed.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-password-length</td>
<td>Minimum password length in characters.</td>
<td>Long passwords are best. The minimum length should not be so long that users have a difficult time entering or remembering the password.</td>
</tr>
<tr>
<td>password-complexity</td>
<td>A list of cases that a new password must contain. By default, the list is empty.</td>
<td>You can specify as many as four cases. The following cases are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- uppercase</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- lowercase</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- symbol (excluding # and @)</td>
</tr>
<tr>
<td>min-password-age</td>
<td>The minimum password age. You can set this value using characters for units; for example, 4W for 4 weeks, 2d for 2 Days.</td>
<td>A minimum password age ensures that a user cannot enter a temporary password and then immediately change it to the previous password. Attempts to check or set a password before the time expires are denied.</td>
</tr>
<tr>
<td>max-password-age</td>
<td>The maximum password age. You can set this value using characters for units; for example, 4W for 4 weeks, 2d for 2 Days.</td>
<td>Attempts to login after a password expires forces a password change. If a password change dialog cannot be presented, the user is not allowed to login.</td>
</tr>
<tr>
<td>password-history-length</td>
<td>The number of historical passwords to keep. New passwords are checked against this list and rejected if the password is already present. The max history length is 24.</td>
<td>To avoid recycling of passwords, you can specify the number of previous passwords to remember. If a new password matches a remembered previous password, it is rejected.</td>
</tr>
<tr>
<td>lockout-duration</td>
<td>The length of time in seconds that an account is locked after a configurable number of bad passwords are entered.</td>
<td>After an account is locked, it is unavailable from all sources until it is unlocked. OneFS provides two configurable options to avoid administrator interaction for every locked account:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Specify how much time must elapse before the account is unlocked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Automatically reset the incorrect-password counter after a specified time, in seconds.</td>
</tr>
</tbody>
</table>
### Setting Description Comments

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>lockout-threshold</td>
<td>The number of incorrect password attempts before an account is locked. A value of zero disables account lockout.</td>
<td>After an account is locked, it is unavailable from all sources until it is unlocked.</td>
</tr>
<tr>
<td>lockout-window</td>
<td>The time that elapses before the incorrect password attempts count is reset.</td>
<td>If the configured number of incorrect password attempts is reached, the account is locked and lockout-duration determines the length of time that the account is locked. A value of zero disables the window.</td>
</tr>
</tbody>
</table>

### Modify a local user

You can modify any setting for a local user account except the user name.

**Procedure**

1. Run the following command to modify a local group, where `<name>` or `<gid>` or `<sid>` are placeholders for the user identifiers and `<provider-name>` is a placeholder for the name of the local provider associated with the user:

   ```bash
   isi auth users modify (<name> or --gid <gid> or --sid <sid>) --provider "local:<provider-name>"
   ```

### Modify a local group

You can add or remove members from a local group.

**Procedure**

1. Run the following command to modify a local group, where `<name>` or `<gid>` or `<sid>` are placeholders for the group identifiers and `<provider-name>` is a placeholder for the name of the local provider associated with the group:

   ```bash
   isi auth groups modify (<name> or --gid <gid> or --sid <sid>) --provider "local:<provider-name>"
   ```

### Delete a local user

A deleted user can no longer access the cluster through the command-line interface, web administration interface, or file access protocol. When you delete a local user account, its home directory remains in place.

**Procedure**

1. Run the following command to delete a local user, where `<uid>` and `<sid>` are placeholders for the UID and SID of the user that you want to delete, and
<provider-name> is a placeholder for the local provider associated with the user.

```
isi auth users delete <name> --uid <uid> --sid <sid> \
   --provider "local:<provider-name>"
```

**Delete a local group**

You can delete a local group even if members are assigned to it. Deleting a group does not affect the members of that group.

**Procedure**

1. Run the following command to delete a local group, where `<group>` is a placeholder for the name of the group that you want to delete:

```
isi auth groups delete <group>
```

**Note**

You can run the command with `<gid>` or `<sid>` instead of `<group>`.

**Authentication and access control commands**

You can control access to your cluster through the authentication and access control commands.

**isi auth access**

Lists the permissions that a user has to access a given file or directory.

**Note**

This command does not display SMB share permissions or privileges.

**Syntax**

```
isi auth access {
   <user> | --uid <integer> | --sid <string>
   [-zone <string>]
   [-numeric]
   [-verbose]
```

**Options**

- `<name>`
  Specifies the user name.
- `--sid <string>`
  Specifies the user by SID.
- `--uid <integer>`
  Specifies the user by UID
Specifies the path of the file or directory under /ifs.

--zone <string>
Specifies the access zone.

{---numeric | -n}
Displays the numeric identifier of the user.

{---verbose | -v}
Displays more detailed information.

**isi auth ads create**

Configures an Active Directory provider and joins an Active Directory domain.

**Syntax**

```bash
isi auth ads create <name> <user>
  [--password <string>]
  [--organizational-unit <string>]
  [--kerberos-nfs-spn {yes | no}]
  [--kerberos-hdfs-spn {yes | no}]
  [--dns-domain <dns-domain>]
  [--groupnet <groupnet>]
  [--allocate-gids {yes | no}]
  [--allocate-uids {yes | no}]
  [--check-online-interval <duration>]
  [--create-home-directory {yes | no}]
  [--domain-offline-alerts {yes | no}]
  [--findable-groups <string>...]
  [--findable-users <string>...]
  [--home-directory-template <path>]
  [--ignore-all-trusts {yes | no}]
  [--ignore-trusted-domains <dns-domain>...]
  [--include-trusted-domains <dns-domain>...]
  [--machine-name <string>]
  [--ldap-sign-and-seal {yes | no}]
  [--login-shell <path>]
  [--lookup-domains <dns-domain>...]
  [--lookup-groups {yes | no}]
  [--lookup-normalize-groups {yes | no}]
  [--lookup-normalize-users {yes | no}]
  [--lookup-users {yes | no}]
  [--machine-password-changes {yes | no}]
  [--machine-password-lifespan <duration>]
  [--node-dc-affinity <string>]
  [--node-dc-affinity-timeout <timestamp>]
  [--nss-enumeration {yes | no}]
  [--restrict-findable {yes | no}]
  [--sfu-support {none | rfc2307}]
  [--store-sfu-mappings {yes | no}]
  [--unfindable-groups <string>...]
  [--unfindable-users <string>...]
  [--verbose]
```

**Options**

<name>
Specifies the fully-qualified Active Directory domain name, which can be resolved to an IPv4 or an IPv6 address. The domain name will also be used as the provider name.

<user>
Specifies the user name of an account that has permission to join machine accounts to the Active Directory domain.

--password <string>
Specifies the password of the provided user account. If you omit this option, you will be prompted to supply a password.

--organizational-unit <string>
Specifies the name of the organizational unit (OU) to connect to on the Active Directory server. Specify the OU in the form OuName or OuName1/SubName2.

--kerberos-nfs-spn {yes | no}
Specifies whether to add SPNs for using Kerberized NFS.

--kerberos-hdfs-spn {yes | no}
Specifies whether to add SPNs for using Kerberized HDFS.

--dns-domain <dns-domain>
Specifies a DNS search domain to use instead of the domain that is specified in the --name setting.

--groupnet <groupnet>
Specifies the groupnet referenced by the Active Directory provider. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the Active Directory provider will use when communicating with external servers.

--allocate-gids {yes | no}
Enables or disables GID allocation for unmapped Active Directory groups. Active Directory groups without GIDs can be proactively assigned a GID by the ID mapper. If this option is disabled, GIDs are not proactively assigned, but when a user’s primary group does not include a GID, the system may allocate one.

--allocate-uids {yes | no}
Enables or disables UID allocation for unmapped Active Directory users. Active Directory users without UIDs can be proactively assigned a UID by the ID mapper. If this option is disabled, UIDs are not proactively assigned, but when a user’s identity does not include a UID, the system may allocate one.

--check-online-interval <duration>
Specifies the time between provider online checks, in the format <integer>{Y|M|W|D|H|m|s}.

--create-home-directory {yes | no}
Specifies whether to create a home directory the first time that a user logs in, if a home directory does not already exist for the user.

--domain-offline-alerts {yes | no}
Specifies whether to send an alert if the domain goes offline. If this option is set to yes, notifications are sent as specified in the global notification rules. The default value is no.

--findable-groups <string>...
Specifies a list of groups that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

```bash
--findable-users <string>...
```

Specifies a list of users that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

```bash
--home-directory-template <path>
```

Specifies the template path to use when creating home directories. The path must begin with `/ifs` and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, `%U`, `%D`, and `%Z` are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

**Note**

If you are using Active Directory with Services for UNIX (SFU), spaces in Windows-created directory names are converted to underscores for UNIX compatibility.

```bash
--ignore-all-trusts {yes | no}
```

Specifies whether to ignore all trusted domains.

```bash
--ignored-trusted-domains <dns-domain>...
```

Specifies a list of trusted domains to ignore if `--ignore-all-trusts` is disabled. Repeat this option to specify multiple list items.

```bash
--include-trusted-domains <dns-domain>...
```

Specifies a list of trusted domain to include if `--ignore-all-trusts` is enabled. Repeat this option to specify multiple list items.

```bash
--machine-name <string>
```

Specifies hostname or machine name used to join the authentication provider as a record in the machines list.

```bash
--ldap-sign-and-seal {yes | no}
```

Specifies whether to use encryption and signing for LDAP requests to a domain controller.

```bash
--login-shell <path>
```

Specifies the full path to the login shell to use if the Active Directory server does not provide login-shell information. This setting applies only to users who access the file system through SSH.

```bash
--lookup-domains <string>...
```

Specifies a list of domains to which user and group lookups are to be limited. Repeat this option to specify multiple list items.

```bash
--lookup-groups {yes | no}
```

Specifies whether to look up Active Directory groups in other providers before allocating a GID.

```bash
--lookup-normalize-groups {yes | no}
```
Specifies whether to normalize Active Directory group names to lowercase before looking them up.

--lookup-normalize-users {yes | no}
  Specifies whether to normalize Active Directory user names to lowercase before looking them up.

--lookup-users {yes | no}
  Specifies whether to look up Active Directory users in other providers before allocating a UID.

--machine-password-changes {yes | no}
  Specifies whether to enable periodic changes of the machine account password for security purposes.

--machine-password-lifespan <duration>
  Sets the maximum age of the machine account password, in the format <integer>{Y|M|W|D|h|m}s).

{-node-dc-affinity | -x} <string>
  Specifies the domain controller that the node should exclusively communicate with (affinitize to). This option should be used with a timeout value, which is configured using the --node-dc-affinity-timeout option. Otherwise, the default timeout value of 30 minutes is assigned.

  Note
  This setting is for debugging purposes and should be left unconfigured during normal operation. To disable this feature, use a timeout value of 0.

{-node-dc-affinity-timeout} <timestamp>
  Specifies the timeout setting for the local node affinity to a domain controller, using the date format <YYYY>-<MM>-<DD> or the date/time format <YYYY>-<MM>-<DD>T<hh>:<mm>[:<ss>].

  Note
  A value of 0 disables the affinity. When affinitization is disabled, communication with the specified domain controller may not end immediately. It may persist until another domain controller can be chosen.

--nss-enumeration {yes | no}
  Specifies whether to allow the Active Directory provider to respond to getpwent and getgrent requests.

--restrict-findable {yes | no}
  Specifies whether to check the authentication provider for filtered lists of findable and unfindable users and groups.

--sfu-support {none | rfc2307}
  Specifies whether to support RFC 2307 attributes for Windows domain controllers. RFC 2307 is required for Windows UNIX Integration and for Services For UNIX (SFU) technologies.

--store-sfu-mappings {yes | no}
Specifies whether to store SFU mappings permanently in the ID mapper.

`--unfindable-groups <string>...`
Specifies a list of groups that cannot be resolved by this authentication provider. Repeat this option to specify multiple list items.

`--unfindable-users <string>...`
Specifies a list of users that cannot be resolved by this authentication provider. Repeat this option to specify multiple list items.

```
{--verbose | -v}
Displays the results of running the command.
```

**isi auth ads delete**

Deletes an Active Directory provider, which includes leaving the Active Directory domain that the provider is joined to. Leaving an Active Directory domain disrupts service for users who are accessing the domain. After you leave an Active Directory domain, users can no longer access the domain from the cluster.

**Syntax**

```
isi auth ads delete <provider-name>
    [--force]
    [--verbose]
```

**Options**

`<provider-name>`
Specifies the name of the provider to delete.

```
{--force | -f}
Suppresses command-line prompts and messages.
```

```
{--verbose | -v}
Displays the results of running the command.
```

**Examples**

To leave an Active Directory domain named some.domain.org and delete the authentication provider that is associated with it, run the following command:

```
isi auth ads delete some.domain.org
```

At the confirmation prompt, type `y`.

**isi auth ads list**

Displays a list of Active Directory providers.

**Syntax**

```
isi auth ads list
    [--limit <integer>]
    [--format {table | json | csv | list}]
```

 isi auth ads delete 263
Options

`{--limit | -l} <integer>`
Displays no more than the specified number of items.

`--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`
Displays table and CSV output without headers.

`{--no-footer | -z}`
Displays table output without footers.

`{--verbose | -v}`
Displays more detailed information.

Examples

To view a list of all the Active Directory providers that the cluster is joined to, run the following command:

```
isi auth ads list
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Name</th>
<th>Authentication</th>
<th>Status</th>
<th>DC Name</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD.EAST.EMC.COM</td>
<td>Yes</td>
<td>online</td>
<td>BOS</td>
<td></td>
</tr>
<tr>
<td>AD.NORTH.EMC.COM</td>
<td>Yes</td>
<td>online</td>
<td>VAN</td>
<td></td>
</tr>
<tr>
<td>AD.SOUTH.EMC.COM</td>
<td>No</td>
<td>online</td>
<td>TIJ</td>
<td></td>
</tr>
<tr>
<td>AD.WEST.EMC.COM</td>
<td>Yes</td>
<td>online</td>
<td>SEA</td>
<td></td>
</tr>
</tbody>
</table>

Total: 4

**isi auth ads modify**

Modifies an Active Directory authentication provider.

**Syntax**

```
isi auth ads modify <provider-name>
  [--reset-schannel {yes | no}]
  [--domain-controller <string>]
  [--allocate-gids {yes | no}]
  [--allocate-uids {yes | no}]
  [--check-online-interval <duration>]
  [--create-home-directory {yes | no}]
  [--domain-offline-alerts {yes | no}]
  [--findable-groups <string>...]
  [--clear-findable-groups]
  [--add-findable-groups <string>...]
  [--remove-findable-groups <string>...]
```
Options

<provider-name>

Specifies the domain name that the Active Directory provider is joined to, which is also the Active Directory provider name.

--reset-schannel {yes | no}

Resets the secure channel to the primary domain.

--domain-controller <dns-domain>

Specifies a domain controller.

--allocate-gids {yes | no}

Enables or disables GID allocation for unmapped Active Directory groups. Active Directory groups without GIDs can be proactively assigned a GID by the ID mapper. If this option is disabled, GIDs are not assigned proactively, but when a user’s primary group does not include a GID, the system may allocate one.

--allocate-uids {yes | no}
Enables or disables UID allocation for unmapped Active Directory users. Active Directory users without UIDs can be proactively assigned a UID by the ID mapper. If this option is disabled, UIDs are not assigned proactively, but when a user’s identity does not include a UID, the system may allocate one.

--check-online-interval <duration>
Specifies the time between provider online checks, in the format <integer>{Y|M|W|D|H|m|s}.

--create-home-directory {yes | no}
Specifies whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user.

--domain-offline-alerts {yes | no}
Specifies whether to send an alert if the domain goes offline. If this option is set to yes, notifications are sent as specified in the global notification rules. The default value is no.

--findable-groups <string>...
Specifies a list of groups that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--clear-findable-groups
Removes all entries from the list of findable groups.

--add-findable-groups <string>...
Adds an entry to the list of groups that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--remove-findable-groups <string>...
Removes an entry from the list of groups that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--findable-users <string>...
Specifies a list of users that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--clear-findable-users
Removes all entries from the list of findable users.

--add-findable-users <string>...
Adds an entry to the list of users that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--remove-findable-users <string>...
Removes an entry from the list of users that can be resolved by this authentication provider. Repeat this option to specify multiple list items.

--home-directory-template <path>
Specifies the template path to use when creating home directories. The path must begin with /ifs and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, %U, %D, and %Z are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.
Note

If you are using Active Directory with Services for UNIX (SFU), spaces in Windows-created directory names are converted to underscores for UNIX compatibility.

`--ignore-all-trusts {yes | no}`

Specifies whether to ignore all trusted domains.

`--ignored-trusted-domains <dns-domain>`

Specifies a list of trusted domains to ignore if `--ignore-all-trusts` is disabled. Repeat this option to specify multiple list items.

`--clear-ignored-trusted-domains`

Cleans the list of ignored trusted domains if `--ignore-all-trusts` is disabled.

`--add-ignored-trusted-domains <dns-domain>`

Adds a domain to the list of trusted domains to ignore if `--ignore-all-trusts` is disabled. Repeat this option to specify multiple list items.

`--remove-ignored-trusted-domains <dns-domain>`

Removes a specified domain from the list of trusted domains to ignore if `--ignore-all-trusts` is disabled. Repeat this option to specify multiple list items.

`--include-trusted-domains <dns-domain>`

Specifies a list of trusted domains to include if `--ignore-all-trusts` is enabled. Repeat this option to specify multiple list items.

`--clear-include-trusted-domains`

Clears the list of trusted domains to include if `--ignore-all-trusts` is enabled.

`--add-include-trusted-domains <dns-domain>`

Adds a domain to the list of trusted domains to include if `--ignore-all-trusts` is enabled. Repeat this option to specify multiple list items.

`--remove-include-trusted-domains <dns-domain>`

Removes a specified domain from the list of trusted domains to include if `--ignore-all-trusts` is enabled. Repeat this option to specify multiple list items.

`--machine-name <string>`

Specifies hostname or machine name used to join the authentication provider as a record in the machines list.

`--ldap-sign-and-seal {yes | no}`

Specifies whether to use encryption and signing on LDAP requests to a domain controller.

`{--node-dc-affinity | -x} <string>`

Specifies the domain controller that the node should exclusively communicate with (affinitize). This option should be used with a timeout value, which is
configured using the `--node-dc-affinity-timeout` option. Otherwise, the default timeout value of 30 minutes is assigned.

**Note**

This setting is for debugging purposes and should be left unconfigured during normal operation. To disable this feature, use a timeout value of 0.

```bash
--node-dc-affinity-timeout <timestamp>
```

Specifies the timeout setting for the local node affinity to a domain controller, using the date format `<YYYY>-<MM>-<DD>` or the date/time format `<YYYY>-<MM>-<DD>T<hh>:<mm>[:<ss>]`.

**Note**

A value of 0 disables the affinity. When affinitization is disabled, communication with the specified domain controller may not end immediately. It may persist until another domain controller can be chosen.

```bash
--login-shell <path>
```

Specifies the path to the login shell to use if the Active Directory server does not provide login-shell information. This setting applies only to users who access the file system through SSH.

```bash
--lookup-domains <string>
```

Specifies a list of domains to which user and group lookups are to be limited. Repeat this option to specify multiple list items.

```bash
--clear-lookup-domains
```

Clears the list of restricted domains for user and group lookups.

```bash
--add-lookup-domains <string>
```

Adds an entry to the restricted list of domains to use for user and group lookups. Repeat this option to specify multiple list items.

```bash
--remove-lookup-domains <string>
```

Removes an entry from the list of domains to use for user and group lookups. Repeat this option to specify multiple list items.

```bash
--lookup-groups {yes | no}
```

Specifies whether to look up Active Directory groups in other providers before allocating a GID.

```bash
--lookup-normalize-groups {yes | no}
```

Specifies whether to normalize Active Directory group names to lowercase before looking them up.

```bash
--lookup-normalize-users {yes | no}
```

Specifies whether to normalize Active Directory user names to lowercase before looking them up.

```bash
--lookup-users {yes | no}
```

Specifies whether to look up Active Directory users in other providers before allocating a UID.
--machine-password-changes {yes | no}
   Specifies whether to enable periodic changes of the machine account password
   for security purposes.

--machine-password-lifespan <duration>
   Sets the maximum age of the machine account password, in the format
   <integer>{Y|M|D|H|m|s}.

--nss-enumeration {yes | no}
   Specifies whether to allow the Active Directory provider to respond to getpwent
   and getgrent requests.

--restrict-findable {yes | no}
   Specifies whether to check the authentication provider for filtered lists of
   findable and unfindable users and groups.

--sfu-support {none | rfc2307}
   Specifies whether to support RFC 2307 attributes for domain controllers. RFC
   2307 is required for Windows UNIX Integration and for Services For UNIX (SFU)
   technologies.

--store-sfu-mappings {yes | no}
   Specifies whether to store SFU mappings permanently in the ID mapper.

--unfindable-groups <string>...
   Specifies a list of groups that cannot be resolved by this authentication provider.
   Repeat this option to specify multiple list items.

--clear-unfindable-groups
   Removes all entries from the list of unfindable groups.

--add-unfindable-groups <string>...
   Adds an entry to the list of groups that cannot be resolved by this authentication
   provider. Repeat this option to specify multiple list items.

--remove-unfindable-groups <string>...
   Removes an entry from the list of groups that cannot be resolved by this
   authentication provider. Repeat this option to specify multiple list items.

--unfindable-users <string>...
   Specifies a list of users that cannot be resolved by this authentication provider.
   Repeat this option to specify multiple list items.

--clear-unfindable-users
   Removes all entries from the list of unfindable users.

--add-unfindable-users <string>...
   Adds an entry to the list of users that cannot be resolved by this authentication
   provider. Repeat this option to specify multiple list items.

--remove-unfindable-users <string>...
   Removes an entry from the list of users that cannot be resolved by this
   authentication provider. Repeat this option to specify multiple list items.

{--verbose | -v}
Displays the results of running the command.

**isi auth ads view**

Displays the properties of an Active Directory provider.

**Syntax**

```
isi auth ads view <provider-name>

|--verbose
```

**Options**

- `<provider-name>`
  - Specifies the name of the provider to view.
- `|--verbose | -v`
  - Displays more detailed information.

**isi auth ads spn check**

Checks valid service principal names (SPNs).

**Syntax**

```
isi auth ads spn check <provider-name>
```

**Options**

- `<provider-name>`
  - Specifies the Active Directory provider name.

**isi auth ads spn create**

Adds one or more service principal names (SPNs) for a machine account. SPNs must be propagated to all domain controllers to make them available to clients.

**Syntax**

```
isi auth ads spn create <provider-name>

|--user <string>

|--password <string>
```

**Options**

- `<provider-name>`
  - Specifies the Active Directory provider name.
- `|--user | -U <string>`
  - Specifies an administrative user account name with permission to create SPNs in the Active Directory domain.
- `|--password | -P <string>`
Specifies the administrative user account password.

**isi auth ads spn delete**

Deletes one or more SPNs that are registered against a machine account.

**Syntax**

```bash
isi auth ads spn delete <provider-name>
   [--user <string>]
   [--password <string>]
```

**Options**

`<provider-name>`

Specifies the Active Directory provider name.

`[--user | -U] <string>`

Specifies an administrative user account name with permission to modify SPNs in the Active Directory domain.

`[--password | -P] <string>`

Specifies the administrative user account password.

**isi auth ads spn fix**

Adds missing service principal names (SPNs) for an Active Directory provider.

**Syntax**

```bash
isi auth ads spn fix <provider-name>
   [--spn <string>]
   [--user <string>]
   [--password <string>]
```

**Options**

`<provider-name>`

Specifies the Active Directory provider name.

`--spn <string>`

Specifies the service principal name.

`--user <string>`

Specifies an administrative user account name with permission to add SPNs for the Active Directory domain.

`--password <string>`

Specifies the administrative user account password.
### isi auth ads spn list

Displays a list of service principal names (SPNs) that are registered against a machine account.

**Syntax**

```bash
isi auth ads spn list <provider-name>
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

- `<provider-name>`
  Specifies the Active Directory provider name.
- `--limit | -l` `<integer>`
  Displays no more than the specified number of items.
- `--format {table | json | csv | list}`
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
- `--no-header | -a`
  Displays table and CSV output without headers.
- `--no-footer | -z`
  Displays table output without footers.
- `--verbose | -v`
  Displays more detailed information.

### isi auth ads trusts controllers list

Displays a list of domain controllers for a trusted domain.

**Syntax**

```bash
isi auth ads trusts controllers list <provider>
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

- `<provider>`
  Specifies an Active Directory provider.
- `--limit | -l` `<integer>`
  Displays no more than the specified number of items.
--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
    Displays table and CSV output without headers.

{--no-footer | -z}
    Displays table output without footers.

{--verbose | -v}
    Displays more detailed information.

Examples
The following command displays a list of trusted domains in an Active Directory provider named ad.isilon.com:

    isi auth ads trusts controllers list ad.isilon.com

isi auth ads trusts list
Displays a list of trusted domains.

Syntax

    isi auth ads trusts list <provider>

Options

    <provider>
        Specifies an Active Directory provider.

isi auth ads trusts view
Displays the properties of a trusted domain.

Syntax

    isi auth ads trusts view <provider> <domain>

Options

    <provider>
        Specifies an Active Directory provider.

    <domain>
        Specifies the trusted domain to view.
isi auth error

Displays error code definitions from the authentication log files.

Syntax

```
isi auth error <error-code>
```

Options

```
<error-code>
```

Specifies the error code to convert.

Examples

To view the definition of error code 4, run the following command:

```
isi auth error 4
```

The system displays output similar to the following example:

```
4 = ERROR_TOO_MANY_OPEN_FILES
```

isi auth file create

Creates a file provider.

Syntax

```
isi auth file create <name>
    [--password-file <path>]
    [--group-file <path>]
    [--authentication {yes | no}]
    [--create-home-directory {yes | no}]
    [--enabled {yes | no}]
    [--enumerate-groups {yes | no}]
    [--enumerate-users {yes | no}]
    [--findable-groups <string>]
    [--findable-users <string>]
    [--group-domain <string>]
    [--home-directory-template <path>]
    [--listable-groups <string>]
    [--listable-users <string>]
    [--login-shell <path>]
    [--modifiable-groups <string>]
    [--modifiable-users <string>]
    [--netgroup-file <path>]
    [--normalize-groups {yes | no}]
    [--normalize-users {yes | no}]
    [--ntlm-support {all | v2only | none}]
    [--provider-domain <string>]
    [--restrict-findable {yes | no}]
    [--restrict-listable {yes | no}]
    [--restrict-modifiable {yes | no}]
    [--unfindable-groups <string>]
    [--unfindable-users <string>]
    [--unlistable-groups <string>]
    [--unlistable-users <string>]
    [--unmodifiable-groups <string>]
    [--unmodifiable-users <string>]
```
Options

<name>
Sets the file provider name.

--password-file <path>
Specifies the path to a passwd.db replacement file.

--group-file <path>
Specifies the path to a group replacement file.

--authentication {yes | no}
Enables or disables the use of the provider for authentication as well as identity. The default value is yes.

--create-home-directory {yes | no}
Specifies whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user.

--enabled {yes | no}
Enables or disables the provider.

--findable-groups <string>
Specifies a list of groups that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify each additional findable group. If populated, groups that are not included in this list cannot be resolved.

--findable-users <string>
Specifies a list of users that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify each additional findable user. If populated, users that are not included in this list cannot be resolved.

--group-domain <string>
Specifies the domain that this provider will use to qualify groups. The default group domain is FILE_GROUPS.

--home-directory-template <path>
Specifies the path to use as a template for naming home directories. The path must begin with /ifs and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, %U, %D, and %Z are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

--listable-groups <string>
Specifies a group that can be listed if --restrict-listable is enabled. Repeat this option to specify multiple list items. If populated, any groups that are not included in this list cannot be listed.

--listable-users <string>
Specifies a user that can be listed in this provider if\texttt{--restrict-listable} is enabled. Repeat this option to specify multiple list items. If populated, any users that are not included in this list cannot be listed.

\textbf{--login-shell <path>}

Specifies the path to the user’s login shell. This setting applies only to users who access the file system through SSH.

\textbf{--modifiable-groups <string>}

Specifies a group that can be modified in this provider if \texttt{--restrict-modifiable} is enabled. Repeat this option to specify multiple list items. If populated, any groups that are not included in this list cannot be modified.

\textbf{--modifiable-users <string>}

Specifies a user that can be modified in this provider if \texttt{--restrict-modifiable} is enabled. Repeat this option to specify multiple list items. If populated, any users that are not included in this list cannot be modified.

\textbf{--netgroup-file <path>}

Specifies the path to a netgroup replacement file.

\textbf{--normalize-groups \{yes | no\}}

Normalizes group names to lowercase before lookup.

\textbf{--normalize-users \{yes | no\}}

Normalizes user names to lowercase before lookup.

\textbf{--ntlm-support \{all | v2only | none\}}

For users with NTLM-compatible credentials, specifies which NTLM versions to support. Valid values are \texttt{all}, \texttt{v2only}, and \texttt{none}. NTLMv2 provides additional security over NTLM.

\textbf{--provider-domain <string>}

Specifies the domain that the provider will use to qualify user and group names.

\textbf{--restrict-findable \{yes | no\}}

Specifies whether to check the provider for filtered lists of findable and unfindable users and groups.

\textbf{--restrict-listable \{yes | no\}}

Specifies whether to check the provider for filtered lists of listable and unlistable users and groups.

\textbf{--restrict-modifiable \{yes | no\}}

Specifies whether to check the provider for filtered lists of modifiable and unmodifiable users and groups.

\textbf{--unfindable-groups <string>}

If \texttt{--restrict-findable} is enabled and the findable groups list is empty, specifies a group that cannot be resolved by this provider. Repeat this option to specify multiple list items.

\textbf{--unfindable-users <string>}


If `--restrict-findable` is enabled and the findable users list is empty, specifies a user that cannot be resolved by this provider. Repeat this option to specify multiple list items.

`--unlistable-groups <string>`
If `--restrict-listable` is enabled and the listable groups list is empty, specifies a group that cannot be listed by this provider. Repeat this option to specify multiple list items.

`--unlistable-users <string>`
If `--restrict-listable` is enabled and the listable users list is empty, specifies a user that cannot be listed by this provider. Repeat this option to specify multiple list items.

`--unmodifiable-groups <string>`
If `--restrict-modifiable` is enabled and the modifiable groups list is empty, specifies a group that cannot be modified. Repeat this option to specify multiple list items.

`--unmodifiable-users <string>`
If `--restrict-modifiable` is enabled and the modifiable users list is empty, specifies a user that cannot be modified. Repeat this option to specify multiple list items.

`--user-domain <string>`
Specifies the domain that this provider will use to qualify users. The default user domain is `FILE_USERS`.

`{--verbose | -v}`
Displays more detailed information.

**isi auth file delete**

Deletes a file provider.

**Syntax**

```
isi auth file delete <provider-name>
[--force]
[--verbose]
```

**Options**

`<provider-name>`
Specifies the name of the provider to delete.

`{--force | -f}`
Suppresses command-line prompts and messages.

`{--verbose | -v}`
Displays more detailed information.
isi auth file list

Displays a list of file providers.

Syntax

```
isi auth file list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

```
{-limit | -l} <integer>
    Displays no more than the specified number of items.

--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{-no-header | -a}
    Displays table and CSV output without headers.

{-no-footer | -z}
    Displays table output without footers.

{-verbose | -v}
    Displays more detailed information.
```

isi auth file modify

Modifies a file provider.

Syntax

```
isi auth file modify <provider-name>
    [--name <string>]
    [--password-file <path>]
    [--group-file <path>]
    [--authentication {yes | no}]
    [--create-home-directory {yes | no}]
    [--enabled {yes | no}]
    [--enumerate-groups {yes | no}]
    [--enumerate-users {yes | no}]
    [--findable-groups <string>]
    [--clear-findable-groups]
    [--add-findable-groups <string>]
    [--remove-findable-groups <string>]
    [--findable-users <string>]
    [--clear-findable-users]
    [--add-findable-users <string>]
    [--remove-findable-users <string>]
    [--group-domain <string>]
    [--home-directory-template <path>]
    [--listable-groups <string>]
    [--clear-listable-groups]
```
Options

<provider-name>

Specifies the name of the file provider to modify. This setting cannot be modified.

--name <string>

Specifies an new name for the authentication provider.

--password-file <path>

Specifies the path to a passwd.db replacement file.

--group-file <path>

Specifies the path to a group replacement file.
--authentication {yes | no}
Enables or disables the use of the provider for authentication as well as identity.
The default value is yes.

--cache-entry-expiry <duration>
Specifies the length of time after which the cache entry will expire, in the format
<integer>Y|M|W|D|H|m|s]. To turn off cache expiration, set this value to
off.

--create-home-directory {yes | no}
Specifies whether to create a home directory the first time a user logs in, if a
home directory does not already exist for the user.

--enabled {yes | no}
Enables or disables the provider.

--enumerate-groups {yes | no}
Specifies whether to allow the provider to enumerate groups.

--enumerate-users {yes | no}
Specifies whether to allow the provider to enumerate users.

--findable-groups <string>
Specifies a group that can be found in this provider if --restrict-findable is
enabled. Repeat this option to specify multiple list items. If populated, any groups
that are not included in this list cannot be resolved. This option overwrites any
existing entries in the findable groups list; to add or remove groups without
affecting current entries, use --add-findable-groups or --remove-
findable-groups.

--clear-findable-groups
Removes all entries from the list of findable groups.

--add-findable-groups <string>
Adds an entry to the list of findable groups that is checked if --restrict-
findable is enabled. Repeat this option to specify multiple list items.

--remove-findable-groups <string>
Removes an entry from the list of findable groups that is checked if --
restrict-findable is enabled. Repeat this option to specify multiple list
items.

--findable-users <string>
Specifies a user that can be found in the provider if --restrict-findable is
enabled. Repeat this option to specify multiple list items. If populated, any users
that are not included in this list cannot be resolved. This option overwrites any
existing entries in the findable users list; to add or remove users without affecting
current entries, use --add-findable-users or --remove-findable-
users.

--clear-findable-users
Removes all entries from the list of findable users.

--add-findable-users <string>
Adds an entry to the list of findable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-findable-users <string>
Removes an entry from the list of findable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--group-domain <string>
Specifies the domain that the provider will use to qualify groups. The default group domain is FILE_GROUPS.

--group-file <path>
Specifies the path to a group replacement file.

--home-directory-template <path>
Specifies the path to use as a template for naming home directories. The path must begin with /ifs and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, %U, %D, and %Z are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

--listable-groups <string>
Specifies a group that can be viewed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. If populated, any groups that are not included in this list cannot be viewed. This option overwrites any existing entries in the listable groups list; to add or remove groups without affecting current entries, use --add-listable-groups or --remove-listable-groups.

--clear-listable-groups
Removes all entries from the list of viewable groups.

--add-listable-groups <string>
Adds an entry to the list of viewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-listable-groups <string>
Removes an entry from the list of viewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--listable-users <string>
Specifies a user that can be viewed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. If populated, any users that are not included in this list cannot be viewed. This option overwrites any existing entries in the listable users list; to add or remove users without affecting current entries, use --add-listable-users or --remove-listable-users.

--clear-listable-users
Removes all entries from the list of viewable users.

--add-listable-users <string>
Adds an entry to the list of viewable users that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--remove-listable-users <string>`
Removes an entry from the list of viewable users that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--login-shell <path>`
Specifies the path to the user’s login shell. This setting applies only to users who access the file system through SSH.

`--modifiable-groups <string>`
Specifies a group that can be modified if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items. If populated, any groups that are not included in this list cannot be modified. This option overwrites any existing entries in the modifiable groups list; to add or remove groups without affecting current entries, use `--add-modifiable-groups` or `--remove-modifiable-groups`.

`--clear-modifiable-groups`
Removes all entries from the list of modifiable groups.

`--add-modifiable-groups <string>`
Adds an entry to the list of modifiable groups that is checked if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items.

`--remove-modifiable-groups <string>`
Removes an entry from the list of modifiable groups that is checked if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items.

`--modifiable-users <string>`
Specifies a user that can be modified if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items. If populated, any users that are not included in this list cannot be modified. This option overwrites any existing entries in the modifiable users list; to add or remove users without affecting current entries, use `--add-modifiable-users` or `--remove-modifiable-users`.

`--clear-modifiable-users`
Removes all entries from the list of modifiable users.

`--add-modifiable-users <string>`
Adds an entry to the list of modifiable users that is checked if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items.

`--remove-modifiable-users <string>`
Removes an entry from the list of modifiable users that is checked if `--restrict-modifiable` is enabled. Repeat this option to specify multiple list items.

`--netgroup-file <path>`
Specifies the path to a netgroup replacement file.
--normalize-groups {yes | no}
   Normalizes group names to lowercase before lookup.

--normalize-users {yes | no}
   Normalizes user names to lowercase before lookup.

--ntlm-support {all | v2only | none}
   For users with NTLM-compatible credentials, specifies which NTLM versions to support. Valid values are all, v2only, and none. NTLMv2 provides additional security over NTLM and is recommended.

--password-file <path>
   Specifies the path to a passwd.db replacement file.

--provider-domain <string>
   Specifies the domain that this provider will use to qualify user and group names.

--restrict-findable {yes | no}
   Specifies whether to check this provider for filtered lists of findable and unfindable users and groups.

--restrict-listable {yes | no}
   Specifies whether to check this provider for filtered lists of viewable and unviewable users and groups.

--restrict-modifiable {yes | no}
   Specifies whether to check this provider for filtered lists of modifiable and unmodifiable users and groups.

--unfindable-groups <string>
   If --restrict-findable is enabled and the findable groups list is empty, specifies a group that cannot be resolved by this provider. Repeat this option to specify multiple list items. This option overwrites any existing entries in the unfindable groups list; to add or remove groups without affecting current entries, use --add-unfindable-groups or --remove-unfindable-groups.

--clear-unfindable-groups
   Removes all entries from the list of unfindable groups.

--add-unfindable-groups <string>
   Adds an entry to the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-groups <string>
   Removes an entry from the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unfindable-users <string>
   If --restrict-findable is enabled and the findable users list is empty, specifies a user that cannot be resolved by this provider. Repeat this option to specify multiple list items. This option overwrites any existing entries in the unfindable users list; to add or remove users without affecting current entries, use --add-unfindable-users or --remove-unfindable-users.
--clear-unfindable-users
Removes all entries from the list of unfindable groups.

--add-unfindable-users <string>
Adds an entry to the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-users <string>
Removes an entry from the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unlistable-groups <string>
If --restrict-listable is enabled and the viewable groups list is empty, specifies a group that cannot be listed by this provider. Repeat this option to specify multiple list items. This option overwrites any existing entries in the unlistable groups list; to add or remove groups without affecting current entries, use --add-unlistable-groups or --remove-unlistable-groups.

--clear-unlistable-groups
Removes all entries from the list of unviewable groups.

--add-unlistable-groups <string>
Adds an entry to the list of unviewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-unlistable-groups <string>
Removes an entry from the list of unviewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--unlistable-users <string>
If --restrict-listable is enabled and the viewable users list is empty, specifies a user that cannot be listed by this provider. Repeat this option to specify multiple list items. This option overwrites any existing entries in the unlistable users list; to add or remove users without affecting current entries, use --add-unlistable-users or --remove-unlistable-users.

--clear-unlistable-users
Removes all entries from the list of unviewable users.

--add-unlistable-users <string>
Adds an entry to the list of unviewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-unlistable-users <string>
Removes an entry from the list of unviewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--unmodifiable-groups <string>
If --restrict-modifiable is enabled and the modifiable groups list is empty, specifies a group that cannot be modified. Repeat this option to specify multiple list items. This option overwrites any existing entries in this provider’s unmodifiable groups list; to add or remove groups without affecting current
entries, use --add-unmodifiable-groups or --remove-unmodifiable-groups.

--clear-unmodifiable-groups
Removes all entries from the list of unmodifiable groups.

--add-unmodifiable-groups <string>
Adds an entry to the list of unmodifiable groups that is checked if --restrict-modifiable is enabled. Repeat this option to specify multiple list items.

--remove-unmodifiable-groups <string>
Removes an entry from the list of unmodifiable groups that is checked if --restrict-modifiable is enabled. Repeat this option to specify multiple list items.

--unmodifiable-users <string>
If --restrict-modifiable is enabled and the modifiable users list is empty, specifies a user that cannot be modified. Repeat this option to specify multiple list items. This option overwrites any existing entries in this provider’s unmodifiable users list; to add or remove users without affecting current entries, use --add-unmodifiable-users or --remove-unmodifiable-users.

--clear-unmodifiable-users
Removes all entries from the list of unmodifiable users.

--add-unmodifiable-users <string>
Adds an entry to the list of unmodifiable users that is checked if --restrict-modifiable is enabled. Repeat this option to specify multiple list items.

--remove-unmodifiable-users <string>
Removes an entry from the list of unmodifiable users that is checked if --restrict-modifiable is enabled. Repeat this option to specify multiple list items.

--user-domain <string>
Specifies the domain that this provider will use to qualify users. The default user domain is FILE_USERS.

{---verbose | -v}
Displays detailed information.

isi auth file view
Displays the properties of a file provider.

Syntax

isi auth file view <provider-name>

Options

<provider-name>
Specifies the name of the provider to view.
isi auth groups create

Creates a local group.

Syntax

```
isi auth groups create <name>
    [--gid <integer>]
    [--add-user <name>]
    [--add-uid <integer>]
    [--add-sid <string>]
    [--add-wellknown <name>]
    [--sid <string>]
    [--zone <string>]
    [--provider <string>]
    [--verbose]
    [--force]
```

Options

```
<name>
    Specifies the group name.

--gid <integer>
    Overrides automatic allocation of the UNIX group identifier (GID) with the
    specified value. Setting this option is not recommended.

--add-user <name>
    Specifies the name of the user to add to the group. Repeat this option to specify
    multiple users.

--add-uid <integer>
    Specifies the UID of the user to add to the group. Repeat this option to specify
    multiple users.

--add-sid <string>
    Specifies the SID of the user to add to the group. Repeat this option to specify
    multiple users.

--add-wellknown <name>
    Specifies a wellknown persona name to add to the group. Repeat this option to
    specify multiple personas.

--sid <string>
    Sets the Windows security identifier (SID) for the group, for example
    S-1-5-21-13.

--zone <string>
    Specifies the access zone in which to create the group.

--provider <string>
    Specifies a local authentication provider in the specified access zone.

{--verbose | -v}
    Displays more detailed information.

{--force | -f}
```
Suppresses command-line prompts and messages.

**isi auth groups delete**

Removes a local group from the system. Members of a group are removed before the group is deleted.

**Syntax**

```
isi auth groups delete {<group> | --gid <integer> | --sid <string>} [-f]
    [-v]
```

**Options**

This command requires `<group>`, `--gid <integer>`, or `--sid <string>`.

- `<group>`
  - Specifies the group by name.

- `--gid <integer>`
  - Specifies the group by GID.

- `<group>`
  - Specifies the group by name.

- `--sid <string>`
  - Specifies the group by SID.

- `--zone <string>`
  - Specifies the name of the access zone that contains the group.

- `--provider <string>`
  - Specifies the group's authentication provider.

- `{--force | -f}`
  - Suppresses command-line prompts and messages.

- `{--verbose | -v}`
  - Displays the results of running the command.

**isi auth groups flush**

Flushes cached group information.

**Syntax**

```
isi auth groups flush
```

**Options**

There are no options for this command.
Examples
To flush all cached group information, run the following command:

```bash
isi auth groups flush
```

**isi auth groups list**
Displays a list of groups.

**Syntax**

```bash
isi auth groups list
[--domain <string>]
[--zone <string>]
[--provider <string>]
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

`--domain <string>`
Specifies the provider domain.

`--zone <string>`
Specifies an access zone.

`--provider <string>`
Specifies an authentication provider.

`{--limit | -l} <integer>`
Displays no more than the specified number of items.

`--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`
Displays table and CSV output without headers.

`{--no-footer | -z}`
Displays table output without footers.

`{--verbose | -v}`
Displays more detailed information.
isi auth groups members list

Displays a list of members that are associated with a group.

Syntax

```bash
isi auth groups members list {<group> | --gid <integer> | --sid <string>}
   [--zone <string>]
   [--provider <string>]
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

This command requires `<group>`, `--gid <integer>`, or `--sid <string>`.

`<group>`
- Specifies the group by name.

`--gid <integer>`
- Specifies the group by GID.

`--sid <string>`
- Specifies the group by SID.

`--zone <string>`
- Specifies an access zone.

`--provider <string>`
- Specifies an authentication provider.

`{--limit | -l} <integer>`
- Displays no more than the specified number of items.

`--format {table | json | csv | list}`
- Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`
- Displays table and CSV output without headers.

`{--no-footer | -z}`
- Displays table output without footers.

`{--verbose | -v}`
- Displays more detailed information.
isi auth groups modify

Modifies a local group.

Syntax

```bash
isi auth groups modify {<group> | --gid <integer> | --sid <string>}
    [--new-gid <integer>]
    [--add-uid <integer>]
    [--remove-uid <integer>]
    [--add-user <name>]
    [--remove-user <name>]
    [--add-sid <string>]
    [--remove-sid <string>]
    [--add-wellknown <name>]
    [--remove-wellknown <name>]
    [--zone <string>]
    [--provider <string>]
    [--verbose]
    [--force]
```

Options

This command requires `<group>`, `--gid <integer>`, or `--sid <string>`.

- `<group>`
  Specifies the group by name.

- `--gid <integer>`
  Specifies the group by GID.

- `--sid <string>`
  Specifies the group by SID.

- `--new-gid <integer>`
  Specifies a new GID for the group. Setting this option is not recommended.

- `--add-uid <integer>`
  Specifies the UID of a user to add to the group. Repeat this option to specify multiple list items.

- `--remove-uid <integer>`
  Specifies the UID of a user to remove from the group. Repeat this option to specify multiple list items.

- `--add-user <name>`
  Specifies the name of a user to add to the group. Repeat this option to specify multiple list items.

- `--remove-user <name>`
  Specifies the name of a user to remove from the group. Repeat this option to specify multiple list items.

- `--add-sid <string>`
  Specifies the SID of an object to add to the group, for example S-1-5-21-13. Repeat this option to specify multiple list items.

- `--remove-sid <string>`
Specifies the SID of an object to remove from the group. Repeat this option to specify multiple list items.

--add-wellknown <name>
Specifies a well-known SID to add to the group. Repeat this option to specify multiple list items.

--remove-wellknown <name>
Specifies a well-known SID to remove from the group. Repeat this option to specify multiple list items.

--zone <string>
Specifies the group's access zone.

--provider <string>
Specifies the group's authentication provider.

{--verbose | -v}
Displays more detailed information.

{--force | -f}
Suppresses command-line prompts and messages.

isi auth groups view
Displays the properties of a group.

Syntax

```
isi auth groups view {<group> | --gid <integer> | --sid <string>} [-v | --verbose] [-f | --force] [--cached] [--provider <string>] [--show-groups] [--zone <string>]
```

Options

**<group>**
Specifies the group by name.

--gid <integer>
Specifies the group by GID.

--sid <string>
Specifies the group by SID.

--cached
Displays cached information.

--provider <string>
Specifies the name of an authentication provider.

--show-groups
Displays groups that include this group as a member.

--zone <string>
Specifies an access zone.

**isi auth id**

Displays your access token.

**Syntax**

```bash
isi auth id
```

**Options**

There are no options for this command.

**isi auth krb5 create**

Creates an MIT Kerberos provider and joins a user to an MIT Kerberos realm.

**Syntax**

```bash
isi auth krb5 create <realm> (<user> | --keytab-file <string> )
[--password <string>]
[--spn <string>]
[--groupnet <groupnet>]
[--is-default-realm {yes | no}]
[--kdc <string>]
[--admin-server <string>]
[--default-domain <string>]
[--verbose]
```

**Options**

**<realm>**

Specifies the Kerberos realm name.

**<user>**

Specifies the name of a user with permission to create service principal names (SPNs) in the Kerberos realm.

**--keytab-file <string>**

Specifies the keytab file to import.

**--password <string>**

Specifies the password used for joining a Kerberos realm.

**--spn <string>**

Specifies the SPNs to register. Specify `--spn` for each additional SPN that you want to register.

**--groupnet <groupnet>**

Specifies the groupnet referenced by the Kerberos provider. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the Kerberos provider will use when communicating with external servers.

**--is-default-realm {yes | no}**
Specifies whether the Kerberos realm is the default.

--kdc <string>
Specifies the hostname, IPv4 address, or IPv6 address of the Key Distribution Center (KDC). Specify --kdc for each additional KDC you want to add to the realm.

--admin-server <string>
Specifies the hostname, IPv4 address, or IPv6 address of the administrative server (master KDC).

--default-domain <string>
Specifies the default Kerberos domain for the Kerberos realm used for translating Kerberos v4 principal names.

{---verbose | -v}
Displays detailed information.

isi auth krb5 delete

Deletes an MIT Kerberos authentication provider and removes the user from an MIT Kerberos realm.

Syntax

isi auth krb5 delete <provider-name> [--force]

Options

<provider-name>
Specifies the Kerberos provider name.

{---force | -f}
Specifies not to ask for a confirmation.

isi auth krb5 list

Displays a list of MIT Kerberos authentication providers.

Syntax

isi auth krb5 list
[--limit <integer>] [--format {table | json | csv | list}] [--no-header] [--no-footer]

Options

{---limit | -l} <integer>
Specifies the number of Kerberos providers to display.

--format {table | json | csv | list}
Specifies to display the Kerberos providers in a tabular, JSON, CSV, or list format.

|--no-header|--a|--no-footer|--z|

--no-header|--a
Specifies not to display the headers in the CSV or tabular formats.

--no-footer|--z
Specifies not to display the table summary footer information.

**isi auth krb5 view**

Displays the properties of an MIT Kerberos authentication provider.

**Syntax**

`isi auth krb5 view <provider-name>`

**Options**

*<provider-name>*
Specifies the Kerberos provider name.

**isi auth krb5 domain create**

Creates an MIT Kerberos domain mapping.

**Syntax**

`isi auth krb5 domain create <domain>`

[-realm <string>]

**Options**

*<domain>*
Specifies the name of the Kerberos domain.

--realm <string>
Specifies the name of the Kerberos realm.

**isi auth krb5 domain delete**

Deletes an MIT Kerberos domain mapping.

**Syntax**

`isi auth krb5 domain delete <domain>`

[-force]

**Options**

*<domain>*
Specifies the name of the Kerberos domain.

[-force | -f]
Specifies not to ask for a confirmation.

**isi auth krb5 domain list**

Displays a list of MIT Kerberos domain mappings.

**Syntax**

```
isi auth krb5 domain list
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
```

**Options**

`--limit | -l <integer>`

Specifies the number of Kerberos domain mappings to display.

`--format {table | json | csv | list}`

Specifies whether to display the Kerberos domain mappings in a tabular, JSON, CSV, or list formats.

`--no-header | -a`

Specifies not to display the headers in the CSV or tabular formats.

`--no-footer | -z`

Specifies not to display the table summary footer information.

**isi auth krb5 domain modify**

Modifies an MIT Kerberos domain mapping.

**Syntax**

```
isi auth krb5 domain modify <domain>
[--realm <string>]
```

**Options**

`<domain>`

Specifies the Kerberos domain name.

`--realm <string>`

Specifies the Kerberos realm name.

**isi auth krb5 domain view**

Displays the properties of an MIT Kerberos domain mapping.

**Syntax**

```
isi auth krb5 domain view <domain>
```
Options

<domain>
    Specifies the Kerberos domain name.

isi auth krb5 realm create

Creates an MIT Kerberos realm.

Syntax

isi auth krb5 realm create <realm>
   [--is-default-realm {yes | no}]
   [--kdc <string>]
   [--admin-server <string>]
   [--default-domain <string>]

Options

<realm>
    Specifies the name of the Kerberos realm.

--is-default-realm {yes | no}
    Specifies whether the Kerberos realm is the default realm.

--kdc <string>
    Specifies the hostname, IPv4 address, or IPv6 address of the Key Distribution Center (KDC). Specify --kdc for each additional KDC you want to add to the realm.

--admin-server <string>
    Specifies the hostname, IPv4 address, or IPv6 address of the administrative server (master KDC).

--default-domain <string>
    Specifies the default domain for the realm used for translating the v4 principal names.

isi auth krb5 realm delete

Deletes an MIT Kerberos realm.

Syntax

isi auth krb5 realm delete <realm>
   [--force]

Options

<realm>
    Specifies the Kerberos realm name.

{--force | -f}
    Specifies not to ask for a confirmation.
isi auth krb5 realm modify

Modifies an MIT Kerberos realm.

Syntax

```bash
isi auth krb5 realm modify <realm>
   [--is-default-realm {yes | no}]
   [--kdc <string>]
   [--admin-server <string>]
   [--default-domain <string>]
```

Options

- `<realm>`: Specifies the Kerberos realm name.
- `--is-default-realm {yes | no}`: Specifies whether the Kerberos realm is the default.
- `--kdc <string>`: Specifies the hostname, IPv4 address, or IPv6 address of the Key Distribution Center (KDC). Specify `--kdc` for each additional KDC you want to add to the realm.
- `--admin-server <string>`: Specifies the hostname, IPv4 address, or IPv6 address of the administrative server (master KDC).
- `--default-domain <string>`: Specifies the default domain for the Kerberos realm used for translating v4 principal names.

isi auth krb5 realm list

Displays a list of MIT Kerberos realms.

Syntax

```bash
isi auth krb5 realm list
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
```

Options

- `--limit | -l <integer>`: Specifies the number of Kerberos realms to display.
- `--format {table | json | csv | list}`: Specifies whether to display the Kerberos realms in a tabular, JSON, CSV, or list format.
- `|--no-header | -a`
Specifies not to display the headers in the CSV or tabular formats.

```bash
--no-footer | -z
```

Specifies not to display the table summary footer information.

**isi auth krb5 realm view**

Displays the properties of an MIT Kerberos realm.

**Syntax**

```bash
isi auth krb5 realm view <realm>
```

**Options**

- `<realm>`
  - Specifies the Kerberos realm name.

**isi auth krb5 spn create**

Creates or updates keys for an MIT Kerberos provider.

**Syntax**

```bash
isi auth krb5 spn create <provider-name> <user> <spn> [--password <string>]
```

**Options**

- `<provider-name>`
  - Specifies the Kerberos provider name.
- `<user>`
  - Specifies a user name with permissions to create the service principal names (SPNs) in the Kerberos realm.
- `<spn>`
  - Specifies the SPN.
- `--password <string>`
  - Specifies the password used during the modification of a Kerberos realm.

**isi auth krb5 spn delete**

Deletes keys from an MIT Kerberos provider.

**Syntax**

```bash
isi auth krb5 spn delete <provider-name> <spn> {<kvno> | --all}
```

**Options**

- `<provider-name>`
  - Specifies the Kerberos provider name.
<spn>
    Specifies the service principal name (SPN).

<kvno>
    Specifies the key version number.

--all
    Deletes all the key versions.

**isi auth krb5 spn check**

Checks for missing service principal names (SPNs) for an MIT Kerberos provider.

**Syntax**

```
isi auth krb5 spn check <provider-name>
```

**Options**

`<provider-name>`
    Specifies the Kerberos provider name.

**isi auth krb5 spn fix**

Adds the missing service principal names (SPNs) for an MIT Kerberos provider.

**Syntax**

```
isi auth krb5 spn fix <provider-name> <user>
    [--password <string>]
    [--force]
```

**Options**

`<provider-name>`
    Specifies the Kerberos provider name.

`<user>`
    Specifies a user name with permissions to join clients to the given Kerberos domain.

`--password <string>`
    Specifies the password that was used when modifying the Kerberos realm.

`{--force | -f}`
    Specifies not to ask for a confirmation.
isi auth krb5 spn import

Imports keys from a keytab file for an MIT Kerberos provider.

Syntax

`isi auth krb5 spn import <provider-name> <keytab-file>`

Options

- `<provider-name>`
  Specifies the Kerberos provider name.

- `<keytab-file>`
  Specifies the keytab file to import.

isi auth krb5 spn list

Lists the service principal names (SPNs) and keys registered for an MIT Kerberos provider.

Syntax

`isi auth krb5 spn list <provider-name>`

Options

- `<provider-name>`
  Specifies the Kerberos provider name.

- `[--limit <integer>]`  
  Specifies the number of SPNs and keys to display.

- `[--format {table | json | csv | list}]`
  Specifies to display the SPNs and keys in a tabular, JSON, CSV, or list format.

- `[--no-header]`  
  Specifies not to display the headers in the CSV or tabular formats.

- `[--no-footer]`
  Specifies not to display the table summary footer information.
isi auth ldap create

Creates an LDAP provider.

Syntax

```bash
isi auth ldap create <name>
  [--base-dn <string>]
  [--server-uris <string>]
  [--alternate-security-identities-attribute <string>]
  [--authentication {yes | no}]
  [--balance-servers {yes | no}]
  [--bind-dn <string>]
  [--bind-timeout <integer>]
  [--certificate-authority-file <string>]
  [--check-online-interval <duration>]
  [--cn-attribute <string>]
  [--create-home-directory {yes | no}]
  [--crypt-password-attribute <string>]
  [--email-attribute <string>]
  [--enabled {yes | no}]
  [--enumerate-groups {yes | no}]
  [--enumerate-users {yes | no}]
  [--findable-groups <string>]
  [--findable-users <string>]
  [--gecos-attribute <string>]
  [--gid-attribute <string>]
  [--group-base-dn <string>]
  [--group-domain <string>]
  [--group-filter <string>]
  [--group-members-attribute <string>]
  [--group-search-scope <scope>]
  [--home-directory-template <string>]
  [--homedir-attribute <string>]
  [--ignore-tls-errors {yes | no}]
  [--listable-groups <string>]
  [--listable-users <string>]
  [--login-shell <string>]
  [--member-of-attribute <string>]
  [--name-attribute <string>]
  [--netgroup-base-dn <string>]
  [--netgroup-filter <string>]
  [--netgroup-members-attribute <string>]
  [--netgroup-search-scope <scope>]
  [--netgroup-triple-attribute <string>]
  [--normalize-groups {yes | no}]
  [--normalize-users {yes | no}]
  [--nt-password-attribute <string>]
  [--ntlm-support {all | v2only | none}]
  [--provider-domain <string>]
  [--require-secure-connection {yes | no}]
  [--restrict-findable {yes | no}]
  [--restrict-listable {yes | no}]
  [--search-scope <scope>]
  [--search-timeout <integer>]
  [--shell-attribute <string>]
  [--uid-attribute <string>]
  [--unfindable-groups <string>]
  [--unfindable-users <string>]
  [--unique-group-members-attribute <string>]
  [--unlistable-groups <string>]
  [--unlistable-users <string>]
  [--user-base-dn <string>]
  [--user-domain <string>]
  [--user-filter <string>]
  [--user-search-scope <scope>]
```
Options

<name>
    Sets the LDAP provider name.

--base-dn <string>
    Sets the root of the tree in which to search for identities. For example, CN=Users,DC=mycompany,DC=com.

--server-uris <string>
    Specifies a list of LDAP server URIs to be used when accessing the server. Repeat this option to specify multiple list items.
    Specify the LDAP server URI in the format ldaps://<server>:<port> for secure LDAP or ldap://<server>:<port> for non-secure LDAP.
    The server can be specified as an IPv4 address, an IPv6 address, or a hostname.
    If you do not specify a port number, the default port is used; 389 for secure LDAP or 636 for non-secure LDAP.

Note
    If you specify non-secure LDAP, the bind password is transmitted to the server in clear text.

--alternate-security-identities-attribute <string>
    Specifies the name to be used when searching for alternate security identities. This name is used when OneFS attempts to resolve a Kerberos principal to a user.

--authentication {yes | no}
    Enables or disables the use of the provider for authentication as well as identity. The default value is yes.

--balance-servers {yes | no}
    Makes the provider connect to a random server on each request.

--bind-dn <string>
    Specifies the distinguished name to use when binding to the LDAP server. For example, CN=myuser,CN=Users,DC=mycompany,DC=com.

--bind-timeout <integer>
    Specifies the timeout in seconds when binding to the LDAP server.

--certificate-authority-file <path>
    Specifies the path to the root certificates file.

--check-online-interval <duration>
    Specifies the time between provider online checks, in the format <integer>[{Y | M | W | D | H | m | s}].

--cn-attribute <string>
Specifies the LDAP attribute that contains common names. The default value is cn.

--create-home-directory {yes | no}
Specifies whether to automatically create a home directory the first time a user logs in, if a home directory does not already exist for the user.

--crypt-password-attribute <string>
Specifies the LDAP attribute that contains UNIX passwords. This setting has no default value.

--email-attribute <string>
Specifies the LDAP attribute that contains email addresses. The default value is mail.

--enabled {yes | no}
Enables or disables the provider.

--enumerate-groups {yes | no}
Specifies whether to allow the provider to enumerate groups.

--enumerate-users {yes | no}
Specifies whether to allow the provider to enumerate users.

--findable-groups <string>
Specifies a list of groups that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify each additional findable group. If populated, groups that are not included in this list cannot be resolved.

--findable-users <string>
Specifies a list of users that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify each additional findable user. If populated, users that are not included in this list cannot be resolved.

--gecos-attribute <string>
Specifies the LDAP attribute that contains GECOS fields. The default value is gecos.

--gid-attribute <string>
Specifies the LDAP attribute that contains GIDs. The default value is gidNumber.

--group-base-dn <string>
Specifies the distinguished name of the entry at which to start LDAP searches for groups.

--group-domain <string>
Specifies the domain that the provider will use to qualify groups. The default group domain is LDAP_GROUPS.

--group-filter <string>
Sets the LDAP filter for group objects.

--group-members-attribute <string>
Specifies the LDAP attribute that contains group members. The default value is memberUid.
**--group-search-scope <scope>**
Defines the default depth from the base distinguished name (DN) to perform LDAP searches for groups.
The following values are valid:

*default*
Applies the setting in `--search-scope`.

**Note**
You cannot specify `--search-scope=default`. For example, if you specify `--group-search-scope=default`, the search scope is set to the value of `--search-scope`.

*base*
Searches only the entry at the base DN.

*onelevel*
Searches all entries exactly one level below the base DN.

*subtree*
Searches the base DN and all entries below it.

*children*
Searches all entries below the base DN, excluding the base DN.

**--home-directory-template <path>**
Specifies the path to use as a template for naming home directories. The path must begin with `/ifs` and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, `%U`, `%D`, and `%Z` are replaced with the user name, provider domain name, and zone name, respectively. For more information about home directory variables, see Home directories.

**--homedir-attribute <string>**
Specifies the LDAP attribute that contains home directories. The default value is `homeDirectory`.

**--ignore-tls-errors {yes | no}**
Continues over a secure connection even if identity checks fail.

**--listable-groups <string>**
Specifies a list of groups that can be viewed in this provider if `--restrict-listable` is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be viewed.

**--listable-users <string>**
Specifies a list of users that can be viewed in this provider if `--restrict-listable` is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be viewed.

**--login-shell <path>**
Specifies the pathname of the user’s login shell for users who access the file system through SSH.
--member-of-attribute <string>
Sets the attribute to be used when searching LDAP for reverse memberships.
This LDAP value should be an attribute of the user type posixAccount that
describes the groups in which the POSIX user is a member.

--name-attribute <string>
Specifies the LDAP attribute that contains UIDs, which are used as login names.
The default value is uid.

--netgroup-base-dn <string>
Specifies the distinguished name of the entry at which to start LDAP searches for
netgroups.

--netgroup-filter <string>
Sets the LDAP filter for netgroup objects.

--netgroup-members-attribute <string>
 Specifies the LDAP attribute that contains netgroup members. The default value
is memberNisNetgroup.

--netgroup-search-scope <scope>
 Defines the depth from the base distinguished name (DN) to perform LDAP
searches for netgroups.
The following values are valid:

default
  Applies the setting in --search-scope.

  Note
  You cannot specify --search-scope=default. For example, if you
  specify --group-search-scope=default, the search scope is set to the
  value of --search-scope.

  base
  Searches only the entry at the base DN.

  onelevel
  Searches all entries exactly one level below the base DN.

  subtree
  Searches the base DN and all entries below it.

  children
  Searches all entries below the base DN, excluding the base DN.

--netgroup-triple-attribute <string>
Specifies the LDAP attribute that contains netgroup triples. The default value is
nisNetgroupTriple.

--normalize-groups {yes | no}
Normalizes group names to lowercase before lookup.

--normalize-users {yes | no}
Normalizes user names to lowercase before lookup.

`--nt-password-attribute <string>`
Specify the LDAP attribute that contains Windows passwords. A commonly used value is `ntpasswdhash`.

`--ntlm-support {all | v2only | none}`
For users with NTLM-compatible credentials, specifies which NTLM versions to support.

`--provider-domain <string>`
Specifies the domain that the provider will use to qualify user and group names.

`--require-secure-connection {yes | no}`
Specifies whether to require a TLS connection.

`--restrict-findable {yes | no}`
Specifies whether to check the provider for filtered lists of findable and unfindable users and groups.

`--restrict-listable {yes | no}`
Specifies whether to check the provider for filtered lists of listable and unlistable users and groups.

`--search-scope <scope>`
Defines the default depth from the base distinguished name (DN) to perform LDAP searches.
The following values are valid:
- `base`
  Searches only the entry at the base DN.
- `onelevel`
  Searches all entries exactly one level below the base DN.
- `subtree`
  Searches the base DN and all entries below it.
- `children`
  Searches all entries below the base DN, excluding the base DN itself.

`--search-timeout <integer>`
Specifies the number of seconds after which to stop retrying and fail a search.
The default value is 100.

`--shell-attribute <string>`
Specifies the LDAP attribute that contains a user's UNIX login shell. The default value is `loginShell`.

`--uid-attribute <string>`
Specifies the LDAP attribute that contains UID numbers. The default value is `uidNumber`.

`--unfindable-groups <string>`
If --restrict-findable is enabled and the findable groups list is empty, specifies a list of groups that cannot be resolved by this provider. Repeat this option to specify multiple list items.

```
--unfindable-users <string>
```

If --restrict-findable is enabled and the findable users list is empty, specifies a list of users that cannot be resolved by this provider. Repeat this option to specify multiple list items.

```
--unique-group-members-attribute <string>
```

Specifies the LDAP attribute that contains unique group members. This attribute is used to determine which groups a user belongs to if the LDAP server is queried by the user’s DN instead of the user’s name. This setting has no default value.

```
--unlistable-groups <string>
```

If --restrict-listable is enabled and the listable groups list is empty, specifies a list of groups that cannot be listed by this provider that cannot be viewed. Repeat this option to specify multiple list items.

```
--unlistable-users <string>
```

If --restrict-listable is enabled and the listable users list is empty, specifies a list of users that cannot be listed by this provider that cannot be viewed. Repeat this option to specify multiple list items.

```
--user-base-dn <string>
```

Specifies the distinguished name of the entry at which to start LDAP searches for users.

```
--user-domain <string>
```

Specifies the domain that the provider will use to qualify users. The default user domain is LDAP_USERS.

```
--user-filter <string>
```

Sets the LDAP filter for user objects.

```
--user-search-scope <scope>
```

Defines the depth from the base distinguished name (DN) to perform LDAP searches for users.

The following values are valid:

- `default`
  - Applies the search scope that is defined in the default query settings.

- `base`
  - Searches only the entry at the base DN.

- `onelevel`
  - Searches all entries exactly one level below the base DN.

- `subtree`
  - Searches the base DN and all entries below it.

- `children`
  - Searches all entries below the base DN, excluding the base DN itself.

```
--groupnet <groupnet>
```

Authentication

isi auth ldap create

307
Specifies the groupnet referenced by the LDAP provider. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the LDAP provider will use when communicating with external servers.

```bash
--bind-password <string>
```
Sets the password for the distinguished name that is used when binding to the LDAP server. To set the password interactively, use the `--set-bind-password` option instead.

```
--set-bind-password
```
Interactively sets the password for the distinguished name that is used when binding to the LDAP server. This option cannot be used with `--bind-password`.

```
{--verbose | -v}
```
Displays the results of running the command.

**isi auth ldap delete**

Deletes an LDAP provider.

**Syntax**

```bash
isi auth ldap delete <provider-name>
[--force]
[--verbose]
```

**Options**

**<provider-name>**
Specifies the name of the provider to delete.

```
{--force | -f}
```
Suppresses command-line prompts and messages.

**<provider-name>**
Specifies the name of the provider to delete.

```
{--verbose | -v}
```
Displays more detailed information.

**isi auth ldap list**

Displays a list of LDAP providers.

**Syntax**

```bash
isi auth ldap list
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```
Options

|--limit | -l <integer>
    Displays no more than the specified number of items.

|--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

|--no-header | -a
    Displays table and CSV output without headers.

|--no-footer | -z
    Displays table output without footers.

|--verbose | -v
    Displays more detailed information.

isi auth ldap modify

Modifies an LDAP provider.

Syntax

isi auth ldap modify <provider-name>
    [-name <string>]
    [-base-dn <string>]
    [-server-uris <string>]
    [-clear-server-uris]
    [-add-server-uris <string>]
    [-remove-server-uris <string>]
    [-alternate-security-identities-attribute <string>]
    [-authentication {yes | no}]
    [-balance-servers {yes | no}]
    [-bind-dn <string>]
    [-bind-timeout <integer>]
    [-certificate-authority-file <string>]
    [-check-online-interval <duration>]
    [-cn-attribute <string>]
    [-create-home-directory {yes | no}]
    [-crypt-password-attribute <string>]
    [-email-attribute <string>]
    [-enabled {yes | no}]
    [-enumerate-groups {yes | no}]
    [-enumerate-users {yes | no}]
    [-findable-groups <string>]
    [-clear-findable-groups]
    [-add-findable-groups <string>]
    [-remove-findable-groups <string>]
    [-findable-users <string>]
    [-clear-findable-users]
    [-add-findable-users <string>]
    [-remove-findable-users <string>]
    [-gecos-attribute <string>]
    [-gid-attribute <string>]
    [-group-base-dn <string>]
    [-group-domain <string>]
    [-group-filter <string>]
    [-group-members-attribute <string>]
    [-group-search-scope <scope>]
    [-homedir-attribute <string>]
    [-home-directory-template <string>]

Options

<provider-name>

Specifies the name of the LDAP provider to modify.

--name <string>

Specifies an new name for the authentication provider.

--base-dn <string>

Sets the root of the tree in which to search for identities. For example, CN=Users, DC=mycompany, DC=com.
--server-uris <string>
Specifies a list of LDAP server URIs to be used when accessing the server.
Repeat this option to specify multiple list items.
Specify the LDAP server URI in the format ldaps://<server>:<port> for secure LDAP or ldap://<server>:<port> for non-secure LDAP.
The server can be specified as an IPv4 address, an IPv6 address, or a hostname.
If you do not specify a port number, the default port is used; 389 for secure LDAP or 636 for non-secure LDAP.

Note
If you specify non-secure LDAP, the bind password is transmitted to the server in clear text.

--clear-server-uris
Removes all entries from the list of server URIs.

--add-server-uris <string>
Adds an entry to the list of server URIs. Repeat this option to specify multiple list items.
The server to be added can be specified as an IPv4 address, an IPv6 address, or a hostname.

--remove-server-uris <string>
Removes an entry from the list of server URIs. Repeat this option to specify multiple list items.
The server to be removed can be specified as an IPv4 address, an IPv6 address, or a hostname.

--alternate-security-identities-attribute <string>
Specifies the name to be used when searching for alternate security identities.
This name is used when OneFS attempts to resolve a Kerberos principal to a user.

--authentication {yes | no}
Enables or disables the use of this provider for authentication as well as identity.
The default value is yes.

--balance-servers {yes | no}
Makes this provider connect to a random server on each request.

--bind-dn <string>
Specifies the distinguished name to use when binding to the LDAP server. For example, CN=myuser,CN=Users,DC=mycompany,DC=com.

--bind-timeout <integer>
Specifies the timeout in seconds when binding to the LDAP server.

--certificate-authority-file <path>
Specifies the path to the root certificates file.

--check-online-interval <duration>
Specifies the time between provider online checks, in the format \(<integer>\{Y | M | W | D | H | m | s\}\).

**--cn-attribute <string>**
Specifies the LDAP attribute that contains common names. The default value is cn.

**--create-home-directory {yes | no}**
Specifies whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user. The directory path is specified in the path template through the **--home-directory-template** command.

**--crypt-password-attribute <string>**
Specifies the LDAP attribute that contains UNIX passwords. This setting has no default value.

**--email-attribute <string>**
Specifies the LDAP attribute that contains email addresses. The default value is mail.

**--enabled {yes | no}**
Enables or disables this provider.

**--enumerate-groups {yes | no}**
Specifies whether to allow the provider to enumerate groups.

**--enumerate-users {yes | no}**
Specifies whether to allow the provider to enumerate users.

**--findable-groups <string>**
Specifies a list of groups that can be found in this provider if **--restrict-findable** is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be resolved in this provider. This option overwrites the entries in the findable groups list; to add or remove groups without affecting current entries, use **--add-findable-groups** or **--remove-findable-groups**.

**--clear-findable-groups**
Removes the list of findable groups.

**--add-findable-groups <string>**
Adds an entry to the list of findable groups that is checked if **--restrict-findable** is enabled. Repeat this option to specify multiple list items.

**--remove-findable-groups <string>**
Removes an entry from the list of findable groups that is checked if **--restrict-findable** is enabled. Repeat this option to specify multiple list items.

**--findable-users <string>**
Specifies a list of users that can be found in this provider if **--restrict-findable** is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be resolved in this provider. This option overwrites the entries in the findable users list; to add or
remove users without affecting current entries, use `--add-findable-users` or `--remove-findable-users`.

`--clear-findable-users`
Removes the list of findable users.

`--add-findable-users <string>`
Adds an entry to the list of findable users that is checked if `--restrict-findable` is enabled. Repeat this option to specify multiple list items.

`--remove-findable-users <string>`
Removes an entry from the list of findable users that is checked if `--restrict-findable` is enabled. Repeat this option to specify multiple list items.

`--gecos-attribute <string>`
Specifies the LDAP attribute that contains GECOS fields. The default value is `gecos`.

`--gid-attribute <string>`
Specifies the LDAP attribute that contains GIDs. The default value is `gidNumber`.

`--group-base-dn <string>`
Specifies the distinguished name of the entry at which to start LDAP searches for groups.

`--group-domain <string>`
Specifies the domain that this provider will use to qualify groups. The default group domain is `LDAP_GROUPS`.

`--group-filter <string>`
Sets the LDAP filter for group objects.

`--group-members-attribute <string>`
Specifies the LDAP attribute that contains group members. The default value is `memberUid`.

`--group-search-scope <scope>`
Defines the default depth from the base distinguished name (DN) to perform LDAP searches for groups. The following values are valid:

- `default`
  Applies the setting in `--search-scope`.

  **Note**

  You cannot specify `--search-scope=default`. For example, if you specify `--group-search-scope=default`, the search scope is set to the value of `--search-scope`.

- `base`
  Searches only the entry at the base DN.

- `onelevel`
  Searches all entries exactly one level below the base DN.
subtree

Searches the base DN and all entries below it.

children

Searches all entries below the base DN, excluding the base DN.

--home-directory-template <path>

Specifies the path to use as a template for naming home directories. The path
must begin with /ifs and can include special character sequences that are
dynamically replaced with strings at home directory creation time that represent
specific variables. For example, %U, %D, and %Z are replaced with the user
name, provider domain name, and zone name, respectively. For more information,
see the Home directories section.

--homedir-attribute <string>

Specifies the LDAP attribute that is used when searching for the home directory.
The default value is homeDirectory.

--ignore-tls-errors {yes | no}

Continues over a secure connection even if identity checks fail.

--listable-groups <string>

Specifies a list of groups that can be viewed in this provider if --restrict-
listable is enabled. Repeat this option to specify multiple list items. If
populated, groups that are not included in this list cannot be viewed in this
provider. This option overwrites the entries in the listable groups list; to add or
remove groups without affecting current entries, use --add-listable-
groups or --remove-listable-groups.

--clear-listable-groups

Removes all entries from the list of viewable groups.

--add-listable-groups <string>

Adds an entry to the list of listable groups that is checked if --restrict-
listable is enabled. Repeat this option to specify multiple list items.

--remove-listable-groups <string>

Removes an entry from the list of viewable groups that is checked if --
restrict-listable is enabled. Repeat this option to specify multiple list
items.

--listable-users <string>

Specifies a list of users that can be viewed in this provider if --restrict-
listable is enabled. Repeat this option to specify multiple list items. If
populated, users that are not included in this list cannot be viewed in this
provider. This option overwrites the entries in the listable users list; to add or
remove users without affecting current entries, use --add-listable-users
or --remove-listable-users.

--clear-listable-users

Removes all entries from the list of viewable users.

--add-listable-users <string>
Adds an entry to the list of listable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

**--remove-listable-users <string>**
Removes an entry from the list of viewable users that is checked if -- restrict-listable is enabled. Repeat this option to specify multiple list items.

**--login-shell <path>**
Specifies the pathname to the user's login shell, for users who access the file system through SSH.

**--member-of-attribute <string>**
Sets the attribute to be used when searching LDAP for reverse memberships. This LDAP value should be an attribute of the user type posixAccount that describes the groups in which the POSIX user is a member.

**--name-attribute <string>**
Specifies the LDAP attribute that contains UIDs, which are used as login names. The default value is uid.

**--netgroup-base-dn <string>**
Specifies the distinguished name of the entry at which to start LDAP searches for netgroups.

**--netgroup-filter <string>**
Sets the LDAP filter for netgroup objects.

**--netgroup-members-attribute <string>**
Specifies the LDAP attribute that contains netgroup members. The default value is memberNisNetgroup.

**--netgroup-search-scope <scope>**
Defines the depth from the base distinguished name (DN) to perform LDAP searches for netgroups. The following values are valid:

- **default**
  Applies the setting in --search-scope.

  **Note**
  You cannot specify --search-scope=default. For example, if you specify --group-search-scope=default, the search scope is set to the value of --search-scope.

- **base**
  Searches only the entry at the base DN.

- **onelevel**
  Searches all entries exactly one level below the base DN.

- **subtree**
  Searches the base DN and all entries below it.
children
   Searches all entries below the base DN, excluding the base DN.

--netgroup-triple-attribute <string>
   Specifies the LDAP attribute that contains netgroup triples. The default value is nisNetgroupTriple.

--normalize-groups {yes | no}
   Normalizes group names to lowercase before lookup.

--normalize-users {yes | no}
   Normalizes user names to lowercase before lookup.

--nt-password-attribute <string>
   Specifies the LDAP attribute that contains Windows passwords. A commonly used value is ntpasswdhash.

--ntlm-support {all | v2only | none}
   For users with NTLM-compatible credentials, specifies which NTLM versions to support.
   The following values are valid:
      all
      v2only
      none

--provider-domain <string>
   Specifies the domain that this provider will use to qualify user and group names.

--require-secure-connection {yes | no}
   Specifies whether to require a TLS connection.

--restrict-findable {yes | no}
   Specifies whether to check this provider for filtered lists of findable and unfindable users and groups.

--restrict-listable {yes | no}
   Specifies whether to check this provider for filtered lists of viewable and unviewable users and groups.

--search-scope <scope>
   Defines the default depth from the base distinguished name (DN) to perform LDAP searches.
   The following values are valid:
      base
         Searches only the entry at the base DN.
      onelevel
         Searches all entries exactly one level below the base DN.
      subtree
         Searches the base DN and all entries below it.
children

Searches all entries below the base DN, excluding the base DN itself.

--search-timeout <integer>

Specifies the number of seconds after which to stop retrying and fail a search. The default value is 100.

--shell-attribute <string>

Specifies the LDAP attribute that is used when searching for a user’s UNIX login shell. The default value is loginShell.

--uid-attribute <string>

Specifies the LDAP attribute that contains UID numbers. The default value is uidNumber.

--unfindable-groups <string>

Specifies a group that cannot be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unfindable groups list; to add or remove groups without affecting current entries, use --add-unfindable-groups or --remove-unfindable-groups.

--clear-unfindable-groups

Removes all entries from the list of unfindable groups.

--add-unfindable-groups <string>

Adds an entry to the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-groups <string>

Removes an entry from the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unfindable-users <string>

Specifies a user that cannot be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unfindable users list; to add or remove users without affecting current entries, use --add-unfindable-users or --remove-unfindable-users.

--clear-unfindable-users

Removes all entries from the list of unfindable groups.

--add-unfindable-users <string>

Adds an entry to the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-users <string>

Removes an entry from the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unique-group-members-attribute <string>
Specifies the LDAP attribute that contains unique group members. This attribute is used to determine which groups a user belongs to if the LDAP server is queried by the user’s DN instead of the user’s name. This setting has no default value.

`--unlistable-groups <string>`

Specifies a group that cannot be listed in this provider if `--restrict-listable` is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unlistable groups list; to add or remove groups without affecting current entries, use `--add-unlistable-groups` or `--remove-unlistable-groups`.

`--clear-unlistable-groups`

Removes all entries from the list of unviewable groups.

`--add-unlistable-groups <string>`

Adds an entry to the list of unviewable groups that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--remove-unlistable-groups <string>`

Removes an entry from the list of unviewable groups that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--unlistable-users <string>`

Specifies a user that cannot be viewed in this provider if `--restrict-listable` is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unlistable users list; to add or remove users without affecting current entries, use `--add-unlistable-users` or `--remove-unlistable-users`.

`--clear-unlistable-users`

Removes all entries from the list of unviewable users.

`--add-unlistable-users <string>`

Adds an entry to the list of unviewable users that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--remove-unlistable-users <string>`

Removes an entry from the list of unviewable users that is checked if `--restrict-listable` is enabled. Repeat this option to specify multiple list items.

`--user-base-dn <string>`

Specifies the distinguished name of the entry at which to start LDAP searches for users.

`--user-domain <string>`

Specifies the domain that this provider will use to qualify users. The default user domain is `LDAP_USERS`.

`--user-filter <string>`

Sets the LDAP filter for user objects.

`--user-search-scope <scope>`
Defines the depth from the base distinguished name (DN) to perform LDAP searches for users. The valid values are as follows:

The following values are valid:

**default**
- Applies the setting in `--search-scope`.

**Note**
- You cannot specify `--search-scope=default`. For example, if you specify `--user-search-scope=default`, the search scope is set to the value of `--search-scope`.

**base**
- Searches only the entry at the base DN.

**onelevel**
- Searches all entries exactly one level below the base DN.

**subtree**
- Searches the base DN and all entries below it.

**children**
- Searches all entries below the base DN, excluding the base DN.

**--bind-password <string>**
- Sets the password for the distinguished name that is used when binding to the LDAP server. To set the password interactively, use the `--set-bind-password` option instead.

**--set-bind-password**
- Interactively sets the password for the distinguished name that is used when binding to the LDAP server. This option cannot be used with `--bind-password`.

**{--verbose | -v}**
- Displays detailed information.

### isi auth ldap view

Displays the properties of an LDAP provider.

**Syntax**

```
isi auth ldap view <provider-name>
```

**Options**

**<provider-name>**
- Specifies the name of the provider to view.
### isi auth local list

Displays a list of local providers.

#### Syntax

```bash
isi auth local list
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

#### Options

- **{--limit | -l} <integer>**
  Displays no more than the specified number of items.

- **--format {table | json | csv | list}**
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

- **{--no-header | -a}**
  Displays table and CSV output without headers.

- **{--no-footer | -z}**
  Displays table output without footers.

- **{--verbose | -v}**
  Displays more detailed information.

### isi auth local modify

Modifies a local provider.

#### Syntax

```bash
isi auth local modify <provider-name>
   [--authentication {yes | no}]
   [--create-home-directory {yes | no}]
   [--home-directory-template <string>]
   [--lockout-duration <duration>]
   [--lockout-threshold <integer>]
   [--lockout-window <duration>]
   [--login-shell <string>]
   [--machine-name <string>]
   [--min-password-age <duration>]
   [--max-password-age <duration>]
   [--min-password-length <integer>]
   [--password-prompt-time <duration>]
   [--password-complexity {lowercase | uppercase | numeric | symbol}]
   [--clear-password-complexity]
   [--add-password-complexity {lowercase | uppercase | numeric | symbol}]
   [--remove-password-complexity <string>]
   [--password-history-length <integer>]
   [--verbose]
```
Options

<provider-name>
   Specifies the name of the local provider to modify.

--authentication {yes | no}
   Uses the provider for authentication as well as identity. The default setting is yes.

--create-home-directory {yes | no}
   Creates a home directory the first time a user logs in.

--home-directory-template <string>
   Specifies the path to use as a template for naming home directories. The path must begin with /ifs and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, %U, %D, and %Z are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

--lockout-duration <duration>
   Sets the length of time that an account will be inaccessible after multiple failed login attempts.

--lockout-threshold <integer>
   Specifies the number of failed login attempts after which an account will be locked out.

--lockout-window <duration>
   Sets the time in which the number of failed attempts specified by the --lockout-threshold option must be made for an account to be locked out. Duration is specified in the format <integer>[{Y | M | W | D | H | m | s}].

--login-shell <string>
   Specifies the path to the UNIX login shell.

--machine-name <string>
   Specifies the domain to use to qualify user and group names for the provider.

--min-password-age <duration>
   Sets the minimum password age, in the format <integer>[{Y | M | W | D | H | m | s}].

--max-password-age <duration>
   Sets the maximum password age, in the format <integer>[{Y | M | W | D | H | m | s}].

--min-password-length <integer>
   Sets the minimum password length.

--password-prompt-time <duration>
   Sets the remaining time until a user is prompted for a password change, in the format <integer>[{Y | M | W | D | H | m | s}].

--password-complexity {lowercase | uppercase | numeric | symbol}
Specifies the conditions that a password is required to meet. A password must contain at least one character from each specified option to be valid. For example, if lowercase and numeric are specified, a password must contain at least one lowercase character and one digit to be valid. Symbols are valid, excluding # and @.

--clear-password-complexity
Cleans the list of parameters against which to validate new passwords.

--add-password-complexity {lowercase | uppercase | numeric | symbol}
Adds items to the list of parameters against which to validate new passwords. Repeat this command to specify additional password-complexity options.

--remove-password-complexity <string>
Removes items from the list of parameters against which to validate new passwords. Repeat this command to specify each password-complexity option that you want to remove.

--password-history-length <integer>
Specifies the number of previous passwords to store to prevent reuse of a previous password. The max password history length is 24.

{--verbose | -v}
Displays more detailed information.

isi auth local view
Displays the properties of a local provider.

Syntax

isi auth local view <provider-name>

Options

<provider-name>
Specifies the name of the provider to view.

isi auth log-level modify
Specifies the logging level for the authentication service on the node.

Syntax

isi auth log-level modify <level> [--verbose]

Options

<level>
Sets the log level for the current node. The log level determines how much information is logged.
The following values are valid and are organized from least to most information:

- always
• error
• warning
• info
• verbose
• debug
• trace

Note
Levels verbose, debug, and trace may cause performance issues. Levels debug and trace log information that likely will be useful only when consulting EMC Isilon Technical Support.

{--verbose | -v}
Displays detailed information.

isi auth log-level view
Displays the logging level for the authentication service on the node.

Syntax

isi auth log-level view

Options
There are no options for this command.

isi auth mapping create
Creates a manual mapping between a source identity and target identity or automatically generates a mapping for a source identity.

Syntax

isi auth mapping create {<source>| --source-uid <integer> |
| --source-gid <integer> | --source-sid <string>} |
|{--uid | --gid | --sid}}
|--on-disk
|--2way
|{--target <string> | --target-uid <integer> |
| | --target-gid <integer> | --target-sid <string>}|
|--zone<string>]

Options

<source>
Specifies the mapping source by identity type, in the format <type>:<value>—for example, UID:2002.

--source-uid <integer>
Specifies the mapping source by UID.

--source-gid <integer>
Specifies the mapping source by GID.
--source-sid <string>
  Specifies the mapping source by SID.

--uid
  Generates a mapping if one does not exist for the identity; otherwise, retrieves
  the mapped UID.

--gid
  Generates a mapping if one does not exist for the identity; otherwise, retrieves
  the mapped GID.

--sid
  Generates a mapping if one does not exist for the identity; otherwise, retrieves
  the mapped SID.

--on-disk
  Specifies that the source on-disk identity should be represented by the target
  identity.

--2way
  Specifies a two-way, or reverse, mapping.

--target <string>
  Specifies the mapping target by identity type, in the format <type>:<value>—for
  example, UID:2002.

--target-uid <integer>
  Specifies the mapping target by UID.

--target-gid <integer>
  Specifies the mapping target by GID.

--target-sid <string>
  Specifies the mapping target by SID.

--zone <string>
  Specifies the access zone that the ID mapping is applied to. If no access zone is
  specified, the mapping is applied to the default System zone.

isi auth mapping delete

Deletes one or more identity mappings.

Syntax

isi auth mapping delete [<source>| --source-uid <integer>  
  | --source-gid <integer> | --source-sid <string> | --all]   
  [{--only-generated | --only-external | --2way | --target <string>  
  | --target-uid <integer> | --target-gid <integer> | --target-sid <string>]}  
  [--zone <string>]

Options

<source>
Specifies the mapping source by identity type, in the format `<type>:<value>`—for example, `UID:2002`.

`--source-uid <integer>`
   Specifies the mapping source by UID.

`--source-gid <integer>`
   Specifies the mapping source by GID.

`--source-sid <string>`
   Specifies the mapping source by SID.

`--all`
   Deletes all identity mappings in the specified access zone. Can be used in conjunction with `--only-generated` and `--only-external` for additional filtering.

`--only-generated`
   Only deletes identity mappings that were created automatically and that include a generated UID or GID from the internal range of user and group IDs. Must be used in conjunction with `--all`.

`--only-external`
   Only deletes identity mappings that were created automatically and that include a UID or GID from an external authentication source. Must be used in conjunction with `--all`.

`--2way`
   Specifies or deletes a two-way, or reverse, mapping.

`--target <string>`
   Specifies the mapping target by identity type, in the format `<type>:<value>`—for example, `UID:2002`.

`--target-uid <integer>`
   Specifies the mapping target by UID.

`--target-gid <integer>`
   Specifies the mapping target by GID.

`--target-sid <string>`
   Specifies the mapping target by SID.

`--zone <string>`
   Deletes identity mappings in the specified access zone. If no access zone is specified, mappings are deleted from the default System zone.
**isi auth mapping dump**

Displays or prints the kernel mapping database.

**Syntax**

```
isi auth mapping dump
    [--file <path>]
    [--zone <string>]
```

**Options**

If no option is specified, the full kernel mapping database is displayed.

- `[--file | -f] <path>`
  Prints the database to the specified output file.

- `--zone <string>`
  Displays the database from the specified access zone. If no access zone is specified, displays all mappings.

**Examples**

To view the kernel mapping database, run the following command:

```
isi auth mapping dump
```

The system displays output similar to the following example:

```
["ZID:1", "UID:6299", ["SID:S-1-5-21-1195855716-1407", 128]]
["ZID:1", "GID:1000000", ["SID:S-1-5-21-1195855716-513", 48]]
["ZID:1", "UID:6299", ["GID:1000000", 32]]
```

**isi auth mapping flush**

Flushes the cache for one or all identity mappings. Flushing the cache might be useful if the ID mapping rules have been modified.

**Syntax**

```
isi auth mapping flush (--all | --source <string>)
    | --source-uid <integer> | --source-gid <integer>
    | --source-sid <string>
    [--zone <string>]
```

**Options**

You must specify either `--all` or one of the source options.

- `--all`
  Flushes all identity mappings on the EMC Isilon cluster.

- `--source <string>`
  Specifies the mapping source by identity type, in the format `<type>:<value>`—for example, `UID:2002`.

- `--source-uid <integer>`

- `--source-gid <integer>`

- `--source-sid <string>`
Specifies the source identity by UID.

--source-gid <integer>
  Specifies the source identity by GID.

--source-sid <string>
  Specifies the source identity by SID.

--zone <string>
  Specifies the access zone of the source identity. If no access zone is specified, any mapping for the specified source identity is flushed from the default System zone.

isi auth mapping import

Imports mappings from a source file to the ID mapping database.

Syntax

isi auth mapping import <file>
  [--replace]
  [--verbose]

Options

<file>
  Specifies the full path to the file to import. File content must be in the same format as the output that is displayed by running the isi auth mapping dump command. File must exist with the /ifs file structure.

{--replace | -o}
  Overwrites existing entries in the mapping database file with the file content.

{--verbose | -v}
  Displays detailed information.

isi auth mapping list

Displays the ID mapping database for an access zone.

Syntax

isi auth mapping list
  [--zone <string>]

Options

--zone <string>
  Specifies an access zone.
isi auth mapping modify

Sets or modifies a mapping between two identities.

Syntax

```
isi auth mapping modify {<source>| --source-uid <integer>
 | --source-gid <integer> | --source-sid <string> | --target
 <string>
 | --target-uid <integer> | --target-gid <string> |
 --target-sid <string>}
 [--on-disk]
 [--2way]
 [--zone <string>]
```

Options

**<source>**

Specifies the mapping source by identity type, in the format `<type>:<value>`—for example, `UID:2002`.

**--source-uid <integer>**

Specifies the mapping source by UID.

**--source-gid <integer>**

Specifies the mapping source by GID.

**--source-sid <string>**

Specifies the mapping source by SID.

**--target <string>**

Specifies the mapping target by identity type, in the format `<type>:<value>`—for example, `UID:2002`.

**--target-uid <integer>**

Specifies the mapping target by UID.

**--target-gid <integer>**

Specifies the mapping target by GID.

**--target-sid <string>**

Specifies the mapping target by SID.

**--on-disk**

Specifies that the source on-disk identity should be represented by the target identity.

**--2way**

Specifies a two-way, or reverse, mapping.

**--zone <string>**

Specifies the access zone that the ID mapping is applied to. If no access zone is specified, the mapping is applied to the default System zone.
isi auth mapping token

Displays the access token that is calculated for a user during authentication.

Syntax

```
isi auth mapping token {<user> | --uid <integer>
    | --kerberos-principal <string>}
    [--zone <string>]
    [--primary-gid <integer>]
    [--gid <integer>]
```

Options

This command requires `<user>` or `--uid <integer>` or `--kerberos-principal <string>`.

`<user>`

Specifies the user by name.

`--uid <integer>`

Specifies the user by UID.

`--kerberos-principal <string>`

Specifies the Kerberos principal by name. For example, user@realm.com.

`--zone <string>`

Specifies the name of the access zone that contains the mapping.

`--primary-gid <integer>`

Specifies the primary GID.

`--gid <integer>`

Specifies a token GID. Repeat this option to specify multiple GIDs.

isi auth mapping view

Displays mappings for an identity.

Syntax

```
isi auth mapping view {<id>| --uid <integer>
    | --gid <integer> | --sid <string>}
    [--nocreate]
    [--zone <string>]
```

Options

`<id>`

Specifies the ID of the source identity type in the format `<type>:<value>—for example, UID:2002.`

`--uid <integer>`

Specifies the mapping source by UID.
--gid <integer>
   Specifies the mapping source by GID.

--sid <string>
   Specifies the mapping source by SID.

--nocreate
   Specifies that nonexistent mappings should not be created.

--zone
   Specifies the access zone of the source identity. If no access zone is specified, OneFS displays mappings from the default System zone.

Examples
The following command displays mappings for a user whose UID is 2002 in the zone3 access zone:

```
isi auth mapping view uid:2002 --zone=zone3
```

The system displays output similar to the following example:

```
Type       Mapping
---------- ----------------------------------------------
Name       test1                                  
On-disk    UID:2002
Unix UID   2002
Unix GID   None
SMB        S-1-5-21-1776575851-2890035977-2418728619-1004
NFSv4      test1
```

**isi auth netgroups view**

Displays information about a netgroup.

**Syntax**

```
isi auth netgroups view <netgroup>
   [--zone <string>]
   [--provider <string>]
   [--recursive {true | false}]
   [--ignore-errors {true | false}]
```

**Options**

**<netgroup>**
   Specifies the netgroup name.

--zone <string>
   Specifies the access zone.

--provider <string>
   Specifies the authentication provider.

--recursive {true | false}
   Specifies wether to recursively resolve nested netgroups. The default value is true.
--ignore {true | false}
    Specifies whether to ignore errors and unresolvable netgroups. The default value is false.

isi auth nis create

Creates an NIS provider.

Syntax

    isi auth nis create <name>
        [--nis-domain <string>]
        [--servers <string>]
        [--authentication {yes | no}]
        [--balance-servers {yes | no}]
        [--check-online-interval <duration>]
        [--create-home-directory {yes | no}]
        [--enabled {yes | no}]
        [--enumerate-groups {yes | no}]
        [--enumerate-users {yes | no}]
        [--findable-groups <string>]
        [--findable-users <string>]
        [--group-domain <string>]
        [--home-directory-template <path>]
        [--hostname-lookup {yes | no}]
        [--listable-groups <string>]
        [--listable-users <string>]
        [--login-shell <path>]
        [--normalize-groups {yes | no}]
        [--normalize-users {yes | no}]
        [--provider-domain <string>]
        [--ntlm-support {all | v2only | none}]
        [--request-timeout <integer>]
        [--restrict-findable {yes | no}]
        [--restrict-listable {yes | no}]
        [--retry-time <integer>]
        [--unfindable-groups <string>]
        [--unfindable-users <string>]
        [--unlistable-groups <string>]
        [--unlistable-users <string>]
        [--user-domain <string>]
        [--ypmatch-using-tcp {yes | no}]
        [--groupnet <groupnet>]
        [--verbose]

Options

    <name>
        Sets the name of the NIS provider.

    --nis-domain <string>
        Specifies the NIS domain name.

    --servers <string>
        Specifies a list of NIS servers to be used by this provider. Specify the NIS server as an IPv4 address or hostname. Repeat this option to specify multiple list items.

    --authentication {yes | no}
        Enables or disables the use of the provider for authentication as well as identity. The default value is yes.
--balance-servers \{yes | no\}
Makes the provider connect to a random server on each request.

--check-online-interval \texttt{<duration>}
Specifies the time between provider online checks, in the format \texttt{<integer>\{[Y | M | W | D | H | m | s]\}}.

--create-home-directory \{yes | no\}
Specifies whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user.

--enabled \{yes | no\}
Enables or disables the provider.

--enumerate-groups \{yes | no\}
Specifies whether to allow the provider to enumerate groups.

--enumerate-users \{yes | no\}
Specifies whether to allow the provider to enumerate users.

--findable-groups \texttt{<string>}
Specifies a group that can be found in this provider if \texttt{--restrict-findable} is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be resolved.

--findable-users \texttt{<string>}
Specifies a user that can be found in this provider if \texttt{--restrict-findable} is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be resolved.

--group-domain \texttt{<string>}
Specifies the domain that this provider will use to qualify groups. The default group domain is \texttt{NIS\_GROUPS}.

--home-directory-template \texttt{<path>}
Specifies the path to use as a template for naming home directories. The path must begin with \texttt{/ifs} and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, \texttt{%U}, \texttt{%D}, and \texttt{%Z} are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

--hostname-lookup \{yes | no\}
Enables or disables host name lookups.

--listable-groups \texttt{<string>}
Specifies a group that can be viewed in this provider if \texttt{--restrict-listable} is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be viewed.

--listable-users \texttt{<string>}
Specifies a user that can be viewed in this provider if \texttt{--restrict-listable} is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be viewed.
--login-shell <path>
    Specifies the path to the user's login shell. This setting applies only to users who
    access the file system through SSH.

--normalize-groups {yes | no}
    Normalizes group name to lowercase before lookup.

--normalize-users {yes | no}
    Normalizes user name to lowercase before lookup.

--provider-domain <string>
    Specifies the domain that this provider will use to qualify user and group names.

--ntlm-support {all | v2only | none}
    For users with NTLM-compatible credentials, specifies which NTLM versions to
    support. Valid values are all, v2only, and none. NTLMv2 provides additional
    security over NTLM.

--request-timeout <integer>
    Specifies the request timeout interval in seconds. The default value is 20.

--restrict-findable {yes | no}
    Specifies whether to check this provider for filtered lists of findable and
    unfindable users and groups.

--restrict-listable {yes | no}
    Specifies whether to check this provider for filtered lists of viewable and
    unviewable users and groups.

--retry-time <integer>
    Sets the timeout period in seconds after which a request will be retried. The
    default value is 5.

--unfindable-groups <string>
    If --restrict-findable is enabled and the findable groups list is empty,
    specifies a group that cannot be resolved by this provider. Repeat this option to
    specify multiple list items.

--unfindable-users <string>
    If --restrict-findable is enabled and the findable users list is empty,
    specifies a user that cannot be resolved by this provider. Repeat this option to
    specify multiple list items.

--unlistable-groups <string>
    If --restrict-listable is enabled and the listable groups list is empty,
    specifies a group that cannot be viewed by this provider. Repeat this option to
    specify multiple list items.

--unlistable-users <string>
    If --restrict-listable is enabled and the listable users list is empty,
    specifies a user that cannot be viewed by this provider. Repeat this option to
    specify multiple list items.

--user-domain <string>
Specifies the domain that this provider will use to qualify users. The default user domain is **NIS_USERS**.

```
--ypmatch-using-tcp {yes | no}
```

Uses TCP for YP Match operations.

```
--groupnet <groupnet>
```

Specifies the groupnet referenced by the NIS provider. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the NIS provider will use when communicating with external servers.

```
|--verbose | -v
```

Displays the results of running the command.

### isi auth nis delete

Deletes an NIS provider.

**Syntax**

```
isi auth nis delete <provider-name>
```

#### Options

```
<provider-name>
```

Specifies the name of the provider to delete.

```
|--force | -f
```

Suppresses command-line prompts and messages.

```
|--verbose | -v
```

Returns a success or fail message after running the command.

### isi auth nis list

Displays a list of NIS providers and indicates whether a provider is functioning correctly.

**Syntax**

```
isi auth nis list
```

#### Options

```
|--limit <integer>
```

Displays no more than the specified number of items.
--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

**isi auth nis modify**

Modifies an NIS provider.

**Syntax**

```
isi auth nis modify <provider-name>
[--name <string>]
[--nis-domain <string>]
[--servers <string>]
[--clear-servers]
[--add-servers <string>]
[--remove-servers <string>]
[--authentication {yes | no}]
[--balance-servers {yes | no}]
[--check-online-interval <duration>]
[--create-home-directory {yes | no}]
[--enabled {yes | no}]
[--enumerate-groups {yes | no}]
[--enumerate-users {yes | no}]
[--findable-groups <string>]
[--clear-findable-groups]
[--add-findable-groups <string>]
[--remove-findable-groups <string>]
[--findable-users <string>]
[--clear-findable-users]
[--add-findable-users <string>]
[--remove-findable-users <string>]
[--group-domain <string>]
[--home-directory-template <string>]
[--hostname-lookup {yes | no}]
[--listable-groups <string>]
[--clear-listable-groups]
[--add-listable-groups <string>]
[--remove-listable-groups <string>]
[--listable-users <string>]
[--clear-listable-users]
[--add-listable-users <string>]
[--remove-listable-users <string>]
[--login-shell <string>]
[--normalize-groups {yes | no}]
[--normalize-users {yes | no}]
[--provider-domain <string>]
[--ntlm-support {all | v2only | none}]
[--request-timeout <integer>]
[--restrict-findable {yes | no}]
[--restrict-listable {yes | no}]
[--retry-time <integer>]
[--unfindable-groups <string>]
[--clear-unfindable-groups]
```
Options

<provider-name>
   Specifies the name of the NIS provider to modify.

--name <string>
   Specifies a new name for the authentication provider.

--nis-domain <string>
   Specifies the NIS domain name.

--servers <string>
   Specifies a list of NIS server to be used by this provider. Repeat this option to specify multiple list items. Specify the NIS server as an IPv4 address or hostname. This option overwrites the entries in the NIS servers list; to add or remove servers without affecting current entries, use --add-servers or --remove-servers.

--clear-servers
   Removes all entries from the list of NIS servers.

--add-servers <string>
   Adds an entry to the list of NIS servers. Repeat this option to specify multiple items.

--remove-servers <string>
   Removes an entry from the list of NIS servers. Repeat this option to specify multiple items.

--authentication {yes | no}
   Enables or disables the use of this provider for authentication as well as identity. The default value is yes.

--balance-servers {yes | no}
   Makes this provider connect to a random server on each request.

--check-online-interval <duration>
   Specifies the time between provider online checks, in the format <integer>[:Y | M | W | D | H | m | s].
--create-home-directory {yes | no}
Specifies whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user.

--enabled {yes | no}
Enables or disables this provider.

--enumerate-groups {yes | no}
Specifies whether to allow this provider to enumerate groups.

--enumerate-users {yes | no}
Specifies whether to allow this provider to enumerate users.

--findable-groups <string>
Specifies a group that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be resolved. This option overwrites the entries in the findable groups list; to add or remove groups without affecting current entries, use --add-findable-groups or --remove-findable-groups.

--clear-findable-groups
Removes all entries from the list of findable groups.

--add-findable-groups <string>
Adds an entry to the list of findable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-findable-groups <string>
Removes an entry from the list of findable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--findable-users <string>
Specifies a user that can be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be resolved. This option overwrites the entries in the findable users list; to add or remove users without affecting current entries, use --add-findable-users or --remove-findable-users.

--clear-findable-users
Removes all entries from the list of findable users.

--add-findable-users <string>
Adds an entry to the list of findable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-findable-users <string>
Removes an entry from the list of findable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--group-domain <string>
Specifies the domain that this provider will use to qualify groups. The default group domain is NIS_GROUPS.

--home-directory-template <path>
Specifies the path to use as a template for naming home directories. The path must begin with /ifs and can include special character sequences that are dynamically replaced with strings at home directory creation time that represent specific variables. For example, %U, %D, and %Z are replaced with the user name, provider domain name, and zone name, respectively. For more information, see the Home directories section.

--hostname-lookup {yes | no}
Enables or disables host name lookups.

--listable-groups <string>
Specifies a group that can be viewed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. If populated, groups that are not included in this list cannot be viewed. This option overwrites the entries in the listable groups list; to add or remove groups without affecting current entries, use --add-listable-groups or --remove-listable-groups.

--clear-listable-groups
Removes all entries from the list of viewable groups.

--add-listable-groups <string>
Adds an entry to the list of viewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-listable-groups <string>
Removes an entry from the list of viewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--listable-users <string>
Specifies a user that can be viewed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. If populated, users that are not included in this list cannot be viewed. This option overwrites the entries in the listable users list; to add or remove users without affecting current entries, use --add-listable-users or --remove-listable-users.

--clear-listable-users
Removes all entries from the list of viewable users.

--add-listable-users <string>
Adds an entry to the list of viewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-listable-users <string>
Removes an entry from the list of viewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--login-shell <path>
Specifies the path to the user's login shell. This setting applies only to users who access the file system through SSH.

--normalize-groups {yes | no}
Normalizes group names to lowercase before lookup.
--normalize-users {yes | no}
   Normalizes user names to lowercase before lookup.

--provider-domain <string>
   Specifies the domain that this provider will use to qualify user and group names.

--ntlm-support {all | v2only | none}
   For users with NTLM-compatible credentials, specifies which NTLM versions to support. Valid values are all, v2only, and none. NTLMv2 provides additional security over NTLM.

--request-timeout <integer>
   Specifies the request timeout interval in seconds. The default value is 20.

--restrict-findable {yes | no}
   Specifies whether to check this provider for filtered lists of findable and unfindable users and groups.

--restrict-listable {yes | no}
   Specifies whether to check this provider for filtered lists of viewable and unviewable users and groups.

--retry-time <integer>
   Sets the timeout period in seconds after which a request will be retried. The default value is 5.

--unfindable-groups <string>
   Specifies a group that cannot be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unfindable groups list; to add or remove groups without affecting current entries, use --add-unfindable-groups or --remove-unfindable-groups.

--clear-unfindable-groups
   Removes all entries from the list of unfindable groups.

--add-unfindable-groups <string>
   Adds an entry to the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-groups <string>
   Removes an entry from the list of unfindable groups that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unfindable-users <string>
   Specifies a user that cannot be found in this provider if --restrict-findable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unfindable users list; to add or remove users without affecting current entries, use --add-unfindable-users or --remove-unfindable-users.

--clear-unfindable-users
   Removes all entries from the list of unfindable groups.
--add-unfindable-users <string>
Adds an entry to the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--remove-unfindable-users <string>
Removes an entry from the list of unfindable users that is checked if --restrict-findable is enabled. Repeat this option to specify multiple list items.

--unlistable-groups <string>
Specifies a group that cannot be listed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unlistable groups list; to add or remove groups without affecting current entries, use --add-unlistable-groups or --remove-unlistable-groups.

--clear-unlistable-groups
Removes all entries from the list of unlistable groups.

--add-unlistable-groups <string>
Adds an entry to the list of unviewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-unlistable-groups <string>
Removes an entry from the list of unviewable groups that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--unlistable-users <string>
Specifies a user that cannot be listed in this provider if --restrict-listable is enabled. Repeat this option to specify multiple list items. This option overwrites the entries in the unlistable users list; to add or remove users without affecting current entries, use --add-unlistable-users or --remove-unlistable-users.

--clear-unlistable-users
Removes all entries from the list of unviewable users.

--add-unlistable-users <string>
Adds an entry to the list of unviewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--remove-unlistable-users <string>
Removes an entry from the list of unviewable users that is checked if --restrict-listable is enabled. Repeat this option to specify multiple list items.

--user-domain <string>
Specifies the domain that this provider will use to qualify users. The default user domain is NIS_USERS.

--ypmatch-using-tcp {yes | no}
Uses TCP for YP Match operations.
isi auth nis view

Displays the properties of an NIS provider.

Syntax

```
isi auth nis view <provider-name>
```

Options

```
<provider-name>
```

Specifies the name of the provider to view.

isi auth privileges

Displays a list of system privileges.

Syntax

```
isi auth privileges
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

```
--format {table | json | csv | list}
```

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

```
{--no-header | -a}
```

Displays table and CSV output without headers.

```
{--no-footer | -z}
```

Displays table output without footers.

```
{--verbose | -v}
```

Displays more detailed information.

Note

When using the `--verbose` option, the output `Read Write: No` means that the privileges are read-only.
isi auth refresh

Refreshes authentication system configuration settings.

**Syntax**

```bash
isi auth refresh
```

**Options**

There are no options for this command.

isi auth roles create

Creates a custom role.

This command creates an empty role. To assign privileges and add members to the role, run the `isi auth roles modify` command.

**Syntax**

```bash
isi auth roles create <name>
  [--description <string>]
  [--verbose]
```

**Options**

- `<name>`
  - Specifies the name of the role.

- `--description <string>`
  - Specifies a description of the role.

- `{--verbose | -v}`
  - Displays the results of running the command.

isi auth roles delete

Deletes a role.

**Syntax**

```bash
isi auth roles delete <role>
  [--force]
  [--verbose]
```

**Options**

- `<role>`
  - Specifies the name of the role to delete.

- `{--force | -f}`
  - Suppresses command-line prompts and messages.

- `{--verbose | -v}`
Displays more detailed information.

**isi auth roles list**

Displays a list of roles.

**Syntax**

```
isi auth roles list
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

```
|--limit |--l|--limit <integer>
   Displays no more than the specified number of items.

|--format |--table | json | csv | list
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

|--no-header | -a
   Displays table and CSV output without headers.

|--no-footer | -z
   Displays table output without footers.

|--verbose | -v
   Displays more detailed information.
```

**isi auth roles members list**

Displays a list of the members of a role.

**Syntax**

```
isi auth roles members list <role>
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

```
<role>
   Specifies a role by name.

|--limit | -l|--limit <integer>
   Displays no more than the specified number of items.

|--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
```
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{-no-header | -a}
Displays table and CSV output without headers.

{-no-footer | -z}
Displays table output without footers.

{-verbose | -v}
Displays more detailed information.

Examples
To view the members of the SystemAdmin role, run the following command:

    isi auth roles members list systemadmin

In the following sample output, the SystemAdmin role currently contains one member, a user named admin:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>admin</td>
</tr>
</tbody>
</table>

Total: 1

isi auth roles modify

Modifies a role.

Syntax

    isi auth roles modify <role>
    [-name <string>]
    [-description <string>]
    [-add-group <string>]
    [-remove-group <string>]
    [-add-gid <integer>]
    [-remove-gid <integer>]
    [-add-uid <integer>]
    [-remove-uid <integer>]
    [-add-user <string>]
    [-remove-user <string>]
    [-add-sid <string>]
    [-remove-sid <string>]
    [-add-wellknown <string>]
    [-remove-wellknown <string>]
    [-add-priv <string>]
    [-add-priv-ro <string>]
    [-remove-priv <string>]
    [-verbose]

Options

<role>
    Specifies the name of the role to modify.

--name <string>
    Specifies a new name for the role. Applies to custom roles only.
--description <string>
    Specifies a description of the role.

--add-group <string>
    Adds a group with the specified name to the role. Repeat this option for each
    additional item.

--remove-group <string>
    Removes a group with the specified name from the role. Repeat this option for
    each additional item.

--add-gid <integer>
    Adds a group with the specified GID to the role. Repeat this option for each
    additional item.

--remove-gid <integer>
    Removes a group with the specified GID from the role. Repeat this option for
    each additional item.

--add-uid <integer>
    Adds a user with the specified UID to the role. Repeat this option for each
    additional item.

--remove-uid <integer>
    Removes a user with the specified UID from the role. Repeat this option for each
    additional item.

--add-user <string>
    Adds a user with the specified name to the role. Repeat this option for each
    additional item.

--remove-user <string>
    Removes a user with the specified name from the role. Repeat this option for each
    additional item.

--add-sid <string>
    Adds a user or group with the specified SID to the role. Repeat this option for
    each additional item.

--remove-sid <string>
    Removes a user or group with the specified SID from the role. Repeat this option for
    each additional item.

--add-wellknown <string>
    Adds a well-known SID with the specified name—for example, Everyone—to the
    role. Repeat this option for each additional item.

--remove-wellknown <string>
    Removes a well-known SID with the specified name from the role. Repeat this
    option for each additional item.

--add-priv <string>
    Adds a read/write privilege to the role. Applies to custom roles only. Repeat this
    option for each additional item.

--add-priv-ro <string>
Adds a read-only privilege to the role. Applies to custom roles only. Repeat this option for each additional item.

--remove-priv <string>
Removes a privilege from the role. Applies to custom roles only. Repeat this option for each additional item.

{--verbose | -v}
Displays the results of running the command.

isi auth roles privileges list
Displays a list of privileges that are associated with a role.

Syntax

isi auth roles privileges list <role>
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]

Options

<role>
   Specifies a role by name.

{--limit | -l} <integer>
   Displays no more than the specified number of items.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
   Displays table and CSV output without headers.

{--no-footer | -z}
   Displays table output without footers.

{--verbose | -v}
   Displays more detailed information.

Examples
To list the privileges that are associated with the built-in SecurityAdmin role, run the following command:

isi auth roles privileges list securityadmin

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>----------------------</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td></td>
</tr>
</tbody>
</table>
isi auth roles view

Displays the properties of a role.

Syntax

isi auth roles view <role>

Options

<role>

Specifies the name of the role to view.

isi auth settings acls modify

Modifies access control list (ACL) settings for OneFS.

Syntax

isi auth settings acls modify
[--create-over-smb {allow | disallow}]
[--chmod {remove | replace | replace_users_and_groups | merge |
deny | ignore}]
[--chmod-inheritable {yes | no}]
[--chown {owner_group_and_acl | owner_group_only | ignore}]
[--access {unix | windows}]
[--rwx {retain | full_control}]
[--group-owner-inheritance {native | parent | creator}]
[--chmod-007 {default | remove}]
[--chmod-owner {owner_acls | owner_only}]
[--calcmode-owner {group_aces | group_only}]
[--synthetic-denies {none | remove}]
[--utimes {only_owner | owner_and_write}]
[--dos-attr {deny_smb | deny_smb_and_nfs}]
[--calcmode {approx | 777}]
[--verbose]

Options

--create-over-smb {allow | disallow}

Specifies whether to allow or deny creation of ACLs over SMB.

Note

Inheritable ACLs on the system take precedence over this setting. If inheritable
ACLs are set on a folder, any new files and folders created in that folder will
inherit the folder's ACL. Disabling this setting does not remove ACLs currently set
on files. If you want to clear an existing ACL, run the chmod -b <mode>
<file> command to remove the ACL and set the correct permissions.
--chmod {remove | replace | replace_users_and_groups | merge | deny | ignore}

Specifies how permissions are handled when a chmod operation is initiated on a file with an ACL, either locally or over NFS. This setting controls any elements that affect UNIX permissions, including File System Explorer. Enabling this policy setting does not change how chmod operations affect files that do not have ACLs. The following values are valid:

remove
For chmod operations, removes any existing ACL and instead sets the chmod permissions. Select this option only if you do not need permissions to be set from Windows.

replace
Removes the existing ACL and creates an ACL equivalent to the UNIX permissions. Select this option only if you want to remove Windows permissions but do not want files to have synthetic ACLs.

replace_users_and_groups
Removes the existing ACL and creates an ACL equivalent to the UNIX permissions for all users/groups referenced in old ACL. Select this option only if you want to remove Windows permissions but do not want files to have synthetic ACLs.

merge
Merges permissions that are applied by chmod with existing ACLs. An ACE for each identity (owner, group, and everyone) is either modified or created, but all other ACEs are unmodified. Inheritable ACEs are also left unmodified to enable Windows users to continue to inherit appropriate permissions. UNIX users can set specific permissions for each of those three standard identities, however.

deny
Prevents users from making NFS and local chmod operations. Enable this setting if you do not want to allow permission sets over NFS.

ignore
Ignores the chmod operation if file has an existing ACL, which prevents an NFS client from making changes to the ACL. Select this option if you defined an inheritable ACL on a directory and want to use that ACL for permissions.

CAUTION
If you attempt to run the chmod command on the same permissions that are currently set on a file with an ACL, you may cause the operation to silently fail. The operation appears to be successful, but if you were to examine the permissions on the cluster, you would notice that the chmod command had no effect. As an alternative, you can run the chmod command away from the current permissions and then perform a second chmod command to revert to the original permissions. For example, if your file shows 755 UNIX permissions and you want to confirm this number, you could run chmod 700 file; chmod 755 file.

--chmod-inheritable {yes | no}
On Windows systems, the ACEs for directories can define detailed inheritance rules. On a UNIX system, the mode bits are not inherited. Making ACLs that are created on directories by the chmod command inheritable is more secure for tightly controlled environments but may deny access to some Windows users who would otherwise expect access.

--chown {owner_group_and_acl | owner_group_only | ignore}
Changes the user or group that has ownership of a file or folder. The following values are valid:

owner_group_and_acl
Modifies only the owner or group, which enables the chown or chgrp operation to perform as it does in UNIX. Enabling this setting modifies any ACEs in the ACL associated with the old and new owner or group.

owner_group_only
Modifies the owner or group and ACL permissions, which enables the NFS chown or chgrp operation to function as it does in Windows. When a file owner is changed over Windows, no permissions in the ACL are changed.

ignore
Ignores the chown and chgrp operations if file has an existing ACL, which prevents an NFS client from making changes to the owner or group.

Note
Over NFS, the chown or chgrp operation changes the permissions and user or group that has ownership. For example, a file owned by user Joe with rwx------ (700) permissions indicates rwx permissions for the owner, but no permissions for anyone else. If you run the chown command to change ownership of the file to user Bob, the owner permissions are still rwx but they now represent the permissions for Bob, rather than for Joe, who lost all of his permissions. This setting does not affect UNIX chown or chgrp operations performed on files with UNIX permissions, and it does not affect Windows chown or chgrp operations, which do not change any permissions.

--access {unix | windows}
In UNIX environments, only the file owner or superuser has the right to run a chmod or chown operation on a file. In Windows environments, you can implement this policy setting to give users the right to perform chmod operations that change permissions, or the right to perform chown operations that take ownership, but do not give ownership away. The following values are valid:

unix
Allows only the file owner to change the mode or owner of the file, which enable chmod and chown access checks to operate with UNIX-like behavior.

windows
Allow the file owner and users with WRITE_DAC and WRITE_OWNER permissions to change the mode or owner of the file, which enables chmod and chown access checks to operate with Windows-like behavior.

--rwx {retain | full_control}
Specifies how to handle rwx permissions mapped to windows rights. In UNIX environments, rwx permissions indicate that a user or group has read, write, and execute permissions and that a user or group has the maximum level of permissions.

When you assign UNIX permissions to a file, no ACLs are stored for that file. Because a Windows system processes only ACLs, the Isilon cluster must translate the UNIX permissions into an ACL when you view a file's permissions on a Windows system. This type of ACL is called a synthetic ACL. Synthetic ACLs are not stored anywhere; instead, they are dynamically generated and discarded as needed. If a file has UNIX permissions, you may notice synthetic ACLs when you run the `ls` file command to view a file's ACLs.

When you generate a synthetic ACL, the Isilon cluster maps UNIX permissions to Windows rights. Windows supports a more granular permissions model than UNIX does, and it specifies rights that cannot easily be mapped from UNIX permissions. The following values are valid:

**retain**
Retains rwx permissions and generates an ACE that provides only read, write, and execute permissions.

**full_control**
Treats rwx permissions as full control and generates an ACE that provides the maximum Windows permissions for a user or a group by adding the change permissions right, the take ownership right, and the delete right.

**--group-owner-inheritance {native | parent | creator}**
Specifies how to handle inheritance of group ownership and permissions. If you enable a setting that causes the group owner to be inherited from the creator's primary group, you can override it on a per-folder basis by running the `chmod` command to set the set-gid bit. This inheritance applies only when the file is created. The following values are valid:

**native**
Specifies that if an ACL exists on a file, the group owner will be inherited from the file creator's primary group. If there is no ACL, the group owner is inherited from the parent folder.

**parent**
Specifies that the group owner be inherited from the file's parent folder.

**creator**
Specifies that the group owner be inherited from the file creator's primary group.

**--chmod-007 {default | remove}**
Specifies whether to remove ACLs when running the `chmod (007)` command. The following values are valid:

**default**
Sets 007 UNIX permissions without removing an existing ACL.

**remove**
Removes ACLs from files over UNIX file sharing (NFS) and locally on the cluster through the `chmod (007)` command. If you enable this setting, be sure to run the `chmod` command on the file immediately after using `chmod`
(007) to clear an ACL. In most cases, you do not want to leave 007 permissions on the file.

--calcmode-owner {owner_acces | owner_only}
Specifies how to approximate owner mode bits. The following values are valid:

owner_acces
Approximates owner mode bits using all possible group ACEs. This causes the owner permissions to appear more permissive than the actual permissions on the file.

owner_only
Approximates owner mode bits using only the ACE with the owner ID. This causes the owner permissions to appear more accurate, in that you see only the permissions for a particular owner and not the more permissive set. This may cause access-denied problems for UNIX clients, however.

--calcmode-group {group_acces | group_only}
Specifies how to approximate group mode bits. The following values are valid:

group_acces
Approximates group mode bits using all possible group ACEs. This causes the group permissions to appear more permissive than the actual permissions on the file.

group_only
Approximates group mode bits using only the ACE with the owner ID. This causes the group permissions to appear more accurate, in that you see only the permissions for a particular group and not the more permissive set. This may cause access-denied problems for UNIX clients, however.

--synthetic-denies {none | remove}
Specifies how to handle synthetic ACLs. The Windows ACL user interface cannot display an ACL if any deny ACEs are out of canonical ACL order. To correctly represent UNIX permissions, deny ACEs may be required to be out of canonical ACL order. The following values are valid:

none
Does not modify synthetic ACLs and mode bit approximations, which prevents modifications to synthetic ACL generation and allows “deny” ACEs to be generated when necessary.

remove
Removes deny ACEs when generating synthetic ACLs. This setting can cause ACLs to be more permissive than the equivalent mode bits.

--utimes {only_owner | owner_and_write}
specifies who can change utimes, which are the access and modification times of a file.

only_owner
Allows only owners to change utimes to client-specific times, which complies with the POSIX standard.

owner_and_write
Allows owners as well as users with write access to modify utimes to client-specific times, which is less restrictive.

--dos-attr {deny_smb | deny_smb_and_nfs}
Specifies how to handle the read-only DOS attribute for NFS and SMB. The following values are valid:

deny_smb
Denies permission to modify files with DOS read-only attribute over SMB only.

deny_smb_nfs
Denies permission to modify files with DOS read-only attribute through both NFS and SMB.

--calmode {approx | 777}
Specifies how to display mode bits. The following values are valid

approx
Specifies to use ACL to approximate mode bits. Displays the approximation of the NFS mode bits that are based on ACL permissions.

777
Specifies to always display 777 if an ACL exists. If the approximated NFS permissions are less permissive than those in the ACL, you may want to use this setting so the NFS client does not stop at the access check before performing its operation. Use this setting when a third-party application may be blocked if the ACL does not provide the proper access.

{--verbose | -v}
Displays more detailed information.

isi auth settings acls view
Displays access control list (ACL) settings for OneFS.

Syntax

isi auth settings acls view

Options
There are no options for this command.
isi auth settings global modify

Modifies the global authentication settings.

Syntax

```bash
isi auth settings global modify
[--send-ntlmv2 {yes | no}]
[--revert-send-ntlmv2]
[--space-replacement <character>]
[--revert-space-replacement]
[--workgroup <string>]
[--revert-workgroup]
[--provider-hostname-lookup {dns-first | nis-first | disabled}]
[--user-object-cache-size <size>]
[--revert-user-object-cache-size]
[--on-disk-identity {native | unix | sid}]
[--revert-on-disk-identity]
[--rpc-block-time <duration>]
[--revert-block-time]
[--rpc-max-requests <integer>]
[--revert-rpc-max-requests]
[--unknown-gid <integer>]
[--revert-unknown-gid]
[--unknown-uid <integer>]
[--revert-unknown-uid]
[--verbose]
```

Options

`--send-ntlmv2 {yes | no}`

Specifies whether to send only NTLMv2 responses to an SMB client. The default value is `no`. Valid values are `yes, no`. The default value is `no`.

`--revert-send-ntlmv2`

Reverts the `--send-ntlmv2` setting to the system default value.

`--space-replacement <character>`

For clients that have difficulty parsing spaces in user and group names, specifies a substitute character. Be careful to choose a character that is not in use.

`--revert-space-replacement`

Reverts the `--space-replacement` setting to the system default value.

`--workgroup <string>`

Specifies the NetBIOS workgroup. The default value is `WORKGROUP`.

`--revert-workgroup`

Reverts the `--workgroup` setting to the system default value.

`--provider-hostname-lookup {dns-first | nis-first | disabled}`

Allows hostname lookup through authentication providers. Applies to NIS only. The default value is `disabled`.

`--user-object-cache-size <size>`

Specifies the maximum size (in bytes) of the security object cache in the authentication service.

`--revert-user-object-cache-size`
Reverts the --user-object-cache-size setting to the system default value.

--on-disk-identity <string>
Controls the preferred identity to store on disk. If OneFS is unable to convert an identity to the preferred format, it is stored as is. This setting does not affect identities that are already stored on disk.
The accepted values are listed below.

native
Allows OneFS to determine the identity to store on disk. This is the recommended setting.

unix
Always stores incoming UNIX identifiers (UIDs and GIDs) on disk.

sid
Stores incoming Windows security identifiers (SIDs) on disk unless the SID was generated from a UNIX identifier. If the SID was generated from a UNIX identifier, OneFS converts it back to the UNIX identifier and stores it on disk.

Note
To prevent permission errors after changing the on-disk identity, run the Repair Permissions job with the convert mode specified.

--revert-on-disk-identity
Sets the --on-disk-identity setting to the system default value.

--rpc-block-time <integer>
Specifies the length of time, in milliseconds, before an ID mapper request becomes asynchronous.

--revert-rpc-block-time
Sets the --rpc-block-time setting to the system default value.

--rpc-max-requests <integer>
Specifies the maximum number of simultaneous ID mapper requests allowed. The default value is 64.

--revert-rpc-max-requests
Sets the --rpc-max-requests setting to the system default value.

--unknown-gid <integer>
Specifies the GID to use for the unknown (anonymous) group.

--revert-unknown-gid
Sets the --unknown-gid setting to the system default value.

--unknown-uid <integer>
Specifies the UID to use for the unknown (anonymous) user.

--revert-unknown-uid
Sets the --unknown-uid setting to the system default value.

{--verbose | -v}
isi auth settings global view

Displays more detailed information.

Displays global authentication settings.

Syntax

isi auth settings global view

Options

There are no options for this command.

Examples

To view the current authentication settings on the cluster, run the following command:

isi auth settings global view

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send NTLMv2</td>
<td>No</td>
</tr>
<tr>
<td>Space Replacement</td>
<td></td>
</tr>
<tr>
<td>Workgroup</td>
<td>WORKGROUP</td>
</tr>
<tr>
<td>Provider Hostname Lookup</td>
<td>disabled</td>
</tr>
<tr>
<td>Alloc Retries</td>
<td>5</td>
</tr>
<tr>
<td>Cache Cred Lifetime</td>
<td>15m</td>
</tr>
<tr>
<td>Cache ID Lifetime</td>
<td>15m</td>
</tr>
<tr>
<td>On Disk Identity</td>
<td>native</td>
</tr>
<tr>
<td>RPC Block Time</td>
<td>5s</td>
</tr>
<tr>
<td>RPC Max Requests</td>
<td>16</td>
</tr>
<tr>
<td>RPC Timeout</td>
<td>30s</td>
</tr>
<tr>
<td>System GID Threshold</td>
<td>80</td>
</tr>
<tr>
<td>System UID Threshold</td>
<td>80</td>
</tr>
<tr>
<td>GID Range Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>GID Range Min</td>
<td>10000000</td>
</tr>
<tr>
<td>GID Range Max</td>
<td>20000000</td>
</tr>
<tr>
<td>UID Range Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>UID Range Min</td>
<td>10000000</td>
</tr>
<tr>
<td>UID Range Max</td>
<td>20000000</td>
</tr>
<tr>
<td>Min Mapped Rid</td>
<td>2147483648</td>
</tr>
<tr>
<td>Group UID</td>
<td>4294967292</td>
</tr>
<tr>
<td>Null GID</td>
<td>4294967293</td>
</tr>
<tr>
<td>Null UID</td>
<td>4294967293</td>
</tr>
<tr>
<td>Unknown GID</td>
<td>4294967294</td>
</tr>
<tr>
<td>Unknown UID</td>
<td>4294967294</td>
</tr>
</tbody>
</table>

isi auth settings krb5 modify

Modifies the global settings of an MIT Kerberos authentication provider.

Syntax

isi auth settings krb5 modify
   [--always-send-preauth <boolean> | --revert-always-send-preauth]
   [--default-realm <string>]
   [--dns-lookup-kdc <boolean> | --revert-dns-lookup-kdc]
   [--dns-lookup-realm <boolean> | --revert-dns-lookup-realm]
Options

--always-send-preauth <boolean>
   Specifies whether to send preauth.

--revert-always-send-preauth
   Sets the value of --always-send-preauth to the system default.

--default-realm <string>
   Specifies the default Kerberos realm name.

--dns-lookup-kdc <boolean>
   Allows DNS to find Key Distribution Centers (KDCs).

--revert-dns-lookup-kdc
   Sets the value of --dns-lookup-kdc to the system default.

--dns-lookup-realm <boolean>
   Allows DNS to find the Kerberos realm names.

--revert-dns-lookup-realm
   Sets the value of --dns-lookup-realm to the system default.

isi auth settings krb5 view

Displays MIT Kerberos provider authentication settings.

Syntax

isi auth settings krb5 view

isi auth settings mapping modify

Modifies identity mapping settings.

Syntax

isi auth settings mapping modify
   [--gid-range-enabled {yes | no}]
   [--revert-gid-range-enabled]
   [--gid-range-min <integer>]
   [--revert-gid-range-min]
   [--gid-range-max <integer>]
   [--revert-gid-range-max]
   [--uid-range-enabled {yes | no}]
   [--revert-uid-range-enabled]
   [--uid-range-min <integer>]
   [--revert-uid-range-min]
   [--uid-range-max <integer>]
   [--revert-uid-range-max]
   [--zone <string>]

Options

If no option is specified, the kernel mapping database is displayed.

--gid-range-enabled {yes | no}
Enables automatic allocation of GIDs by the ID mapping service. This setting is enabled by default.

--revert-gid-range-enabled
Sets the value of --gid-range-enabled to the system default.

--gid-range-min <integer>
Specifies the lower value in the range of GIDs that are available for allocation. The default value is 1000000.

--revert-gid-range-min
Sets the value of --gid-range-min to the system default.

--gid-range-max <integer>
Specifies the upper value in the range of GIDs that are available for allocation. The default value is 2000000.

--revert-gid-range-max
Sets the value of --gid-range-max to the system default.

--uid-range-enabled {yes | no}
Enables automatic allocation of UIDs by the ID mapping service. This setting is enabled by default.

--revert-uid-range-enabled
Sets the value of --uid-range-enabled to the system default.

--uid-range-min <integer>
Specifies the lower value in the range of UIDs that are available for allocation. The default value is 1000000.

--revert-uid-range-min
Sets the value of --uid-range-min to the system default.

--uid-range-max <integer>
Specifies the upper value in the range of UIDs that are available for allocation. The default value is 2000000.

--revert-uid-range-max
Sets the value of --uid-range-max to the system default.

--zone <string>
Specifies the access zone in which to modify ID mapping settings. If no access zone is specified, settings in the default System zone will be modified.

**isi auth settings mapping view**

Displays identity mapping settings in an access zone.

**Syntax**

```bash
isi auth settings mapping view
    [--zone <string>]
```
Options

--zone <string>
Displays mapping settings from the specified access zone. If no access zone is specified, displays mappings from the default System zone.

isi auth status
Displays provider status, including available authentication providers and which providers are functioning correctly.

Syntax

isi auth status
[--zone <string>]
[--groupnet <string>]
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]

Options

--zone <string>
Specifies an access zone by name.

--groupnet <string>
Specifies a groupnet by name.

--limit [-l | <integer>]
Specifies the number of providers to display.

--format {table | json | csv | list}
Displays providers in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

isi auth users create
Creates a user account.

Syntax

isi auth users create <name>
[--enabled {yes | no}]
[--expiry <timestamp>]
[--email <string>]
Options

<name>
Specifies the user name.

--enabled {yes | no}
Enables or disables the user.

{--expiry | -x} <timestamp>
Specifies the time at which the user account will expire, using the date format
<YYYY>-<MM>-<DD> or the date/time format <YYYY>-<MM>-<DD>T<hh>:<mm>[:ss]].

--email <string>
Specifies the email address of the user.

--gecos <string>
Specifies the values for the following Gecos field entries in the user's password file:

Full Name:
Office Location:
Office Phone:
Home Phone:
Other information:

Values must be entered as a comma-separated list, and values that contain
spaces must be enclosed in quotation marks. For example, the --gecos="Jane
Doe",Seattle,555-5555,,"Temporary worker" option with these values
results in the following entries:

Full Name: Jane Doe
Office Location: Seattle
Office Phone: 555-5555
Home Phone:
Other information: Temporary worker

--home-directory <path>
Specifies the path to the user's home directory.

--password <string>
Sets the user's password to the specified value. This option cannot be used with
the --set-password option.
--password-expires {yes | no}
   Specifies whether to allow the password to expire.

--primary-group <name>
   Specifies the user’s primary group by name.

--primary-group-gid <integer>
   Specifies the user’s primary group by GID.

--primary-group-sid <string>
   Specifies the user’s primary group by SID.

--prompt-password-change {yes | no}
   Prompts the user to change the password during the next login.

--shell <path>
   Specifies the path to the UNIX login shell.

--uid <integer>
   Overrides automatic allocation of the UNIX user identifier (UID) with the specified
   value. Setting this option is not recommended.

--zone <string>
   Specifies the access zone in which to create the user.

--provider <string>
   Specifies a local authentication provider in the specified access zone.

--set-password
   Sets the password interactively. This option cannot be used with the
   --password option.

{--verbose | -v}
   Displays the results of running the command.

{--force | -f}
   Suppresses command-line prompts and messages.

isi auth users delete

Deletes a local user from the system.

Syntax

    isi auth users delete {<user> | --uid <integer> | --sid <string>}
      [--zone <string>]
      [--provider <string>]
      [--force]
      [--verbose]

Options
This command requires <user>, --uid <integer>, or --sid <string>.

<user>
   Specifies the user by name.
--uid <integer>
   Specifies the user by UID.

--sid <string>
   Specifies the user by SID.

--zone <string>
   Specifies the name of the access zone that contains the user.

--provider <string>
   Specifies the name of the authentication provider that contains the user.

{---force | -f}
   Suppresses command-line prompts and messages.

{---verbose | -v}
   Displays the results of running the command.

**isi auth users flush**

Flushes cached user information.

**Syntax**

isi auth users flush

**Options**

There are no options for this command.

**Examples**

To flush all cached user information, run the following command:

isi auth user flush

**isi auth users list**

Displays a list of users. If no options are specified, all users in the System access zone are displayed.

---

**Note**

The `--domain` option must be specified to list Active Directory users.

**Syntax**

isi auth users list
   [--domain <string>]
   [--zone <string>]
   [--provider <string>]
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
Options

--domain <string>
Displays only the users in the specified provider domain.

--zone <string>
Specifies the access zone whose users you want to list. The default access zone is System.

--provider <string>
Displays only the users in the specified authentication provider. The syntax for specifying providers is <provider-type>:<provider-name>, being certain to use the colon separator; for example, isi auth users list --provider="lsa-ldap-provider:Unix LDAP".

{--limit | -l} <integer>.
Displays no more than the specified number of items.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

isi auth users modify
Modifies a local user.

Syntax

isi auth users modify {<user> | --uid <integer> | --sid <string>}  
   [--enabled {yes | no}] 
   [--expiry <timestamp>] 
   [--unlock] 
   [--email <string>] 
   [--gecos <string>] 
   [--home-directory <path>] 
   [--password <string>]
   [--password-expires {yes | no}]
   [|--primary-group <string> | --primary-group-gid <integer> 
    | --primary-group-sid <string>]]
   |--prompt-password-change {yes | no}]
   |--shell <path>]
   |--new-uid <integer>]
   |--zone <string>]
   |--add-group <name>]
   |--add-gid <id>]
   |--remove-group <name>]
   |--remove-gid <id>]
   |--provider <string>]
   |--set-password]
Options
This command requires <user>, --uid <integer>, or --sid <string>.

=user>
Specifies the user by name.

--uid <integer>
Specifies the user by UID.

--sid <string>
Specifies the user by SID.

--enabled {yes | no}
Enables or disables the user.

{--expiry | -x} <timestamp>
Specifies the time at which the user account will expire, using the date format
<YYYY>-<MM>-<DD> or the date/time format <YYYY>-<MM>-<DD>T<hh>:<mm>:<ss>.

--unlock
Unlocks the user account if locked.

--email <string>
Specifies the email address of the user.

--gecos <string>
Specifies the values for the following Gecos field entries in the user’s password file:

Full Name:
Office Location:
Office Phone:
Home Phone:
Other information:

Values must be entered as a comma-separated list, and values that contain
spaces must be enclosed in quotation marks. For example, the --gecos= "Jane
Doe",Seattle,555-5555,,"Temporary worker" option with these values
results in the following entries:

Full Name: Jane Doe
Office Location: Seattle
Office Phone: 555-5555
Home Phone:
Other information: Temporary worker

--home-directory <path>
Specifies the path to the user’s home directory.

--password <string>
Sets the user’s password to the specified value. This option cannot be used with
the --set-password option.
--password-expires {yes | no}
   Specifies whether to allow the password to expire.

--primary-group <name>
   Specifies the user's primary group by name.

--primary-group-gid <integer>
   Specifies the user's primary group by GID.

--primary-group-sid <string>
   Specifies the user's primary group by SID.

--prompt-password-change {yes | no}
   Prompts the user to change the password during the next login.

--shell <path>
   Specifies the path to the UNIX login shell.

--new-uid <integer>
   Specifies a new UID for the user. Setting this option is not recommended.

--zone <string>
   Specifies the name of the access zone that contains the user.

--add-group <name>
   Specifies the name of a group to add the user to. Repeat this option to specify
   multiple list items.

--add-gid <integer>
   Specifies the GID of a group to add the user to. Repeat this option to specify
   multiple list items.

--remove-group <name>
   Specifies the name of a group to remove the user from. Repeat this option to
   specify multiple list items.

--remove-gid <integer>
   Specifies the GID of a group to remove the user from. Repeat this option to
   specify multiple list items.

--provider <string>
   Specifies an authentication provider of the format <type>:<instance>. Valid
   provider types are ads, ldap, nis, file, and local. For example, an LDAP
   provider named auth1 can be specified as ldap:auth1.

--set-password
   Sets the password interactively. This option cannot be used with the --
   password option.

{--verbose | -v}
   Displays the results of running the command.

{--force | -f}
   Suppresses command-line prompts and messages.
isi auth users view

Displays the properties of a user.

Syntax

\[
\text{isi auth users view } \{<\text{user}> \mid --\text{uid }<\text{integer}> \mid --\text{sid }<\text{string}>\}
\]

[--cached]  
[--show-groups]  
[--resolve-names]  
[--zone <string>]  
[--provider <string>]

Options

This command requires <user>, --uid <integer>, or --sid <string>.

<user>

  Specifies the user by name.

--uid <integer>

  Specifies the user by UID.

--sid <string>

  Specifies the user by SID.

--cached

  Returns only cached information.

--show-groups

  Displays groups that include the user as a member.

--resolve-names

  Resolves the names of all related groups and related identities.

--zone <string>

  Specifies the name of the access zone that contains the user.

--provider <string>

  Specifies the name of the authentication provider that contains the user in the format <type>:<instance>. Valid values for type are ads, ldap, nis, file, and local. For example an LDAP provider named auth1 can be specified as ldap:auth1, or an Active Directory provider can be specified as ads:YORK.east.com.
CHAPTER 7

Administrative roles and privileges

This section contains the following topics:

- Role-based access ................................................................. 368
- Roles ..................................................................................... 368
- Privileges ............................................................................. 372
- Managing roles ................................................................. 380
Role-based access

You can assign role-based access to delegate administrative tasks to selected users.

Role based access control (RBAC) allows the right to perform particular administrative actions to be granted to any user who can authenticate to a cluster. Roles are created by a Security Administrator, assigned privileges, and then assigned members. All administrators, including those given privileges by a role, must connect to the System zone to configure the cluster. When these members log in to the cluster through a configuration interface, they have these privileges. All administrators can configure settings for access zones, and they always have control over all access zones on the cluster.

Roles also give you the ability to assign privileges to member users and groups. By default, only the root user and the admin user can log in to the web administration interface through HTTP or the command-line interface through SSH. Using roles, the root and admin users can assign others to built-in or customer roles that have login and administrative privileges to perform specific administrative tasks.

Note

As a best practice, assign users to roles that contain the minimum set of necessary privileges. For most purposes, the default permission policy settings, system access zone, and built-in roles are sufficient. You can create role-based access management policies as necessary for your particular environment.

Roles

You can permit and limit access to administrative areas of your EMC Isilon cluster on a per-user basis through roles. OneFS includes several built-in administrator roles with predefined sets of privileges that cannot be modified. You can also create custom roles and assign privileges.

The following list describes what you can and cannot do through roles:

- You can assign privileges to a role.
- You can create custom roles and assign privileges to those roles.
- You can copy an existing role.
- You can add any user or group of users, including well-known groups, to a role as long as the users can authenticate to the cluster.
- You can add a user or group to more than one role.
- You cannot assign privileges directly to users or groups.

Note

When OneFS is first installed, only users with root- or admin-level access can log in and assign users to roles.

Custom roles

Custom roles supplement built-in roles.

You can create custom roles and assign privileges mapped to administrative areas in your EMC Isilon cluster environment. For example, you can create separate administrator roles for security, auditing, storage provisioning, and backup.
You can designate certain privileges as read-only or read/write when adding the privilege to a role. You can modify this option at any time to add or remove privileges as user responsibilities grow and change.

**Built-in roles**

Built-in roles are included in OneFS and have been configured with the most likely privileges necessary to perform common administrative functions. You cannot modify the list of privileges assigned to each built-in role; however, you can assign users and groups to built-in roles.

The following sections describe each of the built-in roles and include the privileges and read/write access levels assigned to each role.

**SecurityAdmin built-in role**

The SecurityAdmin built-in role enables security configuration on the cluster, including authentication providers, local users and groups, and role membership.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

**SystemAdmin built-in role**

The SystemAdmin built-in role enables administration of all cluster configuration that is not specifically handled by the SecurityAdmin role.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SHUTDOWN</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SUPPORT</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
### Privileges

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### AuditAdmin built-in role

The AuditAdmin built-in role enables you to view all system configuration settings.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Read-only</td>
</tr>
<tr>
<td>Privileges</td>
<td>Read/write access</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

**BackupAdmin built-in role**

The BackupAdmin built-in role enables backup and restore of files from /ifs.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_IFS_BACKUP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_IFS_RESTORE</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
VMwareAdmin built-in role

The VMwareAdmin built-in role enables remote administration of storage needed by VMware vCenter.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCHIQ</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Privileges

Privileges permit users to complete tasks on an EMC Isilon cluster.

Privileges are associated with an area of cluster administration such as Job Engine, SMB, or statistics.

Privileges have one of two forms:

**Action**

Allows a user to perform a specific action on a cluster. For example, the ISI_PRIV_LOGIN_SSH privilege allows a user to log in to a cluster through an SSH client.

**Read/Write**

Allows a user to view or modify a configuration subsystem such as statistics, snapshots, or quotas. For example, the ISI_PRIV_SNAPSHOT privilege allows an administrator to create and delete snapshots and snapshot schedules. A read/write privilege can grant either read-only or read/write access. Read-only access allows a user to view configuration settings; read/write access allows a user to view and modify configuration settings.

Privileges are granted to the user on login to a cluster through the OneFS API, the web administration interface, SSH, or a console session. A token is generated for the user, which includes a list of all privileges granted to the user. Each URI, web-administration interface page, and command requires a specific privilege to view or modify the information available through any of these interfaces.

In some cases, privileges cannot be granted or there are privilege limitations.

- Privileges are not granted to users that do not connect to the System Zone during login or to users that connect through the deprecated Telnet service, even if they are members of a role.
- Privileges do not provide administrative access to configuration paths outside of the OneFS API. For example, the ISI_PRIV_SMB privilege does not grant a user the right to configure SMB shares using the Microsoft Management Console (MMC).
Privileges do not provide administrative access to all log files. Most log files require root access.

**Supported OneFS privileges**

Privileges supported by OneFS are categorized by the type of action or access that is granted to the user—for example, login, security, and configuration privileges.

**Login privileges**

The login privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>Log in from the console.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>Log in to the Platform API and the web administration interface.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>Log in through SSH.</td>
<td>Action</td>
</tr>
</tbody>
</table>

**System privileges**

The system privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_SYS_SHUTDOWN</td>
<td>Shut down the system.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SUPPORT</td>
<td>Run cluster diagnostic tools.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Change the system time.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Upgrades the OneFS system.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

**Security privileges**

The security privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>Configure external authentication providers, including root-level accounts.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>Create new roles and assign privileges, including root-level accounts.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
Configuration privileges

The configuration privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Configure antivirus scanning.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Configure audit capabilities.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>Configure CloudPools.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Configure cluster identity and general settings.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Create new roles and assign privileges.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>View and modify system events.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Configure file filtering settings.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Configure FTP server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Configure HDFS server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Configure HTTP server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Schedule cluster-wide jobs.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Activate OneFS software licenses.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Register applications monitoring the cluster.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Configure NDMP server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Configure network interfaces.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Configure the NFS server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Configure NTP.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Configure file system quotas.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>Configure remote support.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Configure storage pools.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Configure the SMB server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Schedule, take, and view snapshots.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Configure SNMP server.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>View file system performance statistics.</td>
<td>Read/寫</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Configure Swift.</td>
<td>Read/寫</td>
</tr>
</tbody>
</table>
### File access privileges

The file access privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_IFS_BACKUP</td>
<td>Back up files from /ifs.</td>
<td>Action</td>
</tr>
<tr>
<td>Note</td>
<td>This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.</td>
<td></td>
</tr>
<tr>
<td>ISI_PRIV_IFS_RESTORE</td>
<td>Restore files from /ifs.</td>
<td>Action</td>
</tr>
<tr>
<td>Note</td>
<td>This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.</td>
<td></td>
</tr>
<tr>
<td>ISI_PRIV_IFS_WORM_DELETE</td>
<td>Perform privileged delete operation on WORM committed files.</td>
<td>Action</td>
</tr>
<tr>
<td>Note</td>
<td>If you are not logged in through the root user account, you must also have the ISI_PRIV_NS_IFS_ACCESS privilege.</td>
<td></td>
</tr>
</tbody>
</table>
Namespace privileges

The namespace privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>Traverse and view directory metadata.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>Access the /ifs directory through the OneFS API.</td>
<td>Action</td>
</tr>
</tbody>
</table>

Data backup and restore privileges

You can assign privileges to a user that are explicitly for cluster data backup and restore actions.

Two privileges allow a user to backup and restore cluster data over supported client-side protocols: ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE.

⚠️ CAUTION ⚠️

These privileges circumvent traditional file access checks, such as mode bits or NTFS ACLs.

Most cluster privileges allow changes to cluster configuration in some manner. The backup and restore privileges allow access to cluster data from the System zone, the traversing of all directories, and reading of all file data and metadata regardless of file permissions.

Users assigned these privileges use the protocol as a backup protocol to another machine without generating access-denied errors and without connecting as the root user. These two privileges are supported over the following client-side protocols:

- SMB
- NFS
- RAN API
- FTP
- SSH

Over SMB, the ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE privileges emulate the Windows privileges SE_BACKUP_NAME and SE_RESTORE_NAME. The emulation means that normal file-open procedures are protected by file system permissions. To enable the backup and restore privileges over the SMB protocol, you must open files with the FILE_OPEN_FOR_BACKUP_INTENT option, which occurs automatically through Windows backup software such as Robocopy. Application of the option is not automatic when files are opened through general file browsing software such as Windows File Explorer.

Both ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE privileges primarily support Windows backup tools such as Robocopy. A user must be a member of the BackupAdmin built-in role to access all Robocopy features, which includes copying file DACL and SACL metadata.
Command-line interface privileges

You can perform most tasks granted by a privilege through the command-line interface (CLI). Some OneFS commands require root access.

Command-to-privilege mapping

Each CLI command is associated with a privilege. Some commands require root access.

<table>
<thead>
<tr>
<th>isi command</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>isi antivirus</td>
<td>ISI_PRIV_ANTIVIRUS</td>
</tr>
<tr>
<td>isi audit</td>
<td>ISI_PRIV_AUDIT</td>
</tr>
<tr>
<td>isi auth, excluding isi auth roles</td>
<td>ISI_PRIV_AUTH</td>
</tr>
<tr>
<td>isi auth roles</td>
<td>ISI_PRIV_ROLE</td>
</tr>
<tr>
<td>isi batterystatus</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td>isi cloud</td>
<td>ISI_PRIV_CLOUDPOOLS</td>
</tr>
<tr>
<td>isi config</td>
<td>root</td>
</tr>
<tr>
<td>isi dedupe, excluding isi dedupe stats</td>
<td>ISI_PRIV_JOB_ENGINE</td>
</tr>
<tr>
<td>isi dedupe stats</td>
<td>ISI_PRIV_STATISTICS</td>
</tr>
<tr>
<td>isi devices</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td>isi email</td>
<td>ISI_PRIV_CLUSTER</td>
</tr>
<tr>
<td>isi event</td>
<td>ISI_PRIV_EVENT</td>
</tr>
<tr>
<td>isi fc</td>
<td>ISI_PRIV_NDMP</td>
</tr>
<tr>
<td>isi file-filter</td>
<td>ISI_PRIV_FILE_FILTER</td>
</tr>
<tr>
<td>isi filepool</td>
<td>ISI_PRIV_SMARTPOOLS</td>
</tr>
<tr>
<td>isi ftp</td>
<td>ISI_PRIV_FTP</td>
</tr>
<tr>
<td>isi get</td>
<td>root</td>
</tr>
<tr>
<td>isi hardening</td>
<td>ISI_PRIV_HARDENING</td>
</tr>
<tr>
<td>isi hdfs</td>
<td>ISI_PRIV_HDFS</td>
</tr>
<tr>
<td>isi http</td>
<td>ISI_PRIV_HTTP</td>
</tr>
<tr>
<td>isi job</td>
<td>ISI_PRIV_JOB_ENGINE</td>
</tr>
<tr>
<td>isi license</td>
<td>ISI_PRIV_LICENSE</td>
</tr>
<tr>
<td>isi ndmp</td>
<td>ISI_PRIV_NDMP</td>
</tr>
<tr>
<td>isi network</td>
<td>ISI_PRIV_NETWORK</td>
</tr>
<tr>
<td>isi nfs</td>
<td>ISI_PRIV_NFS</td>
</tr>
<tr>
<td>ifs ntp</td>
<td>ISI_PRIV_NTP</td>
</tr>
<tr>
<td>isi quota</td>
<td>ISI_PRIV_QUOTA</td>
</tr>
<tr>
<td>isi readonly</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
</tbody>
</table>
### Administrative roles and privileges

<table>
<thead>
<tr>
<th>isi command</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>isi remotesupport</td>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
</tr>
<tr>
<td>isi servicelight</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td>isi services</td>
<td>root</td>
</tr>
<tr>
<td>isi set</td>
<td>root</td>
</tr>
<tr>
<td>isi smb</td>
<td>ISI_PRIV_SMB</td>
</tr>
<tr>
<td>isi snapshot</td>
<td>ISI_PRIV_SNAPSHOT</td>
</tr>
<tr>
<td>isi snmp</td>
<td>ISI_PRIV_SNMP</td>
</tr>
<tr>
<td>isi statistics</td>
<td>ISI_PRIV_STATISTICS</td>
</tr>
<tr>
<td>isi status</td>
<td>ISI_PRIV_EVENT</td>
</tr>
<tr>
<td></td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td></td>
<td>ISI_PRIV_JOB_ENGINE</td>
</tr>
<tr>
<td></td>
<td>ISI_PRIV_NETWORK</td>
</tr>
<tr>
<td></td>
<td>ISI_PRIV_SMARTPOOLS</td>
</tr>
<tr>
<td></td>
<td>ISI_PRIV_STATISTICS</td>
</tr>
<tr>
<td>isi storagepool</td>
<td>ISI_PRIV_SMARTPOOLS</td>
</tr>
<tr>
<td>isi swift</td>
<td>ISI_PRIV_SWIFT</td>
</tr>
<tr>
<td>isi sync</td>
<td>ISI_PRIV_SYNCIQ</td>
</tr>
<tr>
<td>isi tape</td>
<td>ISI_PRIV_NDMP</td>
</tr>
<tr>
<td>isi time</td>
<td>ISI_PRIV_SYS_TIME</td>
</tr>
<tr>
<td>isi upgrade</td>
<td>ISI_PRIV_SYS_UPGRADE</td>
</tr>
<tr>
<td>isi version</td>
<td>ISI_PRIV_CLUSTER</td>
</tr>
<tr>
<td>isi worm excluding isi worm files delete</td>
<td>ISI_PRIV_WORM</td>
</tr>
<tr>
<td>isi worm files delete</td>
<td>ISI_PRIV_IFS_WORM_DELETE</td>
</tr>
<tr>
<td>isi zone</td>
<td>ISI_PRIV_AUTH</td>
</tr>
</tbody>
</table>

### Privilege-to-command mapping

Each privilege is associated with one or more commands. Some commands require root access.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>isi commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>isi antivirus</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>isi audit</td>
</tr>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>isi auth - excluding isi auth role</td>
</tr>
<tr>
<td></td>
<td>isi zone</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>isi cloud</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>isi email</td>
</tr>
<tr>
<td></td>
<td>isi version</td>
</tr>
<tr>
<td>Privilege</td>
<td>isi commands</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>isi batterystatus</td>
</tr>
<tr>
<td></td>
<td>isi devices</td>
</tr>
<tr>
<td></td>
<td>isi readonly</td>
</tr>
<tr>
<td></td>
<td>isi servicelight</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>isi event</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>isi file-filter</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>isi ftp</td>
</tr>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>isi hardening</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>isi hdfs</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>isi http</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>isi job</td>
</tr>
<tr>
<td></td>
<td>isi dedupe</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>isi license</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>isi fc</td>
</tr>
<tr>
<td></td>
<td>isi tape</td>
</tr>
<tr>
<td></td>
<td>isi ndmp</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>isi network</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>isi nfs</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>isi ntp</td>
</tr>
<tr>
<td>ISI_PRIV QUOTA</td>
<td>isi quota</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>isi remotesupport</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>isi auth role</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>isi filepool</td>
</tr>
<tr>
<td></td>
<td>isi storagepool</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>isi smb</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>isi snapshot</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>isi snmp</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>isi status</td>
</tr>
<tr>
<td></td>
<td>isi statistics</td>
</tr>
<tr>
<td></td>
<td>isi dedupe stats</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>isi swift</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>isi sync</td>
</tr>
</tbody>
</table>
### Administrative roles and privileges

<table>
<thead>
<tr>
<th>Privilege</th>
<th>isi commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>isi time</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>isi upgrade</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>isi worm excluding isi worm files delete</td>
</tr>
<tr>
<td>ISI_PRIV_IFS_WORM_DELETE</td>
<td>isi worm files delete</td>
</tr>
<tr>
<td>root</td>
<td>• isi config</td>
</tr>
<tr>
<td></td>
<td>• isi get</td>
</tr>
<tr>
<td></td>
<td>• isi services</td>
</tr>
<tr>
<td></td>
<td>• isi set</td>
</tr>
</tbody>
</table>

### Managing roles

You can view, add, or remove members of any role. Except for built-in roles, whose privileges you cannot modify, you can add or remove OneFS privileges on a role-by-role basis.

**Note**

Roles take both users and groups as members. If a group is added to a role, all users who are members of that group are assigned the privileges associated with the role. Similarly, members of multiple roles are assigned the combined privileges of each role.

### View roles

You can view information about built-in and custom roles.

**Procedure**

1. Run one of the following commands to view roles.
   - To view a basic list of all roles on the cluster, run the following command:
     ```bash
     isi auth roles list
     ```
   - To view detailed information about each role on the cluster, including member and privilege lists, run the following command:
     ```bash
     isi auth roles list --verbose
     ```
   - To view detailed information about a single role, run the following command, where `<role>` is the name of the role:
     ```bash
     isi auth roles view <role>
     ```
View privileges

You can view user privileges.

This procedure must be performed through the command-line interface (CLI). You can view a list of your privileges or the privileges of another user using the following commands:

**Procedure**

1. Establish an SSH connection to any node in the cluster.
2. To view privileges, run one of the following commands.
   - To view a list of all privileges, run the following command:
     
     ```
     isi auth privileges --verbose
     ```
   - To view a list of your privileges, run the following command:
     
     ```
     isi auth id
     ```
   - To view a list of privileges for another user, run the following command, where `<user>` is a placeholder for another user by name:
     
     ```
     isi auth mapping token <user>
     ```

Create and modify a custom role

You can create an empty custom role and then add users and privileges to the role.

**Procedure**

1. Establish an SSH connection to any node in the cluster.
2. Run the following command to create a role, where `<name>` is the name that you want to assign to the role and `<string>` specifies an optional description:

   ```
   isi auth roles create <name> [--description <string>]
   ```

3. Run the following command to add a user to the role, where `<role>` is the name of the role and `<string>` is the name of the user:

   ```
   isi auth roles modify <role> [--add-user <string>]
   ```

**Note**

You can also modify the list of users assigned to a built-in role.

4. Run the following command to add a privilege with read/write access to the role, where `<role>` is the name of the role and `<string>` is the name of the privilege:

   ```
   isi auth roles modify <role> [--add-priv <string>]
   ```
5. Run the following command to add a privilege with read-only access to the role, where `<role>` is the name of the role and `<string>` is the name of the privilege:

```bash
isi auth roles modify <role> [--add-priv-ro <string>]
```

### Delete a custom role

Deleting a role does not affect the privileges or users that are assigned to it. Built-in roles cannot be deleted.

**Procedure**

1. Run the following command to delete a custom role, where `<name>` is the name of the role that you want to delete:

```bash
isi auth roles delete <name>
```
CHAPTER 8

Identity management

This section contains the following topics:

- Identity management overview ................................................................. 384
- Identity types ............................................................................................ 384
- Access tokens .......................................................................................... 385
- Access token generation ........................................................................... 386
- Managing ID mappings ........................................................................... 392
- Managing user identities .......................................................................... 395
Identity management overview

In environments with several different types of directory services, OneFS maps the users and groups from the separate services to provide a single unified identity on an EMC Isilon cluster and uniform access control to files and directories, regardless of the incoming protocol. This process is called identity mapping.

Isilon clusters are frequently deployed in multiprotocol environments with multiple types of directory services, such as Active Directory and LDAP. When a user with accounts in multiple directory services logs in to a cluster, OneFS combines the user’s identities and privileges from all the directory services into a native access token. You can configure OneFS settings to include a list of rules for access token manipulation to control user identity and privileges. For example, you can set a user mapping rule to merge an Active Directory identity and an LDAP identity into a single token that works for access to files stored over both SMB and NFS. The token can include groups from Active Directory and LDAP. The mapping rules that you create can solve identity problems by manipulating access tokens in many ways, including the following examples:

- Authenticate a user with Active Directory but give the user a UNIX identity.
- Select a primary group from competing choices in Active Directory or LDAP.
- Disallow login of users that do not exist in both Active Directory and LDAP.

For more information about identity management, see the white paper Managing identities with the Isilon OneFS user mapping service at EMC Online Support.

Identity types

OneFS supports three primary identity types, each of which you can store directly on the file system. Identity types are user identifier and group identifier for UNIX, and security identifier for Windows.

When you log on to an EMC Isilon cluster, the user mapper expands your identity to include your other identities from all the directory services, including Active Directory, LDAP, and NIS. After OneFS maps your identities across the directory services, it generates an access token that includes the identity information associated with your accounts. A token includes the following identifiers:

- A UNIX user identifier (UID) and a group identifier (GID). A UID or GID is a 32-bit number with a maximum value of 4,294,967,295.
- A security identifier (SID) for a Windows user account. A SID is a series of authorities and sub-authorities ending with a 32-bit relative identifier (RID). Most SIDs have the form S-1-5-21-<A>-<B>-<C>-<RID>, where <A>, <B>, and <C> are specific to a domain or computer and <RID> denotes the object in the domain.
- A primary group SID for a Windows group account.
- A list of supplemental identities, including all groups in which the user is a member.

The token also contains privileges that stem from administrative role-based access control.

On an Isilon cluster, a file contains permissions, which appear as an access control list (ACL). The ACL controls access to directories, files, and other securable system objects.

When a user tries to access a file, OneFS compares the identities in the user’s access token with the file’s ACL. OneFS grants access when the file’s ACL includes an access...
control entry (ACE) that allows the identity in the token to access the file and that does not include an ACE that denies the identity access. OneFS compares the access token of a user with the ACL of a file.

Note

For more information about access control lists, including a description of the permissions and how they correspond to POSIX mode bits, see the white paper titled *EMC Isilon multiprotocol data access with a unified security model* on the EMC Online Support web site.

When a name is provided as an identifier, it is converted into the corresponding user or group object and the correct identity type. You can enter or display a name in various ways:

- UNIX assumes unique case-sensitive namespaces for users and groups. For example, Name and name represent different objects.
- Windows provides a single, case-insensitive namespace for all objects and also specifies a prefix to target an Active Directory domain; for example, domain\name.
- Kerberos and NFSv4 define principals, which require names to be formatted the same way as email addresses; for example, name@domain.com.

Multiple names can reference the same object. For example, given the name support and the domain example.com, support, EXAMPLE\support and support@example.com are all names for a single object in Active Directory.

## Access tokens

An access token is created when the user first makes a request for access.

Access tokens represent who a user is when performing actions on the cluster and supply the primary owner and group identities during file creation. Access tokens are also compared against the ACL or mode bits during authorization checks.

During user authorization, OneFS compares the access token, which is generated during the initial connection, with the authorization data on the file. All user and identity mapping occurs during token generation; no mapping takes place during permissions evaluation.

An access token includes all UIDs, GIDs, and SIDs for an identity, in addition to all OneFS privileges. OneFS reads the information in the token to determine whether a user has access to a resource. It is important that the token contains the correct list of UIDs, GIDs, and SIDs. An access token is created from one of the following sources:

<table>
<thead>
<tr>
<th>Source</th>
<th>Authentication</th>
</tr>
</thead>
</table>
| Username | • SMB impersonate user  
• Kerberized NFSv3  
• Kerberized NFSv4  
• NFS export user mapping  
• HTTP  
• FTP  
• HDFS |
### Access token generation

For most protocols, the access token is generated from the username or from the authorization data that is retrieved during authentication.

The following steps present a simplified overview of the complex process through which an access token is generated:

**Step 1: User identity lookup**

Using the initial identity, the user is looked up in all configured authentication providers in the access zone, in the order in which they are listed. The user identity and group list are retrieved from the authenticating provider. Next, additional group memberships that the user and group list are looked up for all other authentication providers. All of these SIDs, UIDs, are GIDs are added to the initial token.

**Note**

An exception to this behavior occurs if the AD provider is configured to call other providers, such as LDAP or NIS.

**Step 2: ID mapping**

The user's identifiers are associated across directory services. All SIDs are converted to their equivalent UID/GID and vice versa. These ID mappings are also added to the access token.

**Step 3: User mapping**

Access tokens from other directory services are combined. If the username matches any user mapping rules, the rules are processed in order and the token is updated accordingly.

**Step 4: On-disk identity calculation**

The default on-disk identity is calculated from the final token and the global setting. These identities are used for newly created files.

### ID mapping

The ID mapping service maintains relationship information between mapped Windows and UNIX identifiers to provide consistent access control across file sharing protocols within an access zone.

**Note**

ID mapping and user mapping are different services, despite the similarity in names.
During authentication, the authentication daemon requests identity mappings from the ID mapping service in order to create access tokens. Upon request, the ID mapping service returns Windows identifiers mapped to UNIX identifiers or UNIX identifiers mapped to Windows identifiers. When a user authenticates to a cluster over NFS with a UID or GID, the ID mapping service returns the mapped Windows SID, allowing access to files that another user stored over SMB. When a user authenticates to the cluster over SMB with a SID, the ID mapping service returns the mapped UNIX UID and GID, allowing access to files that a UNIX client stored over NFS.

Mappings between UIDs or GIDs and SIDs are stored according to access zone in a cluster-distributed database called the ID map. Each mapping in the ID map is stored as a one-way relationship from the source to the target identity type. Two-way mappings are stored as complementary one-way mappings.

Mapping Windows IDs to UNIX IDs

When a Windows user authenticates with an SID, the authentication daemon searches the external Active Directory provider to look up the user or group associated with the SID. If the user or group has only an SID in the Active Directory, the authentication daemon requests a mapping from the ID mapping service.

Note
User and group lookups may be disabled or limited, depending on the Active Directory settings. You enable user and group lookup settings through the `isi auth ads modify` command.

If the ID mapping service does not locate and return a mapped UID or GID in the ID map, the authentication daemon searches other external authentication providers configured in the same access zone for a user that matches the same name as the Active Directory user.

If a matching user name is found in another external provider, the authentication daemon adds the matching user's UID or GID to the access token for the Active Directory user, and the ID mapping service creates a mapping between the UID or GID and the Active Directory user's SID in the ID map. This is referred to as an external mapping.

Note
When an external mapping is stored in the ID map, the UID is specified as the on-disk identity for that user. When the ID mapping service stores a generated mapping, the SID is specified as the on-disk identity.

If a matching user name is not found in another external provider, the authentication daemon assigns a UID or GID from the ID mapping range to the Active Directory user's SID, and the ID mapping service stores the mapping in the ID map. This is referred to as a generated mapping. The ID mapping range is a pool of UIDs and GIDs allocated in the mapping settings.

After a mapping has been created for a user, the authentication daemon retrieves the UID or GID stored in the ID map upon subsequent lookups for the user.

Mapping UNIX IDs to Windows IDs

The ID mapping service creates temporary UID-to-SID and GID-to-SID mappings only if a mapping does not already exist. The UNIX SIDs that result from these mappings are never stored on disk.

UIDs and GIDs have a set of predefined mappings to and from SIDs.
If a UID-to-SID or GID-to-SID mapping is requested during authentication, the ID mapping service generates a temporary UNIX SID in the format S-1-22-1-<UID> or S-1-22-2-<GID> by applying the following rules:

- For UIDs, the ID mapping service generates a UNIX SID with a domain of S-1-22-1 and a resource ID (RID) matching the UID. For example, the UNIX SID for UID 600 is S-1-22-1-600.
- For GIDs, the ID mapping service generates a UNIX SID with a domain of S-1-22-2 and an RID matching the GID. For example, the UNIX SID for GID 800 is S-1-22-2-800.

ID mapping ranges

In access zones with multiple external authentication providers, such as Active Directory and LDAP, it is important that the UIDs and GIDs from different providers that are configured in the same access zone do not overlap. Overlapping UIDs and GIDs between providers within an access zone might result in some users gaining access to other users' directories and files.

The range of UIDs and GIDs that can be allocated for generated mappings is configurable in each access zone through the `isi auth settings mappings modify` command. The default range for both UIDs and GIDs is 1000000–2000000 in each access zone.

Do not include commonly used UIDs and GIDs in your ID ranges. For example, UIDs and GIDs below 1000 are reserved for system accounts and should not be assigned to users or groups.

User mapping

User mapping provides a way to control permissions by specifying a user's security identifiers, user identifiers, and group identifiers. OneFS uses the identifiers to check file or group ownership.

With the user-mapping feature, you can apply rules to modify which user identity OneFS uses, add supplemental user identities, and modify a user's group membership. The user-mapping service combines a user's identities from different directory services into a single access token and then modifies it according to the rules that you create.

Note

You can configure mapping rules on a per-zone basis. Mapping rules must be configured separately in each access zone that uses them. OneFS maps users only during login or protocol access.

Default user mappings

Default user mappings determine access if explicit user-mapping rules are not created.

If you do not configure rules, a user who authenticates with one directory service receives the identity information in other directory services when the account names are the same. For example, a user who authenticates with an Active Directory domain as Desktop\jane automatically receives identities in the final access token for the corresponding UNIX user account for jane from LDAP or NIS.

In the most common scenario, OneFS is connected to two directory services, Active Directory and LDAP. In such a case, the default mapping provides a user with the following identity attributes:
- A UID from LDAP
- The user SID from Active Directory
- An SID from the default group in Active Directory

The user’s groups come from Active Directory and LDAP, with the LDAP groups and the autogenerated group GID added to the list. To pull groups from LDAP, the mapping service queries the memberUid attribute. The user’s home directory, gecos, and shell come from Active Directory.

Elements of user-mapping rules

You combine operators with user names to create a user-mapping rule. The following elements affect how the user mapper applies a rule:
- The operator, which determines the operation that a rule performs
- Fields for usernames
- Options
- A parameter
- Wildcards

User-mapping best practices

You can follow best practices to simplify user mapping.

Use Active Directory with RFC 2307 and Windows Services for UNIX

Use Microsoft Active Directory with Windows Services for UNIX and RFC 2307 attributes to manage Linux, UNIX, and Windows systems. Integrating UNIX and Linux systems with Active Directory centralizes identity management and eases interoperability, reducing the need for user-mapping rules. Make sure your domain controllers are running Windows Server 2003 or later.

Employ a consistent username strategy

The simplest configurations name users consistently, so that each UNIX user corresponds to a similarly named Windows user. Such a convention allows rules with wildcard characters to match names and map them without explicitly specifying each pair of accounts.

Do not use overlapping ID ranges

In networks with multiple identity sources, such as LDAP and Active Directory with RFC 2307 attributes, you should ensure that UID and GID ranges do not overlap. It is also important that the range from which OneFS automatically allocates UIDs and GIDs does not overlap with any other ID range. OneFS automatically allocates UIDs and GIDs from the range 1,000,000–2,000,000. If UIDs and GIDs overlap multiple directory services, some users might gain access to other users’ directories and files.

Avoid common UIDs and GIDs

Do not include commonly used UIDs and GIDs in your ID ranges. For example, UIDs and GIDs below 1000 are reserved for system accounts; do not assign them to users or groups.

Do not use UPNs in mapping rules

You cannot use a user principal name (UPN) in a user mapping rule. A UPN is an Active Directory domain and username that are combined into an Internet-style name with an @ symbol, such as an email address: jane@example. If you include a
UPN in a rule, the mapping service ignores it and may return an error. Instead, specify names in the format DOMAIN\user.com.

**Group rules by type and order them**

The system processes every mapping rule by default, which can present problems when you apply a deny-all rule—for example, to deny access to all unknown users. In addition, replacement rules might interact with rules that contain wildcard characters. To minimize complexity, it is recommended that you group rules by type and organize them in the following order:

1. Replacement rules: Specify all rules that replace an identity first to ensure that OneFS replaces all instances of the identity.
2. Join, add, and insert rules: After the names are set by any replacement operations, specify join, add, and insert rules to add extra identifiers.
3. Allow and deny rules: Specify rules that allow or deny access last.

**Note**

Stop all processing before applying a default deny rule. To do so, create a rule that matches allowed users but does nothing, such as an add operator with no field options, and has the break option. After enumerating the allowed users, you can place a catchall deny at the end to replace anybody unmatched with an empty user.

To prevent explicit rules from being skipped, in each group of rules, order explicit rules before rules that contain wildcard characters.

**Add the LDAP or NIS primary group to the supplemental groups**

When an Isilon cluster is connected to Active Directory and LDAP, a best practice is to add the LDAP primary group to the list of supplemental groups. This lets OneFS honor group permissions on files created over NFS or migrated from other UNIX storage systems. The same practice is advised when an Isilon cluster is connected to both Active Directory and NIS.

**On-disk identity**

After the user mapper resolves a user’s identities, OneFS determines an authoritative identifier for it, which is the preferred on-disk identity.

OneFS stores either UNIX or Windows identities in file metadata on disk. On-disk identity types are UNIX, SID, and native. Identities are set when a file is created or a file’s access control data is modified. Almost all protocols require some level of mapping to operate correctly, so choosing the preferred identity to store on disk is important. You can configure OneFS to store either the UNIX or the Windows identity, or you can allow OneFS to determine the optimal identity to store.

On-disk identity types are UNIX, SID, and native. Although you can change the type of on-disk identity, the native identity is best for a network with UNIX and Windows systems. In native on-disk identity mode, setting the UID as the on-disk identity improves NFS performance.
Note
The SID on-disk identity is for a homogeneous network of Windows systems managed only with Active Directory. When you upgrade from a version earlier than OneFS 6.5, the on-disk identity is set to UNIX. When you upgrade from OneFS 6.5 or later, the on-disk identity setting is preserved. On new installations, the on-disk identity is set to native.

The native on-disk identity type allows the OneFS authentication daemon to select the correct identity to store on disk by checking for the identity mapping types in the following order:

<table>
<thead>
<tr>
<th>Order</th>
<th>Mapping type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Algorithmic mapping</td>
<td>An SID that matches S-1-22-1-UID or S-1-22-2-GID in the internal ID mapping database is converted back to the corresponding UNIX identity, and the UID and GID are set as the on-disk identity.</td>
</tr>
<tr>
<td>2</td>
<td>External mapping</td>
<td>A user with an explicit UID and GID defined in a directory service (such as Active Directory with RFC 2307 attributes, LDAP, NIS, or the OneFS file provider or local provider) has the UNIX identity set as the on-disk identity.</td>
</tr>
<tr>
<td>3</td>
<td>Persistent mapping</td>
<td>Mappings are stored persistently in the identity mapper database. An identity with a persistent mapping in the identity mapper database uses the destination of that mapping as the on-disk identity, which occurs primarily with manual ID mappings. For example, if there is an ID mapping of GID: 10000 to S-1-5-32-545, a request for the on-disk storage of GID:10000 returns S-1-5-32-545.</td>
</tr>
<tr>
<td>4</td>
<td>No mapping</td>
<td>If a user lacks a UID or GID even after querying the other directory services and identity databases, its SID is set as the on-disk identity. In addition, to make sure a user can access files over NFS, OneFS allocates a UID and GID from a preset range of</td>
</tr>
</tbody>
</table>
Managing ID mappings

You can create, modify, and delete identity mappings and configure ID mapping settings.

Create an identity mapping

You can create a manual identity mapping between source and target identities or automatically generate a mapping for a source identity.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping create` command.

The following command specifies IDs of source and target identities in the zone3 access zone to create a two-way mapping between the identities:

```
isi auth mapping create --2way --source-sid=S-1-5-21-12345 --target-uid=5211 --zone=zone3
```

Modify an identity mapping

You can modify the configuration of an identity mapping.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping modify` command.

The following command modifies the mapping of the user with UID 4236 in the zone3 access zone to include a reverse, 2-way mapping between the source and target identities:

```
isi auth mapping modify --source-uid=4236 --target-sid=S-1-5-21-12345 --zone=zone3 --2way
```
Delete an identity mapping

You can delete one or more identity mappings.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping delete` command.

The following command deletes all identity mappings in the zone3 access zone:

```
isi auth mapping delete --all --zone=zone3
```

The following command deletes all identity mappings in the zone3 access zone that were both created automatically and include a UID or GID from an external authentication source:

```
isi auth mapping delete --all --only-external --zone=zone3
```

The following command deletes the identity mapping of the user with UID 4236 in the zone3 access zone:

```
isi auth mapping delete --source-uid=4236 --zone=zone3
```

View an identity mapping

You can display mapping information for a specific identity.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping view` command.

The following command displays mappings for the user with UID 4236 in the zone3 access zone:

```
isi auth mapping view --uid=4236 --zone=zone3
```

The system displays output similar to the following example:

```
Name: user_36
On-disk: UID: 4236
Unix uid: 4236
Unix gid: -100000
SMB: S-1-22-1-4236
```
Flush the identity mapping cache

You can flush the ID map cache to remove in-memory copies of all or specific identity mappings.

Modifications to ID mappings may cause the cache to become out-of-sync and users might experience slowness or stalls when authenticating. You can flush the cache to synchronize the mappings.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping flush` command.

   The following command flushes all identity mappings on the EMC Isilon cluster:

   ```
   isi auth mapping flush --all
   ```

   The following command flushes the mapping of the user with UID 4236 in the zone3 access zone:

   ```
   isi auth mapping flush --source-uid-4236 --zone=zone3
   ```

View a user token

You can view the contents of an access token generated for a user during authentication.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping token` command.

   The following command displays the access token of a user with UID 4236 in the zone3 access zone:

   ```
   isi auth mapping token --uid=4236 --zone=zone3
   ```

   The system displays output similar to the following example:

   ```
   User
   Name: user_36
   UID: 4236
   SID: S-1-22-1-4236
   On Disk: 4236
   ZID: 3
   Zone: zone3
   Privileges: -
   Primary Group
   Name: user_36
   GID: 4236
   SID: S-1-22-2-4236
   On Disk: 4236
   ```
Configure identity mapping settings

You can enable or disable automatic allocation of UIDs and GIDS and customize the range of ID values in each access zone. The default range is 1000000–2000000.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth settings mapping modify` command.

   The following command enables automatic allocation of both UIDs and GIDs in the zone3 access zone and sets their allocation ranges to 25000–50000:

   ```bash
   isi auth settings mapping modify --gid-range-enabled=yes --gid-range-min=25000 --gid-range-max=50000 --uid-range-enabled=yes --uid-range-min=25000 --uid-range-max=50000 --zone=zone3
   ```

View identity mapping settings

You can view the current configuration of identity mapping settings in each zone.

This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth settings mapping view` command.

   The following command displays the current settings in the zone3 access zone:

   ```bash
   isi auth settings mapping view --zone=zone3
   ```

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>GID Range Enabled: Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>GID Range Min: 25000</td>
</tr>
<tr>
<td>GID Range Max: 50000</td>
</tr>
<tr>
<td>UID Range Enabled: Yes</td>
</tr>
<tr>
<td>UID Range Min: 25000</td>
</tr>
<tr>
<td>UID Range Max: 50000</td>
</tr>
</tbody>
</table>

Managing user identities

You can manage user identities by creating user-mapping rules.

When you create user-mapping rules, it is important to remember the following information:

- You can only create user-mapping rules if you are connected to the EMC Isilon cluster through the System zone; however, you can apply user-mapping rules to specific access zones. If you create a user-mapping rule for a specific access zone, the rule applies only in the context of its zone.

- When you change user-mapping on one node, OneFS propagates the change to the other nodes.
After you make a user-mapping change, the OneFS authentication service reloads the configuration.

### View user identity

You can view the identities and group membership that a specified user has within the Active Directory and LDAP directory services.

This procedure must be performed through the command-line interface (CLI).

**Note**

The OneFS user access token contains a combination of identities from Active Directory and LDAP if both directory services are configured. You can run the following commands to discover the identities that are within each specific directory service.

**Procedure**

1. Establish an SSH connection to any node in the cluster.

2. **View a user identity from Active Directory only by running the `isi auth users view` command.**

   The following command displays the identity of a user named stand in the Active Directory domain named YORK:

   ```bash
   isi auth users view --user=YORK\stand --show-groups
   ```

   The system displays output similar to the following example:

   ```
   Name: YORK\stand
   DN:
   CN=stand,CN=Users,DC=york,DC=hull,DC=example,DC=com
   DNS Domain: york.hull.example.com
   Domain: YORK
   Provider: lsa-activedirectory-provider:YORK.HULL.EXAMPLE.COM
   Sam Account Name: stand
   UID: 4326
   SID:
   S-1-5-21-1195855716-1269722693-1240286574-591111
   Primary Group
      ID : GID:1000000
      Name : YORK\york_sh_ug
   Additional Groups: YORK\ad-york_space_group
      YORK\york_sh_ug
      YORK\sd-york-group
      YORK\sd-group
      YORK\domain users
   ```

3. **View a user identity from LDAP only by running the `isi auth users view` command.**

   The following command displays the identity of an LDAP user named stand:

   ```bash
   isi auth user view --user=stand --show-groups
   ```

   The system displays output similar to the following example:

   ```
   Name: stand
   DN:
   ```
Create a user-mapping rule

You can create user-mapping rules to manage user identities on the cluster.

You can create the first mapping rule with the --user-mapping-rules option for the isi zone zones modify System command. If you try to add a second rule with the command above, however, it replaces the existing rule rather than adding the new rule to the list of rules. To add more rules to the list of rules, you must use the --add-user-mapping-rules option with the isi zone zones modify System command.

Note

If you do not specify an access zone, user-mapping rules are created in the System zone.

Procedure

1. To create a rule to merge the Active Directory user with a user from LDAP, run the following command, where <user-a> and <user-b> are placeholders for the identities to be merged; for example, user_9440 and lduser_010, respectively:

   ```
   isi zone zones modify System --add-user-mapping-rules "<DOMAIN> <user-a> &= <user-b>
   ```

   Run the following command to view the rule:

   ```
   isi zone zones view System
   ```

   If the command runs successfully, the system displays the mapping rule, which is visible in the User Mapping Rules line of the output:
2. To verify the changes to the token, run a command similar to the following example:

```
isi auth mapping token <DOMAIN>\<user-a>
```

If the command runs successfully, the system displays output similar to the following example:

```
User
   Name: <DOMAIN>\<user-a>
   UID: 1000201
   SID: S-1-5-21-1195855716-1269722693-1240286574-11547
   ZID: 1
   Zone: System
   Privileges: -
Primary Group
   Name: <DOMAIN>\domain users
   GID: 1000000
   SID: S-1-5-21-1195855716-1269722693-1240286574-513
Supplemental Identities
   Name: Users
   GID: 1545
   SID: S-1-5-32-545
   Name: lduser_010
   UID: 10010
   SID: S-1-22-1-10010
   Name: example
   GID: 10000
   SID: S-1-22-2-10000
   Name: ldgroup_20user
   GID: 10026
   SID: S-1-22-2-10026
```

### Merge Windows and UNIX tokens

You can use either the join or append operator to merge two user names into a single token.

When Windows and UNIX user names do not match across directory services, you can write user-mapping rules that use either the join or the append operator to merge two user names into a single token. For example, if a user's Windows username is win_bob and the users UNIX username is UNIX_bob, you can join or append them.

When you append an account to another account, the append operator adds information from one identity to another. OneFS appends the fields that the options specify from the source identity to the target identity. OneFS appends the identifiers to the additional group list.

**Procedure**

1. Establish an SSH connection to any node in the cluster.
2. Write a rule similar to the following example to join the Windows and UNIX user names, where `<win-username>` and `<UNIX-username>` are placeholders for the user's Windows and UNIX accounts:

```
MYDOMAIN\<win-username> &= <UNIX-username> []
```
3. Write a rule similar to the following example to append the UNIX account to the Windows account with the groups option:

```
MYDOMAIN\<win-username> ++ <UNIX-username> [groups]
```

### Retrieve the primary group from LDAP

You can create a user-mapping rule to insert or append primary group information from LDAP into a user's access token.

By default, the user-mapping service combines information from AD and LDAP but gives precedence to the information from AD. Mapping rules control how OneFS combines the information. You can retrieve the primary group information from LDAP instead of AD.

**Procedure**

1. Establish an SSH connection to any node in the cluster.
2. Write a rule similar to the following example to insert information from LDAP into a user's access token:

```
*\* += * [group]
```

3. Write a rule similar to the following example to append other information from LDAP to a user's access token:

```
*\* ++ * [user,groups]
```

### Mapping rule options

Mapping rules can contain options that target the fields of an access token.

A field represents an aspect of a cross-domain access token, such as the primary UID and primary user SID from a user that you select. You can see some of the fields in the OneFS web administration interface. User in the web administration interface is the same as username. You can also see fields in an access token by running the command `isi auth mapping token`.

When you create a rule, you can add an option to manipulate how OneFS combines aspects of two identities into a single token. For example, an option can force OneFS to append the supplement groups to a token.

A token includes the following fields that you can manipulate with user mapping rules:

- `username`
- `unix_name`
- `primary_uid`
- `primary_user_sid`
- `primary_gid`
- `primary_group_sid`
- `additional_ids` (includes supplemental groups)
Options control how a rule combines identity information in a token. The break option is the exception: It stops OneFS from processing additional rules.

Although several options can apply to a rule, not all options apply to all operators. The following table describes the effect of each option and the operators that they work with.

<table>
<thead>
<tr>
<th>Option</th>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>insert, append</td>
<td>Copies the primary UID and primary user SID, if they exist, to the token.</td>
</tr>
<tr>
<td>groups</td>
<td>insert, append</td>
<td>Copies the primary GID and primary group SID, if they exist, to the token.</td>
</tr>
<tr>
<td>default_user</td>
<td>all operators except remove groups</td>
<td>If the mapping service fails to find the second user in a rule, the service tries to find the username of the default user. The name of the default user cannot include wildcards. When you set the option for the default user in a rule with the command-line interface, you must set it with an underscore: default_user.</td>
</tr>
<tr>
<td>break</td>
<td>all operators</td>
<td>Stops the mapping service from applying rules that follow the insertion point of the break option. The mapping service generates the final token at the point of the break.</td>
</tr>
</tbody>
</table>

**Mapping rule operators**

The operator determines what a mapping rule does.

You can create user-mapping rules through either the web-administration interface, where the operators are spelled out in a list, or from the command-line interface.

When you create a mapping rule with the OneFS command-line interface (CLI), you must specify an operator with a symbol. The operator affects the direction in which the mapping service processes a rule. For more information about creating a mapping rule, see the white paper *Managing identities with the Isilon OneFS user mapping service*. The following table describes the operators that you can use in a mapping rule.

A mapping rule can contain only one operator.
<table>
<thead>
<tr>
<th>Operator</th>
<th>Web interface</th>
<th>CLI</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>append</td>
<td>Append fields from a user</td>
<td>++</td>
<td>Left-to-right</td>
<td>Modifies an access token by adding fields to it. The mapping service appends the fields that are specified in the list of options (user, group, groups) to the first identity in the rule. The fields are copied from the second identity in the rule. All appended identifiers become members of the additional groups list. An append rule without an option performs only a lookup operation; you must include an option to alter a token.</td>
</tr>
<tr>
<td>insert</td>
<td>Insert fields from a user</td>
<td>+=</td>
<td>Left-to-right</td>
<td>Modifies an existing access token by adding fields to it. Fields specified in the options list (user, group, groups) are copied from the new identity and inserted into the identity in the token. When the rule inserts a primary user or primary group, it become the new primary user and primary group in the token. The previous primary user and primary group move to the additional identifiers list.</td>
</tr>
<tr>
<td>Operator</td>
<td>Web interface</td>
<td>CLI</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>replace</td>
<td>Replace one user with a different user</td>
<td>=&gt;</td>
<td>Left-to-right</td>
<td>Removes the token and replaces it with the new token that is identified by the second username. If the second username is empty, the mapping service removes the first username in the token, leaving no username. If a token contains no username, OneFS denies access with a no such user error.</td>
</tr>
<tr>
<td>remove groups</td>
<td>Remove supplemental groups from a user</td>
<td>--</td>
<td>Unary</td>
<td>Modifies a token by removing the supplemental groups.</td>
</tr>
<tr>
<td>join</td>
<td>Join two users together</td>
<td>&amp;=</td>
<td>Bidirectional</td>
<td>Inserts the new identity into the token. If the new identity is the second user, the mapping service inserts it after the existing identity; otherwise, the service inserts it before the existing identity.</td>
</tr>
<tr>
<td>Operator</td>
<td>Web interface</td>
<td>CLI</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>-----</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The location of the insertion point is relevant when the existing identity is already the first in the list because OneFS uses the first identity to determine the ownership of new file system objects.</td>
</tr>
</tbody>
</table>
CHAPTER 9

Home directories

This section contains the following topics:

- Home directories overview ................................................................. 406
- Home directory permissions ................................................................. 406
- Authenticating SMB users ................................................................. 406
- Home directory creation through SMB ................................................. 406
- Home directory creation through SSH and FTP ..................................... 410
- Home directory creation in a mixed environment .................................. 414
- Interactions between ACLs and mode bits ........................................... 414
- Default home directory settings in authentication providers .................. 414
- Supported expansion variables ......................................................... 415
- Domain variables in home directory provisioning .................................. 417
Home directories overview

When you create a local user, OneFS automatically creates a home directory for the user. OneFS also supports dynamic home directory provisioning for users who access the cluster by connecting to an SMB share or by logging in through FTP or SSH.

Regardless of the method by which a home directory was created, you can configure access to the home directory through a combination of SMB, SSH, and FTP.

Home directory permissions

You can set up a user's home directory with a Windows ACL or with POSIX mode bits, which are then converted into a synthetic ACL. The method by which a home directory is created determines the initial permissions that are set on the home directory.

When you create a local user, the user's home directory is created with mode bits by default.

For users who authenticate against external sources, you can specify settings to create home directories dynamically at login time. If a home directory is created during a login through SSH or FTP, it is set up with mode bits; if a home directory is created during an SMB connection, it receives either mode bits or an ACL. For example, if an LDAP user first logs in through SSH or FTP, the user's home directory is created with mode bits. If the same user first connects through an SMB share, the home directory is created with the permissions indicated by the configured SMB settings. If the --inheritable-path-acl option is enabled, an ACL is generated; otherwise, mode bits are used.

Authenticating SMB users

You can authenticate SMB users from authentication providers that can handle NT hashes.

SMB sends an NT password hash to authenticate SMB users, so only users from authentication providers that can handle NT hashes can log in over SMB. The following OneFS-supported authentication providers can handle NT hashes:

- Active Directory
- Local
- LDAPSAM (LDAP with Samba extensions enabled)

Home directory creation through SMB

You can create SMB shares by including expansion variables in the share path. Expansion variables give users to access their home directories by connecting to the
You can also enable dynamic provisioning of home directories that do not exist at SMB connection time.

**Note**

Share permissions are checked when files are accessed, before the underlying file system permissions are checked. Either of these permissions can prevent access to the file or directory.

### Create home directories with expansion variables

You can configure settings with expansion variables to create SMB share home directories.

When users access the EMC Isilon cluster over SMB, home directory access is through SMB shares. You can configure settings with a path that uses a variable expansion syntax, allowing a user to connect to their home directory share.

**Note**

Home directory share paths must begin with `/ifs/` and must be in the root path of the access zone in which the home directory SMB share is created.

In the following commands, the `--allow-variable-expansion` option is enabled to indicate that `%U` should be expanded to the user name, which is `user411` in this example. The `--auto-create-directory` option is enabled to create the directory if it does not exist:

```bash
isi smb shares create HOMEDIR --path=/ifs/home/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes
isi smb shares permission modify HOMEDIR --wellknown Everyone \
   --permission-type allow --permission full
isi smb shares view HOMEDIR
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Share Name: HOMEDIR</th>
<th>Path: /ifs/home/%U</th>
<th>Description:</th>
<th>Client-side Caching Policy: manual</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Automatically expand user names or domain names: True</td>
<td>Automatically create home directories for users: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Browsable: True</td>
<td></td>
</tr>
<tr>
<td>Permissions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>Account Type</td>
<td>Run as Root</td>
<td>Permission Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Everyone</td>
<td>wellknown</td>
<td>False</td>
<td>allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total: 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When `user411` connects to the share with the `net use` command, the user's home directory is created at `/ifs/home/user411`. On `user411`'s Windows client, the `net use m:` command connects `/ifs/home/user411` through the HOMEDIR share:

```bash
net use m: \cluster.company.com\HOMEDIR /u:user411
```
**Procedure**

1. Run the following commands on the cluster with the `--allow-variable-expansion` option enabled. The `%U` expansion variable expands to the user name, and the `--auto-create-directory` option is enabled to create the directory if it does not exist:

   ```
   isi smb shares create HOMEDIR --path=/ifs/home/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes
   isi smb shares permission modify HOMEDIR --wellknown Everyone \
   --permission-type allow --permission full
   ```

2. Run the following command to view the home directory settings:

   ```
   isi smb shares view HOMEDIR
   ```

   The system displays output similar to the following example:

   ```
   Share Name: HOMEDIR
   Path: /ifs/home/%U
   Description:
   Client-side Caching Policy: manual
   Automatically expand user names or domain names: True
   Automatically create home directories for users: True
  Browsable: True
   Permissions:
   Account    Account Type Run as Root Permission Type Permission
   ---------------------------------------------------------------
   Everyone wellknown    False       allow           full
   ---------------------------------------------------------------
   Total: 1
   ```

If user411 connects to the share with the `net use` command, user411's home directory is created at `/ifs/home/user411`. On user411's Windows client, the `net use m:` command connects `/ifs/home/user411` through the `HOMEDIR` share, mapping the connection similar to the following example:

```
net use m: \\cluster.company.com\HOMEDIR /u:user411
```

### Create home directories with the `--inheritable-path-acl` option

You can enable the `--inheritable-path-acl` option on a share to specify that it is to be inherited on the share path if the parent directory has an inheritable ACL.

**Before you begin**

To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

By default, an SMB share's directory path is created with a synthetic ACL based on mode bits. You can enable the `--inheritable-path-acl` option to use the inheritable ACL on all directories that are created, either at share creation time or for those dynamically provisioned when connecting to that share.
Procedure

1. Run commands similar to the following examples to enable the --inheritable-path-acl option on the cluster to dynamically provision a user home directory at first connection to a share on the cluster:

   ```
   isi smb shares create HOMEDIR_ACL --path=/ifs/home/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes \
   --inheritable-path-acl=yes
   ```

   ```
   isi smb shares permission modify HOMEDIR_ACL \ 
   --wellknown Everyone \ 
   --permission-type allow --permission full
   ```

2. Run a `net use` command, similar to the following example, on a Windows client to map the home directory for user411:

   ```
   net use q: \cluster.company.com\HOMEDIR_ACL /u:user411
   ```

3. Run a command similar to the following example on the cluster to view the inherited ACL permissions for the user411 share:

   ```
   cd /ifs/home/user411
   ls -lde .
   ```

   The system displays output similar to the following example:

   ```
   drwx------ +  2 user411 Isilon Users 0 Oct 19 16:23 ./
   OWNER: user:user411
   GROUP: group:Isilon Users
   CONTROL:dacl_auto_inherited,dacl_protected
   0: user:user411 allow
   dir_gen_all,object_inherit,container_inherit
   ```

Create special home directories with the SMB share %U variable

The special SMB share name %U enables you to create a home-directory SMB share that appears the same as a user's user name.

You typically set up a %U SMB share with a share path that includes the %U expansion variable. If a user attempts to connect to a share matching the login name and it does not exist, the user connects to the %U share instead and is directed to the expanded path for the %U share.

---

**Note**

If another SMB share exists that matches the user's name, the user connects to the explicitly named share rather than to the %U share.
Procedure

1. Run the following command to create a share that matches the authenticated user login name when the user connects to the share:

   isi smb share create %U /ifs/home/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes \
   --zone=System

   After running this command, user Zachary will see a share named 'zachary' rather than '%U', and when Zachary tries to connect to the share named 'zachary', he will be directed to /ifs/home/zachary. On a Windows client, if Zachary runs the following commands, he sees the contents of his /ifs/home/zachary directory:

   net use m: \cluster.ip\zachary /u:zachary
   cd m:
   dir

   Similarly, if user Claudia runs the following commands on a Windows client, she sees the directory contents of /ifs/home/claudia:

   net use m: \cluster.ip\claudia /u:claudia
   cd m:
   dir

   Zachary and Claudia cannot access one another's home directory because only the share 'zachary' exists for Zachary and only the share 'claudia' exists for Claudia.

Home directory creation through SSH and FTP

You can configure home directory support for users who access the cluster through SSH or FTP by modifying authentication provider settings.

Set the SSH or FTP login shell

You can use the --login-shell option to set the default login shell for the user.

By default, the --login-shell option, if specified, overrides any login-shell information provided by the authentication provider, except with Active Directory. If the --login-shell option is specified with Active Directory, it simply represents the default login shell if the Active Directory server does not provide login-shell information.

Note

The following examples refer to setting the login shell to /bin/bash. You can also set the shell to /bin/rbash.
Procedure
1. Run the following command to set the login shell for all local users to /bin/bash:

   isi auth local modify System --login-shell /bin/bash

2. Run the following command to set the default login shell for all Active Directory users in your domain to /bin/bash:

   isi auth ads modify YOUR.DOMAIN.NAME.COM --login-shell /bin/bash

Set SSH/FTP home directory permissions
You can specify home directory permissions for a home directory that is accessed through SSH or FTP by setting a umask value.

Before you begin
To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

When a user's home directory is created at login through SSH or FTP, it is created using POSIX mode bits. The permissions setting on a user's home directory is set to 0755, then masked according to the umask setting of the user's access zone to further limit permissions. You can modify the umask setting for a zone with the --home-directory-umask option, specifying an octal number as the umask value.

Procedure
1. Run the following command to view umask setting:

   isi zone zones view System

The system displays output similar to the following example:

   Name: System
   Path: /ifs
   Cache Size: 4.77M
   Map Untrusted: -
   Auth Providers: -
   NetBIOS Name: -
   All Auth Providers: Yes
   User Mapping Rules: -
   Home Directory Umask: 0077
   Skeleton Directory: /usr/share/skel
   Audit Success: create, delete, rename, set_security, close
   Audit Failure: create, delete, rename, set_security, close
   HDFS Authentication: all
   HDFS Keytab: /etc/hdfs.keytab
   HDFS Root Directory: /ifs
   WebHDFS Enabled: Yes
   Syslog Forwarding Enabled: No
   Syslog Audit Events: create, delete, rename, set_security
   Zone ID: 1
In the command result, you can see the default setting for Home Directory Umask for the created home directory is 0700, which is equivalent to (0755 & ~(077)). You can modify the Home Directory Umask setting for a zone with the --home-directory-umask option, specifying an octal number as the umask value. This value indicates the permissions that are to be disabled, so larger mask values indicate fewer permissions. For example, a umask value of 000 or 022 yields created home directory permissions of 0755, whereas a umask value of 077 yields created home directory permissions of 0700.

2. Run a command similar to the following example to allow a group/others write/execute permission in a home directory:

   ```
   isi zone zones modify System --home-directory-umask=022
   ```

   In this example, user home directories will be created with mode bits 0755 masked by the umask field, set to the value of 022. Therefore, user home directories will be created with mode bits 0755, which is equivalent to (0755 & ~(022)).

**Set SSH/FTP home directory creation options**

You can configure home directory support for a user who accesses the cluster through SSH or FTP by specifying authentication provider options.

**Procedure**

1. Run the following command to view settings for an Active Directory authentication provider on the cluster:

   ```
   isi auth ads list
   ```

   The system displays output similar to the following example:

   ```
   Name                 Authentication Status DC Name Site
   ------------------------- ---------------------------------------------------------
   YOUR.DOMAIN.NAME.COM   Yes            online -       SEA
   ------------------------- ---------------------------------------------------------
   Total: 1
   ```

2. Run the `isi auth ads modify` command with the `--home-directory-template` and `--create-home-directory` options.

   ```
   isi auth ads modify YOUR.DOMAIN.NAME.COM \
   --home-directory-template=/ifs/home/ADS/%D/%U \
   --create-home-directory=yes
   ```

3. Run the `isi auth ads view` command with the `--verbose` option.

   The system displays output similar to the following example:

   ```
   Name: YOUR.DOMAIN.NAME.COM
   NetBIOS Domain: YOUR
   ...
   Create Home Directory: Yes
   Home Directory Template: /ifs/home/ADS/%D/%U
   Login Shell: /bin/sh
   ```

4. Run the `id` command.
The system displays output similar to the following example:

```
uid=1000008(<your-domain>\user_100) gid=1000000(<your-domain>\domain users)
groups=1000000(<your-domain>\domain users),1000024(<your-domain>\cit),1545(Users)
```

5. (Optional) To verify this information from an external UNIX node, run the `ssh` command from an external UNIX node.

For example, the following command would create `/ifs/home/ADS/<your-domain>/user_100` if it did not previously exist:

```
ssh <your-domain>\user_100@cluster.isilon.com
```

## Provision home directories with dot files

You can provision home directories with dot files.

**Before you begin**

To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

The skeleton directory, which is located at `/usr/share/skel` by default, contains a set of files that are copied to the user’s home directory when a local user is created or when a user home directory is dynamically created during login. Files in the skeleton directory that begin with `.` are renamed to remove the `.` prefix when they are copied to the user’s home directory. For example, `dot.cshrc` is copied to the user’s home directory as `.cshrc`. This format enables dot files in the skeleton directory to be viewable through the command-line interface without requiring the `ls -a` command.

For SMB shares that might use home directories that were provisioned with dot files, you can set an option to prevent users who connect to the share through SMB from viewing the dot files.

**Procedure**

1. Run the following command to display the default skeleton directory in the System access zone:

   ```
   isi zone zones view System
   ```

   The system displays output similar to the following example:

   ```
   Name: System
   ...\Skeleton Directory: /usr/share/skel
   ```

2. Run the `isi zone zones modify` command to modify the default skeleton directory.

   The following command modifies the default skeleton directory, `/usr/share/skel`, in an access zone, where `System` is the value for the `<zone>` option and `/usr/share/skel2` is the value for the `<path>` option:

   ```
   isi zone zones modify System --skeleton-directory=/usr/share/skel2
   ```
Home directory creation in a mixed environment

If a user logs in through both SMB and SSH, it is recommended that you configure home directory settings so the path template is the same for the SMB share and each authentication provider against which the user is authenticating through SSH.

Interactions between ACLs and mode bits

Home directory setup is determined by several factors, including how users authenticate and the options that specify home directory creation.

A user's home directory may be set up with either ACLs or POSIX mode bits, which are converted into a synthetic ACL. The directory of a local user is created when the local user is created, and the directory is set up with POSIX mode bits by default. Directories can be dynamically provisioned at log in for users who authenticate against external sources, and in some cases for users who authenticate against the File provider. In this situation, the user home directory is created according to how the user first logs in.

For example, if an LDAP user first logs in through SSH or FTP and the user home directory is created, it is created with POSIX mode bits. If that same user first connects through an SMB home directory share, the home directory is created as specified by the SMB option settings. If the `--inherited-path-acl` option is enabled, ACLs are generated. Otherwise, POSIX mode bits are used.

Default home directory settings in authentication providers

The default settings that affect how home directories are set up differ, based on the authentication provider that the user authenticates against.

<table>
<thead>
<tr>
<th>Authentication provider</th>
<th>Home directory template</th>
<th>Home directory creation</th>
<th>UNIX login shell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td><code>--home-directory-template=/ifs/home/%U</code>&lt;br&gt;<code>--create-home-directory=yes</code>&lt;br&gt;<code>--login-shell=/bin/sh</code></td>
<td>Enabled</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>File</td>
<td><code>--home-directory-template=&quot;&quot;</code>&lt;br&gt;<code>--create-home-directory=no</code></td>
<td>Disabled</td>
<td>None</td>
</tr>
</tbody>
</table>
## Supported expansion variables

You can include expansion variables in an SMB share path or in an authentication provider's home directory template.

OneFS supports the following expansion variables. You can improve performance and reduce the number of shares to be managed when you configure shares with expansion variables. For example, you can include the %U variable for a share rather than create a share for each user. When a %U is included in the name so that each user's path is different, security is still ensured because each user can view and access only his or her home directory.

### Note

When you create an SMB share through the web administration interface, you must select the **Allow Variable Expansion** check box or the string is interpreted literally by the system.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%U</td>
<td>User name (for example, user_001)</td>
<td>Expands to the user name to allow different users to use different home directories. This variable is typically included at the end of the path. For example, for a user named user1, the path /ifs/home/%U is mapped to /ifs/home/user1.</td>
</tr>
</tbody>
</table>
| %D       | NetBIOS domain name (for example, YORK for YORK.EAST.EXAMPLE.COM) | Expands to the user's domain name, based on the authentication provider:  
- For Active Directory users, %D expands to the Active Directory NetBIOS name.  
- For local users, %D expands to the cluster name in uppercase characters. For example, for a cluster named cluster1, %D expands to CLUSTER1.  
- For users in the System file provider, %D expands to UNIX_USERS.  
- For users in other file providers, %D expands to FILE_USERS.  
- For LDAP users, %D expands to LDAP_USERS.  
- For NIS users, %D expands to NIS_USERS. |
<p>| %Z       | Zone name (for example, ZoneABC) | Expands to the access zone name. If multiple zones are activated, this variable is useful for differentiating users in separate zones. For example, for a user named user1 in the System zone, the path /ifs/home/%Z/%U is mapped to /ifs/home/ System/user1. |
| %L       | Host name (cluster host name in lowercase) | Expands to the host name of the cluster, normalized to lowercase. Limited use. |</p>
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%0</td>
<td>First character of the user name</td>
<td>Expands to the first character of the user name.</td>
</tr>
<tr>
<td>%1</td>
<td>Second character of the user name</td>
<td>Expands to the second character of the user name.</td>
</tr>
<tr>
<td>%2</td>
<td>Third character of the user name</td>
<td>Expands to the third character of the user name.</td>
</tr>
</tbody>
</table>

**Note**

If the user name includes fewer than three characters, the %0, %1, and %2 variables wrap around. For example, for a user named ab, the variables maps to a, b, and a, respectively. For a user named a, all three variables map to a.

## Domain variables in home directory provisioning

You can use domain variables to specify authentication providers when provisioning home directories.

The domain variable (%D) is typically used for Active Directory users, but it has a value set that can be used for other authentication providers. %D expands as described in the following table for the various authentication providers.

<table>
<thead>
<tr>
<th>Authenticated user</th>
<th>%D expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory user</td>
<td>Active Directory NetBIOS name—for example, YORK for provider YORK.EAST.EXAMPLE.COM.</td>
</tr>
<tr>
<td>Local user</td>
<td>The cluster name in all-uppercase characters—for example, if the cluster is named MyCluster, %D expands to MYCLUSTER.</td>
</tr>
</tbody>
</table>
| File user          | • UNIX_USERS (for System file provider)  
                      • FILE_USERS (for all other file providers) |
| LDAP user          | LDAP_USERS (for all LDAP authentication providers)                           |
| NIS user           | NIS_USERS (for all NIS authentication providers)                             |
CHAPTER 10

Data access control

This section contains the following topics:

- Data access control overview ................................................................. 420
- ACLs ........................................................................................................ 420
- UNIX permissions ..................................................................................... 421
- Mixed-permission environments .............................................................. 421
- Managing access permissions ................................................................. 422
Data access control overview

OneFS supports two types of permissions data on files and directories that control who has access: Windows-style access control lists (ACLs) and POSIX mode bits (UNIX permissions). You can configure global policy settings that enable you to customize default ACL and UNIX permissions to best support your environment.

The OneFS file system installs with UNIX permissions as the default. You can give a file or directory an ACL by using Windows Explorer or OneFS administrative tools. Typically, files created over SMB or in a directory that has an ACL, receive an ACL. If a file receives an ACL, OneFS stops enforcing the file's mode bits; the mode bits are provided for only protocol compatibility, not for access control.

OneFS supports multiprotocol data access over Network File System (NFS) and Server Message Block (SMB) with a unified security model. A user is granted or denied the same access to a file when using SMB for Windows file sharing as when using NFS for UNIX file sharing.

NFS enables Linux and UNIX clients to remotely mount any subdirectory, including subdirectories created by Windows or SMB users. Linux and UNIX clients also can mount ACL-protected subdirectories created by a OneFS administrator. SMB provides Windows users access to files, directories and other file system resources stored by UNIX and Linux systems. In addition to Windows users, ACLs can affect local, NIS, and LDAP users.

By default, OneFS maintains the same file permissions regardless of the client’s operating system, the user’s identity management system, or the file sharing protocol. When OneFS must transform a file’s permissions from ACLs to mode bits or vice versa, it merges the permissions into an optimal representation that uniquely balances user expectations and file security.

ACLs

In Windows environments, file and directory permissions, referred to as access rights, are defined in access control lists (ACLs). Although ACLs are more complex than mode bits, ACLs can express much more granular sets of access rules. OneFS checks the ACL processing rules commonly associated with Windows ACLs.

A Windows ACL contains zero or more access control entries (ACEs), each of which represents the security identifier (SID) of a user or a group as a trustee. In OneFS, an ACL can contain ACEs with a UID, GID, or SID as the trustee. Each ACE contains a set of rights that allow or deny access to a file or folder. An ACE can optionally contain an inheritance flag to specify whether the ACE should be inherited by child folders and files.

Note

Instead of the standard three permissions available for mode bits, ACLs have 32 bits of fine-grained access rights. Of these, the upper 16 bits are general and apply to all object types. The lower 16 bits vary between files and directories but are defined in a way that allows most applications to apply the same bits for files and directories.

Rights grant or deny access for a given trustee. You can block user access explicitly through a deny ACE or implicitly by ensuring that a user does not directly, or indirectly through a group, appear in an ACE that grants the right.
UNIX permissions

In a UNIX environment, file and directory access is controlled by POSIX mode bits, which grant read, write, or execute permissions to the owning user, the owning group, and everyone else.

OneFS supports the standard UNIX tools for viewing and changing permissions, `ls`, `chmod`, and `chown`. For more information, run the `man ls`, `man chmod`, and `man chown` commands.

All files contain 16 permission bits, which provide information about the file or directory type and the permissions. The lower 9 bits are grouped as three 3-bit sets, called triples, which contain the read, write, and execute (rwx) permissions for each class of users—owner, group, and other. You can set permissions flags to grant permissions to each of these classes.

Unless the user is root, OneFS checks the class to determine whether to grant or deny access to the file. The classes are not cumulative: The first class matched is applied. It is therefore common to grant permissions in decreasing order.

Mixed-permission environments

When a file operation requests an object’s authorization data, for example, with the `ls -l` command over NFS or with the Security tab of the Properties dialog box in Windows Explorer over SMB, OneFS attempts to provide that data in the requested format. In an environment that mixes UNIX and Windows systems, some translation may be required when performing create file, set security, get security, or access operations.

NFS access of Windows-created files

If a file contains an owning user or group that is a SID, the system attempts to map it to a corresponding UID or GID before returning it to the caller.

In UNIX, authorization data is retrieved by calling `stat(2)` on a file and examining the owner, group, and mode bits. Over NFSv3, the GETATTR command functions similarly. The system approximates the mode bits and sets them on the file whenever its ACL changes. Mode bit approximations need to be retrieved only to service these calls.

Note

SID-to-UID and SID-to-GID mappings are cached in both the OneFS ID mapper and the `stat` cache. If a mapping has recently changed, the file might report inaccurate information until the file is updated or the cache is flushed.

SMB access of UNIX-created files

No UID-to-SID or GID-to-SID mappings are performed when creating an ACL for a file; all UIDs and GIDs are converted to SIDs or principals when the ACL is returned.

OneFS initiates a two-step process for returning a security descriptor, which contains SIDs for the owner and primary group of an object:
1. The current security descriptor is retrieved from the file. If the file does not have a discretionary access control list (DACL), a synthetic ACL is constructed from the file’s lower 9 mode bits, which are separated into three sets of permission triples—one each for owner, group, and everyone. For details about mode bits, see the UNIX permissions topic.

2. Two access control entries (ACEs) are created for each triple: the allow ACE contains the corresponding rights that are granted according to the permissions; the deny ACE contains the corresponding rights that are denied. In both cases, the trustee of the ACE corresponds to the file owner, group, or everyone. After all of the ACEs are generated, any that are not needed are removed before the synthetic ACL is returned.

Managing access permissions

The internal representation of identities and permissions can contain information from UNIX sources, Windows sources, or both. Because access protocols can process the information from only one of these sources, the system may need to make approximations to present the information in a format the protocol can process.

View expected user permissions

You can view the expected permissions for user access to a file or directory.

This procedure must be performed through the command-line interface (CLI).

Procedure

1. Establish an SSH connection to any node in the cluster.
2. View expected user permissions by running the `isi auth access` command.
   
   The following command displays permissions in `/ifs/` for the user that you specify in place of `<username>`:

   ```
   isi auth access <username> /ifs/
   ```

   The system displays output similar to the following example:

   ```
   User
   Name : <username>
   UID : 2018
   SID : SID:S-1-5-21-2141457107-1514332578-1691322784-1018
   File
   Owner : user:root
   Group : group:wheel
   Mode : drwxrwxrwx
   Relevant Mode : d---rwx---
   Permissions
   Expected : user:<username> \n allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
   ```

3. View mode-bits permissions for a user by running the `isi auth access` command.
The following command displays verbose-mode file permissions information in /ifs/ for the user that you specify in place of <username>:

```bash
isi auth access <username> /ifs/ -v
```

The system displays output similar to the following example:

```
User Name : <username> UID \
; 2018 SID : SID:S-1-5-21-2141457107-1514332578-1691322784-1018
File Owner : user:root Group : group:wheel Mode : drwxrwxrwx
Relevant Mode : d---rwx--- Permissions Expected :
user:<username>
allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
```

4. View expected ACL user permissions on a file for a user by running the `isi auth access` command.

The following command displays verbose-mode ACL file permissions for the file `file_with_acl.tx` in /ifs/data/ for the user that you specify in place of <username>:

```bash
isi auth access <username> /ifs/data/file_with_acl.tx -v
```

The system displays output similar to the following example:

```
User Name : <username> \
UID : 2097 SID : \
SID:S-1-7-21-2141457107-1614332578-1691322789-1018
File Owner : user:<username> Group : group:wheel
Permissions Expected : user:<username> allow file_gen_read,file_gen_write,std_write_dac
Relevant Acl: group:<group-name> Users allow file_gen_read user:<username> allow std_write_dac,file_write,append,file_write_ext_attr,file_write_attr
  group:wheel allow file_gen_read,file_gen_write
```

**Configure access management settings**

Default access settings include whether to send NTLMv2 responses for SMB connections, the identity type to store on disk, the Windows workgroup name for running in local mode, and character substitution for spaces encountered in user and group names.

**Procedure**

1. Configure access management settings by running the `isi auth settings global modify` command.

   The following command modifies global settings for a workgroup:

   ```bash
   isi auth settings global modify \  
   --send-ntlmv2=false --on-disk-identity=native \  
   --space-replacement=\"\_\" --workgroup=WORKGROUP
   ```
Modify ACL policy settings

You can modify ACL policy settings but the default ACL policy settings are sufficient for most cluster deployments.

⚠ CAUTION

Because ACL policies change the behavior of permissions throughout the system, they should be modified only as necessary by experienced administrators with advanced knowledge of Windows ACLs. This is especially true for the advanced settings, which are applied regardless of the cluster's environment.

For UNIX, Windows, or balanced environments, the optimal permission policy settings are selected and cannot be modified. You can choose to manually configure the cluster's default permission settings if necessary to support your particular environment, however.

Procedure

1. Run the following command to modify ACL policy settings:

   ```bash
   isi auth settings acls modify
   ```

Run the PermissionsRepair job

You can update file and directory permissions or ownership by running the Repair Permissions job. To prevent permissions issues that can occur after changing the on-disk identity, run this job with the Convert Permissions job to ensure that the changes are fully propagated throughout the cluster.

To prevent permissions issues that can occur after changing the on-disk identity, run this authentication and access control job with `convert` mode specified to ensure that the changes are fully propagated throughout the cluster.

Procedure

1. Update cluster permissions by running the `isi job jobs start` command with the following syntax.

   The following command updates cluster permissions, where `permissionrepair` specifies the job type, where variables in angle brackets are placeholders for values specific to your environment:

   ```bash
   isi job start permissionrepair --priority <1-10> \
   --policy <policy> --mode <clone | inherit | convert > \n   --mapping-type=<system | sid | unix | native> --zone <zone-name>
   ```

Note

You cannot combine the `--template` parameter with the `convert` mode option, but you can combine the parameter with the `clone` and `inherit` mode options. Conversely, you cannot combine the `--mapping-type` and `--zone` parameters with the `clone` and `inherit` mode options, but you can combine the parameters with the `convert` mode option.
Example 1 Examples

The following example updates cluster permissions, where `permissionrepair` specifies the job type, the priority is 3, the chosen mode is `convert`, and the mapping type is `unix`:

```
isi job jobs start permissionrepair --priority=3 \
   --policy myPolicy --mode=convert --mapping-type=unix \
   --template <isi path> --path </ifs directory> --zone zone2
```
CHAPTER 11

File sharing

This section contains the following topics:

- File sharing overview ................................................................. 428
- SMB ............................................................................................ 430
- NFS ............................................................................................ 478
- FTP ............................................................................................. 534
- HTTP and HTTPS ................................................................. 542
**File sharing overview**

Multi-protocol support in OneFS enables files and directories on the Isilon cluster to be accessed through SMB for Windows file sharing, NFS for UNIX file sharing, secure shell (SSH), FTP, and HTTP. By default, only the SMB and NFS protocols are enabled.

OneFS creates the `/ifs` directory, which is the root directory for all file system data on the cluster. The `/ifs` directory is configured as an SMB share and an NFS export by default. You can create additional shares and exports within the `/ifs` directory tree.

---

**Note**

We recommend that you do not save data to the root `/ifs` file path but in directories below `/ifs`. The design of your data storage structure should be planned carefully. A well-designed directory structure optimizes cluster performance and administration.

You can set Windows- and UNIX-based permissions on OneFS files and directories. Users who have the required permissions and administrative privileges can create, modify, and read data on the cluster through one or more of the supported file sharing protocols.

- **SMB.** Allows Microsoft Windows and Mac OS X clients to access files that are stored on the cluster.
- **NFS.** Allows Linux and UNIX clients that adhere to the RFC1813 (NFSv3) and RFC3530 (NFSv4) specifications to access files that are stored on the cluster.
- **HTTP and HTTPS (with optional DAV).** Allows clients to access files that are stored on the cluster through a web browser.
- **FTP.** Allows any client that is equipped with an FTP client program to access files that are stored on the cluster through the FTP protocol.

**Mixed protocol environments**

The `/ifs` directory is the root directory for all file system data in the cluster, serving as an SMB share, an NFS export, and a document root directory. You can create additional shares and exports within the `/ifs` directory tree. You can configure your OneFS cluster to use SMB or NFS exclusively, or both. You can also enable HTTP, FTP, and SSH.

Access rights are consistently enforced across access protocols on all security models. A user is granted or denied the same rights to a file whether using SMB or NFS. Clusters running OneFS support a set of global policy settings that enable you to customize the default access control list (ACL) and UNIX permissions settings.

OneFS is configured with standard UNIX permissions on the file tree. Through Windows Explorer or OneFS administrative tools, you can give any file or directory an ACL. In addition to Windows domain users and groups, ACLs in OneFS can include local, NIS, and LDAP users and groups. After a file is given an ACL, the mode bits are no longer enforced and exist only as an estimate of the effective permissions.

---

**Note**

We recommend that you configure ACL and UNIX permissions only if you fully understand how they interact with one another.
Write caching with SmartCache

Write caching accelerates the process of writing data to the cluster. OneFS includes a write-caching feature called SmartChache, which is enabled by default for all files and directories.

If write caching is enabled, OneFS writes data to a write-back cache instead of immediately writing the data to disk. OneFS can write the data to disk at a time that is more convenient.

Note

We recommend that you keep write caching enabled. You should also enable write caching for all file pool policies.

OneFS interprets writes to the cluster as either synchronous or asynchronous, depending on a client's specifications. The impacts and risks of write caching depend on what protocols clients use to write to the cluster, and whether the writes are interpreted as synchronous or asynchronous. If you disable write caching, client specifications are ignored and all writes are performed synchronously.

The following table explains how clients' specifications are interpreted, according to the protocol.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Synchronous</th>
<th>Asynchronous</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>The stable field is set to data_sync or file_sync.</td>
<td>The stable field is set to unstable.</td>
</tr>
<tr>
<td>SMB</td>
<td>The write-through flag has been applied.</td>
<td>The write-through flag has not been applied.</td>
</tr>
</tbody>
</table>

Write caching for asynchronous writes

Writing to the cluster asynchronously with write caching is the fastest method of writing data to your cluster.

Write caching for asynchronous writes requires fewer cluster resources than write caching for synchronous writes, and will improve overall cluster performance for most workflows. However, there is some risk of data loss with asynchronous writes.

The following table describes the risk of data loss for each protocol when write caching for asynchronous writes is enabled:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>If a node fails, no data will be lost except in the unlikely event that a client of that node also crashes before it can reconnect to the cluster. In that situation, asynchronous writes that have not been committed to disk will be lost.</td>
</tr>
<tr>
<td>SMB</td>
<td>If a node fails, asynchronous writes that have not been committed to disk will be lost.</td>
</tr>
</tbody>
</table>

We recommend that you do not disable write caching, regardless of the protocol that you are writing with. If you are writing to the cluster with asynchronous writes, and you decide that the risks of data loss are too great, we recommend that you configure your clients to use synchronous writes, rather than disable write caching.
Write caching for synchronous writes

Write caching for synchronous writes costs cluster resources, including a negligible amount of storage space. Although it is not as fast as write caching with asynchronous writes, unless cluster resources are extremely limited, write caching with synchronous writes is faster than writing to the cluster without write caching.

Write caching does not affect the integrity of synchronous writes; if a cluster or a node fails, none of the data in the write-back cache for synchronous writes is lost.

SMB

OneFS includes a configurable SMB service to create and manage SMB shares. SMB shares provide Windows clients network access to file system resources on the cluster. You can grant permissions to users and groups to carry out operations such as reading, writing, and setting access permissions on SMB shares.

The /ifs directory is configured as an SMB share and is enabled by default. OneFS supports both user and anonymous security modes. If the user security mode is enabled, users who connect to a share from an SMB client must provide a valid user name with proper credentials.

SMB shares act as checkpoints, and users must have access to a share in order to access objects in a file system on a share. If a user has access granted to a file system, but not to the share on which it resides, that user will not be able to access the file system regardless of privileges. For example, assume a share named ABCDocs contains a file named file1.txt in a path such as: /ifs/data/ABCDocs/file1.txt. If a user attempting to access file1.txt does not have share privileges on ABCDocs, that user cannot access the file even if originally granted read and/or write privileges to the file.

The SMB protocol uses security identifiers (SIDs) for authorization data. All identities are converted to SIDs during retrieval and are converted back to their on-disk representation before they are stored on the cluster.

When a file or directory is created, OneFS checks the access control list (ACL) of its parent directory. If the ACL contains any inheritable access control entries (ACEs), a new ACL is generated from those ACEs. Otherwise, OneFS creates an ACL from the combined file and directory create mask and create mode settings.

OneFS supports the following SMB clients:

<table>
<thead>
<tr>
<th>SMB version</th>
<th>Supported operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0 - Multichannel only</td>
<td>Windows 8 or later&lt;br&gt;Windows Server 2012 or later</td>
</tr>
<tr>
<td>2.1</td>
<td>Windows 7 or later&lt;br&gt;Windows Server 2008 R2 or later</td>
</tr>
<tr>
<td>2.0</td>
<td>Windows Vista or later&lt;br&gt;Windows Server 2008 or later&lt;br&gt;Mac OS X 10.9 or later</td>
</tr>
<tr>
<td>1.0</td>
<td>Windows 2000 or later&lt;br&gt;Windows XP or later&lt;br&gt;Mac OS X 10.5 or later</td>
</tr>
</tbody>
</table>
SMB shares in access zones

You can create and manage SMB shares within access zones. You can create access zones that partition storage on the EMC Isilon cluster into multiple virtual containers. Access zones support all configuration settings for authentication and identity management services on the cluster, so you can configure authentication providers and provision SMB shares on a zone-by-zone basis. When you create an access zone, a local provider is created automatically, which allows you to configure each access zone with a list of local users and groups. You can also authenticate through a different Active Directory provider in each access zone, and you can control data access by directing incoming connections to the access zone from a specific IP address in a pool. Associating an access zone with an IP address pool restricts authentication to the associated access zone and reduces the number of available and accessible SMB shares.

Here are a few ways to simplify SMB management with access zones:

- Migrate multiple SMB servers, such as Windows file servers or NetApp filers, to a single Isilon cluster, and then configure a separate access zone for each SMB server.
- Configure each access zone with a unique set of SMB share names that do not conflict with share names in other access zones, and then join each access zone to a different Active Directory domain.
- Reduce the number of available and accessible shares to manage by associating an IP address pool with an access zone to restrict authentication to the zone.
- Configure default SMB share settings that apply to all shares in an access zone.

The Isilon cluster includes a built-in access zone named System, where you manage all aspects of the cluster and other access zones. If you don't specify an access zone when managing SMB shares, OneFS will default to the System zone.

SMB Multichannel

SMB Multichannel supports establishing a single SMB session over multiple network connections.

SMB Multichannel is a feature of the SMB 3.0 protocol that provides the following capabilities:

**Increased throughput**
- OneFS can transmit more data to a client through multiple connections over high speed network adapters or over multiple network adapters.

**Connection failure tolerance**
- When an SMB Multichannel session is established over multiple network connections, the session is not lost if one of the connections has a network fault, which enables the client to continue to work.

**Automatic discovery**
- SMB Multichannel automatically discovers supported hardware configurations on the client that have multiple available network paths and then negotiates and establishes a session over multiple network connections. You are not required to install components, roles, role services, or features.
SMB Multichannel requirements

You must meet software and NIC configuration requirements to support SMB Multichannel on the EMC Isilon cluster.

OneFS can only support SMB Multichannel when the following software requirements are met:

- Windows Server 2012, 2012 R2 or Windows 8, 8.1 clients
- SMB Multichannel must be enabled on both the EMC Isilon cluster and the Windows client computer. It is enabled on the Isilon cluster by default.

SMB Multichannel establishes a single SMB session over multiple network connections only on supported network interface card (NIC) configurations. SMB Multichannel requires at least one of the following NIC configurations on the client computer:

- Two or more network interface cards.
- One or more network interface cards that support Receive Side Scaling (RSS).
- One or more network interface cards configured with link aggregation. Link aggregation enables you to combine the bandwidth of multiple NICs on a node into a single logical interface.

Client-side NIC configurations supported by SMB Multichannel

SMB Multichannel automatically discovers supported hardware configurations on the client that have multiple available network paths.

Each node on the EMC Isilon cluster has at least one RSS-capable network interface card (NIC). Your client-side NIC configuration determines how SMB Multichannel establishes simultaneous network connections per SMB session.

<table>
<thead>
<tr>
<th>Client-side NIC Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single RSS-capable NIC</td>
<td>SMB Multichannel establishes a maximum of four network connections to the Isilon cluster over the NIC. The connections are more likely to be spread across multiple CPU cores, which reduces the likelihood of performance bottleneck issues and achieves the maximum speed capability of the NIC.</td>
</tr>
<tr>
<td>Multiple NICs</td>
<td>If the NICs are RSS-capable, SMB Multichannel establishes a maximum of four network connections to the Isilon cluster over each NIC. If the NICs on the client are not RSS-capable, SMB Multichannel establishes a single network connection to the Isilon cluster over each NIC. Both configurations allow SMB Multichannel to leverage the combined bandwidth of multiple NICs and provides connection fault tolerance if a connection or a NIC fails.</td>
</tr>
</tbody>
</table>

Note

SMB Multichannel cannot establish more than eight simultaneous network connections per session. In a multiple NIC configuration, this might limit the number connections allowed per NIC. For example, if the configuration contains three RSS-capable NICs, SMB Multichannel might establish three connections over the first NIC, three connections over the second NIC and two connections over the third NIC.
### Client-side NIC Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated NICs</td>
<td>SMB Multichannel establishes multiple network connections to the Isilon cluster over aggregated NICs, which results in balanced connections across CPU cores, effective consumption of combined bandwidth, and connection fault tolerance.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The aggregated NIC configuration inherently provides NIC fault tolerance that is not dependent upon SMB.</td>
</tr>
</tbody>
</table>

### SMB share management through MMC

OneFS supports the Shared Folders snap-in for the Microsoft Management Console (MMC), which allows SMB shares on the EMC Isilon cluster to be managed using the MMC tool.

Typically, you connect to the global System zone through the web administration interface or the command line interface to manage and configure shares. If you configure access zones, you can connect to a zone through the MMC Shared Folders snap-in to directly manage all shares in that zone.

You can establish a connection through the MMC Shared Folders snap-in to an Isilon node and perform the following SMB share management tasks:

- Create and delete shared folders
- Configure access permission to an SMB share
- View a list of active SMB sessions
- Close open SMB sessions
- View a list of open files
- Close open files

When you connect to a zone through the MMC Shared Folders snap-in, you can view and manage all SMB shares assigned to that zone; however, you can only view active SMB sessions and open files on the specific node that you are connected to in that zone. Changes you make to shares through the MMC Shared Folders snap-in are propagated across the cluster.

### MMC connection requirements

You can connect to an EMC Isilon cluster through the MMC Shared Folders snap-in if you meet access requirements.

The following conditions are required to establish a connection through the MMC Shared Folders snap-in:

- You must run the Microsoft Management Console (MMC) from a Windows workstation that is joined to the domain of an Active Directory (AD) provider configured on the cluster.
- You must be a member of the local `<cluster>\Administrators` group.

**Note**

Role-based access control (RBAC) privileges do not apply to the MMC. A role with SMB privileges is not sufficient to gain access.
You must log in to a Windows workstation as an Active Directory user that is a member of the local `<cluster>\Administrators group.

**SMB server-side copy**

In order to increase system performance, SMB 2 and later clients can utilize the server-side copy feature in OneFS.

Windows clients making use of server-side copy support may experience performance improvements for file copy operations, because file data no longer needs to traverse the network. The server-side copy feature reads and writes files only on the server, avoiding the network round-trip and duplication of file data. This feature only affects file copy or partial copy operations in which the source and destination file handles are open on the same share, and does not work for cross-share operations.

This feature is enabled by default across OneFS clusters, and can only be disabled system-wide across all zones. Additionally, server-side copy in OneFS is incompatible with the SMB continuous availability feature. If continuous availability is enabled for a share and the client opens a persistent file handle, server-side copy is automatically disabled for that file.

---

**Note**

You can only disable or enable SMB server-side copy for OneFS using the command line interface (CLI).

---

**Enable or disable SMB server-side copy**

You can enable or disable the SMB server-side copy feature.

The SMB server-side copy feature is enabled in OneFS by default.

**Procedure**

1. Open a secure shell (SSH) connection to the EMC Isilon cluster.
2. Run the `isi smb settings global modify` command.
3. Modify the `--server-side-copy` option as necessary.
   
   This feature is enabled by default.

   For example, the following command disables SMB server-side copy:

   ```
   isi smb settings global modify --server-side-copy=no
   ```

---

**SMB continuous availability**

If you are running OneFS in an SMB 3.0 environment, you allow certain Windows clients to open files on a server with continuous availability enabled.

If a server is using Windows 8 or Windows Server 2012, clients can create persistent file handles that can be reclaimed after an outage such as a network-related disconnection or a server failure. You can specify how long the persistent handle is retained after a disconnection or server failure, and also force strict lockouts on users attempting to open a file belonging to another handle. Furthermore, through the OneFS command-line interface (CLI), you can configure write integrity settings to control the stability of writes to the share.
If continuous availability is enabled for a share and the client opens a persistent file handle, server-side copy is automatically disabled for that file.

---

**Note**

You can only enable continuous availability when creating a share, but you can update timeout, lockout, and write integrity settings when creating or modifying a share.

---

### Enable SMB continuous availability

You can enable SMB 3.0 continuous availability and configure settings when you create a share.

You can also update continuous availability timeout, lockout, and write integrity settings when you modify a share.

**Procedure**

- Run `isi smb shares create` to enable this feature and configure settings, and `isi smb shares modify` or `isi smb settings shares modify` to change settings.

The following command enables continuous availability on a new share named Share4, sets the timeout for the handle to three minutes (180 seconds), enforces a strict lockout, and changes the write integrity setting to `full`:

```bash
isi smb shares create --name=Share4 --path=/ifs/data/Share4 --continuously-available=yes --ca-timeout=180 --strict-ca-lockout=yes --ca-write-integrity=full
```

### SMB file filtering

You can use SMB file filtering to allow or deny file writes to a share or access zone. This feature enables you to deny certain types of files that might cause throughput issues, security problems, storage clutter, or productivity disruptions. You can restrict writes by allowing writes of certain file types to a share.

- If you choose to deny file writes, you can specify file types by extension that are not allowed to be written. OneFS permits all other file types to be written to the share.

- If you choose to allow file writes, you can specify file types by extension that are allowed to be written. OneFS denies all other file types to be written to the share.

You can add or remove file extensions if your restriction policies change.

**Enable SMB file filtering**

You can enable or disable SMB file filtering when you create or modify a share.

**Procedure**

- Run `isi smb shares create` or `isi smb shares modify`.

The following command enables file filtering on a share named Share2 and denies writes by the file types `.wav` and `.mpg`:

```bash
isi smb shares modify Share2 --file-filtering-enabled=yes --file-filter-extensions=.wav,.mpg
```
The following command enables file filtering on a share named Share3, specifies the file type .xml, and specifies to allow writes for that file type:

```
isi smb shares modify Share3 --file-filtering-enabled=yes \file-filter-extensions=.xml --file-filter-type=allow```

### Symbolic links and SMB clients

OneFS enables SMB2 clients to access symbolic links in a seamless manner. Many administrators deploy symbolic links to virtually reorder file system hierarchies, especially when crucial files or directories are scattered around an environment.

In an SMB share, a symbolic link (also known as a symlink or a soft link) is a type of file that contains a path to a target file or directory. Symbolic links are transparent to applications running on SMB clients, and they function as typical files and directories. Support for relative and absolute links is enabled by the SMB client. The specific configuration depends on the client type and version.

A symbolic link that points to a network file or directory that is not in the path of the active SMB session is referred to as an absolute (or remote) link. Absolute links always point to the same location on a file system, regardless of the present working directory, and usually contain the root directory as part of the path. Conversely, a relative link is a symbolic link that points directly to a user's or application's working directory, so you do not have to specify the full absolute path when creating the link.

OneFS exposes symbolic links through the SMB2 protocol, enabling SMB2 clients to resolve the links instead of relying on OneFS to resolve the links on behalf of the clients. To transverse a relative or absolute link, the SMB client must be authenticated to the SMB shares that the link can be followed through. However, if the SMB client does not have permission to access the share, access to the target is denied and Windows will not prompt the user for credentials.

SMB2 and NFS links are interoperable for relative links only. For maximum compatibility, create these links from a POSIX client.

---

**Note**

SMB1 clients (such as Windows XP or 2002) may still use relative links, but they are traversed on the server side and referred to as "shortcut files." Absolute links do not work in these environments.

---

### Enabling symbolic links

Before you can fully use symbolic links in an SMB environment, you must enable them.

For Windows SMB clients to traverse each type of symbolic link, you must enable them on the client. Windows supports the following link types:

- local to local
- remote to remote
- local to remote
- remote to local

You must run the following Windows command to enable all four link types:

```
fsutil behavior set SymlinkEvaluation L2L:1 R2R:1 L2R:1 R2L:1```
For POSIX clients using Samba, you must set the following options in the [global] section of your Samba configuration file (smb.conf) to enable Samba clients to traverse relative and absolute links:

```plaintext
follow_syalinks=yes
wide_links=yes
```

In this case, "wide links" in the smb.conf file refers to absolute links. The default setting in this file is no.

Managing symbolic links

After enabling symbolic links, you can create or delete them from the Windows command prompt or a POSIX command line.

Create symbolic links using the Windows mklink command on an SMB2 client or the ln command from a POSIX command-line interface. For example, an administrator may want to give a user named User1 access to a file named File1.doc in the /ifs/data/ directory without giving specific access to that directory by creating a link named Link1:

```plaintext
mklink /ifs/home/users/User1/Link1 /ifs/data/Share1/File1.doc
```

When you create a symbolic link, it is designated as a file link or directory link. Once the link is set, the designation cannot be changed. You can format symbolic link paths as either relative or absolute.

To delete symbolic links, use the del command in Windows, or the rm command in a POSIX environment.

Keep in mind that when you delete a symbolic link, the target file or directory still exists. However, when you delete a target file or directory, a symbolic link continues to exist and still points to the old target, thus becoming a broken link.

Anonymous access to SMB shares

You can configure anonymous access to SMB shares by enabling the local Guest user and allowing impersonation of the guest user.

For example, if you store files such as browser executables or other data that is public on the internet, anonymous access allows any user to access the SMB share without authenticating.

Managing SMB settings

You can enable or disable the SMB service, configure global settings for the SMB service, and configure default SMB share settings that are specific to each access zone.

View global SMB settings

You can view the global SMB settings that are applied to all nodes on the EMC Isilon cluster. This task can only be performed through the OneFS command-line interface.

Procedure

1. Establish an SSH connection to any node in the cluster.
2. Run the `isi smb settings global view` command.

The system displays output similar to the following example:

```
Access Based Share Enum: No
Dot Snap Accessible Child: Yes
Dot Snap Accessible Root: Yes
Dot Snap Visible Child: No
Dot Snap Visible Root: Yes
Enable Security Signatures: No
  Guest User: nobody
  Ignore Eas: No
Onefs Cpu Multiplier: 4
Onefs Num Workers: 0
Require Security Signatures: No
Server Side Copy: Yes
  Server String: Isilon Server
Srv Cpu Multiplier: 4
Srv Num Workers: 0
Support Multichannel: Yes
Support NetBIOS: No
Support Smb2: Yes
```

Configure global SMB settings

You can configure global settings for SMB file sharing. This task can only be performed through the OneFS command-line interface.

⚠️ CAUTION

Modifying global SMB file sharing settings could result in operational failures. Be aware of the potential consequences before modifying these settings.

Procedure

1. Establish an SSH connection to any node in the cluster.
2. Run the `isi smb settings global modify` command.

   The following example command disables SMB server-side copy:

   ```
   isi smb settings global modify --server-side-copy=no
   ```

Enable or disable the SMB service

The SMB service is enabled by default.

Note

You can determine whether the service is enabled or disabled by running the `isi services -l` command.

Procedure

- Run the `isi services command`.

  The following command disables the SMB service:

  ```
  isi services smb disable
  ```
The following command enables the SMB service:

```
isi services smb enable
```

Enable or disable SMB Multichannel

SMB Multichannel is required for multiple, concurrent SMB sessions from a Windows client computer to a node in an EMC Isilon cluster. SMB Multichannel is enabled in the Isilon cluster by default.

You can enable or disable SMB Multichannel only through the command-line interface.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi smb settings global modify` command.

The following command enables SMB Multichannel on the EMC Isilon cluster:

```
isi smb settings global modify --support-multichannel=yes
```

The following command disables SMB Multichannel on the EMC Isilon cluster:

```
isi smb settings global modify --support-multichannel=no
```

View default SMB share settings

You can view the default SMB share settings specific to an access zone.

**Procedure**

- Run the `isi smb settings shares view` command.

The following example command displays the default SMB share settings configured for zone5:

```
isi smb settings shares view --zone=zone5
```

The system displays output similar to the following example:

```
Access Based Enumeration: No
Access Based Enumeration Root Only: No
Allow Delete Readonly: No
Allow Execute Always: No
Ca Timeout: 120
Strict Ca Lockout: No
Change Notify: norecurse
Create Permissions: default acl
Directory Create Mask: 0700
Directory Create Mode: 0000
File Create Mask: 0700
File Create Mode: 0100
File Filtering Enabled: Yes
File Filter Extensions: .wav
File Filter Type: deny
Hide Dot Files: No
Host ACL: -
Impersonate Guest: never
Impersonate User: -
```
Configure default SMB share settings

You can configure SMB share settings specific to each access zone.

The default settings are applied to all new shares that are added to the access zone.

⚠️ **CAUTION**

If you modify the default settings, the changes are applied to all existing shares in the access zone.

**Procedure**

1. Run the `isi smb settings shares modify` command.

   The following command specifies that guests are never allowed access to shares in zone5:

   ```
   isi smb settings global modify --zone=zone5 --impersonate-guest=never
   ```

Managing SMB shares

You can configure the rules and other settings that govern the interaction between your Windows network and individual SMB shares on the cluster.

OneFS supports %U, %D, %Z, %L, %0, %1, %2, and %3 variable expansion and automatic provisioning of user home directories.

You can configure the users and groups that are associated with an SMB share, and view or modify their share-level permissions.

**Note**

We recommend that you configure advanced SMB share settings only if you have a solid understanding of the SMB protocol.

Create an SMB share

When you create an SMB share, you can override the default permissions, performance, and access settings. You can configure SMB home directory provisioning by including expansion variables in the share path to automatically create and redirect users to their own home directories.

**Before you begin**

You must specify a path to use as the SMB share. Shares are specific to access zones and the share path must exist under the zone path. You can specify an existing path or create the path at the time you create the share. Create access zones before you create SMB shares.

You can specify one or more expansion variables in the directory path but you must set the flags to true for both the `--allow-variable-expansion` and `--auto-`
create-directory parameters. If you do not specify these settings, the variable expansion string is interpreted literally by the system.

**Procedure**

1. Run the `isi smb shares create` command.

   The following commands creates a directory at `/ifs/zone5/data/share1`, creates a share named `share1` using that path, and adds the share to the existing access zone named `zone5`:

   ```bash
   mkdir /ifs/data/share1 isi smb shares create --name=share1 --path=/ifs/data/share1 --zone=zone5 --browsable=true --description="Example Share 1"
   ```

   **Note**

   Share names can contain up to 80 characters, except for the following: " \/ [ ] : | < > + = ; , * ?

   Also, if the cluster character encoding is not set to UTF-8, SMB share names are case-sensitive.

   The following command creates a directory at `/ifs/data/share2`, converts it to an SMB share, and adds the share to the default System zone because no zone is specified:

   ```bash
   isi smb shares create share2 --path=/ifs/data/share2 --create-path --browsable=true --description="Example Share 2"
   ```

   The following command creates a directory at `/ifs/data/share3` and converts it to an SMB share. The command also applies an ACL to the share:

   ```bash
   isi smb shares create share3 --path=/ifs/data/share3 --create-path --browsable=true --description="Example Share 3" --inheritable-path-acl=true --create-permissions="default acl"
   ```

   **Note**

   If no default ACL is configured and the parent directory does not have an inheritable ACL, an ACL is created for the share with the directory-create-mask and directory-create-mode settings.

   The following command creates the directory `/ifs/data/share4` and converts it to a non-browsable SMB share. The command also configures the use of mode bits for permissions control:

   ```bash
   isi smb shares create --name=share4 --path=/ifs/data/share4 --create-path --browsable=false --description="Example Share 4" --inheritable-path-acl=true --create-permissions="use create mask and mode"
   ```

2. The following command creates home directories for each user that connects to the share, based on the user's NetBIOS domain and user name.
In this example, if a user is in a domain named DOMAIN and has a username of user_1, the path `/ifs/home/%D/%U` expands to `/ifs/home/DOMAIN/user_1`.

```bash
isi smb shares modify HOMEDIR --path=/ifs/home/%D/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes
```

The following command creates a share named HOMEDIR with the existing path `/ifs/share/home`:

```bash
isi smb shares create HOMEDIR /ifs/share/home
```

3. Run the `isi smb shares permission modify` command to enable access to the share.

The following command allows the well-known user Everyone full permissions to the HOMEDIR share:

```bash
isi smb shares permission modify HOMEDIR --wellknown Everyone \ 
   --permission-type allow --permission full
```

Modify an SMB share

You can modify the settings of individual SMB shares.

Before you begin

SMB shares are zone-specific. When you modify a share, you must identify the access zone that the share belongs to. If you do not identify the access zone, OneFS defaults to the System zone. If the share you want to modify has the same name as a share in the System zone, the share in the System zone is modified.

Procedure

1. Run the `isi smb shares modify` command.

   In the following example, the file path for share1 in zone5 points to `/ifs/zone5/data`. The following commands modifies the file path of share1 to `/ifs/zone5/etc`, which is another directory in the zone5 path:

   ```bash
   isi smb shares modify share1 --zone=zone5 \ 
   --path=/ifs/zone5/etc
   ```

Note

If the cluster character encoding is not set to UTF-8, SMB share names are case-sensitive.

Delete an SMB share

You can delete SMB shares that are no longer needed.

Before you begin

SMB shares are zone-specific. When you delete a share, you must identify the access zone that the share belongs to. If you do not identify the access zone, OneFS defaults to the System zone. If the share you want to delete has the same name as a share in the System zone, the share in the System zone is deleted.
If you delete an SMB share, the share path is deleted but the directory it referenced still exists. If you create a new share with the same path as the share that was deleted, the directory that the previous share referenced will be accessible again through the new share.

**Procedure**

1. Run the `isi smb shares delete` command.
   
   The following command deletes a share named Share1 from the access zone named zone-5:
   ```
   isi smb shares delete Share1 --zone=zone-5
   ```

2. Type `yes` at the confirmation prompt.

**Limit access to /ifs share for the Everyone account**

By default, the `/ifs` root directory is configured as an SMB share in the System access zone. It is recommended that you restrict the Everyone account of this share to read-only access.

**Procedure**

1. Run the `isi smb shares permission modify` command.
   
   The following example changes the Everyone account permissions to read-only on the SMB share configured for the `/ifs` directory:
   ```
   isi smb shares permission modify ifs --wellknown=Everyone -d allow -p read
   ```

2. (Optional) Verify the change by running the following command to list permissions on the share:
   ```
   isi smb shares permission list ifs
   ```

**Configure anonymous access to a single SMB share**

You can configure anonymous access to data stored on a single share through Guest user impersonation.

**Procedure**

1. Enable the Guest user account in the access zone that contains the share you want by running the `isi auth users modify` command.
   
   The following command enables the guest user in the access zone named zone3:
   ```
   isi auth users modify Guest --enabled=yes --zone=zone3
   ```

2. Set guest impersonation on the share you want to allow anonymous access to by running the `isi smb share modify` command.
The following command configures guest impersonation on a share named share1 in zone3:

```bash
isi smb share modify share1 --zone=zone3 --impersonate-guest=always
```

3. Verify that the Guest user account has permission to access the share by running the `isi smb share permission list` command.

The following command list the permissions for share1 in zone3:

```bash
isi smb share permission list share1 --zone=zone3
```

The system displays output similar to the following example

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Run as Root</th>
<th>Permission Type</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>wellknown</td>
<td>False</td>
<td>allow</td>
<td>read</td>
</tr>
<tr>
<td>Guest</td>
<td>user</td>
<td>False</td>
<td>allow</td>
<td>full</td>
</tr>
</tbody>
</table>

Configure anonymous access to all SMB shares in an access zone

You can configure anonymous access to data stored in an access zone through Guest user impersonation.

**Procedure**

1. Enable the Guest user account in the access zone that contains the share you want by running the `isi auth users modify` command.

   The following command enables the guest user in the access zone named zone3:

   ```bash
   isi auth users modify Guest --enabled=yes --zone=zone3
   ```

2. Set guest impersonation as the default value for all shares in the access zone by running the `isi smb settings share modify` command.

   The following command configures guest impersonation for all shares in zone3:

   ```bash
   isi smb settings share modify --zone=zone3 --impersonate-guest=always
   ```

3. Verify that the Guest user account has permission to each share in the access zone by running the `isi smb share permission list` command.

   The following command list the permissions for share1 in zone3:

   ```bash
   isi smb share permission list share1 --zone=zone3
   ```

   The system displays output similar to the following example

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Run as Root</th>
<th>Permission Type</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>wellknown</td>
<td>False</td>
<td>allow</td>
<td>read</td>
</tr>
<tr>
<td>Guest</td>
<td>user</td>
<td>False</td>
<td>allow</td>
<td>full</td>
</tr>
</tbody>
</table>
Configure multi-protocol home directory access

For users who will access this share through FTP or SSH, you can make sure that their home directory path is the same whether they connect through SMB or they log in through FTP or SSH. This task may only be performed at the OneFS command-line interface.

This command directs the SMB share to use the home directory template that is specified in the user's authentication provider. This procedure is available only through the command-line interface.

Procedure

1. Establish an SSH connection to any node in the cluster.
2. Run the following command, where `<share>` is the name of the SMB share and `--path` is the directory path of the home directory template specified by the user's authentication provider:

   ```
   isi smb shares modify <share> --path=""
   ```

Supported expansion variables

You can include expansion variables in an SMB share path or in an authentication provider’s home directory template.

OneFS supports the following expansion variables. You can improve performance and reduce the number of shares to be managed when you configure shares with expansion variables. For example, you can include the %U variable for a share rather than create a share for each user. When a %U is included in the name so that each user’s path is different, security is still ensured because each user can view and access only his or her home directory.

Note

When you create an SMB share through the web administration interface, you must select the Allow Variable Expansion check box or the string is interpreted literally by the system.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%U</td>
<td>User name (for example, user_001)</td>
<td>Expands to the user name to allow different users to use different home directories. This variable is typically included at the end of the path. For example, for a user named user1, the path /ifs/home/%U is mapped to /ifs/home/user1.</td>
</tr>
</tbody>
</table>
| %D       | NetBIOS domain name (for example, YORK for YORK.EAST.EXAMPLE.COM) | Expands to the user’s domain name, based on the authentication provider:  
  - For Active Directory users, %D expands to the |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Active Directory NetBIOS name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For local users, %D expands to the cluster name in uppercase characters. For example, for a cluster named cluster1, %D expands to CLUSTER1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For users in the System file provider, %D expands to UNIX_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For users in other file providers, %D expands to FILE_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For LDAP users, %D expands to LDAP_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For NIS users, %D expands to NIS_USERS.</td>
</tr>
<tr>
<td>%Z</td>
<td>ZoneABC</td>
<td>Expands to the access zone name. If multiple zones are activated, this variable is useful for differentiating users in separate zones. For example, for a user named user1 in the System zone, the path /ifs/home/%Z/%U is mapped to /ifs/home/System/user1.</td>
</tr>
<tr>
<td>%L</td>
<td>Host name (cluster host name in lowercase)</td>
<td>Expands to the host name of the cluster, normalized to lowercase. Limited use.</td>
</tr>
<tr>
<td>%0</td>
<td>First character of the user name</td>
<td>Expands to the first character of the user name.</td>
</tr>
<tr>
<td>%1</td>
<td>Second character of the user name</td>
<td>Expands to the second character of the user name.</td>
</tr>
<tr>
<td>%2</td>
<td>Third character of the user name</td>
<td>Expands to the third character of the user name.</td>
</tr>
</tbody>
</table>

**Note**

If the user name includes fewer than three characters, the %0, %1, and %2 variables wrap around. For example, for a user named ab, the variables maps to a, b, and a, respectively. For a user named a, all three variables map to a.
SMB commands

You can access and configure the SMB file sharing service through the SMB commands.

isi smb log-level filters create

Creates a new SMB log filter.

Syntax

isi smb log-level filters create <level>  
[--ops <string>]  
[--ip-addrs <string>]  
[--verbose]

Options

<level>

The logging level for the new filter. Valid logging levels are:

- always
- error
- warning
- info
- verbose
- debug
- trace

{--ops | -o} <string>

List all SMB operations to filter against. Repeat for each operation.

{--ip-addrs | -i} <string>

List IPv4 and IPv6 addresses to filter against. Repeat for each IP address.

isi smb log-level filters delete

Deletes SMB log filters.

Syntax

isi smb log-level filters delete <id> <level>  
[--all]  
[--force]  
[--verbose]

Options

<id>

Deletes a specific SMB log filter, by ID.

<level>

Deletes all SMB log filters at a specified level. The following levels are valid:
**isi smb log-level filters list**

Lists SMB log filters.

**Syntax**

```
isi smb log-level filters list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

```
{--limit | -l} <integer>
    Displays the specified number of SMB log-level filters.

--format {table | json | csv | list}
    Displays SMB log-level filters in table, JSON, comma-separated, or list format.

{--no-header | -a}
    Does not display headers in comma-separated or table format.

{--no-footer | -z}
    Does not display table summary footer information.

{--verbose | -v}
    Displays more detailed information.
```
isi smb log-level filters view

View an individual SMB log-level filter.

Syntax

```
isi smb log-level filters view <id>
    [--level <string>]
```

Options

`<id>`

The ID of the SMB log-level filter to view.

`{--level | -l} <string>`

Specifies a log-level to view. The following levels are valid:

- always
- error
- warning
- info
- verbose
- debug
- trace

isi smb log-level modify

Sets the log level for the SMB service.

Syntax

```
isi smb log-level modify <level>
    [--verbose]
```

Options

`<level>`

Specifies a log level to set for the SMB service. The following levels are valid:

- always
- error
- warning
- info
- verbose
- debug
- trace

`{--verbose | -v}`

Displays more detailed information.
isi smb log-level view

Shows the current log level for the SMB service.

**Syntax**

```
isi smb log-level view
```

**Options**

There are no options for this command.

isi smb openfiles close

Closes an open file.

**Note**

To view a list of open files, run the `isi smb openfiles list` command.

**Syntax**

```
isi smb openfiles close <id>
   [--force]
```

**Options**

```
<id>

  Specifies the ID of the open file to close.

{--force | -f}

  Suppresses command-line prompts and messages.
```

**Examples**

The following command closes a file with an ID of 32:

```
isi smb openfiles close 32
```

isi smb openfiles list

Displays a list of files that are open in SMB shares.

**Syntax**

```
isi smb openfiles list
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

```
{--limit | -l} <integer>
```
Displays no more than the specified number of smb openfiles.

`--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`
Displays table and CSV output without headers.

`{--no-footer | -z}`
Displays table output without footers.

`{--verbose | -v}`
Displays more detailed information.

**isi smb sessions delete**

Deletes SMB sessions, filtered first by computer and then optionally by user.

**Note**

Any open files are automatically closed before an SMB session is deleted.

**Syntax**

```
isi smb sessions delete <computer-name>
  [{--user <name> | --uid <id> | --sid <sid>}]  
  [--force]
  [--verbose]
```

**Options**

**<computer-name>**
Required. Specifies the computer name. If a --user, --uid, or --sid option is not specified, the system deletes all SMB sessions associated with this computer.

**--user <string>**
Specifies the name of the user. Deletes only those SMB sessions to the computer that are associated with the specified user.

**--uid <id>**
Specifies a numeric user identifier. Deletes only those SMB sessions to the computer that are associated with the specified user identifier.

**--sid <sid>**
Specifies a security identifier. Deletes only those SMB sessions to the computer that are associated with the security identifier.

`{--force | -f}`
Specifies that the command execute without prompting for confirmation.
Examples
The following command deletes all SMB sessions associated with a computer named computer1:

```
isi smb sessions delete computer1
```

The following command deletes all SMB sessions associated with a computer named computer1 and a user named user1:

```
isi smb sessions delete computer1 --user=user1
```

isi smb sessions delete-user

Deletes SMB sessions, filtered first by user then optionally by computer.

Note
Any open files are automatically closed before an SMB session is deleted.

Syntax

```
isi smb sessions delete-user {<user> | --uid <id> | --sid <sid>} [--computer-name <string>] [--force] [--verbose]
```

Options

<user>
Required. Specifies the user name. If the --computer-name option is omitted, the system deletes all SMB sessions associated with this user.

{--computer-name | -C} <string>
Deletes only the user’s SMB sessions that are associated with the specified computer.

{--force | -f}
Suppresses command-line prompts and messages.

{--verbose | -v}
Displays more detailed information.

Examples
The following command deletes all SMB sessions associated with a user called user1:

```
isi smb sessions delete-user user1
```
The following command deletes all SMB sessions associated with a user called user1 and a computer called computer1:

```
isi smb sessions delete-user user1 --computer-name=computer1
```

### isi smb sessions list

Displays a list of open SMB sessions.

**Syntax**

```
isi smb sessions list
```

**Options**

```
--limit <integer>
```

Specifies the maximum number of SMB sessions to list.

```
--format {table | json | csv | list}
```

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

```
--no-header
```

Displays table and CSV output without headers.

```
--no-footer
```

Displays table output without footers.

```
--verbose
```

Displays more detailed information.

### isi smb settings global modify

Modifies global SMB settings.

**Syntax**

```
isi smb settings global modify
```

- `--access-based-share-enum {yes | no}`
- `--revert-access-based-share-enum`
- `--dot-snap-accessible-child {yes | no}`
- `--revert-dot-snap-accessible-child`
- `--dot-snap-accessible-root`
- `--revert-dot-snap-accessible-root`
- `--dot-snap-visible-child {yes | no}`
- `--revert-dot-snap-visible-child`
- `--dot-snap-visible-root {yes | no}`
- `--revert-dot-snap-visible-root`
- `--enable-security-signatures {yes | no}`
- `--revert-enable-security-signatures`
Options

--access-based-share-enum {yes | no}
Enumerates only the files and folders that the requesting user has access to.

--revert-access-based-share-enum
Sets the value to the system default for --access-based-share-enum.

--dot-snap-accessible-child {yes | no}
Specifies whether to make the /ifs/.snapshot directory visible in subdirectories of the share root. The default setting is no.

--revert-dot-snap-accessible-child
Sets the value to the system default for --dot-snap-accessible-child.

--dot-snap-accessible-root {yes | no}
Specifies whether to make the /ifs/.snapshot directory accessible at the share root. The default setting is yes.

--revert-dot-snap-accessible-root
Sets the value to the system default for --dot-snap-accessible-root.

--dot-snap-visible-child {yes | no}
Specifies whether to make the /ifs/.snapshot directory visible in subdirectories of the share root. The default setting is no.

--revert-dot-snap-visible-child
Sets the value to the system default for --dot-snap-visible-child.

--dot-snap-visible-root {yes | no}
Specifies whether to make the /ifs/.snapshot directory visible at the root of the share. The default setting is no.

--revert-dot-snap-visible-root
Sets the value to the system default for --dot-snap-visible-root.
--enable-security-signatures {yes | no}
Indicates whether the server supports signed SMB packets.

--revert-enable-security-signatures
Sets the value to the system default for --enable-security-signatures.

--guest-user <integer>
Specifies the fully qualified user to use for guest access.

--revert-guest-user
Sets the value to the system default for --guest-user.

--ignore-eas {yes | no}
Specifies whether to ignore EAs on files.

--revert-ignore-eas
Sets the value to the system default for --ignore-eas.

--onefs-cpu-multiplier <integer>
Specifies the number of OneFS worker threads to configure based on the number of CPUs. Valid numbers are 1-4.

--revert-onefs-cpu-multiplier
Sets the value to the system default for --onefs-cpu-multiplier.

--onefs-num-workers <integer>
Specifies the number of OneFS worker threads that are allowed to be configured. Valid numbers are 0-1024. If set to 0, the number of SRV workers will equal the value specified by --onefs-cpu-multiplier times the number of CPUs.

--revert-onefs-num-workers
Sets the value to the system default for --onefs-num-workers.

--require-security-signatures {yes | no}
Specifies whether packet signing is required. If set to yes, signing is always required. If set to no, signing is not required but clients requesting signing will be allowed to connect if the --enable-security-signatures option is set to yes.

--revert-require-security-signatures
Sets the value to the system default for --require-security-signatures.

--server-side-copy {yes | no}
Enables or disables SMB server-side copy functionality. The default is yes.

--revert-server-side-copy
Sets the value to the system default for --server-side-copy.

--server-string <string>
Provides a description of the server.

--revert-server-string
Sets the value to the system default for --revert-server-string.

--support-multichannel {yes | no}
Specifies whether Multichannel for SMB 3.0 is enabled on the cluster. SMB Multichannel is enabled by default.

```
--revert-support-multichannel
```

Set the value of `--support-multichannel` back to the default system value.

```
--support-netbios {yes | no}
```

Specifies whether to support the NetBIOS protocol.

```
--revert-support-netbios
```

Sets the value to the system default for `--support-netbios`.

```
--support-smb2 {yes | no}
```

Specifies whether to support the SMB 2.0 protocol. The default setting is `yes`.

```
--revert-support-smb2
```

Sets the value to the system default for `--support-smb2`.

### isi smb settings global view
Displays the default SMB configuration settings.

**Syntax**

```
isi smb settings global view
```

**Options**

There are no options for this command.

### isi smb settings shares modify
Modifies default settings for SMB shares.

**Syntax**

```
isi smb settings shares modify
[--access-based-enumeration {yes | no}]
[--revert-access-based-enumeration]
[--access-based-enumeration-root-only {yes | no}]
[--revert-access-based-enumeration-root-only]
[--allow-delete-readonly {yes | no}]
[--revert-allow-delete-readonly]
[--allow-execute-always {yes | no}]
[--revert-allow-execute-always]
[--ca-timeout <integer>]
[--revert-ca-timeout]
[--strict-ca-lockout {yes | no}]
[--revert-strict-ca-lockout]
[--ca-write-integrity {none | write-read-coherent | full}]
[--revert-ca-write-integrity]
[--change-notify {all | norecurse | none}]
[--revert-change-notify]
[--create-permissions {"default acl" | "inherit mode bits" | "use create mask and mode"}]
[--revert-create-permissions]
[--directory-create-mask <integer>]
[--revert-directory-create-mask]
[--directory-create-mode <integer>]
[--revert-directory-create-mode]
[--file-create-mask <integer>]
```
Options

--access-based-enumeration {yes | no}
  Specifies whether access-based enumeration is enabled.

--revert-access-based-enumeration
  Sets the value to the system default for --access-based-enumeration.

--access-based-enumeration-root-only {yes | no}
  Specifies whether access-based enumeration is only enabled on the root directory of the share.

--revert-access-based-enumeration-root-only
  Sets the value to the system default for --access-based-enumeration-root-only.

--allow-delete-readonly {yes | no}
  Specifies whether read-only files can be deleted.

--revert-allow-delete-readonly
  Sets the value to the system default for --allow-delete-readonly.
--allow-execute-always {yes | no}
  Specifies whether a user with read access to a file can also execute the file.

--revert-allow-execute-always
  Sets the value to the system default for --allow-execute-always.

--ca-timeout <integer>
  The amount of time, in seconds, a persistent handle is retained after a client is
disconnected or a server fails. The default is 120 seconds.

--revert-ca-timeout
  Sets the value to the system default for --ca-timeout.

--strict-ca-lockout {yes | no}
  If set to yes, prevents another client from opening a file if a client has an open
but disconnected persistent handle for that file. If set to no, OneFS issues
persistent handles, but discards them if any client other than the original opener
attempts to open the file. This option is only relevant if --continuously-
available was set to yes when the share was created. The default is yes.

--revert-strict-ca-lockout
  Sets the value to the system default for --strict-ca-lockout.

--ca-write-integrity {none | write-read-coherent | full}
  Specifies the level of write integrity on continuously available shares:
  none
    Continuously available writes are not handled differently than other writes to
    the cluster. If you specify none and a node fails, you may experience data
    loss without notification. Therefore, we do not recommend this option.
  write-read-coherent
    Ensures that writes to the share are moved to persistent storage before a
    success message is returned to the SMB client that sent the data. This is the
default setting.
  full
    Ensures that writes to the share are moved to persistent storage before a
    success message is returned to the SMB client that sent the data, and
    prevents OneFS from granting SMB clients write-caching and handle-
caching leases.

--revert-ca-write-integrity
  Sets the value to the system default for --ca-write-integrity.

--change-notify {norecurse | all | none}
  Defines the change notify setting. The acceptable values are norecurse, all,
  and none.

--revert-change-notify
  Sets the value to the system default for --change-notify.

--create-permissions {"default acl" | "inherit mode bits" | "use
create mask and mode"}
Sets the default permissions to apply when a file or directory is created.

--revert-create-permissions
Sets the value to the system default for --create-permissions.

--directory-create-mask <integer>
Defines which mask bits are applied when a directory is created.

--revert-directory-create-mask
Sets the value to the system default for --directory-create-mask.

--directory-create-mode <integer>
Defines which mode bits are applied when a directory is created.

--revert-directory-create-mode
Sets the value to the system default for --directory-create-mode.

--file-create-mask <integer>
Defines which mask bits are applied when a file is created.

--revert-file-create-mask
Sets the value to the system default for --file-create-mask.

--file-create-mode <integer>
Defines which mode bits are applied when a file is created.

--revert-file-create-mode
Sets the value to the system default for --file-create-mode.

--file-filtering-enabled {yes | no}
If set to yes, enables file filtering at the share level. The default setting is no.

--revert-file-filtering-enabled
Sets the value for the system default of --file-filtering-enabled.

--file-filter-type {deny | allow}
If set to allow, allows the specified file types to be written to the share. The default setting is deny.

--revert-file-filter-type
Sets the value for the system default of --file-filter-type.

--file-filter-extensions <string>
Specifies the list of file types to deny or allow writes to the share, depending on the setting of --file-filter-type. File types may be specified in a list of comma separated values.

--clear-file-filter-extensions
Clears the list of file filtering extensions for the share.

--add-file-filter-extensions <string>
Adds entries to the list of file filter extensions. Repeat for each file extension to add.

--remove-file-filter-extensions <string>
Removes entries to the list of file filter extensions. Repeat for each file extension to remove.

--revert-file-filter-extensions
Sets the value for the system default of --file-filter-extensions.

--hide-dot-files {yes | no}
Specifies whether to hide files that begin with a period—for example, UNIX configuration files.

--revert-hide-dot-files
Sets the value to the system default for --hide-dot-files.

--host-acl <string>
Specifies which hosts are allowed access. Specify --host-acl for each additional host ACL clause. This will replace any existing ACL.

--revert-host-acl
Sets the value to the system default for --host-acl.

--clear-host-acl <string>
Clears the value for an ACL expressing which hosts are allowed access.

--add-host-acl <string>
Adds an ACE to the already-existing host ACL. Specify --add-host-acl for each additional host ACL clause to be added.

--remove-host-acl <string>
Removes an ACE from the already-existing host ACL. Specify --remove-host-acl for each additional host ACL clause to be removed.

--impersonate-guest {always | "bad user" | never}
Allows guest access to the share. The acceptable values are always, "bad user", and never.

--revert-impersonate-guest
Sets the value to the system default for --impersonate-guest.

--impersonate-user <string>
Allows all file access to be performed as a specific user. This must be a fully qualified user name.

--revert-impersonate-user
Sets the value to the system default for --impersonate-user.

--mangle-byte-start <string>
Specifies the wchar_t starting point for automatic invalid byte mangling.

--revert-mangle-byte-start
Sets the value to the system default for --mangle-byte-start.

--mangle-map <string>
Maps characters that are valid in OneFS but are not valid in SMB names.

--revert-mangle-map
Sets the value to the system default for --mangle-map.

--clear-mangle-map <string>
Clears the values for character mangle map.

--add-mangle-map <string>
Adds a character mangle map. Specify --add-mangle-map for each additional Add character mangle map.

--remove-mangle-map <string>
Removes a character mangle map. Specify --remove-mangle-map for each additional Remove character mangle map.

--ntfs-acl-support {yes | no}
Specifies whether ACLs can be stored and edited from SMB clients.

--revert-ntfs-acl-support
Sets the value to the system default for --ntfs-acl-support.

--oplocks {yes | no}
Specifies whether to allow oplock requests.

--revert-oplocks
Sets the value to the system default for --oplocks.

--strict-flush {yes | no}
Specifies whether to always honor flush requests.

--revert-strict-flush
Sets the value to the system default for --strict-flush.

--strict-locking {yes | no}
Specifies whether the server will check for and enforce file locks.

--revert-strict-locking
Sets the value to the system default for --strict-locking.

--zone <string>
Specifies the name of the access zone.

isi smb settings shares view
Displays default settings for all SMB shares or for SMB shares in a specified access zone.

Syntax

isi smb settings shares view
[--zone <string>]

Options

--zone <string>
Specifies the name of the access zone. Displays only the settings for shares in the specified zone.
Example
This is an example of the output generated by `isi smb settings shares view`:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Based Enumeration</td>
<td>No</td>
</tr>
<tr>
<td>Access Based Enumeration Root</td>
<td>Only: No</td>
</tr>
<tr>
<td>Allow Delete Readonly</td>
<td>No</td>
</tr>
<tr>
<td>Allow Execute Always</td>
<td>No</td>
</tr>
<tr>
<td>Ca Timeout</td>
<td>120</td>
</tr>
<tr>
<td>Continuously Available</td>
<td>Yes</td>
</tr>
<tr>
<td>Strict Ca Lockout</td>
<td>Yes</td>
</tr>
<tr>
<td>Ca Write Integrity</td>
<td>write-read-coherent</td>
</tr>
<tr>
<td>Change Notify</td>
<td>norecurse</td>
</tr>
<tr>
<td>Create Permissions</td>
<td>default acl</td>
</tr>
<tr>
<td>Directory Create Mask</td>
<td>0700</td>
</tr>
<tr>
<td>Directory Create Mode</td>
<td>0000</td>
</tr>
<tr>
<td>File Create Mask</td>
<td>0700</td>
</tr>
<tr>
<td>File Create Mode</td>
<td>0100</td>
</tr>
<tr>
<td>File Filtering Enabled</td>
<td>No</td>
</tr>
<tr>
<td>File Filter Extensions</td>
<td>-</td>
</tr>
<tr>
<td>File Filter Type</td>
<td>deny</td>
</tr>
<tr>
<td>Hide Dot Files</td>
<td>No</td>
</tr>
<tr>
<td>Host ACL</td>
<td>-</td>
</tr>
<tr>
<td>Impersonate Guest</td>
<td>never</td>
</tr>
<tr>
<td>Impersonate User</td>
<td>-</td>
</tr>
<tr>
<td>Mangle Byte Start</td>
<td>0XED00</td>
</tr>
<tr>
<td>Mangle Map</td>
<td>0x01-0x1F:-1, 0x22:-1, 0x2A:-1, 0x3A:-1, 0x3C:-1, 0x3E:-1, 0x3F:-1, 0x5C:-1</td>
</tr>
<tr>
<td>Ntfs ACL Support</td>
<td>Yes</td>
</tr>
<tr>
<td>Oplocks</td>
<td>Yes</td>
</tr>
<tr>
<td>Strict Flush</td>
<td>Yes</td>
</tr>
<tr>
<td>Strict Locking</td>
<td>No</td>
</tr>
<tr>
<td>Change Notify</td>
<td>norecurse</td>
</tr>
<tr>
<td>Create Permissions</td>
<td>default acl</td>
</tr>
<tr>
<td>Directory Create Mask</td>
<td>0700</td>
</tr>
<tr>
<td>Directory Create Mode</td>
<td>0000</td>
</tr>
<tr>
<td>File Create Mask</td>
<td>0700</td>
</tr>
<tr>
<td>File Create Mode</td>
<td>0100</td>
</tr>
<tr>
<td>File Filtering Enabled</td>
<td>No</td>
</tr>
<tr>
<td>File Filter Extensions</td>
<td>-</td>
</tr>
<tr>
<td>File Filter Type</td>
<td>deny</td>
</tr>
<tr>
<td>Hide Dot Files</td>
<td>No</td>
</tr>
<tr>
<td>Host ACL</td>
<td>-</td>
</tr>
<tr>
<td>Impersonate Guest</td>
<td>never</td>
</tr>
<tr>
<td>Impersonate User</td>
<td>-</td>
</tr>
<tr>
<td>Mangle Byte Start</td>
<td>0XED00</td>
</tr>
<tr>
<td>Mangle Map</td>
<td>0x01-0x1F:-1, 0x22:-1, 0x2A:-1, 0x3A:-1, 0x3C:-1, 0x3E:-1, 0x3F:-1, 0x5C:-1</td>
</tr>
<tr>
<td>Ntfs ACL Support</td>
<td>Yes</td>
</tr>
<tr>
<td>Oplocks</td>
<td>Yes</td>
</tr>
<tr>
<td>Strict Flush</td>
<td>Yes</td>
</tr>
<tr>
<td>Strict Locking</td>
<td>No</td>
</tr>
<tr>
<td>Change Notify</td>
<td>norecurse</td>
</tr>
<tr>
<td>Create Permissions</td>
<td>default acl</td>
</tr>
</tbody>
</table>

**isi smb shares create**

Creates an SMB share.

**Syntax**

```
isi smb shares create <name> <path>
   [--zone <string>]
   [--inheritable-path-acl {yes | no}]
   [--create-path]
   [--host-acl <string>]
   [--description <string>]
   [--csc-policy {none | documents | manual | programs}]
   [--allow-variable-expansion {yes | no}]
   [--auto-create-directory {yes | no}]
   [--browsable {yes | no}]
   [--allow-execute-always {yes | no}]
   [--directory-create-mask <integer>]
   [--strict-locking {yes | no}]
   [--hide-dot-files {yes | no}]
   [--impersonate-guest {always | "bad user" | never}]
   [--strict-flush {yes | no}]
   [--access-based-une Numeration {yes | no}]
   [--access-based-une Numeration-root-only {yes | no}]
   [--continuously-available {yes | no}]
   [--ca-timeout <integer>]
   [--strict-ca-lockout {yes | no}]
   [--ca-write-integrity {none | write-read-coherent | full}]
   [--mangle-byte-start <string>]
   [--file-create-mask <integer>]
   [--create-permissions {"default acl" | "inherit mode bits"
   | "use create mask and mode"}]
   [--mangle-map <string>]
   [--impersonate-user <string>]
   [--change-notify <string>]
```
[--oplocks {yes | no}]
[--allow-delete-readonly {yes | no}]
[--directory-create-mode <integer>]
[--ntfs-acl-support {yes | no}]
[--file-create-mode <integer>]
[--file-filtering-enabled {yes | no}]
[--file-filter-type {deny | allow}]
[--file-filter-extensions <string>]

Options

<name>
   Required. Specifies the name for the new SMB share.

<path>
   Required. Specifies the full path of the SMB share to create, beginning at /ifs.

--zone <string>
   Specifies the access zone the new SMB share is assigned to. If no access zone is
   specified, the new SMB share is assigned to the default System zone.

{--inheritable-path-acl | -i} {yes | no}
   If set to yes, if the parent directory has an inheritable access control list (ACL),
   its ACL will be inherited on the share path. The default setting is no.

--create-path
   Creates the SMB-share path if one doesn't exist.

--host-acl <string>
   Specifies the ACL that defines host access. Specify --host-acl for each
   additional host ACL clause.

--description <string>
   Specifies a description for the SMB share.

--csc-policy {none | documents | manual | programs}
   Sets the client-side caching policy for the share.

--allow-variable-expansion {yes | no}
   Specifies automatic expansion of variables for home directories.

--directory-create-mask <integer>
   Creates home directories automatically.

--browsable {yes | no}, -b {yes | no}
   If set to yes, makes the share visible in net view and the browse list. The default
   setting is yes.

--allow-execute-always {yes | no}
   If set to yes, allows a user with read access to a file to also execute the file. The
   default setting is no.

--directory-create-mask <integer>
   Defines which mask bits are applied when a directory is created.
--strict-locking {yes | no}
If set to yes, directs the server to check for and enforce file locks. The default setting is no.

--hide-dot-files {yes | no}
If set to yes, hides files that begin with a decimal—for example, UNIX configuration files. The default setting is no.

--impersonate-guest {always | "bad user" | never}
Allows guest access to the share. The acceptable values are always, "bad user", and never.

--strict-flush {yes | no}
If set to yes, flush requests are always honored. The default setting is yes.

--access-based-enumeration {yes | no}
If set to yes, enables access-based enumeration only on the files and folders that the requesting user can access. The default setting is no.

--access-based-enumeration-root-only {yes | no}
If set to yes, enables access-based enumeration only on the root directory of the SMB share. The default setting is no.

--continuously-available {yes | no}
If set to yes, the share allows certain Windows clients to open persistent handles that can be reclaimed after a network disconnect or server failure. The default is no.

--ca-timeout <integer>
The amount of time, in seconds, a persistent handle is retained after a client is disconnected or a server fails. The default is 120 seconds.

--strict-ca-lockout {yes | no}
If set to yes, prevents a client from opening a file if another client has an open but disconnected persistent handle for that file. If set to no, OneFS issues persistent handles, but discards them if any client other than the original opener attempts to open the file. The default is yes.

--ca-write-integrity {none | write-read-coherent | full}
Specifies the level of write integrity on continuously available shares:

none
Continuously available writes are not handled differently than other writes to the cluster. If you specify none and a node fails, you may experience data loss without notification. Therefore, we do not recommend this option.

write-read-coherent
Ensures that writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data. This is the default setting.

full
Ensures that writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data, and
prevents OneFS from granting SMB clients write-caching and handle-caching leases.

--mangle-byte-start <string>
Specifies the wchar_t starting point for automatic invalid byte mangling.

--file-create-mask <integer>
Defines which mask bits are applied when a file is created.

--create-permissions {"default acl" | "inherit mode bits" | "use create mask and mode"}
Sets the default permissions to apply when a file or directory is created. Valid values are "default acl", "inherit mode bits", and "use create mask and mode"

--mangle-map <string>
Maps characters that are valid in OneFS but are not valid in SMB names.

--impersonate-user <string>
Allows all file access to be performed as a specific user. This value must be a fully qualified user name.

--change-notify {norecurse | all | none}
Defines the change notify setting. The acceptable values are norecurse, all, or none.

--oplocks {yes | no}
If set to yes, allows oplock requests. The default setting is yes.

--allow-delete-readonly {yes | no}
If set to yes, allows read-only files to be deleted. The default setting is no.

--directory-create-mode <integer>
Defines which mode bits are applied when a directory is created.

--ntfs-acl-support {yes | no}
If set to yes, allows ACLs to be stored and edited from SMB clients. The default setting is yes.

--file-create-mode <integer>
Defines which mode bits are applied when a file is created.

--file-filtering-enabled {yes | no}
If set to yes, enables file filtering at the share level. The default setting is no.

--file-filter-type {deny | allow}
If set to allow, allows the specified file types to be written to the share. The default setting is deny.

--file-filter-extensions <string>
Specifies the list of file extensions to deny or allow writes to the share, depending on the setting of --file-filter-type. File types may be specified in a list of comma separated values.
isi smb shares delete

Deletes an SMB share.

Syntax

isi smb shares delete <share>
   [--zone <string>]
   [--force]
   [--verbose]

Options

<share>
   Specifies the name of the SMB share to delete.

--zone <string>
   Specifies the access zone the SMB share is assigned to. If no access zone is specified, the system deletes the SMB share with the specified name assigned to the default System zone, if found.

{--force | -f}
   Suppresses command-line prompts and messages.

{--verbose | -v}
   Displays more detailed information.

Examples

The following command deletes a share named "test-smb" in the "example-zone" access zone without displaying a warning prompt:

isi smb shares delete test-smb --zone example-zone --force

isi smb shares list

Displays a list of SMB shares.

Syntax

isi smb shares list
   [--zone <string>]
   [--limit <integer>]
   [--sort {name | path | description}]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]

Options

--zone <string>
   Specifies the access zone. Displays all SMB shares in the specified zone. If no access zone is specified, the system displays all SMB shares in the default System zone.
--limit | -l <integer>
    Specifies the maximum number of items to list.

--sort {name | path | description}
    Specifies the field to sort items by.

--descending | -d
    Sorts the data in descending order.

--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-
    separated value (CSV), or list format.

--no-header | -a
    Displays table and CSV output without headers.

--no-footer | -z
    Displays table output without footers.

--verbose | -v
    Displays more detailed information.

isi smb shares modify

Modifies an SMB share's settings.

Syntax

isi smb shares modify <share>
    [--name <string>]
    [--path <path>]
    [--zone <string>]
    [--new-zone <string>]
    [--host-acl <host-acl>]
    [--revert-host-acl]
    [--clear-host-acl]
    [--add-host-acl <string>]
    [--remove-host-acl <string>]
    [--description <string>]
    [--csc-policy {manual | documents | programs | none}]
    [--revert-csc-policy]
    [--allow-variable-expansion {yes | no}]
    [--revert-allow-variable-expansion]
    [--auto-create-directory {yes | no}]
    [--revert-auto-create-directory {yes | no}]
    [--browsable {yes | no}]
    [--revert-browsable]
    [--allow-execute-always {yes | no}]
    [--revert-allow-execute-always]
    [--directory-create-mask <integer>]
    [--revert-directory-create-mask]
    [--strict-locking {yes | no}]
    [--revert-strict-locking]
    [--hide-dot-files {yes | no}]
    [--revert-hide-dot-files]
    [--impersonate-guest {always | "bad user" | never}]
    [--revert-impersonate-guest]
    [--strict-flush {yes | no}]
    [--revert-strict-flush]
    [--access-based-enumeration {yes | no}]
    [--revert-access-based-enumeration]
Options

<share>
  Required. Specifies the name of the SMB share to modify.

--name <name>
  Specifies the name for the SMB share.

--path <path>
  Specifies a new path for the SMB share, starting in /ifs.

--zone <string>
  Specifies the access zone that the SMB share is assigned to. If no access zone is specified, the system modifies the SMB share with the specified name assigned to the default System zone, if found.

--new-zone <string>
  Specifies the new access zone that SMB share will be reassigned to.
--host-acl <host-acl>
An ACL expressing which hosts are allowed access. Specify --host-acl for each additional host ACL clause.

--revert-host-acl
Sets the value to the system default for --host-acl.

--clear-host-acl
Clears the value of an ACL that expresses which hosts are allowed access.

--add-host-acl <string>
Adds an ACL expressing which hosts are allowed access. Specify --add-host-acl for each additional host ACL clause to add.

--remove-host-acl <string>
Removes an ACL expressing which hosts are allowed access. Specify --remove-host-acl for each additional host ACL clause to remove.

--description <string>
The description for this SMB share.

--csc-policy, -C {manual | documents | programs | none}
Specifies the client-side caching policy for the shares.

--revert-csc-policy
Sets the value to the system default for --csc-policy.

{{--allow-variable-expansion | -a} {yes | no}}
Allows the automatic expansion of variables for home directories.

--revert-allow-variable-expansion
Sets the value to the system default for --allow-variable-expansion.

{{--auto-create-directory | -d} {yes | no}}
Automatically creates home directories.

--revert-auto-create-directory
Sets the value to the system default for --auto-create-directory.

{{--browsable | -b} {yes | no}}
The share is visible in the net view and the browse list.

--revert-browsable
Sets the value to the system default for --browsable.

--allow-execute-always {yes | no}
Allows users to execute files they have read rights for.

--revert-allow-execute-always
Sets the value to the system default for --allow-execute-always.

--directory-create-mask <integer>
Specifies the directory create mask bits.

--revert-directory-create-mask
Sets the value to the system default for `--directory-create-mask`.

`--strict-locking {yes | no}`
Specifies whether byte range locks contend against the SMB I/O.

`--revert-strict-locking`
Sets the value to the system default for `--strict-locking`.

`--hide-dot-files {yes | no}`
Hides files and directories that begin with a period ".".

`--revert-hide-dot-files`
Sets the value to the system default for `--hide-dot-files`.

`--impersonate-guest {always | "bad user" | never}`
Specifies the condition in which user access is done as the guest account.

`--revert-impersonate-guest`
Sets the value to the system default for `--impersonate-guest`.

`--strict-flush {yes | no}`
Handles the SMB flush operations.

`--revert-strict-flush`
Sets the value to the system default for `--strict-flush`.

`--access-based-enumeration {yes | no}`
Specifies to only enumerate files and folders that the requesting user has access to.

`--revert-access-based-enumeration`
Sets the value to the system default for `--access-based-enumeration`.

`--access-based-enumeration-root-only {yes | no}`
Specifies access-based enumeration on only the root directory of the share.

`--revert-access-based-enumeration-root-only`
Sets the value to the system default for `--access-based-enumeration-root-only`.

`--ca-timeout <integer>`
The amount of time, in seconds, a persistent handle is retained after a client is disconnected or a server fails. The default is 120 seconds.

`--revert-ca-timeout`
Sets the value to the system default for `--ca-timeout`.

`--strict-ca-lockout {yes | no}`
If set to yes, prevents another client from opening a file if a client has an open but disconnected persistent handle for that file. If set to no, OneFS issues persistent handles, but discards them if any client other than the original opener attempts to open the file. This option is only relevant if `--continuously-available` was set to yes when the share was created. The default is yes.

`--revert-strict-ca-lockout`
Sets the value to the system default for `--strict-ca-lockout`.

`--ca-write-integrity {none | write-read-coherent | full}`

Specifies the level of write integrity on continuously available shares:

none
- Continuously available writes are not handled differently than other writes to the cluster. If you specify `none` and a node fails, you may experience data loss without notification. Therefore, we do not recommend this option.

write-read-coherent
- Ensures that writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data. This is the default setting.

full
- Ensures that writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data, and prevents OneFS from granting SMB clients write-caching and handle-caching leases.

`--revert-ca-write-integrity`
Sets the value to the system default for `--ca-write-integrity`.

`--mangle-byte-start <integer>`
- Specifies the wchar_t starting point for automatic byte mangling.

`--revert-mangle-byte-start`
Sets the value to the system default for `--mangle-byte-start`.

`--file-create-mask <integer>`
- Specifies the file create mask bits.

`--revert-file-create-mask`
Sets the value to the system default for `--file-create-mask`.

`--create-permissions {"default acl" | "inherit mode bits" | "use create mask and mode"}`
- Sets the create permissions for new files and directories in a share.

`--revert-create-permissions`
Sets the value to the system default for `--create-permissions`.

`--mangle-map <mangle-map>`
- The character mangle map. Specify `--mangle-map` for each additional character mangle map.

`--revert-mangle-map`
Sets the value to the system default for `--mangle-map`.

`--clear-mangle-map`
- Clears the value for character mangle map.

`--add-mangle-map <string>`
Adds a character mangle map. Specify `--add-mangle-map` for each additional Add character mangle map.

`--remove-mangle-map <string>`
Removes a character mangle map. Specify `--remove-mangle-map` for each additional Remove character mangle map.

`--impersonate-user <string>`
The user account to be used as a guest account.

`--revert-impersonate-user`
Sets the value to the system default for `--impersonate-user`.

`--change-notify {all | norecurse | none}`
Specifies the level of change notification alerts on a share.

`--revert-change-notify`
Sets the value to the system default for `--change-notify`.

`--oplocks {yes | no}`
Supports oplocks.

`--revert-oplocks`
Sets the value for the system default of `--oplocks`.

`--allow-delete-readonly {yes | no}`
Allows the deletion of read-only files in the share.

`--revert-allow-delete-readonly`
Sets the value for the system default of `--allow-delete-readonly`.

`--directory-create-mode <integer>`
Specifies the directory create mode bits.

`--revert-directory-create-mode`
Sets the value for the system default of `--directory-create-mode`.

`--ntfs-acl-support {yes | no}`
Supports NTFS ACLs on files and directories.

`--revert-ntfs-acl-support`
Sets the value for the system default of `--ntfs-acl-support`.

`--file-create-mode <integer>`
Specifies the file create mode bits.

`--revert-file-create-mode`
Sets the value for the system default of `--file-create-mode`.

`--file-filtering-enabled {yes | no}`
If set to yes, enables file filtering at the share level. The default setting is no.

`--revert-file-filtering-enabled`
Sets the value for the system default of `--file-filtering-enabled`.

`--file-filter-type {deny | allow}`
If set to **allow**, allows the specified file types to be written to the share. The default setting is **deny**.

**--revert-file-filter-type**
Sets the value for the system default of **--file-filter-type**.

**--file-filter-extensions <string>**
Specifies the list of file types to deny or allow writes to the share, depending on the setting of **--file-filter-type**. File types may be specified in a list of comma separated values.

**--clear-file-filter-extensions**
Clears the list of file filtering extensions for the share.

**--add-file-filter-extensions <string>**
Adds entries to the list of file filter extensions. Repeat for each file extension to add.

**--remove-file-filter-extensions <string>**
Removes entries to the list of file filter extensions. Repeat for each file extension to remove.

**--revert-file-filter-extensions**
Sets the value for the system default of **--file-filter-extensions**.

**{--verbose | -v}**
Displays more detailed information.

### isi smb shares permission create

Creates permissions for an SMB share.

**Syntax**

```
isi smb shares permission create <share> {<user> | --group <name> | --gid <id> | --uid <id> | --sid <string> | --wellknown <string>}{--run-as-root | --permission-type {allow | deny} --permission {full | change | read}} [--zone <zone>] [--verbose]
```

**Options**

**<share>**
Specifies the name of the SMB share.

**<user>**
Specifies a user by name.

**--group <name>**
Specifies a group by name.

**--gid <id>**
Specifies a group by UNIX group identifier.
--uid <id>
  Specifies a user by UNIX user identifier.

--sid <string>
  Specifies an object by its Windows security identifier.

--wellknown <string>
  Specifies a well-known user, group, machine, or account name.

{--permission-type | -d} {deny | allow}
  Specifies whether to allow or deny a permission.

{--permission | -p} {read | full | change}
  Specifies the level of control to allow or deny.

--run-as-root {yes | no}
  If set to yes, allows the account to run as root. The default setting is no.

--zone <zone>
  Specifies an access zone.

{--verbose | -v}
  Displays more detailed information.

isi smb shares permission delete
  Deletes user or group permissions for an SMB share.

Syntax

isi smb shares permission delete <share> {<user> | --group <name> | --gid <id> | --uid <id> | --sid <string> | --wellknown <string>} [--zone <string>] [--force] [--verbose]

Options

<share>
  Required. Specifies the SMB share name.

[user]
  Specifies a user by name.

--group <name>
  Specifies a group by name.

--gid <id>
  Specifies a group by UNIX group identifier.
--uid <id>
   Specifies a user by UNIX user identifier.

--sid <string>
   Specifies an object by its Windows security identifier.

--wellknown <string>
   Specifies a well-known user, group, machine, or account name.

--zone <string>
   Specifies an access zone.

{--force | -f}
   Specifies that you want the command to execute without prompting for
   confirmation.

{--verbose | -v}
   Displays more detailed information.

isi smb shares permission list
   Displays a list of permissions for an SMB share.

Syntax

   isi smb shares permission list <share>
      [--zone <zone>]
      [--format {table | json | csv | list}]
      [--no-header]
      [--no-footer]

Options

<share>
   Specifies the name of the SMB share to display.

--zone <zone>
   Specifies the access zone to display.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-
   separated value (CSV), or list format.

{--no-header | -a}
   Displays table and CSV output without headers.

{--no-footer | -z}
   Displays table output without footers.
isi smb shares permission modify

Modifies permissions for an SMB share.

Syntax

```
isi smb shares permission modify <share> {<user> | --group <name>  | --gid <id> | --uid <id> | --sid <string> | --wellknown <string>}
   |--run-as-root | --permission-type {allow | deny}
   --permission {full | change | read}
   [--zone <zone>]
   [--verbose]
```

Options

**<share>**

Specifies the name of the SMB share.

**<user>**

Specifies a user by name.

**--group <name>**

Specifies a group by name.

**--gid <id>**

Specifies a group by UNIX group identifier.

**--uid <id>**

Specifies a user by UNIX user identifier.

**--sid <string>**

Specifies an object by its Windows security identifier.

**--wellknown <string>**

Specifies a well-known user, group, machine, or account name.

**{-permission-type | -d} {deny | allow}**

Specifies whether to allow or deny a permission.

**{-permission | -p} {read | full | change}**

Specifies the level of control to allow or deny.

**--run-as-root {yes | no}**

If set to yes, allows the account to run as root. The default setting is no.

**--zone <zone>**

Specifies an access zone.

**{-verbose | -v}**

Displays more detailed information.
isi smb shares permission view

Displays a single permission for an SMB share.

Syntax

    isi smb shares permission view <share> {<user> | --group <name> | --gid <integer> | --uid <integer> | --sid <string> | --wellknown <string>} [--zone <string>]

Options

<share>
Specifies the name of the SMB share.

(user>
Specifies a user name.

--group <name>
Specifies a group name.

--gid <integer>
Specifies a numeric group identifier.

--uid <integer>
Specifies a numeric user identifier.

--sid <string>
Specifies a security identifier.

--wellknown <string>
Specifies a well-known user, group, machine, or account name.

--zone <string>
Specifies an access zone.

isi smb shares view

Displays information about an SMB share.

Syntax

    isi smb shares view <share> [--zone <string>]

Options

<share>
Specifies the name of the SMB share to view.

--zone <string>
Specifies the access zone that the SMB share is assigned to. If no access zone is specified, the system displays the SMB share with the specified name assigned to the default System zone, if found.

**NFS**

OneFS provides an NFS server so you can share files on your cluster with NFS clients that adhere to the RFC1813 (NFSv3) and RFC3530 (NFSv4) specifications.

In OneFS, the NFS server is fully optimized as a multi-threaded service running in user space instead of the kernel. This architecture load balances the NFS service across all nodes of the cluster, providing the stability and scalability necessary to manage up to thousands of connections across multiple NFS clients.

NFS mounts execute and refresh quickly, and the server constantly monitors fluctuating demands on NFS services and makes adjustments across all nodes to ensure continuous, reliable performance. Using a built-in process scheduler, OneFS helps ensure fair allocation of node resources so that no client can seize more than its fair share of NFS services.

The NFS server also supports access zones defined in OneFS, so that clients can access only the exports appropriate to their zone. For example, if NFS exports are specified for Zone 2, only clients assigned to Zone 2 can access these exports.

To simplify client connections, especially for exports with large path names, the NFS server also supports aliases, which are shortcuts to mount points that clients can specify directly.

For secure NFS file sharing, OneFS supports NIS and LDAP authentication providers.

**NFS exports**

You can manage individual NFS export rules that define mount-points (paths) available to NFS clients and how the server should perform with these clients.

In OneFS, you can create, delete, list, view, modify, and reload NFS exports.

NFS export rules are zone-aware. Each export is associated with a zone, can only be mounted by clients on that zone, and can only expose paths below the zone root. By default, any export command applies to the client's current zone.

Each rule must have at least one path (mount-point), and can include additional paths. You can also specify that all subdirectories of the given path or paths are mountable. Otherwise, only the specified paths are exported, and child directories are not mountable.

An export rule can specify a particular set of clients, enabling you to restrict access to certain mount-points or to apply a unique set of options to these clients. If the rule does not specify any clients, then the rule applies to all clients that connect to the server. If the rule does specify clients, then that rule is applied only to those clients.

**NFS aliases**

You can create and manage aliases as shortcuts for directory path names in OneFS. If those path names are defined as NFS exports, NFS clients can specify the aliases as NFS mount points.

NFS aliases are designed to give functional parity with SMB share names within the context of NFS. Each alias maps a unique name to a path on the file system. NFS clients can then use the alias name in place of the path when mounting.
Aliases must be formed as top-level Unix path names, having a single forward slash followed by name. For example, you could create an alias named /q4 that maps to /ifs/data/finance/accounting/winter2015 (a path in OneFS). An NFS client could mount that directory through either of:

```
mount cluster_ip:/q4
mount cluster_ip:/ifs/data/finance/accounting/winter2015
```

Aliases and exports are completely independent. You can create an alias without associating it with an NFS export. Similarly, an NFS export does not require an alias.

Each alias must point to a valid path on the file system. While this path is absolute, it must point to a location beneath the zone root (/ifs on the System zone). If the alias points to a path that does not exist on the file system, any client trying to mount the alias would be denied in the same way as attempting to mount an invalid full pathname.

NFS aliases are zone-aware. By default, an alias applies to the client's current access zone. To change this, you can specify an alternative access zone as part of creating or modifying an alias.

Each alias can only be used by clients on that zone, and can only apply to paths below the zone root. Alias names are unique per zone, but the same name can be used in different zones—for example, /home.

When you create an alias in the web administration interface, the alias list displays the status of the alias. Similarly, using the --check option of the isi nfs aliases command, you can check the status of an NFS alias (status can be: good, illegal path, name conflict, not exported, or path not found).

### NFS log files

OneFS writes log messages associated with NFS events to a set of files in /var/log.

With the log level option, you can now specify the detail at which log messages are output to log files. The following table describes the log files associated with NFS.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfs.log</td>
<td>Primary NFS server functionality (v3, v4, mount)</td>
</tr>
<tr>
<td>rpc_lockd.log</td>
<td>NFS v3 locking events through the NLM protocol</td>
</tr>
<tr>
<td>rpc_statd.log</td>
<td>NFS v3 reboot detection through the NSM protocol</td>
</tr>
<tr>
<td>isi_netgroup_d.log</td>
<td>Netgroup resolution and caching</td>
</tr>
</tbody>
</table>

### Managing the NFS service

You can enable or disable the NFS service and specify the NFS versions to support, including NFSv3 and NFSv4. NFS settings are applied across all nodes in the cluster.

**Note**

NFSv4 can be enabled non-disruptively on a OneFS cluster, and it will run concurrently with NFSv3. Any existing NFSv3 clients will not be impacted by enabling NFSv4.
View NFS settings

You can view the global NFS settings that are applied to all nodes in the cluster.

**Procedure**

- Run the `isi nfs settings global view` command.

  The system displays output similar to the following example:

  ```
  NFSv3 Enabled: Yes
  NFSv4 Enabled: No
  NFS Service Enabled: Yes
  ```

Configure NFS file sharing

You can enable or disable the NFS service, and set the lock protection level and security type. These settings are applied across all nodes in the cluster. You can change the settings for individual NFS exports that you define.

**Procedure**

- Run the `isi nfs settings global modify` command.

  The following command enables NFSv4 support:

  ```
  isi nfs settings global modify --nfsv4-enabled=yes
  ```

Enable or disable the NFS service

In OneFS, the NFSv3 service is enabled by default. You can also enable NFSv4.

**Note**

You can determine whether NFS services are enabled or disabled by running the `isi nfs settings global view` command.

**Procedure**

- Run the `isi nfs settings global modify` command.

  The following command disables the NFSv3 service:

  ```
  isi nfs settings global modify --nfsv3-enabled=no
  ```

  The following command enables the NFSv4 service:

  ```
  isi nfs settings global modify --nfsv4-enabled=yes
  ```

Managing NFS exports

You can create NFS exports, view and modify export settings, and delete exports that are no longer needed.

The `/ifs` directory is the top-level directory for data storage in OneFS, and is also the path defined in the default export. By default, the `/ifs` export disallows root access, but other enables UNIX clients to mount this directory and any subdirectories beneath it.
Configure default NFS export settings

The default NFS export settings are applied to new NFS exports. You can override these settings when you create or modify an export.

You can view the current default export settings by running the `isi nfs settings export view` command.

**CAUTION**

We recommend that you not modify default export settings unless you are sure of the result.

Procedure

1. Run the `isi nfs settings export modify` command.

   The following command specifies a maximum export file size of one terabyte:

   ```
   isi nfs settings export modify --max-file-size 1099511627776
   ```

   The following command restores the maximum export file size to the system default:

   ```
   isi nfs settings export modify --revert-max-file-size
   ```

Create a root-squashing rule for an export

By default, the NFS service implements a root-squashing rule for the default NFS export. This prevents root users on NFS clients from exercising root privileges on the NFS server.

In OneFS, the default NFS export is `/ifs`, the top-level directory where cluster data is stored.

Procedure

1. Use the `isi nfs exports view` command to view the current settings of the default export.

   The following command displays the settings of the default export:

   ```
   isi nfs exports view 1
   ```

2. Confirm the following default values for these settings, which show that root is mapped to nobody, thereby restricting root access:

   ```
   Map Root
   Enabled: True
   User: Nobody
   ```
3. If the root-squashing rule, for some reason, is not in effect, you can implement it for the default NFS export by running the `isi nfs export modify` command, as follows:

```
isi nfs exports modify 1 --map-root-enabled true --map-root nobody
```

**Results**

With these settings, regardless of the users' credentials on the NFS client, they would not be able to gain root privileges on the NFS server.

---

## Create an NFS export

You can create NFS exports to share files in OneFS with UNIX-based clients.

### Before you begin

Each directory path that you designate for an export must already exist in the `/ifs` directory tree. A directory path can be used by more than one export, provided those exports do not have any of the same explicit clients.

The NFS service runs in user space and distributes the load across all nodes in the cluster. This enables the service to be highly scalable and support thousands of exports. As a best practice, however, you should avoid creating a separate export for each client on your network. It is more efficient to create fewer exports, and to use access zones and user mapping to control access.

### Procedure

1. Run the `isi nfs exports create` command.

   The following command creates an export supporting client access to multiple paths and their subdirectories:

   ```
   isi nfs exports create /ifs/data/projects,/ifs/home --all-dirs=yes
   ```

2. (Optional) To view the export ID, which is required for modifying or deleting the export, run the `isi nfs exports list` command.

---

## Check NFS exports for errors

You can check for errors in NFS exports, such as conflicting export rules, invalid paths, and unresolvable hostnames and netgroups. This task may be performed only through the OneFS command-line interface.

### Procedure

1. Establish an SSH connection to any node in the cluster.

2. Run the `isi nfs exports check` command.

   In the following example output, no errors were found:

   ```
   ID Message
   ---------
   Total: 0
   ```
In the following example output, export 1 contains a directory path that does not currently exist:

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>'/ifs/test' does not exist</td>
</tr>
</tbody>
</table>

Modify an NFS export

You can modify the settings for an existing NFS export.

⚠️ CAUTION

Changing export settings may cause performance issues. Make sure you understand the potential impact of any settings alterations prior to committing any changes.

**Procedure**

1. Run the `isi nfs exports modify` command.

   For example, the following adds a client with read-write access to NFS export 2:

   ```
   isi nfs exports modify 2 --add-read-write-clients 10.1.249.137
   ```

   This command would override the export's access-restriction setting if there was a conflict. For example, if the export was created with read-write access disabled, the client, 10.1.249.137, would still have read-write permissions on the export.

Delete an NFS export

You can delete unneeded NFS exports. Any current NFS client connections to these exports become invalid.

**Before you begin**

You need the export ID number to delete the export. Run the `isi nfs exports list` command to display a list of exports and their ID numbers.

**Procedure**

1. Run the `isi nfs exports delete` command.

   In the following example, the command deletes an export whose ID is 2:

   ```
   isi nfs exports delete 2
   ```

   In the following example, `isi nfs exports delete` deletes an export whose ID is 3 without displaying a confirmation prompt. Be careful when using the `--force` option.

   ```
   isi nfs exports delete 3 --force
   ```
2. If you did not specify the --force option, type yes at the confirmation prompt.

Managing NFS aliases

You can create NFS aliases to simplify exports that clients connect to. An NFS alias maps an absolute directory path to a simple directory path.

For example, suppose you created an NFS export to /ifs/data/hq/home/archive/first-quarter/finance. You could create the alias /finance1 to map to that directory path.

NFS aliases can be created in any access zone, including the System zone.

Create an NFS alias

You can create an NFS alias to map a long directory path to a simple pathname.

Aliases must be formed as a simple Unix-style directory path, for example, /home.

Procedure

1. Run the isi nfs aliases create command.

The following command creates an alias to a full pathname in OneFS in an access zone named hq-home:

```bash
isi nfs aliases create /home /ifs/data/offices/hq/home --zone hq-home
```

When you create an NFS alias, OneFS performs a health check. If, for example, the full path that you specify is not a valid path, OneFS issues a warning:

```
Warning: health check on alias '/home' returned 'path not found'
```

Nonetheless, the alias is created, and you can create the directory that the alias points to at a later time.

Modify an NFS alias

You can modify an NFS alias, for example, if an export directory path has changed.

Aliases must be formed as a simple Unix-style directory path, for example, /home.

Procedure

1. Run the isi nfs aliases modify command.

The following command changes the name of an alias in the access zone hq-home:

```bash
isi nfs aliases modify /home --zone hq-home --name /homel
```

When you modify an NFS alias, OneFS performs a health check. If, for example, the path to the alias is not valid, OneFS issues a warning:

```
Warning: health check on alias '/home' returned 'not exported'
```

Nonetheless, the alias is modified, and you can create the export at a later time.
Delete an NFS alias

You can delete an NFS alias.

If an NFS alias is mapped to an NFS export, deleting the alias can disconnect clients that used the alias to connect to the export.

Procedure

1. Run the `isi nfs aliases delete` command.

   The following command deletes the alias `/home` in an access zone named hq-home:

   ```
   isi nfs aliases delete /home --zone hq-home
   ```

   When you delete an NFS alias, OneFS asks you to confirm the operation:

   ```
   Are you sure you want to delete NFS alias /home? (yes/[no])
   ```

2. Type `yes`, and then press ENTER.

   The alias is deleted, unless an error condition was found, for example, you typed the name of the alias incorrectly.

List NFS aliases

You can view a list of NFS aliases that have already been defined for a particular zone. Aliases in the system zone are listed by default.

Procedure

1. Run the `isi nfs aliases list` command.

   In the following example, the command lists aliases that have been created in the system zone (the default):

   ```
   isi nfs aliases list
   ```

   In the following example, `isi nfs aliases list` lists aliases that have been created in an access zone named hq-home:

   ```
   isi nfs aliases list --zone hq-home
   ```

   Output from `isi nfs aliases list` looks similar to the following example:

<table>
<thead>
<tr>
<th>Zone</th>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>hq-home</td>
<td>/home</td>
<td>/ifs/data/offices/newyork</td>
</tr>
<tr>
<td>hq-home</td>
<td>/root_alias</td>
<td>/ifs/data/offices</td>
</tr>
<tr>
<td>hq-home</td>
<td>/project</td>
<td>/ifs/data/offices/project</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Total: 3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
View an NFS alias

You can view the settings of an NFS alias in the specified access zone.

Procedure

1. Run the `isi nfs aliases view` command.
   
   The following command provides information on an alias in the access zone, `hq-home`, including the health of the alias:

   ```
   isi nfs aliases view /projects --zone hq-home --check
   ```

   Output from the command looks similar to the following example:

<table>
<thead>
<tr>
<th>Zone</th>
<th>Name</th>
<th>Path</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>hq-home</td>
<td>/projects</td>
<td>/ifs/data/offices/project</td>
<td>good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Total: 1</td>
</tr>
</tbody>
</table>

NFS commands

You can access and configure the NFS file sharing service through the NFS commands.

**isi nfs aliases create**

Creates an NFS alias.

**Syntax**

```
isi nfs aliases create <name> <path>
   [--zone <string>]
   [--force]
   [--verbose]
```

**Options**

**<name>**

The name of the alias. Alias names must be formed as Unix root directory with a single forward slash followed by the name. For example, `/home`.

**<path>**

The OneFS directory pathname the alias links to. The pathname must be an absolute path below the access zone root. For example, `/ifs/data/ugroup1/home`.

**--zone**

The access zone in which the alias is active.

**{--force | -f}**

Forces creation of the alias without requiring confirmation.

**{--verbose | -v}**

Displays more detailed information.
Example
The following command creates an alias in a zone named ugroup1:

```bash
isi nfs aliases create /home /ifs/data/ugroup1/home
--zone ugroup1
```

### isi nfs aliases delete

Deletes an NFS alias.

**Syntax**

```bash
isi nfs aliases delete <name>
  [--zone <string>]
  [--force]
  [--verbose]
```

**Options**

- `<name>`
  - The name of the alias to be deleted.

- `--zone <string>`
  - The access zone in which the alias is active.

- `--force | -f`
  - Forces the alias to be deleted without requiring confirmation.

- `--verbose | -v`
  - Displays more detailed information.

Example
The following command deletes an alias from a zone named ugroup1.

```bash
isi nfs aliases delete /projects --zone ugroup1
```

### isi nfs aliases list

Lists NFS aliases available in the current access zone.

**Syntax**

```bash
isi nfs aliases list
  [--check]
  [--zone <string>]
  [--limit <integer>]
  [--sort {zone | name | path | health}]
  [--descending]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
```

**Options**

- `--check`
For the current zone, displays a list of aliases and their health status.

\[\text{--zone } \text{string}\]

The access zone in which the alias is active.

\[\text{--limit } | \text{-l } \text{integer}\]

Displays no more than the specified number of NFS aliases.

\[\text{--sort } \text{zone } | \text{name } | \text{path } | \text{health}\]

Specifies the field to sort by.

\[\text{--descending } | \text{-d}\]

Specifies to sort the data in descending order.

\[\text{--format } \text{table } | \text{json } | \text{csv } | \text{list}\]

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

\[\text{--no-header } | \text{-a}\]

Displays table and CSV output without headers.

\[\text{--no-footer } | \text{-z}\]

Displays table output without footers.

**Example**
The following command displays a table of the aliases in a zone named `ugroup1` including their health status.

\[\text{isi nfs aliases list --zone ugroup1 --check}\]

Output from the command is similar to the following example:

<table>
<thead>
<tr>
<th>Zone</th>
<th>Name</th>
<th>Path</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>ugroup1</td>
<td>/home</td>
<td>/ifs/data/offices/newyork good</td>
<td>good</td>
</tr>
<tr>
<td>ugroup1</td>
<td>/root_alias</td>
<td>/ifs/data/offices good</td>
<td>good</td>
</tr>
<tr>
<td>ugroup1</td>
<td>/project</td>
<td>/ifs/data/offices/project good</td>
<td>good</td>
</tr>
<tr>
<td>Total: 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**isi nfs aliases modify**

Modifies the name, zone, or absolute path of an alias.

**Syntax**

\[\text{isi nfs aliases modify } \text{alias}\]

\[\text{--zone } \text{string}\]

\[\text{--new-zone } \text{string}\]

\[\text{--name } \text{string}\]

\[\text{--path } \text{path}\]

\[\text{--force}\]

\[\text{--verbose}\]
Options

<alias>
   The current name of the alias, for example, /home.

--zone <string>
   The access zone in which the alias is currently active.

--new-zone <string>
   The new access zone in which the alias is to be active.

--name <string>
   A new name for the alias.

--path <path>
   The new OneFS directory pathname the alias should link to. The pathname must be an absolute path below the access zone root. For example, /ifs/data/ugroup2/home.

{---force | -f}
   Forces modification of the alias without requiring confirmation.

{---verbose | -v}
   Displays more detailed information.

Example

The following command modifies the zone, name, and path of an existing alias:

    isi nfs aliases modify /home --name /users --zone ugroup1 --new-zone ugroup2
    --path /ifs/data/ugroup2/users

isi nfs aliases view

Shows information about an alias in the current zone.

Syntax

    isi nfs aliases view <name>
    [--zone <string>]
    [--check]

Options

<name>
   The name of the alias.

--zone <string>
   The access zone in which the alias is active.

--check
   Include the health status of the alias.
Example
The following command displays a table of information, including the health status, of an alias named `/projects` in the current zone.

`isi nfs aliases view /projects --check`

 isi nfs exports check

Checks NFS exports for configuration errors, including conflicting export rules, bad paths, unresolvable host names, and unresolvable net groups.

Syntax

`isi nfs exports check`

    [--limit <integer>]
    [--zone <string>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--ignore-unresolvable-hosts]
    [--ignore-bad-paths]
    [--ignore-bad-auth]
    [--verbose]

Options

{--limit | -l} <integer>
Displays no more than the specified number of NFS exports.

--zone <string>
Specifies the access zone in which the export was created.

[--format {table | json | csv | list}]
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

--ignore-unresolvable-hosts
Does not present an error condition on unresolvable hosts when creating or modifying an export.

--ignore-bad-paths
Does not present an error condition on bad paths when creating or modifying an export.

--ignore-bad-auth
Ignores bad authentication for mapping options when creating or modifying an export.

{--verbose | -v}
Displays more detailed information.

Examples
The following command checks the exports in a zone named Zone-1:

```
isni nfs exports check --zone Zone-1
```

If the check finds no problems, it returns an empty table. If, however, the check finds a problem, it returns a display similar to the following:

```
ID Message
---------------------------------------
3 '/ifs/data/project' does not exist
---------------------------------------
Total: 1
```

isi nfs exports create

Creates an NFS export.

Note
To view the default NFS export settings that will be applied when creating an export, run the `isi nfs settings export view` command.

Syntax

```
isni nfs exports create <paths>
    [--block-size <size>]
    [--can-set-time {yes | no}]
    [--case-insensitive {yes | no}]
    [--case-preserving {yes | no}]
    [--chown-restricted {yes | no}]
    [--directory-transfer-size <size>]
    [--link-max <integer>]
    [--max-file-size <size>]
    [--name-max-size <integer>]
    [--no-truncate {yes | no}]
    [--return-32bit-file-ids {yes | no}]
    [--symlinks {yes | no}]
    [--zone <string>]
    [--clients <client>]
    [--description <string>]
    [--root-clients <client>]
    [--read-write-clients <client>]
    [--read-only-clients <client>]
    [--all-dirs {yes | no}]
    [--encoding <string>]
    [--security-flavors {unix | krb5 | krb5i | krb5p}]
    [--snapshot <snapshot>]
    [--map-lookup-uid {yes | no}]
    [--map-retry {yes | no}]
    [--map-root-enabled {yes | no}]
    [--map-non-root-enabled {yes | no}]
    [--map-failure-enabled {yes | no}]
    [--map-all <identity>]
    [--map-root <identity>]
    [--map-non-root <identity>]
    [--map-failure <identity>]
    [--map-full {yes | no}]
    [--commit-asynchronous {yes | no}]
    [--read-only {yes | no}]
```
Options

<paths> ...
   Required. Specifies the path to be exported, starting at /ifs. This option can be repeated to specify multiple paths.

--block-size <size>
   Specifies the block size, in bytes.

--can-set-time {yes | no}
   If set to yes, enables the export to set time. The default setting is no.

--case-insensitive {yes | no}
   If set to yes, the server will report that it ignores case for file names. The default setting is no.

--case-preserving {yes | no}
   If set to yes, the server will report that it always preserves case for file names. The default setting is no.

--chown-restricted {yes | no}
   If set to yes, the server will report that only the superuser can change file ownership. The default setting is no.

--directory-transfer-size <size>
   Specifies the preferred directory transfer size. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 128K.

--link-max <integer>
   The reported maximum number of links to a file.

--max-file-size <size>
   Specifies the maximum allowed file size on the server (in bytes). If a file is larger than the specified value, an error is returned.
--name-max-size <integer>
The reported maximum length of characters in a filename.

--no-truncate {yes | no}
If set to yes, too-long file names will result in an error rather than be truncated.

--return-32bit-file-ids {yes | no}
Applies to NFSv3 and NFSv4. If set to yes, limits the size of file identifiers returned from readdir to 32-bit values. The default value is no.

Note
This setting is provided for backward compatibility with older NFS clients, and should not be enabled unless necessary.

--symlinks {yes | no}
If set to yes, advertises support for symlinks. The default setting is no.

--zone <string>
Access zone in which the export should apply. The default zone is system.

--clients <client>
Specifies a client to be allowed access through this export. Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple clients by repeating this option.

Note
This option replaces the entire list of clients. To add or remove a client from the list, specify --add-clients or --remove-clients.

--description <string>
The description for this NFS export.

--root-clients <client>
Allows the root user of the specified client to execute operations as the root user of the cluster. This option overrides the --map-all and --map-root option for the specified client.
Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--read-write-clients <client>
Grants read/write privileges to the specified client for this export. This option overrides the --read-only option for the specified client.
Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--read-only-clients <client>
Makes the specified client read-only for this export. This option overrides the --read-only option for the specified client.
Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--all-dirs {yes | no}
If set to yes, this export will cover all directories. The default setting is no.

`--encoding <string>`

Specifies the character encoding of clients connecting through this NFS export. Valid values and their corresponding character encodings are provided in the following table. These values are taken from the node's `/etc/encodings.xml` file, and are not case sensitive.

<table>
<thead>
<tr>
<th>Value</th>
<th>Encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp932</td>
<td>Windows-SJIS</td>
</tr>
<tr>
<td>cp949</td>
<td>Windows-949</td>
</tr>
<tr>
<td>cp1252</td>
<td>Windows-1252</td>
</tr>
<tr>
<td>euc-kr</td>
<td>EUC-KR</td>
</tr>
<tr>
<td>euc-jp</td>
<td>EUC-JP</td>
</tr>
<tr>
<td>euc-jp-ms</td>
<td>EUC-JP-MS</td>
</tr>
<tr>
<td>utf-8-mac</td>
<td>UTF-8-MAC</td>
</tr>
<tr>
<td>utf-8</td>
<td>UTF-8</td>
</tr>
<tr>
<td>iso-8859-1</td>
<td>ISO-8859-1 (Latin-1)</td>
</tr>
<tr>
<td>iso-8859-2</td>
<td>ISO-8859-2 (Latin-2)</td>
</tr>
<tr>
<td>iso-8859-3</td>
<td>ISO-8859-3 (Latin-3)</td>
</tr>
<tr>
<td>iso-8859-4</td>
<td>ISO-8859-4 (Latin-4)</td>
</tr>
<tr>
<td>iso-8859-5</td>
<td>ISO-8859-5 (Cyrillic)</td>
</tr>
<tr>
<td>iso-8859-6</td>
<td>ISO-8859-6 (Arabic)</td>
</tr>
<tr>
<td>iso-8859-7</td>
<td>ISO-8859-7 (Greek)</td>
</tr>
<tr>
<td>iso-8859-8</td>
<td>ISO-8859-8 (Hebrew)</td>
</tr>
<tr>
<td>iso-8859-9</td>
<td>ISO-8859-9 (Latin-5)</td>
</tr>
<tr>
<td>iso-8859-10</td>
<td>ISO-8859-10 (Latin-6)</td>
</tr>
<tr>
<td>iso-8859-13</td>
<td>ISO-8859-13 (Latin-7)</td>
</tr>
<tr>
<td>iso-8859-14</td>
<td>ISO-8859-14 (Latin-8)</td>
</tr>
<tr>
<td>iso-8859-15</td>
<td>ISO-8859-15 (Latin-9)</td>
</tr>
<tr>
<td>iso-8859-16</td>
<td>ISO-8859-16 (Latin-10)</td>
</tr>
</tbody>
</table>

`--security-flavors {unix | krb5 | krb5i | krb5p}`

Specifies a security flavor to support. To support multiple security flavors, repeat this option for each additional entry. The following values are valid:

unix

UNIX (system) authentication.

krb5

Kerberos V5 authentication.
krb5i
   Kerberos V5 authentication with integrity.

krb5p
   Kerberos V5 authentication with privacy.

--snapshot {<snapshot> | <snapshot-alias>}
   Specifies the ID of a snapshot or snapshot alias to export. If you specify this
   option, directories will be exported in the state captured in either the specified
   snapshot or the snapshot referenced by the specified snapshot alias. If the
   snapshot does not capture the exported path, the export will be inaccessible to
   users.
   If you specify a snapshot alias, and the alias is later modified to reference a new
   snapshot, the new snapshot will be automatically applied to the export.
   Because snapshots are read-only, clients will not be able to modify data through
   the export unless you specify the ID of a snapshot alias that references the live
   version of the file system.
   Specify <snapshot> or <snapshot-alias> as the ID or name of a snapshot or
   snapshot alias.

--map-lookup-uid {yes | no}
   If set to yes, incoming UNIX user identifiers (UIDs) will be looked up locally. The
   default setting is no.

--map-retry {yes | no}
   If set to yes, the system retries failed user-mapping lookups. The default setting
   is no.

--map-root-enabled {yes | no}
   Enable/disable mapping incoming root users to a specific account.

--map-non-root-enabled {yes | no}
   Enable/disable mapping incoming non-root users to a specific account.

--map-failure-enabled {yes | no}
   Enable/disable mapping users to a specific account after failing an auth lookup.

--map-all <identity>
   Specifies the default identity that operations by any user will execute as. If this
   option is not set to root, you can allow the root user of a specific client to
   execute operations as the root user of the cluster by including the client in the --
   root-clients list.

--map-root <identity>
   Map incoming root users to a specific user and/or group ID.

--map-non-root <identity>
   Map non-root users to a specific user and/or group ID.

--map-failure <identity>
   Map users to a specific user and/or group ID after a failed auth attempt.

--map-full {yes | no}
Determines how user mapping is accomplished if a user is specified in an export option such as --map-root or --map-all. When enabled, a user mapping queries the OneFS user database and retrieves users from the applicable authentication subsystem, such as local authentication or Active Directory. When disabled, only local authentication is queried. The default setting is yes.

--commit-asynchronous {yes | no}
If set to yes, enables commit data operations to be performed asynchronously. The default setting is no.

--read-only {yes | no}
Determines the default privileges for all clients accessing the export. If set to yes, you can grant read/write privileges to a specific client by including the client in the --read-write-clients list. If set to no, you can make a specific client read-only by including the client in the --read-only-clients list. The default setting is no.

--readdirplus {yes | no}
Applies to NFSv3 only. If set to yes, enables processing of readdir-plus requests. The default setting is yes.

--read-transfer-max-size <size>
Specifies the maximum read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; k for KB; m for MB; or g for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 1M.

--read-transfer-multiple <integer>
Specifies the suggested multiple read size to report to NFSv3 and NFSv4 clients. Valid values are 0–4294967295. The initial default value is 512.

--read-transfer-size <size>
Specifies the preferred read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; k for KB; m for MB; or g for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b, or lower if the --read-transfer-max-size is set to a lesser value. The initial default value is 128K.

--setattr-asynchronous {yes | no}
If set to yes, performs set-attributes operations asynchronously. The default setting is no.

--time-delta <float>
Specifies server time granularity, in seconds.

--write-datasync-action {datasync | filesync | unstable}
Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync write method. The following values are valid:

- datasync
- filesync
- unstable

The default value is datasync, which performs the request as specified.
Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync reply method. The following values are valid:

- datasync
- filesync

The default value is datasync (does not respond differently).

Applies to NFSv3 and NFSv4 only. Specifies an alternate filesync write method. The following values are valid:

- datasync
- filesync
- unstable

The default value is filesync, which performs the request as specified.

Applies to NFSv3 and NFSv4 only. Specifies an alternate filesync reply method. The only valid value is filesync (does not respond differently).

Specifies an alternate unstable-write method. The following values are valid:

- datasync
- filesync
- unstable

The default value is unstable, which performs the request as specified.

Specifies an alternate unstable-reply method. The following values are valid:

- datasync
- filesync
- unstable

The default value is unstable (does not respond differently).

Specifies the preferred maximum write transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4,294,967,295b. The initial default value is 1M.

Specifies the suggested write transfer multiplier to report to NFSv3 and NFSv4 clients. Valid values are 0–4,294,967,295. The initial default value is 512.

Specifies the preferred write transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by...
default. The maximum value is 4294967295b, or lower if the --write-transfer-max-size is set to a lesser value. The initial default value is 512K.

--ignore-unresolvable-hosts
Does not present an error condition on unresolvable hosts when creating or modifying an export.

--ignore-bad-paths
Does not present an error condition on bad paths when creating or modifying an export.

--ignore-bad-auth
Ignores bad authentication for mapping options when creating or modifying an export.

--ignore-conflicts
Ignores conflicts between the new or modified exports and the existing configuration.

{--force | -f}
If set to no (default), a confirmation prompt displays when the command runs. If set to yes, the command executes without prompting for confirmation.

{--verbose | -v}
Displays more detailed information.

Examples
The following command creates an NFS export for a particular zone and set of clients:

```shell
isi nfs exports create /ifs/data/ugroup1/home
    --description 'Access to home dirs for user group 1'
    --zone ugroup1 --clients 10.1.28.1 --clients 10.1.28.2
```

The following command creates an NFS export with multiple directory paths and a custom security type (Kerberos 5):

```shell
isi nfs exports create /ifs/data/projects /ifs/data/templates
    --security-flavors krb5
```

`isi nfs exports delete`

Deletes an NFS export.

**Syntax**

```shell
isi nfs exports delete <id>
    [--zone <string>]
    [--force]
    [--verbose]
```

**Options**

`<id>`
Specifies the ID of the NFS export to delete. You can use the `isi nfs exports list` command to view a list of exports and their IDs in the current zone.

`--zone <string>`
Specifies the access zone in which the export was created. The default is the current zone.

`{---force | -f}`
Suppresses command-line prompts and messages.

`{---verbose | -v}`
Displays more detailed information.

`isi nfs exports list`
Displays a list of NFS exports.

**Syntax**

```
isi nfs exports list
   [--zone <string>]
   [--limit <integer>]
   [--sort <field>]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

`--zone <string>`
Specifies the name of the access zone in which the export was created.

`{---limit | -l} <integer>`
Displays no more than the specified number of NFS exports.

`--sort <field>`
Specifies the field to sort by. Valid values are as follows:

- id
- zone
- paths
- description
- clients
- root_clients
- read_only_clients
- read_write_clients
- unresolved_clients
- all_dirs
- block_size
- can_set_time
- commit_asynchronous
- directory_transfer_size
- encoding
- map_lookup_uid
- map_retry
- map_all
- map_root
- map_full
- max_file_size
- read_only
- readdirplus
- return_32bit_file_ids
- read_transfer_max_size
- read_transfer_multiple
- read_transfer_size
- security_flavors
- setattr_asynchronous
- symlinks
- time_delta
- write_datasync_action
- write_datasync_reply
- write_filesync_action
- write_filesync_reply
- write_unstable_action
- write_unstable_reply
- write_transfer_max_size
- write_transfer_multiple
- write_transfer_size

--descending

   Specifies to sort the data in descending order.

--format {table | json | csv | list}

   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}

   Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

```
{--verbose | -v}
```

Displays more detailed information.

**Examples**

The following command lists NFS exports, by default in the current zone:

```
isi nfs exports list
```

The following command lists NFS exports in a specific zone:

```
isi nfs exports list --zone hq-home
```

**isi nfs exports modify**

Modifies an NFS export.

**Note**

You can run the `isi nfs settings export view` command to see the full list of default settings for exports.

**Syntax**

```
isi nfs exports modify <id>
    [--block-size <size>]
    [--revert-block-size]
    [--can-set-time {yes | no}]  
    [--revert-can-set-time]
    [--case-insensitive {yes | no}]  
    [--revert-case-insensitive]
    [--case-preserving {yes | no}]
    [--revert-case-preserving]
    [--chown-restricted {yes | no}]
    [--revert-chown-restricted]
    [--directory-transfer-size <size>]
    [--revert-directory-transfer-size]
    [--link-max <integer>]
    [--revert-link-max]
    [--max-file-size <size>]
    [--revert-max-file-size]
    [--name-max-size <integer>]
    [--revert-name-max-size]
    [--no-truncate {yes | no}]
    [--revert-no-truncate]
    [--return-32bit-file-ids {yes | no}]
    [--revert-return-32bit-file-ids]
    [--symlinks {yes | no}]
    [--revert-symlinks]
    [--new-zone <string>]
    [--description <string>]
    [--paths <path>]
    [--clear-paths]
    [--add-paths <string>]
    [--remove-paths <string>]
    [--clients <string>]
    [--clear-clients]
    [--add-clients <string>]
    [--remove-clients <string>]
```
File sharing

[--root-clients <string>]
[--clear-root-clients]
[--add-root-clients <string>]
[--remove-root-clients <string>]
[--read-write-clients <string>]
[--clear-read-write-clients]
[--add-read-write-clients <string>]
[--remove-read-write-clients <string>]
[--read-only-clients <string>]
[--clear-read-only-clients]
[--add-read-only-clients <string>]
[--remove-read-only-clients <string>]
[--all-dirs {yes | no}]
[--revert-all-dirs]
[--encoding <string>]
[--revert-encoding]
[--security-flavors {unix | krb5 | krb5i | krb5p}]
[--revert-security-flavors]
[--clear-security-flavors]
[--add-security-flavors {unix | krb5 | krb5i | krb5p}]
[--remove-security-flavors <string>]
[--snapshot <snapshot>]
[--revert-snapshot]
[--map-lookup-uid {yes | no}]
[--revert-map-lookup-uid]
[--map-retry {yes | no}]
[--revert-map-retry]
[--map-root-enabled {yes | no}]
[--revert-map-root-enabled]
[--map-non-root-enabled {yes | no}]
[--revert-map-non-root-enabled]
[--map-failure-enabled {yes | no}]
[--revert-map-failure-enabled]
[--map-all <identity>]
[--revert-map-all]
[--map-root <identity>]
[--revert-map-root]
[--map-non-root <identity>]
[--revert-map-non-root]
[--map-failure <identity>]
[--revert-map-failure]
[--map-full {yes | no}]
[--revert-map-full]
[--commit-asynchronous {yes | no}]
[--revert-commit-asynchronous]
[--read-only {yes | no}]
[--revert-read-only]
[--readdirplus {yes | no}]
[--revert-readdirplus]
[--read-transfer-max-size <size>]
[--revert-read-transfer-max-size]
[--read-transfer-multiple <integer>]
[--revert-read-transfer-multiple]
[--read-transfer-size <size>]
[--revert-read-transfer-size]
[--setattr-asynchronous {yes | no}]
[--revert-setattr-asynchronous]
[--time-delta <time delta>]
[--revert-time-delta]
[--write-datsync-action {datasync | filesync | unstable}]
[--revert-write-datsync-action]
[--write-datsync-reply {datasync | filesync}]
[--revert-write-datsync-reply]
[--write-filesync-action {datasync | filesync | unstable}]
[--revert-write-filesync-action]
[--write-filesync-reply filesync]
[--write-unstable-action {datasync | filesync | unstable}]
[--revert-write-unstable-action]
### Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--write-unstable-reply</code></td>
<td>Sets or reverts the unstable reply setting.</td>
</tr>
<tr>
<td><code>--write-transfer-max-size</code></td>
<td>Sets or reverts the maximum transfer size.</td>
</tr>
<tr>
<td><code>--write-transfer-multiple</code></td>
<td>Sets or reverts the transfer size multiple.</td>
</tr>
<tr>
<td><code>--write-transfer-size</code></td>
<td>Sets or reverts the transfer size.</td>
</tr>
<tr>
<td><code>--zone</code></td>
<td>Sets or reverts the access zone.</td>
</tr>
<tr>
<td><code>--ignore-unresolvable-hosts</code></td>
<td>Ignores unresolvable hosts.</td>
</tr>
<tr>
<td><code>--ignore-bad-paths</code></td>
<td>Ignores bad paths.</td>
</tr>
<tr>
<td><code>--ignore-bad-auth</code></td>
<td>Ignores bad authentication.</td>
</tr>
<tr>
<td><code>--ignore-conflicts</code></td>
<td>Ignores conflicts.</td>
</tr>
<tr>
<td><code>--force</code></td>
<td>Forces the operation.</td>
</tr>
<tr>
<td><code>--verbose</code></td>
<td>Enables verbose mode.</td>
</tr>
</tbody>
</table>

#### <id>

The export ID number. You can use the `isi nfs exports list` command to view all the exports and their ID numbers in the current access zone.

#### --block-size <size>

Specifies the block size, in bytes.

#### --revert-block-size

Restores the setting to the system default.

#### --can-set-time {yes | no}

If set to `yes`, enables the export to set time. The default setting is `no`.

#### --revert-can-set-time

Restores the setting to the system default.

#### --case-insensitive {yes | no}

If set to `yes`, the server will report that it ignores case for file names. The default setting is `no`.

#### --revert-case-insensitive

Restores the setting to the system default.

#### --case-preserving {yes | no}

If set to `yes`, the server will report that it always preserves case for file names. The default setting is `no`.

#### --revert-case-preserving

Restores the setting to the system default.

#### --chown-restricted {yes | no}

If set to `yes`, the server will report that only the superuser can change file ownership. The default setting is `no`.

#### --revert-chown-restricted

Restores the setting to the system default.

#### --directory-transfer-size <size>

Specifies the preferred directory transfer size. Valid values are a number followed by a case-sensitive unit of measure: `b` for bytes; `K` for KB; `M` for MB; or `G` for GB.
If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 128K.

--revert-directory-transfer-size
Restores the setting to the system default.

--link-max <integer>
The reported maximum number of links to a file.

--revert-link-max
Restores the setting to the system default.

--max-file-size <size>
Specifies the maximum allowed file size on the server (in bytes). If a file is larger than the specified value, an error is returned.

--revert-max-file-size
Restores the setting to the system default.

--name-max-size <integer>
The reported maximum length of characters in a filename.

--revert-name-max-size
Restores the setting to the system default.

--no-truncate {yes | no}
If set to yes, too-long file names will result in an error rather than be truncated.

--revert-no-truncate
Restores the setting to the system default.

--return-32bit-file-ids {yes | no}
Applies to NFSv3 and later. If set to yes, limits the size of file identifiers returned from readdir to 32-bit values. The default value is no.

Note
This setting is provided for backward compatibility with older NFS clients, and should not be enabled unless necessary.

--revert-return-32bit-file-ids
Restores the setting to the system default.

--symlinks {yes | no}
If set to yes, advertises support for symlinks. The default setting is no.

--revert-symlinks
Restores the setting to the system default.

--new-zone <string>
Specifies a new access zone in which the export should apply. The default zone is system.

--description <string>
The description for this NFS export.
--paths <paths> ...
   Required. Specifies the path to be exported, starting at /ifs. This option can be repeated to specify multiple paths.

--clear-paths
   Clear any of the paths originally specified for the export. The path must be within the /ifs directory.

--add-paths <paths> ...
   Add to the paths originally specified for the export. The path must be within /ifs. This option can be repeated to specify multiple paths.

--remove-paths <paths> ...
   Remove a path from the paths originally specified for the export. The path must be within /ifs. This option can be repeated to specify multiple paths to be removed.

--clients <string>
   Specifies a client to be allowed access through this export. Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple clients by repeating this option.

--clear-clients
   Clear the full list of clients originally allowed access through this export.

--add-clients <string>
   Specifies a client to be added to the list of clients with access through this export. Specify clients to be added as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple clients by repeating this option.

--remove-clients <string>
   Specifies a client to be removed from the list of clients with access through this export. Specify clients to be removed as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can remove multiple clients by repeating this option.

--root-clients <string>
   Allows the root user of the specified client to execute operations as the root user of the cluster. This option overrides the --map-all and --map-root option for the specified client. Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--clear-root-clients
   Clear the full list of root clients originally allowed access through this export.

--add-root-clients <string>
   Specifies a root client to be added to the list of root clients with access through this export. Specify root clients to be added as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple root clients by repeating this option.

--remove-root-clients <string>
   Specifies a root client to be removed from the list of root clients with access through this export. Specify root clients to be removed as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can remove multiple root clients by repeating this option.
address, hostname, netgroup, or CIDR range. You can remove multiple root clients by repeating this option.

--read-write-clients <string>
Grants read/write privileges to the specified client for this export. This option overrides the --read-only option for the specified client.
Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--clear-read-write-clients
Clear the full list of read-write clients originally allowed access through this export.

--add-read-write-clients <string>
Specifies a read-write client to be added to the list of read-write clients with access through this export. Specify read-write clients to be added as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple read-write clients by repeating this option.

--remove-read-write-clients <string>
Specifies a read-write client to be removed from the list of read-write clients with access through this export. Specify read-write clients to be removed as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can remove multiple read-write clients by repeating this option.

--read-only-clients <string>
Makes the specified client read-only for this export. This option overrides the --read-only option for the specified client.
Specify clients as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can specify multiple clients in a comma-separated list.

--clear-read-only-clients
Clear the full list of read-only clients originally allowed access through this export.

--add-read-only-clients <string>
Specifies a read-only client to be added to the list of read-only clients with access through this export. Specify read-only clients to be added as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can add multiple read-only clients by repeating this option.

--remove-read-only-clients <string>
Specifies a read-only client to be removed from the list of read-only clients with access through this export. Specify read-only clients to be removed as an IPv4 or IPv6 address, hostname, netgroup, or CIDR range. You can remove multiple read-only clients by repeating this option.

--all-dirs {yes | no}
If set to yes, this export will cover all directories. The default setting is no.

--revert-all-dirs
Restores the setting to the system default.

--encoding <string>
Specifies the character encoding of clients connecting through this NFS export.
Valid values and their corresponding character encodings are provided in the following table. These values are taken from the node’s `/etc/encodings.xml` file, and are not case sensitive.

<table>
<thead>
<tr>
<th>Value</th>
<th>Encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp932</td>
<td>Windows-SJIS</td>
</tr>
<tr>
<td>cp949</td>
<td>Windows-949</td>
</tr>
<tr>
<td>cp1252</td>
<td>Windows-1252</td>
</tr>
<tr>
<td>euc-kr</td>
<td>EUC-KR</td>
</tr>
<tr>
<td>euc-jp</td>
<td>EUC-JP</td>
</tr>
<tr>
<td>euc-jp-ms</td>
<td>EUC-JP-MS</td>
</tr>
<tr>
<td>utf-8-mac</td>
<td>UTF-8-MAC</td>
</tr>
<tr>
<td>utf-8</td>
<td>UTF-8</td>
</tr>
<tr>
<td>iso-8859-1</td>
<td>ISO-8859-1 (Latin-1)</td>
</tr>
<tr>
<td>iso-8859-2</td>
<td>ISO-8859-2 (Latin-2)</td>
</tr>
<tr>
<td>iso-8859-3</td>
<td>ISO-8859-3 (Latin-3)</td>
</tr>
<tr>
<td>iso-8859-4</td>
<td>ISO-8859-4 (Latin-4)</td>
</tr>
<tr>
<td>iso-8859-5</td>
<td>ISO-8859-5 (Cyrillic)</td>
</tr>
<tr>
<td>iso-8859-6</td>
<td>ISO-8859-6 (Arabic)</td>
</tr>
<tr>
<td>iso-8859-7</td>
<td>ISO-8859-7 (Greek)</td>
</tr>
<tr>
<td>iso-8859-8</td>
<td>ISO-8859-8 (Hebrew)</td>
</tr>
<tr>
<td>iso-8859-9</td>
<td>ISO-8859-9 (Latin-5)</td>
</tr>
<tr>
<td>iso-8859-10</td>
<td>ISO-8859-10 (Latin-6)</td>
</tr>
<tr>
<td>iso-8859-13</td>
<td>ISO-8859-13 (Latin-7)</td>
</tr>
<tr>
<td>iso-8859-14</td>
<td>ISO-8859-14 (Latin-8)</td>
</tr>
<tr>
<td>iso-8859-15</td>
<td>ISO-8859-15 (Latin-9)</td>
</tr>
<tr>
<td>iso-8859-16</td>
<td>ISO-8859-16 (Latin-10)</td>
</tr>
</tbody>
</table>

---revert-encoding
Restores the setting to the system default.

--security-flavors {unix | krb5 | krb5i | krb5p}
Specifies a security flavor to support. To support multiple security flavors, repeat this option for each additional entry. The following values are valid:

unix
UNIX (system) authentication.

krb5
Kerberos V5 authentication.

krb5i
Kerberos V5 authentication with integrity.
krb5p
    Kerberos V5 authentication with privacy.

--revert-security-flavors
    Restores the setting to the system default.

--clear-security-flavors
    Clears the value for supported security flavors.

--add-security-flavors {unix | krb5 | krb5i | krb5p}
    Adds supported security flavors. Repeat for each additional supported security flavor to add.

--remove-security-flavors
    Removes supported security flavors. Repeat for each additional supported security flavor to remove from the list.

--snapshot {<snapshot> | <snapshot-alias>}
    Specifies the ID of a snapshot or snapshot alias to export. If you specify this option, directories will be exported in the state captured in either the specified snapshot or the snapshot referenced by the specified snapshot alias. If the snapshot does not capture the exported path, the export will be inaccessible to users.
    If you specify a snapshot alias, and the alias is later modified to reference a new snapshot, the new snapshot will be automatically applied to the export.
    Because snapshots are read-only, clients will not be able to modify data through the export unless you specify the ID of a snapshot alias that references the live version of the file system.
    Specify <snapshot> or <snapshot-alias> as the ID or name of a snapshot or snapshot alias.

--revert-snapshot
    Restores the setting to the system default.

--map-lookup-uid {yes | no}
    If set to yes, incoming UNIX user identifiers (UIDs) will be looked up locally. The default setting is no.

--revert-map-lookup-uid
    Restores the setting to the system default.

--map-retry {yes | no}
    If set to yes, the system will retry failed user-mapping lookups. The default setting is no.

--revert-map-retry
    Restores the setting to the system default.

--map-root-enabled {yes | no}
    Enable/disable mapping incoming root users to a specific account.

--revert-map-root-enabled
    Restores the setting to the system default.

--map-non-root-enabled {yes | no}
Enable/disable mapping incoming non-root users to a specific account.

--revert-map-non-root-enabled
Restores the setting to the system default.

--map-failure-enabled {yes | no}
Enable/disable mapping users to a specific account after failing an auth lookup.

--revert-map-failure-enabled
Restores the setting to the system default.

--map-all <identity>
Specifies the default identity that operations by any user will execute as. If this option is not set to root, you can allow the root user of a specific client to execute operations as the root user of the cluster by including the client in the --root-clients list.

--revert-map-all
Restores the setting to the system default.

--map-root <identity>
Map incoming root users to a specific user and/or group ID.

--revert-map-root
Restores the setting to the system default.

--map-non-root <identity>
Map non-root users to a specific user and/or group ID.

--revert-map-non-root
Restores the setting to the system default.

--map-failure <identity>
Map users to a specific user and/or group ID after a failed auth attempt.

--revert-map-failure
Restores the setting to the system default.

--map-full {yes | no}
Determines how user mapping is accomplished if a user is specified in an export option such as --map-root or --map-all. When enabled, a user mapping queries the OneFS user database and retrieves users from the applicable authentication subsystem, such as local authentication or Active Directory. When disabled, only local authentication is queried. The default setting is yes.

--revert-map-full
Restores the --map-full setting to the system default, yes.

--commit-asynchronous {yes | no}
If set to yes, enables commit data operations to be performed asynchronously.
The default setting is no

--revert-commit-asynchronous
Restores the setting to the system default.
--read-only {yes | no}
Determine the default privileges for all clients accessing the export.
If set to yes, you can grant read/write privileges to a specific client by including the client in the --read-write-clients list.
If set to no, you can make a specific client read-only by including the client in the --read-only-clients list. The default setting is no.

--revert-read-only
Restores the setting to the system default.

--readdirplus {yes | no}
Applies to NFSv3 only. If set to yes, enables processing of readdir-plus requests. The default setting is yes.

--revert-readdirplus
Restores the setting to the system default.

--read-transfer-max-size <size>
Specifies the maximum read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is \(4294967295\)b. The initial default value is \(1\)M.

--revert-read-transfer-max-size
Restores the setting to the system default.

--read-transfer-multiple <integer>
Specifies the suggested multiple read size to report to NFSv3 and NFSv4 clients. Valid values are 0-4294967295. The initial default value is 512.

--revert-read-transfer-multiple
Restores the setting to the system default.

--read-transfer-size <size>
Specifies the preferred read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is \(4294967295\)b, or lower if the --read-transfer-max-size is set to a lesser value. The initial default value is \(128\)K.

--revert-read-transfer-size
Restores the setting to the system default.

--setattr-asynchronous {yes | no}
If set to yes, performs set-attributes operations asynchronously. The default setting is no.

--revert-setattr-asynchronous
Restores the setting to the system default.

--time-delta <float>
Specifies server time granularity, in seconds.

--revert-time-delta
Restores the setting to the system default.
--write-datasync-action {datasync | filesync | unstable}
Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync write method.
The following values are valid:
- datasync
- filesync
- unstable
The default value is datasync, which performs the request as specified.

--revert-write-datasync-action
Restores the setting to the system default.

--write-datasync-reply {datasync | filesync}
Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync reply method.
The following values are valid:
- datasync
- filesync
The default value is datasync (does not respond differently).

--revert-write-datasync-reply
Restores the setting to the system default.

--write-filesync-action {datasync | filesync | unstable}
Applies to NFSv3 and NFSv4 only. Specifies an alternate filesync write method.
The following values are valid:
- datasync
- filesync
- unstable
The default value is filesync, which performs the request as specified.

--revert-write-filesync-action
Restores the setting to the system default.

--write-filesync-reply {filesync}
Applies to NFSv3 and NFSv4 only. Specifies an alternate filesync reply method.
The only valid value is filesync (does not respond differently).

--write-unstable-action {datasync | filesync | unstable}
Specifies an alternate unstable-write method. The following values are valid:
- datasync
- filesync
- unstable
The default value is unstable, which performs the request as specified.

--revert-write-unstable-action
Restores the setting to the system default.

--write-unstable-reply {datasync | filesync | unstable}
Specifies an alternate unstable-reply method. The following values are valid:
The default value is unstable (does not respond differently).

--revert-write-unstable-reply
Restores the setting to the system default.

--write-transfer-max-size <size>
Specifies the preferred maximum write transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 1M.

--revert-write-transfer-max-size
Restores the setting to the system default.

--write-transfer-multiple <integer>
Specifies the suggested write transfer multiplier to report to NFSv3 and NFSv4 clients. Valid values are 0-4294967295. The initial default value is 512.

--revert-write-transfer-multiple
Restores the setting to the system default.

--write-transfer-size <size>
Specifies the preferred write transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b, or lower if the --write-transfer-max-size is set to a lesser value. The initial default value is 512K.

--revert-write-transfer-size
Restores the setting to the system default.

--zone
Access zone in which the export was originally created.

--ignore-unresolvable-hosts
Does not present an error condition on unresolvable hosts when creating or modifying an export.

--ignore-bad-paths
Does not present an error condition on bad paths when creating or modifying an export.

--ignore-bad-auth
Ignores bad authentication for mapping options when creating or modifying an export.

--ignore-conflicts
Ignores conflicts between the new or modified exports and the existing configuration.

{--force | -f}
If set to no (default), a confirmation prompt displays when the command runs. If set to yes, the command executes without prompting for confirmation.

{--verbose | -v}
Displays more detailed information.

isi nfs exports reload
Reloads the NFS exports configuration.

Syntax

isi nfs exports reload

Options
There are no options for this command.

isi nfs exports view
View an NFS export.

Syntax

isi nfs exports view <id>
   [--zone <string>]

Options

<id>
   Specifies the ID of the NFS export to display. If you do not know the ID, use the isi nfs exports list command to view a list of exports and their associated IDs.

--zone <string>
   Specifies the name of the access zone in which the export was created.

isi nfs log-level modify
Sets the logging level for the NFS service.

Syntax

isi nfs log-level modify <level>
   [--verbose]

Options

<level>
Valid logging levels are:

<table>
<thead>
<tr>
<th>Log level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>Specifies that all NFS events are logged in NFS log files.</td>
</tr>
<tr>
<td>error</td>
<td>Specifies that only NFS error conditions are logged in NFS log files.</td>
</tr>
<tr>
<td>Log level</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>warning</td>
<td>Specifies that only NFS warning conditions are logged in NFS log files.</td>
</tr>
<tr>
<td>info</td>
<td>Specifies that only NFS information conditions are logged in NFS log files.</td>
</tr>
<tr>
<td>verbose</td>
<td>Specifies verbose logging.</td>
</tr>
<tr>
<td>debug</td>
<td>Adds information that EMC Isilon can use to troubleshoot issues</td>
</tr>
<tr>
<td>trace</td>
<td>Adds tracing information that EMC Isilon can use to pinpoint issues</td>
</tr>
</tbody>
</table>

```bash
{--verbose | -v}
```

Displays more detailed information.

**isi nfs log-level view**

Shows the logging level for the NFS service.

**Syntax**

```bash
isi nfs log-level view
```

**Options**

There are no options for this command.

**isi nfs netgroup check**

Updates the NFS netgroup cache.

**Syntax**

```bash
isi nfs netgroup check
  [--host <string>]
  [--verbose]
```

**Options**

```bash
--host <string>
```

The IPv4 or IPv6 address of the node to check. The default is the localhost IP address.

```bash
{--verbose | -v}
```

Displays more detailed information.

**isi nfs netgroup flush**

Flushes the NFS netgroup cache.

**Syntax**

```bash
isi nfs netgroup flush
  [--host <string>]
  [--verbose]
```
Options

--host <string>
The IPv4 or IPv6 address of the node to flush. If you do not specify a node, all nodes are flushed (default).

{verbose | -v}
Displays more detailed information.

isi nfs netgroup modify
Modifies the NFS netgroup cache settings.

Syntax

isi nfs netgroup modify
    [--bgwrite <duration>]
    [--expiration <duration>]
    [--lifetime <duration>]
    [--retry <duration>]
    [--verbose]

Options

Note
In the following option definitions, express duration in integer format as [YMWDHms].

{bgwrite | -w} <duration>
    Sets the to-disk backup interval.

{expiration | -e} <duration>
    Sets the netgroup expiration time.

{lifetime | -i} <duration>
    Sets the netgroup lifetime.

{retry | -r} <duration>
    Sets the retry interval.

{verbose | -v}
    Displays more detailed information.

isi nfs exports view
View an NFS export.

Syntax

isi nfs exports view <id>
    [--zone <string>]

Options

<iid>
Specifies the ID of the NFS export to display. If you do not know the ID, use the
 isi nfs exports list command to view a list of exports and their
 associated IDs.

--zone <string>
   Specifies the name of the access zone in which the export was created.

isi nfs nlm locks list

Applies to NFSv3 only. Displays a list of NFS Network Lock Manager (NLM) advisory
locks.

Syntax

    isi nfs nlm locks list
       [--limit <integer>]
       [--sort {client | path | lock_type | range | created}]
       [--descending]
       [--format {table | json | csv | list}]
       [--no-header]
       [--no-footer]
       [--verbose]

Options

{--limit | -l} <integer>
   Displays no more than the specified number of NFS nlm locks.

--sort {client | path | lock_type | range | created}
   Specifies the field to sort by.

{--descending | -d}
   Specifies to sort the data in descending order.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-
   separated value (CSV), or list format.

{--no-header | -a}
   Displays table and CSV output without headers.

{--no-footer | -z}
   Displays table output without footers.

{--verbose | -v}
   Displays more detailed information.

Examples

To view a detailed list of all current NLM locks, run the following command:

    isi nfs nlm locks list --verbose
In the following sample output, there are currently three locks: one on /ifs/home/test1/file.txt and two on /ifs/home/test2/file.txt.

<table>
<thead>
<tr>
<th>Client</th>
<th>Path</th>
<th>Lock Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>machineName/10.72.134.119</td>
<td>/ifs/home/test1/file.txt</td>
<td>exclusive</td>
<td>[0, 2]</td>
</tr>
<tr>
<td>machineName/10.59.166.125</td>
<td>/ifs/home/test2/file.txt</td>
<td>shared</td>
<td>[10, 20]</td>
</tr>
<tr>
<td>machineName/10.63.119.205</td>
<td>/ifs/home/test2/file.txt</td>
<td>shared</td>
<td>[10, 20]</td>
</tr>
</tbody>
</table>

isi nfs nlm locks waiters

Displays a list of clients that are waiting to place a Network Lock Manager (NLM) lock on a currently locked file. This command applies to NFSv3 only.

Syntax

isi nfs nlm locks waiters
  [--limit <integer>]
  [--sort {client | path | lock_type | range | created}]
  [--descending]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]

Options

{--limit | -l} <integer>
  Displays no more than the specified number of NLM locks.

--sort {client | path | lock_type | range | created}
  Specifies the field to sort by.

--descending
  Specifies to sort the data in descending order.

--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
  Displays table and CSV output without headers.

{--no-footer | -z}
  Displays table output without footers.

{--verbose | -v}
  Displays more detailed information.

Examples

The following command displays a detailed list of clients waiting to lock a currently-locked file:

isi nfs nlm locks waiters --verbose
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Client</th>
<th>Path</th>
<th>Lock Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>machineName/1.2.34.5</td>
<td>/ifs/home/test1/file.txt</td>
<td>exclusive</td>
<td>[0, 2]</td>
</tr>
</tbody>
</table>

isi nfs nlm sessions check

Searches for lost locks.

Syntax

    isi nfs nlm sessions check
        [--cluster-ip <string>]
        [--zone <string>]

Example 2  Options

    --cluster-ip <string>
        The cluster IP address to which the client is connected.

    --zone <string>
        The access zone to which the client is connected.

isi nfs nlm sessions delete

Deletes all states associated with an NFS Network Lock Manager (NLM) connection.

Syntax

    isi nfs nlm sessions delete <hostname> <cluster-ip>
        [--zone <string>]
        [--force]
        [--verbose]

Options

    <hostname>
        The name of the client that initiated the session.

    <cluster-ip>
        The cluster IP address to which the client is connected.

    --zone <string>
        The access zone to which the client is connected.

    {force | -f}
        Skips the confirmation prompt.

    {verbose | -v}
        Displays more detailed information.
isi nfs nlm sessions list

Displays a list of clients holding NFS Network Lock Manager (NLM) locks. This command applies to NFSv3 only.

Syntax

isi nfs nlm sessions list
[--limit <integer>]
[--sort {ID | client}]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]

Options

{--limit | -l} <integer>
The number of NFS NLM sessions to display.

--sort {hostname | cluster_ip | is_active | notify_attempts_remaining}
Specifies the field to sort by.

{--descending | -d}
Specifies to sort the data in descending order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

Example

To view a list of active NLM sessions, run the following command:

isi nfs nlm sessions list
isi nfs nlm sessions refresh

Refreshes an NFS Network Lock Manager (NLM) client.

**Syntax**

```
isi nfs nlm sessions refresh <hostname> <cluster-ip>
   [--zone <string>]
   [--force]
   [--verbose]
```

**Options**

**<hostname>**
The name of the client that initiated the session.

**<cluster-ip>**
The cluster IP address to which the client is connected.

**--zone <string>**
The access zone to which the client is connected.

**{--force | -f}**
Skips the confirmation prompt.

**{--verbose | -v}**
Displays more detailed information.

isi nfs nlm sessions view

Displays information about NFS Network Lock Manager (NLM) client connections.

**Syntax**

```
isi nfs nlm sessions view <hostname>
   [--cluster-ip <string>]
   [--zone <string>]
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

**<hostname>**
The name of the client that initiated the session.

**--cluster-ip <string>**
The cluster IP address to which the client is connected.

**--zone <string>**
The access zone to which the client is connected.

**{--limit | -l} <integer>**
Displays no more than the specified number of NFS nlm locks.
--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-
separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

isi nfs settings export modify
Modifies the default settings that are applied when creating NFS exports.

Note
You can view the currently configured default NFS export settings by running the isi
nfs settings export view command.

Syntax

isi nfs exports modify <ID>
[--block-size <size>]
[--revert-block-size]
[--can-set-time {yes|no}]
[--revert-can-set-time]
[--case-insensitive {yes|no}]
[--revert-case-insensitive]
[--case-preserving {yes|no}]
[--revert-case-preserving]
[--chown-restricted {yes|no}]
[--revert-chown-restricted]
[--directory-transfer-size <size>]
[--revert-directory-transfer-size]
[--link-max <integer>]
[--revert-link-max]
[--max-file-size <size>]
[--revert-max-file-size]
[--name-max-size <integer>]
[--revert-name-max-size]
[--no-truncate {yes|no}]
[--revert-no-truncate]
[--return-32bit-file-ids {yes|no}]
[--revert-return-32bit-file-ids]
[--symlinks {yes|no}]
[--revert-symlinks]
[--all-dirs {yes|no}]
[--revert-all-dirs]
[--encoding <string>]
[--revert-encoding]
[--security-flavors {unix|krb5|krb5i|krb5p}]
[--revert-security-flavors]
[--clear-security-flavors]
[--add-security-flavors {unix|krb5|krb5i|krb5p}]
[--remove-security-flavors <string>]
[--snapshot <snapshot>]
[--revert-snapshot]
Options

--block-size <size>

Specifies the block size, in bytes.

--revert-block-size

Restores the setting to the system default.

--can-set-time {yes|no}
If set to `yes`, enables the export to set time. The default setting is `no`.

`--revert-can-set-time`
Restores the setting to the system default.

`--case-insensitive {yes|no}`
If set to `yes`, the server will report that it ignores case for file names. The default setting is `no`.

`--revert-case-insensitive`
Restores the setting to the system default.

`--case-preserving {yes|no}`
If set to `yes`, the server will report that it always preserves case for file names. The default setting is `no`.

`--revert-case-preserving`
Restores the setting to the system default.

`--chown-restricted {yes|no}`
If set to `yes`, the server will report that only the superuser can change file ownership. The default setting is `no`.

`--revert-chown-restricted`
Restores the setting to the system default.

`--directory-transfer-size <size>`
Specifies the preferred directory transfer size. Valid values are a number followed by a case-sensitive unit of measure: `b` for bytes; `K` for KB; `M` for MB; or `G` for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 128K.

`--revert-directory-transfer-size`
Restores the setting to the system default.

`--link-max <integer>`
The reported maximum number of links to a file.

`--revert-link-max`
Restores the setting to the system default.

`--max-file-size <size>`
Specifies the maximum allowed file size on the server (in bytes). If a file is larger than the specified value, an error is returned.

`--revert-max-file-size`
Restores the setting to the system default.

`--name-max-size <integer>`
The reported maximum length of characters in a filename.

`--revert-name-max-size`
Restores the setting to the system default.

`--no-truncate {yes|no}`
If set to `yes`, too-long file names will result in an error rather than be truncated.
--revert-no-truncate
Restores the setting to the system default.

--return-32bit-file-ids {yes|no}
Applies to NFSv3 and later. If set to yes, limits the size of file identifiers returned from readdir to 32-bit values. The default value is no.

**Note**
This setting is provided for backward compatibility with older NFS clients, and should not be enabled unless necessary.

--revert-return-32bit-file-ids
Restores the setting to the system default.

--symlinks {yes|no}
If set to yes, advertises support for symlinks. The default setting is no.

--revert-symlinks
Restores the setting to the system default.

--new-zone <string>
Specifies a new access zone in which the export should apply. The default zone is system.

--all-dirs {yes|yesno}
If set to yes, this export will cover all directories. The default setting is no.

--revert-all-dirs
Restores the setting to the system default.

--encoding <string>
Specifies the character encoding of clients connecting through this NFS export. Valid values and their corresponding character encodings are provided in the following table. These values are taken from the node’s /etc/encodings.xml file, and are not case sensitive.

<table>
<thead>
<tr>
<th>Value</th>
<th>Encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp932</td>
<td>Windows-SJIS</td>
</tr>
<tr>
<td>cp949</td>
<td>Windows-949</td>
</tr>
<tr>
<td>cp1252</td>
<td>Windows-1252</td>
</tr>
<tr>
<td>euc-kr</td>
<td>EUC-KR</td>
</tr>
<tr>
<td>euc-jp</td>
<td>EUC-JP</td>
</tr>
<tr>
<td>euc-jp-ms</td>
<td>EUC-JP-MS</td>
</tr>
<tr>
<td>utf-8-mac</td>
<td>UTF-8-MAC</td>
</tr>
<tr>
<td>utf-8</td>
<td>UTF-8</td>
</tr>
<tr>
<td>iso-8859-1</td>
<td>ISO-8859-1 (Latin-1)</td>
</tr>
<tr>
<td>iso-8859-2</td>
<td>ISO-8859-2 (Latin-2)</td>
</tr>
<tr>
<td>iso-8859-3</td>
<td>ISO-8859-3 (Latin-3)</td>
</tr>
</tbody>
</table>
Value | Encoding
--- | ---
iso-8859-4 | ISO-8859-4 (Latin-4)
iso-8859-5 | ISO-8859-5 (Cyrillic)
iso-8859-6 | ISO-8859-6 (Arabic)
iso-8859-7 | ISO-8859-7 (Greek)
iso-8859-8 | ISO-8859-8 (Hebrew)
iso-8859-9 | ISO-8859-9 (Latin-5)
iso-8859-10 | ISO-8859-10 (Latin-6)
iso-8859-13 | ISO-8859-13 (Latin-7)
iso-8859-14 | ISO-8859-14 (Latin-8)
iso-8859-15 | ISO-8859-15 (Latin-9)
iso-8859-16 | ISO-8859-16 (Latin-10)

--revert-encoding
Restores the setting to the system default.

--security-flavors {unix|krb5|krb5i|krb5p} ...
Specifies a security flavor to support. To support multiple security flavors, repeat this option for each additional entry. The following values are valid:

  sys
  Sys or UNIX authentication.

  krb5
  Kerberos V5 authentication.

  krb5i
  Kerberos V5 authentication with integrity.

  krb5p
  Kerberos V5 authentication with privacy.

--revert-security-flavors
Restores the setting to the system default.

--snapshot {<snapshot>|<snapshot-alias>}
Specifies the ID of a snapshot or snapshot alias to export. If you specify this option, directories will be exported in the state captured in either the specified snapshot or the snapshot referenced by the specified snapshot alias. If the snapshot does not capture the exported path, the export will be inaccessible to users.

If you specify a snapshot alias, and the alias is later modified to reference a new snapshot, the new snapshot will be automatically applied to the export. Because snapshots are read-only, clients will not be able to modify data through the export unless you specify the ID of a snapshot alias that references the live version of the file system.

Specify `<snapshot>` or `<snapshot-alias>` as the ID or name of a snapshot or snapshot alias.
--revert-snapshot
Restores the setting to the system default.

--map-lookup-uid {yes|no}
If set to yes, incoming UNIX user identifiers (UIDs) will be looked up locally. The default setting is no.

--revert-map-lookup-uid
Restores the setting to the system default.

--map-retry {yes|no}
If set to yes, the system will retry failed user-mapping lookups. The default setting is no.

--revert-map-retry
Restores the setting to the system default.

--map-root-enabled {yes|no}
Enable/disable mapping incoming root users to a specific account.

--revert-map-root-enabled
Restores the setting to the system default.

--map-non-root-enabled {yes|no}
Enable/disable mapping incoming non-root users to a specific account.

--revert-map-non-root-enabled
Restores the setting to the system default.

--map-failure-enabled {yes|no}
Enable/disable mapping users to a specific account after failing an auth lookup.

--revert-map-failure-enabled
Restores the setting to the system default.

--map-all <identity>
Specifies the default identity that operations by any user will run as. If this option is not set to root, you can allow the root user of a specific client to run operations as the root user of the cluster by including the client in the --root-clients list.

--revert-map-all
Restores the setting to the system default.

--map-root <identity>
Map incoming root users to a specific user and/or group ID.

--revert-map-root
Restores the setting to the system default.

--map-non-root <identity>
Map non-root users to a specific user and/or group ID.

--revert-map-non-root
Restores the setting to the system default.
--map-failure <identity>
Map users to a specific user and/or group ID after a failed auth attempt.

--revert-map-failure
Restores the setting to the system default.

--map-full {yes|no}
Determines how user mapping is accomplished if a user is specified in an export option such as --map-root or --map-all. When enabled, a user mapping queries the OneFS user database and retrieves users from the applicable authentication subsystem, such as local authentication or Active Directory. When disabled, only local authentication is queried. The default setting is yes.

--revert-map-full
Restores the --map-full setting to the system default, yes.

--commit-asynchronous {yes|no}
If set to yes, enables commit data operations to be performed asynchronously. The default setting is no.

--revert-commit-asynchronous
Restores the setting to the system default.

--read-only {yes|no}
Determines the default privileges for all clients accessing the export. If set to yes, you can grant read/write privileges to a specific client by including the client in the --read-write-clients list. If set to no, you can make a specific client read-only by including the client in the --read-only-clients list. The default setting is no.

--revert-read-only
Restores the setting to the system default.

--readdirplus {yes|no}
Applies to NFSv3 only. If set to yes, enables processing of readdir-plus requests. The default setting is no.

--revert-readdirplus
Restores the setting to the system default.

--read-transfer-max-size <size>
Specifies the maximum read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 512K.

--revert-read-transfer-max-size
Restores the setting to the system default.

--read-transfer-multiple <integer>
Specifies the suggested multiple read size to report to NFSv3 and NFSv4 clients. Valid values are 0-4294967295. The initial default value is 512.

--revert-read-transfer-multiple
Restores the setting to the system default.

```
--read-transfer-size <size>
```

Specifies the preferred read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 128K.

```
--revert-read-transfer-size
```

Restores the setting to the system default.

```
--setattr-asynchronous {yes|no}
```

If set to yes, performs set-attributes operations asynchronously. The default setting is no.

```
--revert-setattr-asynchronous
```

Restores the setting to the system default.

```
--time-delta <integer>
```

Specifies server time granularity, in seconds.

```
--revert-time-delta
```

Restores the setting to the system default.

```
--write-datasync-action {datasync|filesync|unstable}
```

Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync write method. The following values are valid:

- datasync
- filesync
- unstable

The default value is datasync, which performs the request as specified.

```
--revert-write-datasync-action
```

Restores the setting to the system default.

```
--write-datasync-reply {datasync|filesync}
```

Applies to NFSv3 and NFSv4 only. Specifies an alternate datasync reply method. The following values are valid:

- datasync
- filesync

The default value is datasync (does not respond differently).

```
--revert-write-datasync-reply
```

Restores the setting to the system default.

```
--write-filesync-action {datasync|filesync|unstable}
```

Applies to NFSv3 and NFSv4 only. Specifies an alternate filesync write method. The following values are valid:

- datasync
- filesync
- unstable

The default value is filesync, which performs the request as specified.
--revert-write-sync-action
Restores the setting to the system default.

--write-sync-reply {sync}
Applies to NFSv3 and NFSv4 only. Specifies an alternate sync reply method. The only valid value is sync (does not respond differently).

--write-unstable-action {datasync|sync|unstable}
Specifies an alternate unstable-write method. The following values are valid:
- datasync
- sync
- unstable
The default value is unstable, which performs the request as specified.

--revert-write-unstable-action
Restores the setting to the system default.

--write-unstable-reply {datasync|sync|unstable}
Specifies an alternate unstable-reply method. The following values are valid:
- datasync
- sync
- unstable
The default value is unstable (does not respond differently).

--revert-write-unstable-reply
Restores the setting to the system default.

--write-transfer-max-size <size>
Specifies the preferred read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 512K.

--revert-write-transfer-max-size
Restores the setting to the system default.

--write-transfer-multiple <integer>
Specifies the suggested write transfer multiplier to report to NFSv3 and NFSv4 clients. Valid values are 0–4294967295. The initial default value is 512.

--revert-write-transfer-multiple
Restores the setting to the system default.

--write-transfer-size <size>
Specifies the preferred read transfer size to report to NFSv3 and NFSv4 clients. Valid values are a number followed by a case-sensitive unit of measure: b for bytes; K for KB; M for MB; or G for GB. If no unit is specified, bytes are used by default. The maximum value is 4294967295b. The initial default value is 512K.

--revert-write-transfer-size
Restores the setting to the system default.

--zone
Access zone in which the export was originally created.

`--force`
If set to `no` (default), a confirmation prompt displays when the command runs. If set to `yes`, the command runs without prompting for confirmation.

`--verbose`
Displays more detailed information.

**isi nfs settings export view**
Displays default NFS export settings.

**Syntax**

```
isi nfs settings export view
    [--zone <string>]
```

**Options**

`--zone <string>`
Specifies the access zone in which the default settings apply.

**Example**

To view the currently-configured default export settings, run the following command:

```
isi nfs settings export view
```

The system displays output similar to the following example:

```
Read Write Clients: -
Unresolved Clients: -
    All Dirs: No
    Block Size: 8.0K
    Can Set Time: Yes
    Case Insensitive: No
    Case Preserving: Yes
    Chown Restricted: No
    Commit Asynchronous: No
Directory Transfer Size: 128.0K
Encoding: DEFAULT
Link Max: 32767
Map Lookup UID: No
Map Retry: Yes
Map Root
    Enabled: True
    User: nobody
    Primary Group: -
    Secondary Groups: -
Map Non Root
    Enabled: False
    User: nobody
    Primary Group: -
    Secondary Groups: -
    Map Failure
    Enabled: False
    User: nobody
    Primary Group: -
    Secondary Groups: -
    Map Full: Yes
```
isi nfs settings global modify

Modifies the default NFS global settings.

Syntax

isi nfs settings global modify
   [--lock-protection <integer>]
   [--nfsv3-enabled {yes | no}]
   [--nfsv4-enabled {yes | no}]
   [--force]

Options

--lock-protection <integer>
   Specifies the number of nodes failures that can happen before a lock might be lost.

--nfsv3-enabled {yes | no}
   Specifies that NFSv3 is enabled.

--nfsv4-enabled {yes | no}
   Specifies that NFSv4 is enabled.

[--force]
   Causes the command to be executed without your confirmation.
isi nfs settings global view
Displays the global options for NFS settings.

Syntax

isi nfs settings global view

Options
There are no options for this command.

Example
The following is an example of the report generated by this command.

NFSv3 Enabled: Yes
NFSv4 Enabled: No
NFS Service Enabled: Yes

isi nfs settings zone modify
Modifies the default NFS zone settings for the NFSv4 ID mapper.

Syntax

isi nfs settings zone modify
  [--nfsv4-domain <string>]
  [--revert-nfsv4-domain]
  [--nfsv4-replace-domain {yes | no}]
  [--revert-nfsv4-replace-domain]
  [--nfsv4-no-domain {yes | no}]
  [--revert-nfsv4-no-domain]
  [--nfsv4-no-domain-uids {yes | no}]
  [--revert-nfsv4-no-domain-uids]
  [--nfsv4-no-names {yes | no}]
  [--revert-nfsv4-no-names]
  [--nfsv4-allow-numeric-ids {yes | no}]
  [--revert-nfsv4-allow-numeric-ids]
  [--zone <string>]
  [--verbose]

Options

--nfsv4-domain <string>
  Specifies the NFSv4 domain name.

--revert-nfsv4-domain
  Returns the --nfsv4-domain setting to the system default (localhost).

--nfsv4-replace-domain {yes | no}
  Replaces the owner/group domain with the NFSv4 domain name.

--revert-nfsv4-replace-domain
  Returns setting to the system default. Default is yes.

--nfsv4-no-domain {yes | no}
  Sends owners/groups without the NFSv4 domain name.

--revert-nfsv4-no-domain
Returns setting to the system default. Default is no.

--nfsv4-no-domain-uids {yes | no}
Sends UIDs/GIDs without the NFSv4 domain name.

--revert-nfsv4-no-domain-uids
Returns setting to the system default. Default is yes.

--nfsv4-no-names {yes | no}
Always sends owners/groups as UIDs/GIDs.

--revert-nfsv4-no-names
Returns setting to the system default. Default is no.

--nfsv4-allow-numeric-ids {yes | no}
Sends owners/groups as UIDs/GIDs when look-ups fail or if --nfsv4-no-names is enabled.

--revert-nfsv4-allow-numeric-ids
Returns setting to the system default. Default is yes.

--zone <string>
Specifies the access zone.

{--verbose | -v}
Displays more detailed information.

Example
The following command specifies that the NFS server would accept UIDs/GIDs in place of user names:

```
isi nfs settings zone modify --nfsv4-no-names yes
```

**isi nfs settings zone view**
Displays the default NFSv4-related access zone settings.

**Syntax**

```
isi nfs settings zone view
[--zone <string>]
```

**Options**

--zone <string>
Specifies the access zone for which you want to view NFSv4-related settings.

**Example**
The following command specifies that you want to examine NFSv4-related settings for an access zone named Zone1:

```
isi nfs settings zone view --zone=Zone1
```
FTP

OneFS includes a secure FTP service called vsftpd, which stands for Very Secure FTP Daemon, that you can configure for standard FTP and FTPS file transfers.

View FTP settings

You can view a list of current FTP configuration settings.

Procedure

- Run the `isi ftp settings view` command.

The system displays output similar to the following example:

```
Accept Timeout: 1m
Allow Anon Access: No
Allow Anon Upload: Yes
Allow Dirlists: Yes
Allow Downloads: Yes
Allow Local Access: Yes
Allow Writes: Yes
Always Chdir Homedir: Yes
Anon Chown Username: root
Anon Password List: -
  Anon Root Path: /ifs/home/ftp
  Anon Umask: 0077
  Asci Mode: off
Chroot Exception List: -
Chroot Local Mode: none
  Connect Timeout: 1m
  Data Timeout: 5m
  Denied User List: -
  Dirlist Localtime: No
  Dirlist Names: hide
File Create Perm: 0666
Limit Anon Passwords: Yes
Local Root Path: -
  Local Umask: 0077
Server To Server: No
Session Support: Yes
Session Timeout: 5m
User Config Dir: -
FTP Service Enabled: Yes
```

Enable FTP file sharing

The FTP service, vsftpd, is disabled by default.

Note

You can determine whether the service is enabled or disabled by running the `isi services -l` command.

Procedure

1. Run the following command:

   `isi services vsftpd enable`
The system displays the following confirmation message:

```
The service 'vsftpd' has been enabled.
```

**After you finish**
You can configure FTP settings by running the `isi ftp` command.

## Configure FTP file sharing

You can set the FTP service to allow any node in the cluster to respond to FTP requests through a standard user account.

**Before you begin**
You must enable the FTP service before you can use it.

You can enable the transfer of files between remote FTP servers and enable anonymous FTP service on the root by creating a local user named anonymous or ftp.

When configuring FTP access, make sure that the specified FTP root is the home directory of the user who logs in. For example, the FTP root for local user jsmith should be `ifs/home/jsmith`.

**Procedure**

- Run the `isi ftp settings modify` command.
  
  You must run this command separately for each action.

  The following command enables server-to-server transfers:

  ```
  isi ftp settings modify --server-to-server=yes
  ```

  The following command disables anonymous uploads:

  ```
  isi ftp settings modify --allow-anon-upload=no
  ```

  You must run this command separately for each action.

## FTP commands

You can access and configure the FTP service through the FTP commands.

**isi ftp settings modify**

Modifies cluster FTP settings.

**Syntax**

```
isi ftp settings modify
  [---accept-timeout <duration>]
  [---revert-accept-timeout]
  [---allow-anon-access {yes | no}]
  [---revert-allow-anon-access]
  [---allow-anon-upload {yes | no}]
  [---revert-allow-anon-upload]
  [---allow-dirlists {yes | no}]
  [---revert-allow-dirlists]
  [---allow-downloads {yes | no}]
```
Options

**--accept-timeout <duration>**

Specifies the time, in seconds, that a remote client has to establish a PASV style data connection before timeout. All integers between 30 and 600 are valid values. The default value is 60.
--revert-accept-timeout
Sets the value to the system default for --accept-timeout.

--allow-anon-access {yes | no}
Controls whether anonymous logins are permitted. If enabled, both the usernames ftp and anonymous are recognized as anonymous logins. The default value is No.

--revert-allow-anon-access
Sets the value to the system default for --allow-anon-access.

--allow-anon-upload {yes | no}
Controls whether anonymous users are able to upload files under certain conditions. For anonymous users to be able to upload, you must set the --allow-writes option to Yes, and the anonymous user must have write permission on the desired upload location. The default value is Yes.

--revert-allow-anon-upload
Sets the value to the system default for --allow-anon-upload.

--allow-dirlists {yes | no}
Controls whether directory list commands are enabled. The default value is Yes.

--revert-allow-dirlists
Sets the value to the system default for --allow-dirlists.

--allow-downloads {yes | no}
Controls whether files can be downloaded. The default value is Yes.

--revert-allow-downloads
Sets the value to the system default for --allow-downloads.

--allow-local-access {yes | no}
Controls whether local logins are permitted. If set to Yes, normal user accounts can be used to log in. The default value is Yes.

--revert-allow-local-access
Sets the value to the system default for --allow-local-access.

--allow-writes {yes | no}
Sets and displays whether commands that change the file system are permitted. Controls whether any of the following commands are allowed:
- STOR
- DELE
- RNFR
- RNTO
- MKD
- RMD
- APPE
- SITE
The default value is yes.
**--revert-allow-writes**
Sets the value to the system default for --allow-writes.

**--always-chdir-homedir {yes | no}**
Controls whether FTP always initially changes directories to the home directory of the user. If set to No, you can set up a chroot area in FTP without having a home directory for the user. The default value is Yes.

**--revert-always-chdir-homedir**
Sets the value to the system default for --always-chdir-homedir.

**--anon-chown-username <string>**
Gives ownership of anonymously uploaded files to the specified user. The value must be a local username. The default value is root.

**--revert-anon-chown-username**
Sets the value to the system default for --anon-chown-username.

**--anon-password-list <string>**
Displays the list of anonymous user passwords.

**--clear-anon-password-list**
Clears the list of passwords for anonymous users.

**--add-anon-password-list <string>**
Adds items to list of passwords for anonymous users. Specify --add-anon-password-list for each additional password to add.

**--remove-anon-password-list <string>**
Removes items from list of passwords for anonymous users. Specify --remove-anon-password-list for each additional password to remove.

**--revert-anon-password-list**
Sets the value to the system default for --anon-password-list.

**--anon-root-path <path>**
Displays and specifies the root path for anonymous users, which is a directory in /ifs that the Very Secure FTP Daemon (VSFTPD) will try to change to after an anonymous login. Valid paths are in /ifs. The default value is /ifs/home/ftp.

**--revert-anon-root-path**
Sets the value to the system default for --anon-root-path.

**--anon-umask <integer-octal>**
Specifies the umask for file creation by anonymous users. Valid values are octal umask numbers. The default value is 077.

Note
The value must contain the 0 prefix; otherwise it will be interpreted as a base 10 integer.

**--revert-anon-umask**
Sets the value to the system default for --anon-umask.

--ascii-mode {off | upload | download | both}
Enables ASCII downloads, uploads, or both.

--revert-ascii-mode
Sets the value to the system default for --ascii-mode.

--chroot-exception-list <string>
Displays the list of local user chroot exceptions.

--clear-chroot-exception-list
Clears the list of local user chroot exceptions.

--add-chroot-exception-list <string>
Adds users to the chroot exception list.

--remove-chroot-exception-list <string>
Removes users from the chroot exception list.

--revert-chroot-exception-list
Sets the value to the system default for --chroot-exception-list.

--chroot-local-mode {all | none | all-with-exceptions | none-with-exceptions}
Specifies which users are placed in a chroot jail in their home directory after login.

--revert-chroot-local-mode
Sets the value to the system default for --chroot-local-mode.

--connect-timeout <duration>
Specifies the timeout in seconds for a remote client to respond to a PORT style data connection. Valid durations are integers between 30 and 600. The default value is 60 (one minute).

--revert-connect-timeout
Sets the value to the system default for --connect-timeout.

--data-timeout <duration>
Specifies the maximum time (in seconds) data transfers are allowed to stall with no progress before the remote client is removed. Valid durations are integers between 30 and 600. The default value is 300 (five minutes).

--revert-data-timeout
Sets the value to the system default for --data-timeout.

--denied-user-list <string>
Displays the list of denied users.

--clear-denied-user-list
Clears the list of denied users.

--add-denied-user-list <string>
Add users to the list of denied users.
--remove-denied-user-list <string>
Removes users from the list of denied users.

--revert-denied-user-list
Sets the value to the system default for --denied-user-list (empty).

--dirlist-localtime {yes | no}
Specifies whether the time displayed in directory listings is in your local time zone. Valid values are Yes and No. If No, time displays on GMT. If Yes, the time displays in your local time zone. The default value is No. The last-modified times returned by commands issued inside of the FTP shell are also affected by this parameter.

--revert-dirlist-localtime
Sets the value to the system default for --dirlist-localtime.

--dirlist-names {numeric | textual | hide}
Determines what information is displayed about users and groups in directory listings. The following are valid:

  numeric
  Numeric IDs are shown in the user and group fields of directory listings.

  textual
  Names are shown in text format in the user and group fields of directory listings.

  hide
  All user and group information in directory listings is displayed as ftp. This is the default setting.

--revert-dirlist-names
Sets the value to the system default for --dirlist-names.

--file-create-perm <integer-octal>
Specifies the permissions with which uploaded files are created. Valid values are octal permission numbers. The default value is 0666.

Note
For uploaded files to be executable, set the permissions to 0777.

--revert-file-create-perm
Sets the value to the system default for --file-create-perm.

--limit-anon-passwords {yes | no}
Limits anonymous passwords.

--revert-limit-anon-passwords
Sets the value to the system default for --limit-anon-passwords.

--local-root-path <path>
Specifies the initial directory in /ifs for a local login. Valid paths are in /ifs. The default path is the local user home directory.
- **--revert-local-root-path**
  Sets the value to the system default for --local-root-path.

- **--local-umask <integer-octal>**
  Specifies the umask for file creation by local users. Valid values are octal umask numbers. The default value is 077.

  **Note**
  The value must contain the 0 prefix; otherwise it will be interpreted as a base 10 integer.

- **--revert-local-umask**
  Sets the value to the system default for --local-umask.

- **--server-to-server {yes | no}**
  Specifies whether to allow server-to-server (FXP) transfers. Valid values are Yes and No. The default value is No.

- **--revert-server-to-server**
  Sets the value to the system default for --server-to-server.

- **--session-support {yes | no}**
  Enables or disables FTP session support. If set to YES, the command maintains login sessions for each user through Pluggable Authentication Modules (PAM). If set to NO, the command prevents automatic home directory creation if that functionality is otherwise available. The default value is YES.

- **--revert-session-support**
  Sets the value to the system default for --session-support.

- **--session-timeout <duration>**
  Specifies the maximum time (in seconds) that a remote client may spend between FTP commands before the remote client is kicked off. Valid values are integers between 30 and 600. The default value is 300 (five minutes).

- **--revert-session-timeout**
  Sets the value to the system default for --session-timeout.

- **--user-config-dir <path>**
  Specifies the directory where user-specific configurations that override global configurations can be found. The default value is the local user home directory.

- **--revert-user-config-dir**
  Sets the value to the system default for --user-config-dir.

- **--service {yes | no}**
  Specifies whether the FTP service is enabled.
isi ftp settings view

Shows the FTP settings for the cluster.

Syntax

```
isi ftp settings view
```

Options

There are no options for this command.

Example

The following is an example of the output generated by this command:

```
Accept Timeout: 1m
Allow Anon Access: No
Allow Anon Upload: Yes
Allow Dirlists: Yes
Allow Downloads: Yes
Allow Local Access: Yes
Allow Writes: Yes
Always Chdir Homedir: Yes
Anon Chown Username: root
Anon Password List: -
   Anon Root Path: /ifs/home/ftp
   Anon Umask: 0077
   Ascii Mode: off
Chroot Exception List: -
   Chroot Local Mode: none
Connect Timeout: 1m
   Data Timeout: 5m
   Denied User List: -
   Dirlist Localtime: No
   Dirlist Names: hide
File Create Perm: 0666
Limit Anon Passwords: Yes
Local Root Path: -
   Local Umask: 0077
Server To Server: No
   Session Support: Yes
   Session Timeout: 5m
User Config Dir: -
FTP Service Enabled: No
```

HTTP and HTTPS

OneFS includes a configurable Hypertext Transfer Protocol (HTTP) service, which is used to request files that are stored on the cluster and to interact with the web administration interface.

OneFS supports both HTTP and its secure variant, HTTPS. Each node in the cluster runs an instance of the Apache HTTP Server to provide HTTP access. You can configure the HTTP service to run in different modes.

Both HTTP and HTTPS are supported for file transfer, but only HTTPS is supported for Platform API calls. The HTTPS-only requirement includes the web administration interface. In addition, OneFS supports a form of the web-based DAV (WebDAV) protocol that enables users to modify and manage files on remote web servers. OneFS performs distributed authoring, but does not support versioning and does not perform security checks. You can enable DAV in the web administration interface.
Enable and configure HTTP

You can configure HTTP and WebDAV to enable users to edit and manage files collaboratively across remote web servers.

You can use the `isi http settings modify` command to configure HTTP related settings.

**Procedure**

- Run the `isi http settings modify` command.

  The following command enables the HTTP service, WebDAV, and basic authentication:

  ```
  isi http settings modify --service=enabled --dav=yes basic-authentication=yes
  ```

Enable HTTPS through the Apache service

You can access an Isilon cluster through the Apache service over HTTPS.

**Procedure**

- To enable HTTPS, run the following command:

  ```
  isi_gconfig -t http-config https_enabled=true
  ```

**Results**

The HTTPS service is enabled.

**Note**

It might take up to 10 seconds for the configuration change to take effect. As a result, data transfers that are in progress over HTTP might be interrupted.

Disable HTTPS through the Apache service

You can disable access to an Isilon cluster through the Apache service over HTTPS.

**Procedure**

- To disable HTTPS, run the following command:

  ```
  isi_gconfig -t http-config https_enabled=false
  ```

**Results**

The HTTPS service is disabled.

**Note**

It might take up to 10 seconds for the configuration change to take effect. As a result, data transfers that are in progress over HTTP might be interrupted.
**isi http settings modify**

Modifies HTTP global settings.

**Syntax**

```plaintext
isi http settings modify
[--access-control {yes | no}]
[--basic-authentication {yes | no}]
[--dav {yes | no}]
[--enable-access-log {yes | no}]
[--integrated-authentication {yes | no}]
[--server-root <path>]
[--service {enabled | disabled | redirect}]
[--verbose]
```

**Options**

---**--access-control {yes | no}**

Enables access control authentication, which allows the Apache web server to perform access checks. Access control authentication requires at least one type of authentication to be enabled.

---**--basic-authentication {yes | no}**

Enables HTTP basic authentication. User credentials are sent in plain text format.

---**--dav {yes | no}**

Enables multiple users to manage and modify files collaboratively across web servers.

---**Note**

All DAV clients must go through a single node. DAV compliance is not met if you go through SmartConnect, or through two or more node IP addresses.

---**--enable-access-log {yes | no}**

Enables writing to a log when the HTTP server is accessed.

---**--integrated-authentication {yes | no}**

Enables integrated authentication via NTLM, Kerberos, or both.

---**--server-root <path>**

Specifies the root document directory. This must be a valid directory path within /ifs.

---**--service {enabled | disabled | redirect}**

Enables or disables the HTTP service, or redirects to the OneFS web UI.

---**--verbose | -v**

Displays more detailed information.
isi http settings view

Displays HTTP global settings.

Syntax

isi http settings view

Options

There are no options for this command.

Example

The following example shows the output generated by this command:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>No</td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>No</td>
</tr>
<tr>
<td>Dav</td>
<td>No</td>
</tr>
<tr>
<td>Enable Access Log</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated Authentication</td>
<td>No</td>
</tr>
<tr>
<td>Server Root</td>
<td>/ifs</td>
</tr>
<tr>
<td>Service</td>
<td>redirect</td>
</tr>
</tbody>
</table>


File sharing
CHAPTER 12

File filtering

This section contains the following topics:

- File filtering in an access zone ................................................................. 548
- Enable and configure file filtering in an access zone ................................ 548
- Disable file filtering in an access zone ................................................... 548
- View file filtering settings ...................................................................... 549
- File filtering commands ......................................................................... 549
File filtering in an access zone

In an access zone, you can use file filtering to allow or deny file writes based on file type.

If some file types might cause throughput issues, security problems, storage clutter, or productivity disruptions on your EMC Isilon cluster, or if your organizations must adhere to specific file policies, you can restrict writes to specified file types or only allow writes to a specified list of file types. When you enable file filtering in an access zone, OneFS applies file filtering rules only to files in that access zone.

- If you choose to deny file writes, you can specify file types by extension that are not allowed to be written. OneFS permits all other file types to be written.
- If you choose to allow file writes, you can specify file types by extension that are allowed to be written. OneFS denies all other file types to be written.

OneFS does not take into consideration which file sharing protocol was used to connect to the access zone when applying file filtering rules; however, you can apply additional file filtering at the SMB share level. See "SMB file filtering" in the File sharing chapter of this guide.

Enable and configure file filtering in an access zone

You can enable file filtering per access zone and specify which file types users are denied or allowed write access to within the access zone.

Procedure

1. Run the `isi file-filter settings modify` command.

   The following command enables file filtering in the zone3 access zone and allows users to write only to specific file types:

   ```
   isi file-filter settings modify --zone=zone3 \
   file-filtering-enabled=yes file-filter-type=allow \
   file-filter-extensions=.xml,.html,.txt
   ```

   File types are designated by their extension and should start with a "." such as `.txt`.

   The following command enables file filtering in zone3 and denies users write access only to specific file types:

   ```
   isi file-filter settings modify --zone=zone3 \
   file-filtering-enabled=yes file-filter-type=deny \
   file-filter-extensions=.xml,.html,.txt
   ```

Disable file filtering in an access zone

You can disable file filtering per access zone. Previous settings that specify filter type and file type extensions are preserved but no longer applied.

Procedure

1. Run the `isi file-filter settings modify` command.
The following command disables file filtering in the zone3 access zone:

```
isi file-filter settings modify --zone=zone3 \
  file-filtering-enabled=no
```

### View file filtering settings

You can view file filtering settings in an access zone.

#### Procedure

1. Run the `isi file-filter settings view` command.

   The following command displays file filtering settings in the zone3 access zone:

   ```
   isi file-filter settings view --zone=zone3
   ```

   The system displays output similar to the following example:

   ```
   File Filtering Enabled: Yes
   File Filter Extensions: xml, html, txt
   File Filter Type: deny
   ```

### File filtering commands

You can run file filtering commands to allow or deny file writes based on file type within an access zone.

#### `isi file-filter settings modify`

Modifies file filtering settings in an access zone.

#### Syntax

```
isi file-filter settings modify
  [--file-filtering-enabled {yes | no}]
  [--revert-file-filtering-enabled]
  [--file-filter-extensions <string>...]
  [--clear-file-filter-extensions]
  [--add-file-filter-extensions <string>]
  [--remove-file-filter-extensions <string>]
  [--revert-file-filter-extensions]
  [--file-filter-type {allow | deny}]
  [--revert-file-filter-type]
  [--zone <string>]
  [--verbose]
```

#### Options

- `--file-filtering-enabled {yes | no}`
  Enables or disables file filtering in the access zone. File filtering is disabled by default.

- `--revert-file-filtering-enabled`
  Sets the value of `--file-filtering-enabled` to the system default value.
--file-filter-extensions <string>...
   Specifies a list of file types by their extensions. Each extension should start with a
   "." such as .txt. You can specify multiple extensions in a comma-separated list
   or you run --file-filter-extensions for each extension.

--clear-file-filter-extensions
   Deletes the entire list of file filter extensions.

--add-file-filter-extensions <string>
   Adds one or more file filter extensions to the list. Each extension should start with
   a "." such as .txt. You can specify multiple extensions in a comma-separated list
   or you run --add-file-filter-extensions for each extension.

--remove-file-filter-extensions <string>
   Removes one or more file filter extensions from the list. Each extension should
   start with a "." such as .txt. You can specify multiple extensions in a comma-
   separated list or you run --remove-file-filter-extensions for each extension.

--revert-file-filter-extensions
   Sets the value of --file-filter-extensions to the system default value.

--file-filter-type {allow | deny}
   Specifies whether the file types in the extensions list will be allowed or denied
   write access. The default filter type is deny.

--revert-file-filter-type
   Sets the value of --revert-file-filter-type to the system default value.

--zone <string>
   Specifies the access zone to which the settings apply. If you do not specify a
   zone, the settings are applied to the System zone.

{--verbose | -v}
   Displays more detailed information.

isi file-filter settings view

Displays file filtering settings for an access zone.

Syntax

```
isi file-filter settings view
   [--zone <string>]
   [--format {list | json}]
```

Options

--zone
   Specifies the name of the access zone. If you do not specify an access zone, the
   system will display the file filtering settings of the System zone.

--format {list | json}
Specifies whether to display the output as a list (default) or in JavaScript Object Notation (JSON).
File filtering
This section contains the following topics:

- Auditing overview .............................................................. 554
- Syslog .................................................................................. 554
- Protocol audit events .......................................................... 555
- Supported event types .......................................................... 555
- Supported audit tools ........................................................... 556
- Sample audit log ................................................................. 557
- Managing audit settings ...................................................... 558
- Integrating with the EMC Common Event Enabler ................. 561
- Auditing commands ........................................................... 563
Auditing overview

You can audit system configuration changes and protocol activity on an EMC Isilon cluster. All audit data is stored and protected in the cluster file system and organized by audit topics.

Auditing can detect many potential sources of data loss, including fraudulent activities, inappropriate entitlements, and unauthorized access attempts. Customers in industries such as financial services, health care, life sciences, and media and entertainment, as well as in governmental agencies, must meet stringent regulatory requirements developed to protect against these sources of data loss.

System configuration auditing tracks and records all configuration events that are handled by the application programming interface (API) through the command-line interface (CLI). When you enable system configuration auditing, no additional configuration is required. System configuration auditing events are stored in the config audit topic directories.

Protocol auditing tracks and stores activity performed through SMB, NFS, and HDFS protocol connections. You can enable and configure protocol auditing for one or more access zones in a cluster. If you enable protocol auditing for an access zone, file-access events through the SMB, NFS, and HDFS protocols are recorded in the protocol audit topic directories. You can specify which events to log in each access zone. For example, you might want to audit the default set of protocol events in the System access zone but audit only successful attempts to delete files in a different access zone.

The audit events are logged on the individual nodes where the SMB, NFS, or HDFS client initiated the activity. The events are then stored in a binary file under /ifs/.ifsvar/audit/logs. The logs automatically roll over to a new file after the size reaches 1 GB.

The protocol audit log file is consumable by auditing applications that support the EMC Common Event Enabler (CEE).

Syslog

Syslog is a protocol that is used to convey certain event notification messages. You can configure an Isilon cluster to log audit events and forward them to syslog by using the syslog forwarder.

By default, all protocol events that occur on a particular node are forwarded to the /var/log/audit_protocol.log file, regardless of the access zone the event originated from.

Syslog is configured with an identity of audit_protocol, a facility of syslog, and a priority level of info.

To configure auditing on an Isilon cluster, you must either be a root user or you must be assigned to an administrative role that includes auditing privileges (ISI_PRIV_AUDIT).

Syslog forwarding

The syslog forwarder is a daemon that, when enabled, retrieves configuration changes and protocol audit events in an access zone and forwards the events to syslog. Only
user-defined audit success and failure events are eligible for being forwarded to syslog.

On each node there is an audit syslog forwarder daemon running that will log audit events to the same node's syslog daemon.

**Protocol audit events**

By default, audited access zones track only certain events on the EMC Isilon cluster, including successful and failed attempts to access files and directories.

The default tracked events are create, close, delete, rename, and set_security.

The names of generated events are loosely based on the Windows I/O request packet (IRP) model in which all operations begin with a create event to obtain a file handle. A create event is required before all I/O operations, including the following: close, create, delete, get_security, read, rename, set_security, and write. A close event marks when the client is finished with the file handle that was produced by a create event.

These internally stored events are translated to events that are forwarded through the EMC CEE to the auditing application. The EMC CEE export facilities on OneFS perform this mapping. The EMC CEE can be used to connect to any third party application that supports the EMC CEE.

---

**Note**

The EMC CEE does not support forwarding HDFS protocol events to a third-party application.

Different SMB, NFS, and HDFS clients issue different requests, and one particular version of a platform such as Windows or Mac OS X using SMB might differ from another. Similarly, different versions of an application such as Microsoft Word or Windows Explorer might make different protocol requests. For example, a client with a Windows Explorer window open might generate many events if an automatic or manual refresh of that window occurs. Applications issue requests with the logged-in user's credentials, but you should not assume that all requests are purposeful user actions.

When enabled, OneFS audit will track all changes that are made to the files and directories in SMB shares, NFS exports, and HDFS data.

**Supported event types**

You can view or modify the event types that are audited in an access zone.

For the most current list of supported auditing tools, see the Isilon Third-Party Software & Hardware Compatibility Guide.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Example protocol activity</th>
<th>Audited by default</th>
<th>Can be exported through CEE</th>
<th>Cannot be exported through CEE</th>
</tr>
</thead>
</table>
| create     | • Create a file or directory  
• Open a file, directory, or share | X                  | X                           | X                            |
### Supported audit tools

You can configure OneFS to send protocol auditing logs to servers that support the EMC Common Event Enabler (CEE).

CEE has been tested and verified to work on several third-party software vendors. For the most current list of supported auditing tools, see the Isilon Third-Party Software & Hardware Compatibility Guide.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Example protocol activity</th>
<th>Audited by default</th>
<th>Can be exported through CEE</th>
<th>Cannot be exported through CEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>close</td>
<td>- Close a directory&lt;br&gt;- Close a modified or unmodified file</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>rename</td>
<td>Rename a file or directory</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>delete</td>
<td>Delete a file or directory</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>set_security</td>
<td>Attempt to modify file or directory permissions</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>read</td>
<td>The first read request on an open file handle</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>write</td>
<td>The first write request on an open file handle</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>close</td>
<td>The client is finished with an open file handle</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>get_security</td>
<td>The client reads security information for an open file handle</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>logon</td>
<td>SMB session create request by a client</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>logoff</td>
<td>SMB session logoff</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>tree_connect</td>
<td>SMB first attempt to access a share</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
We recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, the large backlog consumed by this feature may cause results to not be updated for a considerable amount of time.

Sample audit log

You can view both configuration audit and protocol audit logs by running the `isi_audit_viewer` command on any node in the Isilon cluster.

You can view protocol access audit logs by running `isi_audit_viewer -t protocol`. You can view system configuration logs by running `isi_audit_viewer -t config`. The following output is an example of a system configuration log:

```
[0: Fri Jan 23 16:17:03 2015] {"id": "524e0928-a35e-11e4-9d0c-005056302134", "timestamp": 1422058623106323, "payload": "PAPI config logging started."}  
[2: Fri Jan 23 16:17:05 2015] {"id": "5249b99d-a35e-11e4-9d0c-005056302134", "timestamp": 1422058625144567, "payload": {"status": 201, "statusmsg": "Created", "body": {"id": "Test"}}}  
[4: Fri Jan 23 16:17:39 2015] {"id": "67e7ca62-a35e-11e4-9d0c-005056302134", "timestamp": 1422058659387928, "payload": {"status": 204, "statusmsg": "No Content", "body": {}}}  
```

Events come in pairs; a **pre event** is logged before the command is carried out and a **post event** is logged after the event is triggered. These events can be correlated by matching the `id` field. In the above logs, events 1 and 2 are paired, and events 3 and 4 are paired.

The pre event always comes first, and contains user token information, the PAPI path, and whatever arguments were passed to the PAPI call. In event 1, a POST request was made to `/1/protocols/smb/shares` with arguments `path=/ifs/data` and `name=Test`. The post event contains the HTTP return status and any output returned from the server.
Managing audit settings

You can enable and disable system configuration and protocol access audit settings, in addition to configuring integration with the EMC Common Event Enabler.

Enable protocol access auditing

You can audit SMB, NFS, and HDFS protocol access to generate events on a per-access zone basis and forward the events to the EMC Common Event Enabler (CEE) for export to third-party products.

Note

Because each audited event consumes system resources, we recommend that you only configure zones for events that are needed by your auditing application. In addition, we recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, the large backlog performed by this feature may cause results to not be updated for a considerable amount of time. Additionally, you can manually configure the time that you want audit events to be forwarded by running the `isi audit settings global modify --cee-log-time` command.

Procedure

1. Run the `isi audit settings global modify` command.
   The following command enables auditing of protocol access events in the zone3 and zone5 access zones, and forwards logged events to a CEE server:

   ```
   isi audit settings global modify --protocol-auditing-enabled=yes \  
   --cee-server-uris=http://sample.com:12228/cee \  
   --hostname=cluster.domain.com --audited-zones=zone3,zone5
   ```

   OneFS logs audited protocol events to a binary file within `/ifs/.ifsvar/audit/logs`. The CEE service forwards the logged events through an HTTP PUT operation to a defined endpoint.

After you finish

You can modify the types of protocol access events to be audited by running the `isi audit settings modify` command. You can also enable forwarding of protocol access events to syslog by running the `isi audit settings modify` command with the `--syslog-forwarding-enabled` option.

Forward protocol access events to syslog

You can enable or disable forwarding of audited protocol access events to syslog in each access zone. Forwarding is not enabled by default when protocol access auditing is enabled. This procedure is available only through the command-line interface.

Before you begin

To enable forwarding of protocol access events in an access zone, you must first enable protocol access auditing in the access zone.

The `--audit-success` and `--audit-failure` options define the event types that are audited, and the `--syslog-audit-events` option defines the event types that
are forwarded to syslog. Only the audited event types are eligible for forwarding to syslog. If syslog forwarding is enabled, protocol access events are written to the `/var/log/audit_protocol.log` file.

**Procedure**

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings modify` command with the `--syslog-forwarding-enabled` option to enable or disable audit syslog.

   The following command enables forwarding of the audited protocol access events in the zone3 access zone and specifies that the only event types forwarded are close, create, and delete events:

   ```
   isi audit settings modify --syslog-forwarding-enabled=yes --syslog-audit-events=close,create,delete --zone=zone3
   ```

   The following command disables forwarding of audited protocol access events from the zone3 access zone:

   ```
   isi audit settings modify --syslog-forwarding-enabled=no --zone=zone3
   ```

**Enable system configuration auditing**

OneFS can audit system configuration events on your Isilon cluster. When enabled, OneFS records all system configuration events that are handled by the platform API including writes, modifications, and deletions. System configuration change logs are populated in the config topic in the audit back-end store under `/ifs/.ifsvar/audit`.

**Note**

Configuration events are not forwarded to the Common Event Enabler (CEE).

**Procedure**

1. Run the `isi audit settings global modify` command.

   The following command enables system configuration auditing on the cluster:

   ```
   isi audit settings global modify --config-auditing-enabled=yes
   ```

**After you finish**

You can enable forwarding of system configuration changes to syslog by running the `isi audit settings global modify` command with the `--config-syslog-enabled` option.
Forward system configuration changes to syslog

You can enable or disable forwarding of system configuration changes on the EMC Isilon cluster to syslog, which is saved to /var/log/audit_config.log. This procedure is available only through the command-line interface.

Before you begin

Forwarding is not enabled by default when system configuration auditing is enabled. To enable forwarding of system configuration changes to syslog, you must first enable system configuration auditing on the cluster.

Procedure

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings global modify` command with the `--config-syslog-enabled` option to enable or disable forwarding of system configuration changes.

   The following command enables forwarding of system configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=yes
   ```

   The following command disables forwarding of system configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=no
   ```

Configure protocol event filters

You can filter the types of protocol access events to be audited in an access zone. You can create filters for successful events and failed events. The following protocol events are collected for audited access zones by default: create, delete, rename, and set_security. This procedure is available only through the command-line interface.

Before you begin

To create protocol event filters, you should first enable protocol access auditing in the access zone.

Procedure

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings modify` command

   The following command creates a filter that audits the failure of create, close, and delete events in the zone3 access zone:

   ```
   isi audit settings modify --audit-failure=create,close,delete --zone=zone3
   ```

   The following command creates a filter that audits the success of create, close, and delete events in the zone5 access zone:

   ```
   isi audit settings modify --audit-success=create,close,delete --zone=zone5
   ```
Integrating with the EMC Common Event Enabler

OneFS integration with the EMC Common Event Enabler (CEE) enables third-party auditing applications to collect and analyze protocol auditing logs.

For the most current list of supported auditing tools, see the Isilon Third-Party Software & Hardware Compatibility Guide.

OneFS supports the Common Event Publishing Agent (CEPA) component of CEE for Windows. For integration with OneFS, you must install and configure CEE for Windows on a supported Windows client.

Note

We recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, the large backlog performed by this feature may cause results to not be updated for a considerable time.

Install CEE for Windows

To integrate CEE with OneFS, you must first install CEE on a computer that is running the Windows operating system.

Before you begin

Be prepared to extract files from the .iso file, as described in the following steps. If you are not familiar with the process, consider choosing one of the following methods:

1. Install WinRAR or another suitable archival program that can open .iso files as an archive, and copy the files.
2. Burn the image to a CD-ROM, and then copy the files.
3. Install SlySoft Virtual CloneDrive, which allows you to mount an ISO image as a drive that you can copy files from.

Note

You should install a minimum of two servers. We recommend that you install CEE 6.6.0 or later.

Procedure

1. Download the CEE framework software from EMC Online Support:
   a. In a web browser, go to https://support.emc.com/search/.
   b. In the search field, type Common Event Enabler for Windows, and then click the Search icon.
   c. Click Common Event Enabler <Version> for Windows, where <Version> is 6.2 or later, and then follow the instructions to open or save the .iso file.
2. From the .iso file, extract the 32-bit or 64-bit EMC_CEE_Pack executable file that you need.
   After the extraction completes, the EMC Common Event Enabler installation wizard opens.
3. Click Next to proceed to the License Agreement page.
4. Select the I accept... option to accept the terms of the license agreement, and then click Next.
5. On the Customer Information page, type your user name and organization, select your installation preference, and then click Next.

6. On the Setup Type page, select Complete, and then click Next.

7. Click Install to begin the installation.

The Installing EMC Common Event Enabler page displays the progress of the installation. When the installation is complete, the InstallShield Wizard Completed page appears.

8. Click Finish to exit the wizard.

9. Restart the system.

Configure CEE for Windows

After you install CEE for Windows on a client computer, you must configure additional settings through the Windows Registry Editor (regedit.exe).

Procedure

1. Open the Windows Registry Editor.

2. Configure the following registry keys, if supported by your audit application:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Registry location</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEE HTTP listen port</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE \Configuration]</td>
<td>HttpPort</td>
<td>12228</td>
</tr>
<tr>
<td>Enable audit remote endpoints</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE \CEPP\Audit\Configuration]</td>
<td>Enabled</td>
<td>1</td>
</tr>
<tr>
<td>Audit remote endpoints</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE \CEPP\Audit\Configuration]</td>
<td>EndPoint</td>
<td>&lt;EndPoint&gt;</td>
</tr>
</tbody>
</table>

Note

- The HttpPort value must match the port in the CEE URIs that you specify during OneFS protocol audit configuration.
- The EndPoint value must be in the format `<EndPoint_Name>@<IP_Address>`. You can specify multiple endpoints by separating each value with a semicolon (;).

The following key specifies a single remote endpoint:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit \Configuration] EndPoint = AuditApplication@10.7.1.2
```

The following key specifies multiple remote endpoints:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit \Configuration] EndPoint =
    AuditApplication@192.168.22.3;AuditApplication@192.168.33.2
```

3. Close the Windows Registry Editor.
Auditing commands

You can audit system configuration events and SMB, NFS, and HDFS protocol access events on the EMC Isilon cluster. All audit data is stored in files called audit topics, which collect log information that you can process further with auditing tools for Windows.

isi audit settings global modify

Enables or disables global auditing configuration changes and protocol access, and configures additional protocol-auditing settings on an EMC Isilon cluster.

Syntax

```
isi audit settings global modify
    [--protocol-auditing-enabled {yes | no}]
    [--audited-zones <zones>]
    [--clear-audited-zones]
    [--add-audited-zones <zones>]
    [--remove-audited-zones <zones>]
    [--cee-server-uris <uris>]
    [--clear-cee-server-uris]
    [--add-cee-server-uris <uris>]
    [--remove-cee-server-uris <uris>]
    [--hostname <string>]
    [--config-auditing-enabled {yes | no}]
    [--config-syslog-enabled {yes | no}]
    [--cee-log-time <string>]
    [--sys-log-time <string>]
    [--verbose]
```

Options

--protocol-auditing-enabled {yes | no}
Enables or disables the auditing of data-access requests through the SMB, NFS, and HDFS protocols.

--audited-zones <access zones>
Specifies one or more access zones, separated by commas, which will be audited if protocol auditing is enabled. This option overwrites all entries in the list of access zones; to add or remove access zones without affecting current entries, use --add-audited-zones or --remove-audited-zones.

--clear-audited-zones
Clears the entire list of access zones to be audited if protocol auditing is enabled.

--add-audited-zones <access zones>
Adds one or more access zones, separated by commas, to the list of zones that will be audited if protocol auditing is enabled.

--remove-audited-zones <access zones>
Removes one or more access zones, separated by commas, which will be audited if protocol auditing is enabled.

--cee-server-uris <uris>
Specifies one or more CEE server URIs, separated by commas, where audit logs will be forwarded if protocol auditing is enabled. The OneFS CEE export service uses round robin load-balancing when exporting events to multiple CEE servers. This option overwrites all entries in the list of CEE server URIs. To add or remove URIs without affecting current entries, use \texttt{--add-cee-server-uris} or \texttt{--remove-cee-server-uris}.

\texttt{--clear-cee-server-uris}
Clears the entire list of CEE server URIs to which audit logs are forwarded if protocol auditing is enabled.

\texttt{--add-cee-server-uris <uris>}
Adds one or more CEE server URIs, separated by commas, to the list of URIs where audit logs are forwarded if protocol auditing is enabled.

\texttt{--remove-cee-server-uris <uris>}
Removes one or more CEE server URIs, separated by commas, from the list of URIs where audit logs are forwarded if protocol auditing is enabled.

\texttt{--hostname <string>}
Specifies the name of the storage cluster to use when forwarding protocol events—typically, the SmartConnect zone name. When SmartConnect is not implemented, the value must match the hostname of the cluster as your third-party audit application recognizes it. If the field is left blank, events from each node are filled with the node name (clustername + inn). This setting is required only if needed by your third-party audit application.

\texttt{--config-auditing-enabled \{yes | no\}}
Enables or disables the auditing of requests made through the API for system configuration changes.

\texttt{--config-syslog-enabled \{yes | no\}}
Enables or disables the forwarding of system configuration changes to syslog.

\texttt{--cee-log-time <date>}
Specifies a date after which the audit CEE forwarder will forward protocol access logs. Specify \texttt{<date>} in the following format:

\begin{verbatim}
[protocol]@<YYYY>-<MM>-<DD> <HH>:<MM>:<SS>
\end{verbatim}

\texttt{--syslog-log-time <date>}
Specifies a date after which the audit syslog forwarder will forward logs. To forward SMB, NFS, and HDFS traffic logs, specify \texttt{protocol}. To forward configuration change logs, specify \texttt{config}. Specify \texttt{<date>} in the following format:

\begin{verbatim}
[protocol|config]@<YYYY>-<MM>-<DD> <HH>:<MM>:<SS>
\end{verbatim}

\{\texttt{--verbose | -v}\}
Displays the results of running the command.
isi audit settings global view
Displays global audit settings configured on the EMC Isilon cluster.

Syntax

```bash
isi audit settings global view
```

Options
There are no options for this command.

Examples
The following command displays the audit settings configured on the cluster:

```bash
isi audit settings global view
```

The system displays output similar to the following text:

```
Protocol Auditing Enabled: Yes
Audited Zones: System, zoneA
CEE Server URIs: http://example.com:12228/cee
Hostname: mycluster
Config Auditing Enabled: Yes
Config Syslog Enabled: Yes
```

isi audit settings modify
Enables you to set filters within an access zone for protocol event types that fail or succeed in an access zone, and to specify which event types to forward to syslog.

Syntax

```bash
isi audit settings modify
[--audit-failure <event types>]
[--clear-audit-failure]
[--add-audit-failure <event types>]
[--remove-audit-failure <event types>]
[--audit-success <event types>]
[--clear-audit-success]
[--add-audit-success <event types>]
[--remove-audit-success <event types>]
[--syslog-audit-events <event types>]
[--clear-syslog-audit-events]
[--add-syslog-audit-events <event types>]
[--remove-syslog-audit-events <event types>]
[--syslog-forwarding-enabled {yes | no}]
[--zone <access zone>]
[--verbose]
```

Options

```bash
--audit-failure <event types>
```

Specifies one or more filters, separated by commas, for auditing protocol event types that failed. The following event types are valid:
- close
- create
- delete
- get_security
- logoff
- logon
- read
- rename
- set_security
- tree_connect
- write
- all

This option overwrites the current list of filtered event types. To add or remove filters without affecting the current list, configure settings with `--add-audit-failure` or `--remove-audit-failure`.

`--clear-audit-failure`
Clears all filters for auditing protocol event types that failed.

`--add-audit-failure <event types>`
Adds one or more filters, separated by commas, for auditing protocol event types that failed. Valid event type values are the same as for `--audit-failure`.

`--remove-audit-failure <event types>`
Removes one or more filters, separated by commas, for auditing protocol event types that failed. Valid event type values are the same as for `--audit-failure`.

`--audit-success <event types>`
Specifies one or more filters, separated by commas, for auditing protocol event types that succeeded. The following event types are valid:

- close
- create
- delete
- get_security
- logoff
- logon
- read
- rename
- set_security
- tree_connect
- write
- all
This option overwrites the current list of filtered event types. To add or remove filters without affecting the current list, configure settings with \(--add-audit-success\) or \(--remove-audit-success\).

\(--clear-audit-success\)
Clears all filters for auditing protocol event types that succeeded.

\(--add-audit-success \ <event types>\)
Adds one or more filters, separated by commas, for auditing protocol event types that succeeded. Valid event type values are the same as for \(--audit-success\).

\(--remove-audit-success \ <event types>\)
Removes one or more filters, separated by commas, for auditing protocol event types that succeeded. Valid event type values are the same as for \(--audit-success\).

\(--syslog-audit-events \ <event types>\)
Specifies the auditing protocol event types to forward to syslog. You can only specify event types that are currently being filtered by the \(--audit-success\) and \(--audit-failure\) options. The following event types are valid:
- close
- create
- delete
- get_security
- logoff
- logon
- read
- rename
- set_security
- tree_connect
- write
- all
This option overwrites the current list of forwarded event types. To add or remove event types without affecting the current list, configure settings with \(--add-syslog-audit-events\) or \(--remove-syslog-audit-events\).

\(--clear-syslog-audit-events\)
Clears all auditing protocol event types that are forwarded to syslog.

\(--add-syslog-audit-events \ <event types>\)
Adds one or more auditing protocol event types, separated by commas, that are forwarded to syslog. Valid event type values are the same as for \(--syslog-audit-events\).

\(--remove-syslog-audit-events \ <event types>\)
Removes one or more auditing protocol event types, separated by commas, that are forwarded to syslog. Valid event type values are the same as for \(--syslog-audit-events\).

\(--syslog-forwarding-enabled \ {yes | no}\)
Enables or disables syslog forwarding audit events in the specified access zone.

```bash
--zone <access zones>
```

Specifies the access zone to which event type filters are applied or forwarded to syslog.

```bash
{--verbose | -v}
```

Displays the results of running the command.

---

**Note**

Each audited event consumes system resources; you should only log events that are supported by your auditing application.

---

**isi audit settings view**

Displays audit filter settings in an access zone and whether syslog forwarding is enabled.

**Syntax**

```bash
isi audit settings view
   [--zone <access zone>]
   [--verbose]
```

**Options**

```bash
--zone <access zone>
```

Specifies the name of the access zone to view.

There are no options for this command.

**Examples**

The following command displays the audit settings configured in the zoneA access zone:

```bash
isi audit settings view --zone=zoneA
```

The system displays output similar to the following text:

```
Audit Failure: create, delete, rename, set_security, close
Audit Success: create, delete, rename, set_security, close
Syslog Audit Events: close
Syslog Forwarding Enabled: No
```
**isi audit topics list**

Displays a list of configured audit topics, which are internal collections of audit data.

**Syntax**

```
isi audit topics list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

```
|--limit | -l | integer>
  Displays no more than the specified number of items.

|--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-
  separated value (CSV), or list format.

|--no-header | -a
  Displays table and CSV output without headers.

|--no-footer | -z
  Displays table output without footers.

|--verbose | -v
  Displays more detailed information.
```

**isi audit topics modify**

Modifies the properties of an audit topic.

**Syntax**

```
isi audit topics modify <name>
    [--max-cached-messages <integer>]
    [--verbose]
```

**Options**

```
<name>
  Specifies the name of the audit topic to modify. Valid values are protocol and
  config.

|--max-cached-messages <integer>
  Specifies the maximum number of audit messages to cache before writing them
  to a persistent store. The larger the number, the more efficiently audit events can
  be processed. If you specify 0, each audit event is sent synchronously.
```
{--verbose | -v}

Displays the results of running the command.

**isi audit topics view**

Displays the properties of an audit topic.

**Syntax**

```
isi audit topics view <name>
```

**Options**

`<name>`

Specifies the name of the audit topic whose properties you want to view. Valid values are `protocol` and `config`.
CHAPTER 14
Snapshots

This section contains the following topics:

- Snapshots overview ................................................................. 572
- Data protection with SnapshotIQ ..................................................... 572
- Snapshot disk-space usage ............................................................. 572
- Snapshot schedules .......................................................................... 573
- Snapshot aliases ............................................................................... 573
- File and directory restoration ............................................................. 573
- Best practices for creating snapshots ............................................... 574
- Best practices for creating snapshot schedules .................................. 574
- File clones ........................................................................................ 575
- Snapshot locks ............................................................................... 576
- Snapshot reserve ............................................................................. 577
- SnapshotIQ license functionality ..................................................... 577
- Creating snapshots with SnapshotIQ................................................. 577
- Managing snapshots ......................................................................... 582
- Restoring snapshot data .................................................................... 585
- Managing snapshot schedules ........................................................ 587
- Managing snapshot aliases ............................................................... 588
- Managing with snapshot locks ......................................................... 590
- Configure SnapshotIQ settings ....................................................... 592
- Set the snapshot reserve ................................................................. 594
- Managing changelists ....................................................................... 594
- Snapshot commands ......................................................................... 596
Snapshots overview

A OneFS snapshot is a logical pointer to data that is stored on a cluster at a specific point in time.

A snapshot references a directory on a cluster, including all data stored in the directory and its subdirectories. If the data referenced by a snapshot is modified, the snapshot stores a physical copy of the data that was modified. Snapshots are created according to user specifications or are automatically generated by OneFS to facilitate system operations.

To create and manage snapshots, you must activate a SnapshotIQ license on the cluster. Some applications must generate snapshots to function but do not require you to activate a SnapshotIQ license; by default, these snapshots are automatically deleted when OneFS no longer needs them. However, if you activate a SnapshotIQ license, you can retain these snapshots. You can view snapshots generated by other modules without activating a SnapshotIQ license.

You can identify and locate snapshots by name or ID. A snapshot name is specified by a user and assigned to the virtual directory that contains the snapshot. A snapshot ID is a numerical identifier that OneFS automatically assigns to a snapshot.

Data protection with SnapshotIQ

You can create snapshots to protect data with the SnapShotIQ software module. Snapshots protect data against accidental deletion and modification by enabling you to restore deleted and modified files. To use SnapshotIQ, you must activate a SnapshotIQ license on the cluster.

Snapshots are less costly than backing up your data on a separate physical storage device in terms of both time and storage consumption. The time required to move data to another physical device depends on the amount of data being moved, whereas snapshots are always created almost instantaneously regardless of the amount of data referenced by the snapshot. Also, because snapshots are available locally, end-users can often restore their data without requiring assistance from a system administrator. Snapshots require less space than a remote backup because unaltered data is referenced rather than recreated.

Snapshots do not protect against hardware or file-system issues. Snapshots reference data that is stored on a cluster, so if the data on the cluster becomes unavailable, the snapshots will also be unavailable. Because of this, it is recommended that you back up your data to separate physical devices in addition to creating snapshots.

Snapshot disk-space usage

The amount of disk space that a snapshot consumes depends on both the amount of data stored by the snapshot and the amount of data the snapshot references from other snapshots.

Immediately after OneFS creates a snapshot, the snapshot consumes a negligible amount of disk space. The snapshot does not consume additional disk space unless the data referenced by the snapshot is modified. If the data that a snapshot references is modified, the snapshot stores read-only copies of the original data. A snapshot consumes only the space that is necessary to restore the contents a directory to the state it was in when the snapshot was taken.
To reduce disk-space usage, snapshots that reference the same directory reference each other, with older snapshots referencing newer snapshots. If a file is deleted, and several snapshots reference the file, a single snapshot stores a copy the file, and the other snapshots reference the file from the snapshot that stored the copy. The reported size of a snapshot reflects only the amount of data stored by the snapshot and does not include the amount of data referenced by the snapshot.

Because snapshots do not consume a set amount of storage space, there is no available-space requirement for creating a snapshot. The size of a snapshot grows according to how the data referenced by the snapshot is modified. A cluster cannot contain more than 20,000 snapshots.

**Snapshot schedules**

You can automatically generate snapshots according to a snapshot schedule.

With snapshot schedules, you can periodically generate snapshots of a directory without having to manually create a snapshot every time. You can also assign an expiration period that determines when SnapshotIQ deletes each automatically generated snapshot.

**Snapshot aliases**

A snapshot alias is a logical pointer to a snapshot. If you specify an alias for a snapshot schedule, the alias will always point to the most recent snapshot generated by that schedule. Assigning a snapshot alias allows you to quickly identify and access the most recent snapshot generated according to a snapshot schedule.

If you allow clients to access snapshots through an alias, you can reassign the alias to redirect clients to other snapshots. In addition to assigning snapshot aliases to snapshots, you can also assign snapshot aliases to the live version of the file system. This can be useful if clients are accessing snapshots through a snapshot alias, and you want to redirect the clients to the live version of the file system.

**File and directory restoration**

You can restore the files and directories that are referenced by a snapshot alias by copying data from the snapshot, cloning a file from the snapshot, or reverting the entire snapshot.

Copying a file from a snapshot duplicates the file, which roughly doubles the amount of storage space consumed. Even if you delete the original file from the non-snapshot directory, the copy of the file remains in the snapshot.

Cloning a file from a snapshot also duplicates the file. However, unlike a copy, which immediately consumes additional space on the cluster, a clone does not consume any additional space on the cluster unless the clone or cloned file is modified.

Reverting a snapshot replaces the contents of a directory with the data stored in the snapshot. Before a snapshot is reverted, SnapshotIQ creates a snapshot of the directory that is being replaced, which enables you to undo the snapshot revert later. Reverting a snapshot can be useful if you want to undo a large number of changes that you made to files and directories. If new files or directories have been created in a directory since a snapshot of the directory was created, those files and directories are deleted when the snapshot is reverted.
Best practices for creating snapshots

Consider the following snapshot best practices when working with a large number of snapshots.

It is recommended that you do not create more than 1,000 snapshots of a single directory to avoid performance degradation. If you create a snapshot of a root directory, that snapshot counts towards the total number of snapshots for any subdirectories of the root directory. For example, if you create 500 snapshots of "/ifs/data" and 500 snapshots of "/ifs/data/media", you have created 1,000 snapshots of "/ifs/data/media". Avoid creating snapshots of directories that are already referenced by other snapshots.

It is recommended that you do not create more than 1,000 hard links per file in a snapshot to avoid performance degradation. Always attempt to keep directory paths as shallow as possible. The deeper the depth of directories referenced by snapshots, the greater the performance degradation.

Creating snapshots of directories higher on a directory tree will increase the amount of time it takes to modify the data referenced by the snapshot and require more cluster resources to manage the snapshot and the directory. However, creating snapshots of directories lower on directories trees will require more snapshot schedules, which can be difficult to manage. It is recommended that you do not create snapshots of "/ifs" or "/ifs/data".

You can create up to 20,000 snapshots on a cluster at a time. If your workflow requires a large number of snapshots on a consistent basis, you might find that managing snapshots through the OneFS command-line interface is preferable to managing snapshots through the OneFS web administration Interface. In the CLI, you can apply a wide variety of sorting and filtering options and redirect lists into text files.

You should mark snapshots for deletion when they are no longer needed, and make sure that the SnapshotDelete system job is enabled. Disabling the SnapshotDelete job prevents unused disk space from being recaptured and can also cause performance degradation over time.

If the system clock is set to a time zone other than Coordinated Universal Time (UTC), SnapShotIQ modifies snapshot duration periods to match Daylight Savings Time (DST). Upon entering DST, snapshot durations are increased by an hour to adhere to DST; when exiting DST, snapshot durations are decreased by an hour to adhere to standard time.

Best practices for creating snapshot schedules

Snapshot schedule configurations can be categorized by how they delete snapshots: ordered deletions and unordered deletions.

An ordered deletion is the deletion of the oldest snapshot of a directory. An unordered deletion is the deletion of a snapshot that is not the oldest snapshot of a directory. Unordered deletions take approximately twice as long to complete and consume more cluster resources than ordered deletions. However, unordered deletions can save space by retaining a smaller total number of snapshots.
The benefits of unordered deletions versus ordered deletions depend on how often the data referenced by the snapshots is modified. If the data is modified frequently, unordered deletions will save space. However, if data remains unmodified, unordered deletions will most likely not save space, and it is recommended that you perform ordered deletions to free cluster resources.

To implement ordered deletions, assign the same duration period for all snapshots of a directory. The snapshots can be created by one or multiple snapshot schedules. Always ensure that no more than 1000 snapshots of a directory are created.

To implement unordered snapshot deletions, create several snapshot schedules for a single directory, and then assign different snapshot duration periods for each schedule. Ensure that all snapshots are created at the same time when possible.

The following table describes snapshot schedules that follow snapshot best practices:

<table>
<thead>
<tr>
<th>Deletion type</th>
<th>Snapshot frequency</th>
<th>Snapshot time</th>
<th>Snapshot expiration</th>
<th>Max snapshots retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordered deletion (for mostly static data)</td>
<td>Every hour</td>
<td>Beginning at 12:00 AM Ending at 11:59 AM</td>
<td>1 month</td>
<td>720</td>
</tr>
<tr>
<td>Unordered deletion (for frequently modified data)</td>
<td>Every other hour</td>
<td>Beginning at 12:00 AM Ending at 11:59 PM</td>
<td>1 day</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Every day</td>
<td>At 12:00 AM</td>
<td>1 week</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every week</td>
<td>Saturday at 12:00 AM</td>
<td>1 month</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every month</td>
<td>The first Saturday of the month at 12:00 AM</td>
<td>3 months</td>
<td></td>
</tr>
</tbody>
</table>

**File clones**

SnapshotIQ enables you to create file clones that share blocks with existing files in order to save space on the cluster. A file clone usually consumes less space and takes less time to create than a file copy. Although you can clone files from snapshots, clones are primarily used internally by OneFS.

The blocks that are shared between a clone and cloned file are contained in a hidden file called a shadow store. Immediately after a clone is created, all data originally contained in the cloned file is transferred to a shadow store. Because both files reference all blocks from the shadow store, the two files consume no more space than the original file; the clone does not take up any additional space on the cluster. However, if the cloned file or clone is modified, the file and clone will share only blocks that are common to both of them, and the modified, unshared blocks will occupy additional space on the cluster.

Over time, the shared blocks contained in the shadow store might become useless if neither the file nor clone references the blocks. The cluster routinely deletes blocks.
that are no longer needed. You can force the cluster to delete unused blocks at any
time by running the ShadowStoreDelete job.

Clones cannot contain alternate data streams (ADS). If you clone a file that contains
alternate data streams, the clone will not contain the alternate data streams.

**Shadow-store considerations**

Shadow stores are hidden files that are referenced by cloned and deduplicated files.
Files that reference shadow stores behave differently than other files.

- Reading shadow-store references might be slower than reading data directly.
  Specifically, reading non-cached shadow-store references is slower than reading
  non-cached data. Reading cached shadow-store references takes no more time
  than reading cached data.

- When files that reference shadow stores are replicated to another Isilon cluster or
  backed up to a Network Data Management Protocol (NDMP) backup device, the
  shadow stores are not transferred to the target Isilon cluster or backup device.
  The files are transferred as if they contained the data that they reference from
  shadow stores. On the target Isilon cluster or backup device, the files consume the
  same amount of space as if they had not referenced shadow stores.

- When OneFS creates a shadow store, OneFS assigns the shadow store to a
  storage pool of a file that references the shadow store. If you delete the storage
  pool that a shadow store resides on, the shadow store is moved to a pool occupied
  by another file that references the shadow store.

- OneFS does not delete a shadow-store block immediately after the last reference
  to the block is deleted. Instead, OneFS waits until the ShadowStoreDelete job is
  run to delete the unreferenced block. If a large number of unreferenced blocks
  exist on the cluster, OneFS might report a negative deduplication savings until the
  ShadowStoreDelete job is run.

- Shadow stores are protected at least as much as the most protected file that
  references it. For example, if one file that references a shadow store resides in a
  storage pool with +2 protection and another file that references the shadow store
  resides in a storage pool with +3 protection, the shadow store is protected at +3.

- Quotas account for files that reference shadow stores as if the files contained the
  data referenced from shadow stores; from the perspective of a quota, shadow-
  store references do not exist. However, if a quota includes data protection
  overhead, the quota does not account for the data protection overhead of shadow
  stores.

**Snapshot locks**

A snapshot lock prevents a snapshot from being deleted. If a snapshot has one or
more locks applied to it, the snapshot cannot be deleted and is referred to as a locked
snapshot. If the duration period of a locked snapshot expires, OneFS will not delete
the snapshot until all locks on the snapshot have been deleted.

OneFS applies snapshot locks to ensure that snapshots generated by OneFS
applications are not deleted prematurely. For this reason, it is recommended that you
do not delete snapshot locks or modify the duration period of snapshot locks.

A limited number of locks can be applied to a snapshot at a time. If you create
snapshot locks, the limit for a snapshot might be reached, and OneFS could be unable
to apply a snapshot lock when necessary. For this reason, it is recommended that you
do not create snapshot locks.
Snapshot reserve

The snapshot reserve enables you to set aside a minimum percentage of the cluster storage capacity specifically for snapshots. If specified, all other OneFS operations are unable to access the percentage of cluster capacity that is reserved for snapshots.

**Note**

The snapshot reserve does not limit the amount of space that snapshots can consume on the cluster. Snapshots can consume a greater percentage of storage capacity specified by the snapshot reserve. It is recommended that you do not specify a snapshot reserve.

SnapshotIQ license functionality

You can create snapshots only if you activate a SnapshotIQ license on a cluster. However, you can view snapshots and snapshot locks that are created for internal use by OneFS without activating a SnapshotIQ license.

The following table describes what snapshot functionality is available depending on whether the SnapshotIQ license is active:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Inactive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create snapshots and snapshot schedules</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure SnapshotIQ settings</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>View snapshot schedules</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete snapshots</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Access snapshot data</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View snapshots</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If you a SnapshotIQ license becomes inactive, you will no longer be able to create new snapshots, all snapshot schedules will be disabled, and you will not be able to modify snapshots or snapshot settings. However, you will still be able to delete snapshots and access data contained in snapshots.

Creating snapshots with SnapshotIQ

To create snapshots, you must configure the SnapshotIQ licence on the cluster. You can create snapshots either by creating a snapshot schedule or manually generating an individual snapshot.

Manual snapshots are useful if you want to create a snapshot immediately, or at a time that is not specified in a snapshot schedule. For example, if you plan to make changes to your file system, but are unsure of the consequences, you can capture the current state of the file system in a snapshot before you make the change.

Before creating snapshots, consider that reverting a snapshot requires that a SnapRevert domain exist for the directory that is being reverted. If you intend on reverting snapshots for a directory, it is recommended that you create SnapRevert
domains for those directories while the directories are empty. Creating a domain for a
directory that contains less data takes less time.

Create a SnapRevert domain

Before you can revert a snapshot that contains a directory, you must create a
SnapRevert domain for the directory. It is recommended that you create SnapRevert
domains for a directory while the directory is empty.

The root path of the SnapRevert domain must be the same root path of the snapshot.
For example, a domain with a root path of /ifs/data/media cannot be used to
revert a snapshot with a root path of /ifs/data/media/archive. To
revert /ifs/data/media/archive, you must create a SnapRevert domain with a
root path of /ifs/data/media/archive.

Procedure

1. Run the isi job jobs start command.

The following command creates a SnapRevert domain for /ifs/data/media:

```
isi job jobs start domainmark --root /ifs/data/media
   --dm-type SnapRevert
```

Create a snapshot schedule

You can create a snapshot schedule to continuously generate snapshots of directories.

Procedure

1. Run the isi snapshot schedules create command.

The following command creates a snapshot schedule for /ifs/data/media:

```
isi snapshot schedules create hourly /ifs/data/media
   HourlyBackup_%m-%d-%Y_%H:%M "Every day every hour"
   --duration 1M
```

The following commands create multiple snapshot schedules for /ifs/data/
media that generate and expire snapshots at different rates:

```
isi snapshot schedules create every-other-hour
   /ifs/data/media EveryOtherHourBackup_%m-%d-%Y%H%M
   "Every day every 2 hours" --duration 1D
isi snapshot schedules create daily /ifs/data/media
   DailyBackup_%m-%d-%Y%H%M "Every day at 12:00 AM"
   --duration 1W
isi snapshot schedules create weekly /ifs/data/media
   WeeklyBackup_%m-%d-%Y%H%M "Every Saturday at 12:00 AM"
   --duration 1M
isi snapshot schedules create monthly /ifs/data/media
   MonthlyBackup_%m-%d-%Y%H%M
   "The 1st Saturday of every month at 12:00 AM"
   --duration 3M
```

Create a snapshot

You can create a snapshot of a directory.

Procedure

1. Run the isi snapshot snapshots create command.
The following command creates a snapshot for /ifs/data/media:

```
is snap snap snapshots create /ifs/data/media --name media-snap
```

## Snapshot naming patterns

If you schedule snapshots to be automatically generated, either according to a snapshot schedule or a replication policy, you must assign a snapshot naming pattern that determines how the snapshots are named. Snapshot naming patterns contain variables that include information about how and when the snapshot was created.

The following variables can be included in a snapshot naming pattern:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%A</td>
<td>The day of the week.</td>
</tr>
<tr>
<td>%a</td>
<td>The abbreviated day of the week. For example, if the snapshot is generated on a Sunday, %a is replaced with Sun.</td>
</tr>
<tr>
<td>%B</td>
<td>The name of the month.</td>
</tr>
<tr>
<td>%b</td>
<td>The abbreviated name of the month. For example, if the snapshot is generated in September, %b is replaced with Sep.</td>
</tr>
<tr>
<td>%C</td>
<td>The first two digits of the year. For example, if the snapshot is created in 2014, %C is replaced with 20.</td>
</tr>
<tr>
<td>%c</td>
<td>The time and day. This variable is equivalent to specifying %a %b %e %T %Y.</td>
</tr>
<tr>
<td>%d</td>
<td>The two digit day of the month.</td>
</tr>
<tr>
<td>%e</td>
<td>The day of the month. A single-digit day is preceded by a blank space.</td>
</tr>
<tr>
<td>%F</td>
<td>The date. This variable is equivalent to specifying %Y-%m-%d.</td>
</tr>
<tr>
<td>%G</td>
<td>The year. This variable is equivalent to specifying %Y. However, if the snapshot is created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %G is replaced with 2016, because only one day of that week is in 2017.</td>
</tr>
</tbody>
</table>
| %g       | The abbreviated year. This variable is equivalent to specifying %y. However, if the snapshot was created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%g</td>
<td>Calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %g is replaced with 16, because only one day of that week is in 2017.</td>
</tr>
<tr>
<td>%H</td>
<td>The hour. The hour is represented on the 24-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 AM, %H is replaced with 01.</td>
</tr>
<tr>
<td>%h</td>
<td>The abbreviated name of the month. This variable is equivalent to specifying %b.</td>
</tr>
<tr>
<td>%I</td>
<td>The hour represented on the 12-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 PM, %I is replaced with 01.</td>
</tr>
<tr>
<td>%j</td>
<td>The numeric day of the year. For example, if a snapshot is created on February 1, %j is replaced with 32.</td>
</tr>
<tr>
<td>%k</td>
<td>The hour represented on the 24-hour clock. Single-digit hours are preceded by a blank space.</td>
</tr>
<tr>
<td>%l</td>
<td>The hour represented on the 12-hour clock. Single-digit hours are preceded by a blank space. For example, if a snapshot is created at 1:45 AM, %l is replaced with 1.</td>
</tr>
<tr>
<td>%M</td>
<td>The two-digit minute.</td>
</tr>
<tr>
<td>%m</td>
<td>The two-digit month.</td>
</tr>
<tr>
<td>%p</td>
<td>AM or PM.</td>
</tr>
<tr>
<td>%{PolicyName}</td>
<td>The name of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.</td>
</tr>
<tr>
<td>%R</td>
<td>The time. This variable is equivalent to specifying %H:%M.</td>
</tr>
<tr>
<td>%r</td>
<td>The time. This variable is equivalent to specifying %I:%M:%S %p.</td>
</tr>
<tr>
<td>%S</td>
<td>The two-digit second.</td>
</tr>
<tr>
<td>%s</td>
<td>The second represented in UNIX or POSIX time.</td>
</tr>
<tr>
<td>%{SrcCluster}</td>
<td>The name of the source cluster of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%T</td>
<td>The time. This variable is equivalent to specifying %H:%M:%S</td>
</tr>
<tr>
<td>%U</td>
<td>The two-digit numerical week of the year. Numbers range from 00 to 53. The first day of the week is calculated as Sunday.</td>
</tr>
<tr>
<td>%u</td>
<td>The numerical day of the week. Numbers range from 1 to 7. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, %u is replaced with 7.</td>
</tr>
<tr>
<td>%V</td>
<td>The two-digit numerical week of the year that the snapshot was created in. Numbers range from 01 to 53. The first day of the week is calculated as Monday. If the week of January 1 is four or more days in length, then that week is counted as the first week of the year.</td>
</tr>
<tr>
<td>%v</td>
<td>The day that the snapshot was created. This variable is equivalent to specifying %e-%b-%Y.</td>
</tr>
<tr>
<td>%W</td>
<td>The two-digit numerical week of the year that the snapshot was created in. Numbers range from 00 to 53. The first day of the week is calculated as Monday.</td>
</tr>
<tr>
<td>%w</td>
<td>The numerical day of the week that the snapshot was created on. Numbers range from 0 to 6. The first day of the week is calculated as Sunday. For example, if the snapshot was created on Sunday, %w is replaced with 0.</td>
</tr>
<tr>
<td>%X</td>
<td>The time that the snapshot was created. This variable is equivalent to specifying %H:%M:%S.</td>
</tr>
<tr>
<td>%Y</td>
<td>The year that the snapshot was created in.</td>
</tr>
<tr>
<td>%y</td>
<td>The last two digits of the year that the snapshot was created in. For example, if the snapshot was created in 2014, %y is replaced with 14.</td>
</tr>
<tr>
<td>%Z</td>
<td>The time zone that the snapshot was created in.</td>
</tr>
<tr>
<td>%z</td>
<td>The offset from coordinated universal time (UTC) of the time zone that the snapshot was created in. If preceded by a plus sign, the time zone is east of UTC. If preceded by a minus sign, the time zone is west of UTC.</td>
</tr>
<tr>
<td>%+</td>
<td>The time and date that the snapshot was created. This variable is equivalent to specifying %a %b %e %X %Z %Y.</td>
</tr>
</tbody>
</table>
Managing snapshots

You can delete and view snapshots. You can also modify the name, duration period, and snapshot alias of an existing snapshot. However, you cannot modify the data contained in a snapshot; the data contained in a snapshot is read-only.

Reducing snapshot disk-space usage

If multiple snapshots contain the same directories, deleting one of the snapshots might not free the entire amount of space that the system reports as the size of the snapshot. The size of a snapshot is the maximum amount of data that might be freed if the snapshot is deleted.

Deleting a snapshot frees only the space that is taken up exclusively by that snapshot. If two snapshots reference the same stored data, that data is not freed until both snapshots are deleted. Remember that snapshots store data contained in all subdirectories of the root directory; if snapshot_one contains /ifs/data/, and snapshot_two contains /ifs/data/dir, the two snapshots most likely share data.

If you delete a directory, and then re-create it, a snapshot containing the directory stores the entire re-created directory, even if the files in that directory are never modified.

Deleting multiple snapshots that contain the same directories is more likely to free data than deleting multiple snapshots that contain different directories.

If multiple snapshots contain the same directories, deleting older snapshots is more likely to free disk-space than deleting newer snapshots.

Snapshots that are assigned expiration dates are automatically marked for deletion by the snapshot daemon. If the daemon is disabled, snapshots will not be automatically deleted by the system. It is recommended that you do not disable the snapshot daemon.

Delete a snapshot

You can delete a snapshot if you no longer want to access the data contained in the snapshot.

OneFS frees disk space occupied by deleted snapshots when the SnapshotDelete job is run. Also, if you delete a snapshot that contains clones or cloned files, data in a shadow store might no longer be referenced by files on the cluster; OneFS deletes unreferenced data in a shadow store when the ShadowStoreDelete job is run. OneFS routinely runs both the shadow store delete and SnapshotDelete jobs. However, you can also manually run the jobs at any time.

Procedure

1. Delete a snapshot by running the `isi snapshot snapshots delete` command.
   The following command deletes a snapshot named OldSnapshot:

   ```bash
   isi snapshot snapshots delete OldSnapshot
   ```
2. (Optional) To increase the speed at which deleted snapshot data is freed on the cluster, start the SnapshotDelete job by running the following command:

```
isi job jobs start snapshotdelete
```

3. To increase the speed at which deleted data shared between deduplicated and cloned files is freed on the cluster, start the ShadowStoreDelete job by running the following command:

```
isi job jobs start shadowstoredelete
```

### Modify snapshot attributes

You can modify the name and expiration date of a snapshot.

**Procedure**

1. Run the `isi snapshot snapshots modify` command.

   The following command causes HourlyBackup_07-15-2014_22:00 to expire on 1:30 PM on July 25th, 2014:

   ```
   isi snapshot snapshots modify HourlyBackup_07-15-2014_22:00 \
   --expires 2014-07-25T01:30
   ```

### Modify a snapshot alias

You can modify the alias of a snapshot to assign an alternative name for the snapshot.

**Procedure**

1. Run the `isi snapshot snapshots modify` command.

   The following command assigns an alias of LastKnownGood to HourlyBackup_07-15-2013_22:00:

   ```
   isi snapshot snapshots modify HourlyBackup_07-15-2013_22:00 \
   --alias LastKnownGood
   ```

### View snapshots

You can view a list of snapshots or detailed information about a specific snapshot.

**Procedure**

1. View all snapshots by running the following command:

   ```
   isi snapshot snapshots list
   ```

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
Snapshots

2. (Optional) To view detailed information about a specific snapshot, run the `isi snapshot snapshots view` command.

   The following command displays detailed information about `HourlyBackup_07-15-2013_22:00`:

   ```
   isi snapshot snapshots view HourlyBackup_07-15-2013_22:00
   ```

   The system displays output similar to the following example:

   ```
   ID: 14
   Name: HourlyBackup_07-15-2013_22:00
   Path: /ifs/data/media
   Has Locks: No
   Schedule: hourly
   Alias: -
   Created: 2013-07-15T22:00:10
   Expires: 2013-08-14T22:00:00
   Size: 0b
   Shadow Bytes: 0b
   % Reserve: 0.00%
   % Filesystem: 0.00%
   State: active
   ```

Snapshot information

You can view information about snapshots through the output of the `isi snapshot snapshots list` command.

ID

The ID of the snapshot.

Name

The name of the snapshot.

Path

The path of the directory contained in the snapshot.
Restoring snapshot data

You can restore snapshot data through various methods. You can revert a snapshot or access snapshot data through the snapshots directory.

From the snapshots directory, you can either clone a file or copy a directory or a file. The snapshots directory can be accessed through Windows Explorer or a UNIX command line. You can disable and enable access to the snapshots directory for any of these methods through snapshots settings.

Revert a snapshot

You can revert a directory back to the state it was in when a snapshot was taken.

Before you begin

- Create a SnapRevert domain for the directory.
- Create a snapshot of a directory.

Procedure

1. (Optional) To identify the ID of the snapshot you want to revert, run the `isi snapshot snapshots view` command.
   
   The following command displays the ID of HourlyBackup_07-15-2014_23:00:
   
   ```
   isi snapshot snapshots view HourlyBackup_07-15-2014_23:00
   ```
   
   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Path</th>
<th>Has Locks</th>
<th>Schedule</th>
<th>Alias</th>
<th>Created</th>
<th>Expires</th>
<th>Size</th>
<th>Shadow Bytes</th>
<th>% Reserve</th>
<th>% Filesystem</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>HourlyBackup_07-15-2014_23:00</td>
<td>/ifs/data/media</td>
<td>No</td>
<td>hourly</td>
<td>-</td>
<td>2014-07-15T23:00:05</td>
<td>2014-08-14T23:00:00</td>
<td>0b</td>
<td>0b</td>
<td>0.00%</td>
<td>0.00%</td>
<td>active</td>
</tr>
</tbody>
</table>

2. Revert a snapshot by running the `isi job jobs start` command.
   
   The following command reverts HourlyBackup_07-15-2014_23:00:
   
   ```
   isi job jobs start snaprevert --snapid 18
   ```

Restore a file or directory using Windows Explorer

If the Microsoft Shadow Copy Client is installed on your computer, you can use it to restore files and directories that are stored in snapshots.

This method of restoring files and directories does not preserve the original permissions. Instead, this method assigns the file or directory the same permissions as the directory you are copying that file or directory into. To preserve permissions while restoring data from a snapshot, run the `cp` command with the `-a` option on a UNIX command line.
### Snapshots

#### Note

You can access up to 64 snapshots of a directory through Windows explorer, starting with the most recent snapshot. To access more than 64 snapshots for a directory, access the cluster through a UNIX command line.

#### Procedure

1. In Windows Explorer, navigate to the directory that you want to restore or the directory that contains the file that you want to restore.
   
   If the directory has been deleted, you must recreate the directory.

2. Right-click the folder, and then click **Properties**.

3. In the **Properties** window, click the **Previous Versions** tab.

4. Select the version of the folder that you want to restore or the version of the folder that contains the version of the file that you want to restore.

5. Restore the version of the file or directory.
   - To restore all files in the selected directory, click **Restore**.
   - To copy the selected directory to another location, click **Copy**, and then specify a location to copy the directory to.
   - To restore a specific file, click **Open**, and then copy the file into the original directory, replacing the existing copy with the snapshot version.

#### Restore a file or directory through a UNIX command line

You can restore a file or directory from a snapshot through a UNIX command line.

**Procedure**

1. Open a connection to the cluster through a UNIX command line.

2. (Optional) To view the contents of the snapshot you want to restore a file or directory from, run the `ls` command for a directory contained in the snapshots root directory.

   For example, the following command displays the contents of the `/archive` directory contained in Snapshot2014Jun04:

   ```
   ls /ifs/.snapshot/Snapshot2014Jun04/archive
   ```

3. Copy the file or directory by using the `cp` command.

   For example, the following command creates a copy of the `file1` file:

   ```
   cp -a /ifs/.snapshot/Snapshot2014Jun04/archive/file1 /ifs/archive/file1_copy
   ```

#### Clone a file from a snapshot

You can clone a file from a snapshot.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.

2. To view the contents of the snapshot you want to restore a file or directory from, run the `ls` command for a subdirectory of the snapshots root directory.
For example, the following command displays the contents of the `/archive` directory contained in Snapshot2014Jun04:

```
ls /ifs/.snapshot/Snapshot2014Jun04/archive
```

3. Clone a file from the snapshot by running the `cp` command with the `-c` option. For example, the following command clones `test.txt` from Snapshot2014Jun04:

```
cp -c /ifs/.snapshot/Snapshot2014Jun04/archive/test.txt /ifs/archive/test_clone.txt
```

## Managing snapshot schedules

You can modify, delete, and view snapshot schedules.

### Modify a snapshot schedule

You can modify a snapshot schedule. Any changes to a snapshot schedule are applied only to snapshots generated after the modifications are made. Existing snapshots are not affected by schedule modifications.

If you modify the alias of a snapshot schedule, the alias is assigned to the next snapshot generated based on the schedule. However, if you do this, the old alias is not removed from the last snapshot that it was assigned to. Unless you manually remove the old alias, the alias will remain attached to the last snapshot that it was assigned to.

**Procedure**

1. Run the `isi snapshot schedules modify` command.

   The following command causes snapshots created according to the snapshot schedule `hourly_media_snap` to be deleted 15 days after they are created:

   ```
   isi snapshot schedules modify hourly_media_snap --duration 15D
   ```

### Delete a snapshot schedule

You can delete a snapshot schedule. Deleting a snapshot schedule will not delete snapshots that were previously generated according to the schedule.

**Procedure**

1. Run the `isi snapshot schedules delete` command.

   The following command deletes a snapshot schedule named `hourly_media_snap`:

   ```
   isi snapshot schedules delete hourly_media_snap
   ```
**View snapshot schedules**

You can view snapshot schedules.

**Procedure**

1. View snapshot schedules by running the following command:

   ```
   isi snapshot snapshots list
   ```

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>every-other-hour</td>
</tr>
<tr>
<td>2</td>
<td>daily</td>
</tr>
<tr>
<td>3</td>
<td>weekly</td>
</tr>
<tr>
<td>4</td>
<td>monthly</td>
</tr>
</tbody>
</table>

2. (Optional) View detailed information about a specific snapshot schedule by running the `isi snapshot schedules view` command.

   The following command displays detailed information about the snapshot schedule every-other-hour:

   ```
   isi snapshot schedules view every-other-hour
   ```

   The system displays output similar to the following example:

   ```
   ID: 1
   Name: every-other-hour
   Path: /ifs/data/media
   Pattern: EveryOtherHourBackup_%m-%d-%Y_%H:%M
   Schedule: Every day every 2 hours
   Duration: 1D
   Alias: -
   Next Run: 2013-07-16T18:00:00
   Next Snapshot: EveryOtherHourBackup_07-16-2013_18:00
   ```

**Managing snapshot aliases**

You can configure snapshot schedules to assign a snapshot alias to the most recent snapshot created by a snapshot schedule. You can also manually assign snapshot aliases to specific snapshots or the live version of the file system.

**Configure a snapshot alias for a snapshot schedule**

You can configure a snapshot schedule to assign a snapshot alias to the most recent snapshot created by the schedule.

If you configure an alias for a snapshot schedule, the alias is assigned to the next snapshot generated based on the schedule. However, if you do this, the old alias is not removed from the last snapshot that it was assigned to. Unless you manually remove the old alias, the alias will remain attached to the last snapshot that it was assigned to.
Snapshots

Assign a snapshot alias to a snapshot

You can assign a snapshot alias to a snapshot.

Procedure

1. Run the `isi snapshot schedules modify` command.

The following command configures the alias LatestWeekly for the snapshot schedule WeeklySnapshot:

   ```bash
   isi snapshot schedules modify WeeklySnapshot --alias LatestWeekly
   ```

Reassign a snapshot alias to the live file system

You can reassign a snapshot alias to redirect clients from a snapshot to the live file system.

This procedure is available only through the command-line interface (CLI).

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi snapshot aliases modify` command.

The following command reassigns the latestWeekly alias to the live file system:

   ```bash
   isi snapshot aliases modify latestWeekly --target LIVE
   ```

View snapshot aliases

You can view a list of all snapshot aliases.

This procedure is available only through the command-line interface (CLI).

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. View a list of all snapshot aliases by running the following command:

   ```bash
   isi snapshot aliases list
   ```

   If a snapshot alias references the live version of the file system, the Target ID is -1.

3. (Optional) View information about a specific snapshot by running the `isi snapshot aliases view` command.
The following command displays information about latestWeekly:

```
isi snapshot aliases view latestWeekly
```

**Snapshot alias information**

You can view information about snapshot aliases through the output of the `isi snapshot aliases view` command.

- **ID**
  - The numerical ID of the snapshot alias.
- **Name**
  - The name of the snapshot alias.
- **Target ID**
  - The numerical ID of the snapshot that is referenced by the alias.
- **Target Name**
  - The name of the snapshot that is referenced by the alias.
- **Created**
  - The date that the snapshot alias was created.

**Managing with snapshot locks**

You can delete, create, and modify the expiration date of snapshot locks.

⚠️ **CAUTION**

It is recommended that you do not create, delete, or modify snapshot locks unless you are instructed to do so by Isilon Technical Support.

Deleting a snapshot lock that was created by OneFS might result in data loss. If you delete a snapshot lock that was created by OneFS, it is possible that the corresponding snapshot might be deleted while it is still in use by OneFS. If OneFS cannot access a snapshot that is necessary for an operation, the operation will malfunction and data loss might result. Modifying the expiration date of a snapshot lock created by OneFS can also result in data loss because the corresponding snapshot can be deleted prematurely.

**Create a snapshot lock**

You can create snapshot locks that prevent snapshots from being deleted.

Although you can prevent a snapshot from being automatically deleted by creating a snapshot lock, it is recommended that you do not create snapshot locks. To prevent a snapshot from being automatically deleted, it is recommended that you extend the duration period of the snapshot.

**Procedure**

1. Create a snapshot lock by running the `isi snapshot locks create` command.
For example, the following command applies a snapshot lock to SnapshotApril2016, sets the lock to expire in one month, and adds a description of "Maintenance Lock":

```bash
isi snapshot locks create SnapshotApril2016 --expires 1M --comment "Maintenance Lock"
```

### Modify a snapshot lock expiration date

You can modify the expiration date of a snapshot lock.

⚠️ **CAUTION**

It is recommended that you do not modify the expiration dates of snapshot locks.

This procedure is available only through the command-line interface (CLI).

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi snapshot locks modify` command.

   The following command sets an expiration date two days from the present date for a snapshot lock with an ID of 1 that is applied to a snapshot named SnapshotApril2014:

```bash
isi snapshot locks modify SnapshotApril2014 1 --expires 2D
```

### Delete a snapshot lock

You can delete a snapshot lock.

⚠️ **CAUTION**

It is recommended that you do not delete snapshot locks.

This procedure is available only through the command-line interface (CLI).

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Delete a snapshot lock by running the `isi snapshot locks delete` command.

   The following command deletes a snapshot lock that is applied to SnapshotApril2014 and has a lock ID of 1:

```bash
isi snapshot locks delete Snapshot2014Apr16 1
```

   The system prompts you to confirm that you want to delete the snapshot lock.
3. Type `yes` and then press ENTER.
Snapshot lock information

You can view snapshot lock information through the `isi snapshot locks view` and `isi snapshot locks list` commands.

**ID**
Numerical identification number of the snapshot lock.

**Comment**
Description of the snapshot lock. This can be any string specified by a user.

**Expires**
The date that the snapshot lock will be automatically deleted by OneFS.

**Count**
The number of times the snapshot lock is held.
The file clone operation can hold a single snapshot lock multiple times. If multiple file clones are created simultaneously, the file clone operation holds the same lock multiple times, rather than creating multiple locks. If you delete a snapshot lock that is held more than once, you will delete only one of the instances that the lock is held. In order to delete a snapshot lock that is held multiple times, you must delete the snapshot lock the same number of times as displayed in the count field.

Configure SnapshotIQ settings

You can configure SnapshotIQ settings that determine how snapshots can be created and the methods that users can access snapshot data.

**Procedure**

1. (Optional) View current SnapshotIQ settings by running the following command:

   ```
   isi snapshot settings view
   ```

   The system displays output similar to the following example:

   ````
   Service: Yes
   Autocreate: Yes
   Autodelete: Yes
   Reserve: 0.00%
   Global Visible Accessible: Yes
   NFS Root Accessible: Yes
   NFS Root Visible: Yes
   NFS Subdir Accessible: Yes
   SMB Root Accessible: Yes
   SMB Root Visible: Yes
   SMB Subdir Accessible: Yes
   Local Root Accessible: Yes
   Local Root Visible: Yes
   Local Subdir Accessible: Yes
   ```

2. Configure SnapshotIQ settings by running the `isi snapshot settings modify` command:
The following command prevents snapshots from being created on the cluster:

```
isi snapshot settings modify --service disable
```

**SnapshotIQ settings**

SnapshotIQ settings determine how snapshots behave and can be accessed.

The following settings are displayed in the output of the `isi snapshot settings view` command:

- **Service**
  Determines whether SnapshotIQ is enabled on the cluster.

- **Autocreate**
  Determines whether snapshots are automatically generated according to snapshot schedules.

  **Note**
  Disabling snapshot generation might cause some OneFS operations to fail. It is recommended that you do not disable this setting.

- **Autodelete**
  Determines whether snapshots are automatically deleted according to their expiration dates.

- **Reserve**
  Specifies the percentage of disk space on the cluster that is reserved for snapshots.

- **NFS Root Accessible**
  Determines whether snapshot directories are accessible through NFS.

- **NFS Root Visible**
  Determines whether snapshot directories are visible through NFS.

- **NFS Subdir Accessible**
  Determines whether snapshot subdirectories are accessible through NFS.

- **SMB Root Accessible**
  Determines whether snapshot directories are accessible through SMB.

- **SMB Root Visible**
  Determines whether snapshot directories are visible through SMB.

- **SMB Subdir Accessible**
  Determines whether snapshot subdirectories are accessible through SMB.

- **Local Root Accessible**
  Determines whether snapshot directories are accessible through an SSH connection or the local console.

- **Local Root Visible**
  Determines whether snapshot directories are visible through the an SSH connection or the local console.
Local Subdir Accessible
Determine whether snapshot subdirectories are accessible through an SSH connection or the local console.

Set the snapshot reserve
You can specify a minimum percentage of cluster-storage capacity that you want to reserve for snapshots.

The snapshot reserve does not limit the amount of space that snapshots are allowed to consume on the cluster. Snapshots can consume more than the percentage of capacity specified by the snapshot reserve. It is recommended that you do not specify a snapshot reserve.

This procedure is available only through the command-line interface (CLI).

Procedure
1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Set the snapshot reserve by running the `isi snapshot settings modify` command with the `--reserve` option.
   
   For example, the following command sets the snapshot reserve to 20%:
   
   ```
   isi snapshot settings modify --reserve 20
   ```

Managing changelists
You can create and view changelists that describe the differences between two snapshots. You can create a changelist for any two snapshots that have a common root directory.

Changelists are most commonly accessed by applications through the OneFS Platform API. For example, a custom application could regularly compare the two most recent snapshots of a critical directory path to determine whether to back up the directory, or to trigger other actions.

Create a changelist
You can create a changelist that shows what data was changed between snapshots.

Procedure
1. (Optional) To view the IDs of the snapshots you want to create a changelist for, run the following command:
   
   ```
   isi snapshot snapshots list
   ```

2. Create a changelist by running the `isi job jobs start` command with the ChangelistCreate option.
   
   The following command creates a changelist:
   
   ```
   isi job jobs start ChangelistCreate --older-snapid 2 --newer-snapid 6
   ```
Delete a changelist

You can delete a changelist

Procedure

1. Run the isi_changelist_mod command with the -k option.

   The following command deletes changelist 22_24:

   ```
   isi_changelist_mod -k 22_24
   ```

View a changelist

You can view a changelist that describes the differences between two snapshots. This procedure is available only through the command-line interface (CLI).

Procedure

1. View the IDs of changelists by running the following command:

   ```
   isi_changelist_mod -l
   ```

   Changelist IDs include the IDs of both snapshots used to create the changelist. If OneFS is still in the process of creating a changelist, `inprog` is appended to the changelist ID.

2. (Optional) View all contents of a changelist by running the isi_changelist_mod command with the -a option.

   The following command displays the contents of a changelist named 2_6:

   ```
   isi_changelist_mod -a 2_6
   ```

Changelist information

You can view the information contained in changelists.

---

Note

The information contained in changelists is meant to be consumed by applications through the OneFS Platform API.

---

The following information is displayed for each item in the changelist when you run the isi_changelist_mod command:

- **st_ino**
  - Displays the inode number of the specified item.

- **st_mode**
  - Displays the file type and permissions for the specified item.

- **st_size**
  - Displays the total size of the item in bytes.
Snapshots

**st_atime**
Displays the POSIX timestamp of when the item was last accessed.

**st_mtime**
Displays the POSIX timestamp of when the item was last modified.

**st_ctime**
Displays the POSIX timestamp of when the item was last changed.

**cl_flags**
Displays information about the item and what kinds of changes were made to the item.

- **01**
  The item was added or moved under the root directory of the snapshots.

- **02**
  The item was removed or moved out of the root directory of the snapshots.

- **04**
  The path of the item was changed without being removed from the root directory of the snapshot.

- **10**
  The item either currently contains or at one time contained Alternate Data Streams (ADS).

- **20**
  The item is an ADS.

- **40**
  The item has hardlinks.

---

**Note**
These values are added together in the output. For example, if an ADS was added, the code would be `cl_flags=021`.

---

**path**
The absolute path of the specified file or directory.

---

**Snapshot commands**
You can control and access snapshots through the snapshot commands. Most snapshot commands apply specifically to the SnapshotIQ tool and are available only if a SnapshotIQ license is configured on the cluster.

**Snapshot naming patterns**
If you schedule snapshots to be automatically generated, either according to a snapshot schedule or a replication policy, you must assign a snapshot naming pattern that determines how the snapshots are named. Snapshot naming patterns contain variables that include information about how and when the snapshot was created.

The following variables can be included in a snapshot naming pattern:
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%A</td>
<td>The day of the week.</td>
</tr>
<tr>
<td>%a</td>
<td>The abbreviated day of the week. For example, if the snapshot is generated on a Sunday, %a is replaced with Sun.</td>
</tr>
<tr>
<td>%B</td>
<td>The name of the month.</td>
</tr>
<tr>
<td>%b</td>
<td>The abbreviated name of the month. For example, if the snapshot is generated in September, %b is replaced with Sep.</td>
</tr>
<tr>
<td>%C</td>
<td>The first two digits of the year. For example, if the snapshot is created in 2014, %C is replaced with 20.</td>
</tr>
<tr>
<td>%c</td>
<td>The time and day. This variable is equivalent to specifying %a %b %e %T %Y.</td>
</tr>
<tr>
<td>%d</td>
<td>The two digit day of the month.</td>
</tr>
<tr>
<td>%e</td>
<td>The day of the month. A single-digit day is preceded by a blank space.</td>
</tr>
<tr>
<td>%F</td>
<td>The date. This variable is equivalent to specifying %Y-%m-%d.</td>
</tr>
<tr>
<td>%G</td>
<td>The year. This variable is equivalent to specifying %Y. However, if the snapshot is created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %G is replaced with 2016, because only one day of that week is in 2017.</td>
</tr>
<tr>
<td>%g</td>
<td>The abbreviated year. This variable is equivalent to specifying %y. However, if the snapshot was created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %g is replaced with 16, because only one day of that week is in 2017.</td>
</tr>
<tr>
<td>%H</td>
<td>The hour. The hour is represented on the 24-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 AM, %H is replaced with 01.</td>
</tr>
<tr>
<td>%h</td>
<td>The abbreviated name of the month. This variable is equivalent to specifying %b.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%I</td>
<td>The hour represented on the 12-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 PM, %I is replaced with 01.</td>
</tr>
<tr>
<td>%j</td>
<td>The numeric day of the year. For example, if a snapshot is created on February 1, %j is replaced with 32.</td>
</tr>
<tr>
<td>%k</td>
<td>The hour represented on the 24-hour clock. Single-digit hours are preceded by a blank space.</td>
</tr>
<tr>
<td>%l</td>
<td>The hour represented on the 12-hour clock. Single-digit hours are preceded by a blank space. For example, if a snapshot is created at 1:45 AM, %l is replaced with 1.</td>
</tr>
<tr>
<td>%M</td>
<td>The two-digit minute.</td>
</tr>
<tr>
<td>%m</td>
<td>The two-digit month.</td>
</tr>
<tr>
<td>%p</td>
<td>AM or PM.</td>
</tr>
<tr>
<td>%{PolicyName}</td>
<td>The name of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.</td>
</tr>
<tr>
<td>%R</td>
<td>The time. This variable is equivalent to specifying %H:%M.</td>
</tr>
<tr>
<td>%r</td>
<td>The time. This variable is equivalent to specifying %I:%M:%S %p.</td>
</tr>
<tr>
<td>%S</td>
<td>The two-digit second.</td>
</tr>
<tr>
<td>%s</td>
<td>The second represented in UNIX or POSIX time.</td>
</tr>
<tr>
<td>%{SrcCluster}</td>
<td>The name of the source cluster of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.</td>
</tr>
<tr>
<td>%T</td>
<td>The time. This variable is equivalent to specifying %H:%M:%S</td>
</tr>
<tr>
<td>%U</td>
<td>The two-digit numerical week of the year. Numbers range from 00 to 53. The first day of the week is calculated as Sunday.</td>
</tr>
<tr>
<td>%u</td>
<td>The numerical day of the week. Numbers range from 1 to 7. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, %u is replaced with 7.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%V</td>
<td>The two-digit numerical week of the year that the snapshot was created in. Numbers range from 01 to 53. The first day of the week is calculated as Monday. If the week of January 1 is four or more days in length, then that week is counted as the first week of the year.</td>
</tr>
<tr>
<td>%v</td>
<td>The day that the snapshot was created. This variable is equivalent to specifying <code>%e-%b-%Y</code>.</td>
</tr>
<tr>
<td>%W</td>
<td>The two-digit numerical week of the year that the snapshot was created in. Numbers range from 00 to 53. The first day of the week is calculated as Monday.</td>
</tr>
<tr>
<td>%w</td>
<td>The numerical day of the week that the snapshot was created on. Numbers range from 0 to 6. The first day of the week is calculated as Sunday. For example, if the snapshot was created on Sunday, %w is replaced with 0.</td>
</tr>
<tr>
<td>%X</td>
<td>The time that the snapshot was created. This variable is equivalent to specifying <code>%H:%M:%S</code>.</td>
</tr>
<tr>
<td>%Y</td>
<td>The year that the snapshot was created in.</td>
</tr>
<tr>
<td>%y</td>
<td>The last two digits of the year that the snapshot was created in. For example, if the snapshot was created in 2014, %y is replaced with 14.</td>
</tr>
<tr>
<td>%Z</td>
<td>The time zone that the snapshot was created in.</td>
</tr>
<tr>
<td>%z</td>
<td>The offset from coordinated universal time (UTC) of the time zone that the snapshot was created in. If preceded by a plus sign, the time zone is east of UTC. If preceded by a minus sign, the time zone is west of UTC.</td>
</tr>
<tr>
<td>%+</td>
<td>The time and date that the snapshot was created. This variable is equivalent to specifying <code>%a %b %e %X %Z %Y</code>.</td>
</tr>
<tr>
<td>%%</td>
<td>Escapes a percent sign. For example, 100%% is replaced with 100%.</td>
</tr>
</tbody>
</table>
isi snapshot schedules create

Creates a snapshot schedule. A snapshot schedule determines when OneFS regularly generates snapshots on a recurring basis.

Syntax

```bash
isi snapshot schedules create <name> <path> <pattern> <schedule> 
    [--alias <alias>] 
    [--duration <duration>] 
    [--verbose]
```

Options

- `<name>`
  Specifies a name for the snapshot schedule.

- `<path>`
  Specifies the path of the directory to include in the snapshots.

- `<pattern>`
  Specifies a naming pattern for snapshots created according to the schedule.

- `<schedule>`
  Specifies how often snapshots are created.
  Specify in the following format:

```
"<interval> [<frequency>]"
```

Specify `<interval>` in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>, ...] [of every [{other | <integer}>] week]
- The last {day | weekday | <day>} of every [{other | <integer}>] month
- The <integer> {weekday | <day>} of every [{other | <integer}>] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify `<frequency>` in one of the following formats:

- at <hh>[::<mm>] [{AM | PM}]
every $\langle$integer$\rangle$ {hours | minutes} [between $\langle$hh$\rangle$[:$mm$] [{AM | PM}] and $\langle$hh$\rangle$[:$mm$] [{AM | PM}]]

You can optionally append "st", "th", or "rd" to $\langle$integer$\rangle$. For example, you can specify "Every 1st month".

Specify $\langle$day$\rangle$ as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

--alias $\langle$alias$\rangle$

Specifies an alias for the latest snapshot generated based on the schedule. The alias enables you to quickly locate the most recent snapshot that was generated according to the schedule. Specify as any string.

{--duration | -x} $\langle$duration$\rangle$

Specifies how long snapshots generated according to the schedule are stored on the cluster before OneFS automatically deletes them. Specify in the following format:

$\langle$integer$\rangle$$\langle$units$\rangle$

The following $\langle$units$\rangle$ are valid:

Y

Specifies years

M

Specifies months

W

Specifies weeks

D

Specifies days

H

Specifies hours

{--verbose | -v}

Displays a message confirming that the snapshot schedule was created.

isi snapshot schedules modify

Modifies the attributes of an existing snapshot schedule.

If you modify a snapshot schedule, snapshots that have already been generated based on the schedule are not affected by the changes.
Syntax

`isi snapshot schedules modify <schedule-name>`
{-name <name> | --alias <name> | --path <path>
| --pattern <naming-pattern> | --schedule <schedule>
| --duration <duration> | --clear-duration}...
[--verbose]`

Options

`<schedule-name>`

Modifies the specified snapshot schedule.
Specify as a snapshot schedule name or ID.

`--name <name>`

Specifies a new name for the schedule.
Specify as any string.

`{---alias | -a} <name>`

Specifies an alias for the latest snapshot generated based on the schedule. The alias enables you to quickly locate the most recent snapshot that was generated according to the schedule. If specified, the specified alias will be applied to the next snapshot generated by the schedule, and all subsequently generated snapshots.
Specify as any string.

`--path <path>`

Specifies a new directory path for this snapshot schedule. If specified, snapshots generated by the schedule will contain only this directory path.
Specify as a directory path.

`--pattern <naming-pattern>`

Specifies a pattern by which snapshots created according to the schedule are named.

`--schedule <schedule>`

Specifies how often snapshots are created.
Specify in the following format:

"<interval> [<frequency>]"

Specify `<interval>` in one of the following formats:

- Every {{other | <integer>}} {weekday | day}
- Every {{other | <integer>}} week [on <day>]
- Every {{other | <integer>}} month [on the <integer>]
- Every [<day>[, ...] [of every {{other | <integer>}} week]]
- The last {day | weekday | <day>} of every {{other | <integer>}} month
- The `<integer>` {weekday | <day> of every [{other | <integer>]}] month

- Yearly on <month> `<integer>`

- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify `<frequency>` in one of the following formats:

- at `<hh>[:<mm>]` [{AM | PM}]

- every `<integer>` {hours | minutes} [between `<hh>[:<mm>]` [{AM | PM}] and `<hh>[:<mm>]` [{AM | PM}]]

- every `<integer>` {hours | minutes} [from `<hh>[:<mm>]` [{AM | PM}] to `<hh>[:<mm>]` [{AM | PM}]]

You can optionally append "st", "th", or "rd" to `<integer>`. For example, you can specify "Every 1st month"

Specify `<day>` as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

```
{--duration | -x} <duration>
```

Specifies how long snapshots generated according to the schedule are stored on the cluster before OneFS automatically deletes them.

Specify in the following format:

```
<integer><units>
```

The following `<units>` are valid:

```
Y
  Specifies years
```

```
M
  Specifies months
```

```
W
  Specifies weeks
```

```
D
  Specifies days
```

```
H
  Specifies hours
```

```
--clear-duration
```

Removes the duration period for snapshots created according to the schedule. If specified, generated snapshots will exist on the cluster indefinitely.

```
{--verbose | -v}
```
Displays a message confirming that the snapshot schedule was modified.

**isi snapshot schedules delete**

Deletes a snapshot schedule. Once a snapshot schedule is deleted, snapshots will no longer be generated according to the schedule. However, snapshots previously generated according to the schedule are not affected.

**Syntax**

```
isi snapshot schedules delete <schedule-name>  
  [--force]  
  [--verbose]
```

**Options**

- `<schedule-name>`
  
  Deletes the specified snapshot schedule. Specify as a snapshot schedule name or ID.
  
  `{--force | -f}`
  
  Does not prompt you to confirm that you want to delete this snapshot schedule.
  
  `{--verbose | -v}`
  
  Displays a message confirming that the snapshot schedule was deleted.

**isi snapshot schedules list**

Displays a list of all snapshot schedules.

**Syntax**

```
isi snapshot schedules list  
  [--limit <integer>]  
  [--sort <attribute>]  
  [--descending]  
  [--format {table | json | csv | list}]  
  [--no-header]  
  [--no-footer]  
  [--verbose]
```

**Options**

- `{--limit | -l} <integer>`
  
  Displays no more than the specified number of items.
  
  `--sort <attribute>`
  
  Sorts output displayed by the specified attribute.
  
  The following values are valid:
  
  - `id`
    
    Sorts output by the ID of a snapshot schedule.
  
  - `name`
    
    Sorts output alphabetically by the name of a snapshot schedule.
path
Sorts output by the absolute path of the directory contained by snapshots created according to a schedule.

pattern
Sorts output alphabetically by the snapshot naming pattern assigned to snapshots generated according to a schedule.

schedule
Sorts output alphabetically by the schedule. For example, "Every week" precedes "Yearly on January 3rd"

duration
Sorts output by the length of time that snapshots created according to the schedule endure on the cluster before being automatically deleted.

alias
Sorts output alphabetically by the name of the alias assigned to the most recent snapshot generated according to the schedule.

next_run
Sorts output by the next time that a snapshot will be created according to the schedule.

next_snapshot
Sorts output alphabetically by the name of the snapshot that is scheduled to be created next.

{--descending | -d}
Displays output in reverse order.

--format <output-format>
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

isi snapshot schedules view
Displays information about a snapshot schedule.

Syntax

`isi snapshot schedules view <schedule-name>`
Options

<schedule-name>
Displays information about the specified snapshot schedule.
Specify as a snapshot schedule name or ID.

isi snapshot schedules pending list
Displays a list of snapshots that are scheduled to be generated by snapshot schedules.

Syntax

isi snapshot schedules pending list
|--begin <timestamp>
|--end <timestamp>
|--limit <integer>
|--format {table | json | csv | list}
|--no-header
|--no-footer
|--verbose

Options

|--begin | -b} <timestamp>
Displays only snapshots that are scheduled to be generated after the specified date.
Specify <timestamp> in the following format:

<yyyy>-<mm>-<dd>T<HH>:<MM>:<SS>]

If this option is not specified, the output displays a list of snapshots that are scheduled to be generated after the current time.

|--end | -e} <time>
Displays only snapshots that are scheduled to be generated before the specified date.
Specify <time> in the following format:

<yyyy>-<mm>-<dd>T<HH>:<MM>:<SS>]

If this option is not specified, the output displays a list of snapshots that are scheduled to be generated before 30 days after the begin time.

|--limit | -l} <integer>
Displays no more than the specified number of items.

--format <output-format>
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

|--no-header | -a
Displays table and CSV output without headers.

|--no-footer | -z
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

**isi snapshot snapshots create**

Creates a snapshot of a directory.

**Syntax**

```bash
isi snapshot snapshots create <path>
    [--name <name>]
    [--expires {<timestamp> | <duration>}]  
    [--alias <name>]
    [--verbose]
```

**Options**

**<path>**
Specifies the path of the directory to include in this snapshot.

**--name <name>**
Specifies a name for the snapshot.

**{--expires | -x} {<timestamp> | <duration>}**
Specifies when OneFS will automatically delete this snapshot. If this option is not specified, the snapshot will exist indefinitely.

Specify **<timestamp>** in the following format:

```
<yyyy>-<mm>-<dd>[T<HH>:<MM>[:<SS>]]
```

Specify **<duration>** in the following format:

```
<integer><units>
```

The following **<units>** are valid:

- **Y**
  Specifies years

- **M**
  Specifies months

- **W**
  Specifies weeks

- **D**
  Specifies days

- **H**
  Specifies hours

**{--alias | -a} <name>**
Specifies an alias for this snapshot. A snapshot alias is an alternate name for a snapshot. Specify as any string.

{--verbose | -v}
Displays a message confirming that the snapshot was created.

**isi snapshot snapshots modify**

Modifies attributes of a snapshot or snapshot alias.

**Syntax**

```
isi snapshot snapshots modify <snapshot> {--name <name> | --expires {<timestamp> | <duration>} | --clear-expires | --alias <name>}... [--verbose]
```

**Options**

**<snapshot>**
Modifies the specified snapshot or snapshot alias. Specify as the name or ID of a snapshot or snapshot alias.

**--name <name>**
Specifies a new name for the snapshot or snapshot alias. Specify as any string.

{--expires | -x} {<timestamp> | <duration>}
Specifies when OneFS will automatically delete this snapshot. Specify `<timestamp>` in the following format:

```
<yyyymmddTHHMMSS]
```

Specify `<duration>` in the following format:

```
<integer><time>
```

The following `<time>` values are valid:

Y
 specifies years

M
 specifies months

W
 specifies weeks

D
 specifies days
Specifies hours

You cannot modify the expiration date of a snapshot alias.

--clear-expires
Removes the expiration date from the snapshot, allowing the snapshot to exist on
the cluster indefinitely.
You cannot modify the expiration date of a snapshot alias.

{--alias | -a} <name>
Specifies an alias for the snapshot. A snapshot alias is an alternate name for a
snapshot. You cannot specify an alias for a snapshot alias.
Specify as any string.

{--verbose | -v}
Displays a message confirming that the snapshot or snapshot alias was modified.

**isi snapshot snapshots delete**

Deletes a snapshot. If a snapshot is deleted, it can no longer be accessed by a user or
the system.

**Syntax**

```
isistage snapshot snapshots delete {--all | --snapshot <snapshot>
| --schedule <schedule> | --type <type>}
[--force]
[--verbose]
```

**Options**

--all
Deletes all snapshots.

--snapshot <snapshot>
Deletes the specified snapshot.
Specify as a snapshot name or ID.

--schedule <schedule>
Deletes all snapshots created according to the specified schedule.
Specify as a snapshot schedule name or ID.

--type <type>
Deletes all snapshots of the specified type.
The following types are valid:
alias
Deletes all snapshot aliases.
real
Deletes all snapshots.
Snapsots

|--force | -f
     Does not prompt you to confirm that you want to delete the snapshot.

|--verbose | -v
     Displays a message confirming that the snapshot was deleted.

Examples
The following command deletes newSnap1:

    isi snapshot snapshots delete --snapshot newSnap1

isi snapshot snapshots list

Displays a list of all snapshots and snapshot aliases.

Syntax

    isi snapshot snapshots list
    [--state <state>]
    [--limit <integer>]
    [--sort <attribute>]
    [--descending]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]

Options

|--state <state>
    Displays only snapshots and snapshot aliases that exist in the specified state.
    The following states are valid:
        all
            Displays all snapshots and snapshot aliases that are currently occupying
            space on the cluster.
        active
            Displays only snapshots and snapshot aliases that have not been deleted.
        deleting
            Displays only snapshots that have been deleted but are still occupying space
            on the cluster. The space occupied by deleted snapshots will be freed the
            next time the snapshot delete job is run.

|--limit | -l <integer>
    Displays no more than the specified number of items.

|--sort <attribute>
    Sorts command output by the specified attribute.
    The following attributes are valid:
        id
            Sorts output by the ID of a snapshot.
name
   Sorts output alphabetically by the name of a snapshot.

path
   Sorts output by the absolute path of the directory contained in a snapshot.

has_locks
   Sorts output by whether any snapshot locks have been applied to a snapshot.

schedule
   If a snapshot was generated according to a schedule, sorts output alphabetically by the name of the snapshot schedule.

target_id
   If a snapshot is an alias, sorts output by the snapshot ID of the target snapshot instead of the snapshot ID of the alias.

target_name
   If a snapshot is an alias, sorts output by the name of the target snapshot instead of the name of the alias.

created
   Sorts output by the time that a snapshot was created.

expires
   Sorts output by the time at which a snapshot is scheduled to be automatically deleted.

size
   Sorts output by the amount of disk space taken up by a snapshot.

shadow_bytes
   Sorts output based on the amount of data that a snapshot references from shadow stores. Snapshots reference shadow store data if a file contained in a snapshot is cloned or a snapshot is taken of a cloned file.

pct_reserve
   Sorts output by the percentage of the snapshot reserve that a snapshot occupies.

pct_filesystem
   Sorts output by the percent of the file system that a snapshot occupies.

state
   Sorts output based on the state of snapshots.

{--descending | -d}
   Displays output in reverse order.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
   Displays table output without headers.
Displays table output without footers. Footers display snapshot totals, such as the total amount of storage space consumed by snapshots.

Displays more detailed information.

### isi snapshot snapshots view

Displays the properties of an individual snapshot.

**Syntax**

```bash
isi snapshot snapshots view <snapshot>
```

**Options**

- `<snapshot>`
  Displays information about the specified snapshot.
  Specify as a snapshot name or ID.

### isi snapshot settings modify

Modifies snapshot settings.

**Syntax**

```bash
isi snapshot settings modify
  |--service {enable | disable}
  |--autocreate {enable | disable}
  |--autodelete {enable | disable}
  |--reserve <integer>
  |--global-visible-accessible {yes | no}
  |--nfs-root-accessible {yes | no}
  |--nfs-root-visible {yes | no}
  |--nfs-subdir-accessible {yes | no}
  |--smb-root-accessible {yes | no}
  |--smb-root-visible {yes | no}
  |--smb-subdir-accessible {yes | no}
  |--local-root-accessible {yes | no}
  |--local-root-visible {yes | no}
  |--local-subdir-accessible {yes | no}...```

**Options**

- `--service {enable | disable}`
  Determines whether snapshots can be generated.

  **Note**
  Disabling snapshot generation might cause some OneFS operations to fail. It is recommended that you do not disable this setting.

- `--autocreate {enable | disable}`
Determines whether snapshots are automatically generated according to snapshot schedules. Specifying `disable` does not prevent OneFS applications from generating snapshots.

`--autodelete {enable | disable}`
Determines whether snapshots are automatically deleted according to their expiration dates. All snapshots that pass their expiration date while this option is disabled will immediately be deleted when the option is enabled again.

`--reserve <integer>`
Specifies the percentage of the file system to reserve for snapshot usage. Specify as a positive integer between 1 and 100.

Note
This option limits only the amount of space available to applications other than SnapshotIQ. It does not limit the amount of space that snapshots are allowed to occupy. Snapshots can occupy more than the specified percentage of system storage space.

`--global-visible-accessible {yes | no}`
Specifying `yes` causes snapshot directories and sub-directories to be visible and accessible through all protocols, overriding all other snapshot visibility and accessibility settings. Specifying `no` causes visibility and accessibility settings to be controlled through the other snapshot visibility and accessibility settings.

`--nfs-root-accessible {yes | no}`
Determines whether snapshot directories are accessible through NFS.

`--nfs-root-visible {yes | no}`
Determines whether snapshot directories are visible through NFS.

`--nfs-subdir-accessible {yes | no}`
Determines whether snapshot subdirectories are accessible through NFS.

`--smb-root-accessible {yes | no}`
Determines whether snapshot directories are accessible through SMB.

`--smb-root-visible {yes | no}`
Determines whether snapshot directories are visible through SMB.

`--smb-subdir-accessible {yes | no}`
Determines whether snapshot subdirectories are accessible through SMB.

`--local-root-accessible {yes | no}`
Determines whether snapshot directories are accessible through the local file system.

`--local-root-visible {yes | no}`
Determines whether snapshot directories are visible through the local file system.
Determines whether snapshot subdirectories are accessible through the local file system.

`--verbose | -v`

Displays a message displaying which snapshot settings were modified.

**isi snapshot settings view**

Displays current SnapshotIQ settings.

**Syntax**

```
isi snapshot settings view
```

**Options**

There are no options for this command.

**isi snapshot locks create**

Creates a snapshot lock.

**Note**

It is recommended that you do not create snapshot locks and do not use this command. If the maximum number of locks on a snapshot is reached, some applications, such as SyncIQ, might not function properly.

**Syntax**

```
isi snapshot locks create <snapshot>
   [--comment <string>]
   [--expires {<timestamp> | <duration>}] 
   [--verbose]
```

**Options**

**<snapshot>**

Specifies the name of the snapshot to apply this lock to.

**{--comment | -c} <string>**

Specifies a comment to describe the lock.

Specify as any string.

**{--expires | -x} {<timestamp> | <duration>]**

Specifies when the lock will be automatically deleted by the system.

If this option is not specified, the snapshot lock will exist indefinitely.

Specify `<timestamp>` in the following format:

```
<yyyy>-<mm>-<dd>T<HH>:<MM>[;:<SS>]
```
Specify `<duration>` in the following format:

```
<integer><time>
```

The following `<time>` values are valid:

- **Y**
  - Specifies years
- **M**
  - Specifies months
- **W**
  - Specifies weeks
- **D**
  - Specifies days
- **H**
  - Specifies hours

```{--verbose | -v}```
Displays a message confirming that the snapshot lock was deleted.

### isi snapshot locks modify

Modifies the expiration date of a snapshot lock.

⚠️ **CAUTION**

It is recommended that you do not modify the expiration date of snapshot locks and do not run this command. Modifying the expiration date of a snapshot lock that was created by OneFS might result in data loss.

**Syntax**

```
isi snapshot locks modify <snapshot> <id>
    {--expires {<timestamp> | <duration>} | --clear-expires} 
    [--verbose]
```

**Options**

- `<snapshot>`
  - Modifies a snapshot lock that has been applied to the specified snapshot. Specify as a snapshot name or ID.

- `<id>`
  - Modifies the snapshot lock of the specified ID.

- `{--expires | -x}{<timestamp> | <duration>}`
  - Specifies when the lock will be automatically deleted by the system. If this option is not specified, the snapshot lock will exist indefinitely.
Snapshots

Specify <timestamp> in the following format:

<yyyy>-<mm>-<dd>[T<HH>:<MM>[:<SS>]]

Specify <duration> in the following format:

<integer><time>

The following <time> values are valid:

Y
  Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours

--clear.expires
  Removes the duration period for the snapshot lock. If specified, the snapshot lock will exist on the cluster indefinitely.

{--verbose | -v}
  Displays a message confirming that the snapshot lock was modified.

Examples
The following command causes a snapshot lock applied to Wednesday_Backup to expire in three weeks:

isi snapshot locks modify Wednesday_Backup 1 --expires 3W

isi snapshot locks delete
Deletes a snapshot lock. Deleting a snapshot lock might result in data loss.

⚠ CAUTION
It is recommended that you do not delete snapshot locks and do not run this command. Deleting a snapshot lock that was created by OneFS might result in data loss.
### Syntax

```bash
isi snapshot locks delete <snapshot> <id>
    [--force]
    [--verbose]
```

### Options

**<snapshot>**

- Deletes a snapshot lock that has been applied to the specified snapshot.
  - Specify as a snapshot name or ID.

**<id>**

- Modifies the snapshot lock of the specified ID.

**{--force | -f}**

- Does not prompt you to confirm that you want to delete this snapshot lock.

**{--verbose | -v}**

- Displays a message confirming that the snapshot lock was deleted.

### isi snapshot locks list

Displays a list of all locks applied to a specific snapshot.

### Syntax

```bash
isi snapshot locks list <snapshot>
    [--limit <integer>]
    [--sort <attribute>]
    [--descending]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

### Options

**<snapshot>**

- Displays all locks belonging to the specified snapshot.
  - Specify as a snapshot name.

**{--limit | -l} <integer>**

- Displays no more than the specified number of items.

**--sort <attribute>**

- Sorts output displayed by the specified attribute.
  - The following values are valid:
    - `id`
      - Sorts output by the ID of a snapshot lock.
    - `comment`
      - Sorts output alphabetically by the description of a snapshot lock.
expires
Sorts output by the length of time that a lock endures on the cluster before being automatically deleted.

count
Sorts output by the number of times that a lock is held.

{--descending | -d}
Displays output in reverse order.

--format <output-format>
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

**isi snapshot locks view**
Displays information about a snapshot lock.

**Syntax**

```
isi snapshot locks view <snapshot> <id>
```

**Options**

**<name>**
Specifies the snapshot to view locks for.
Specify as a snapshot name or ID.

**<id>**
Displays the specified lock.
Specify as a snapshot lock ID.

**isi snapshot aliases create**
Assigns a snapshot alias to a snapshot or to the live version of the file system.

**Syntax**

```
isi snapshot aliases create <name> <target>
```

**Options**

**<name>**
Specifies the a name for the alias.

<target>
Assigns the alias to the specified snapshot or to the live version of the file system. Specify as a snapshot ID or name. To target the live version of the file system, specify LIVE.

{--verbose | -v}
Displays more detailed information.

**isi snapshot aliases modify**
Modifies a snapshot alias.

**Syntax**

```bash
isi snapshot aliases modify <alias>
   {--name <name> | --target <snapshot>}
   [--verbose]
```

**Options**

<alias>
Modifies the specified snapshot alias.
Specify as a snapshot-alias name or ID.

--name <name>
Specifies a new name for the snapshot alias.

--target <snapshot>
Reassigns the snapshot alias to the specified snapshot or the live version of the file system.
Specify as a snapshot ID or name. To target the live version of the file system, specify LIVE.

{--verbose | -v}
Displays more detailed information.

**isi snapshot aliases delete**
Deletes a snapshot alias.

**Syntax**

```bash
isi snapshot aliases delete {<alias> | --all}
   [--force]
   [--verbose]
```

**Options**

<alias>
Deletes the snapshot alias of the specified name.
Specify as a snapshot-alias name or ID.
--all
   Deletes all snapshot aliases.

{--force | -f}
   Runs the command without prompting you to confirm that you want to delete the snapshot alias.

{--verbose | -v}
   Displays more detailed information.

isi snapshot aliases list
Displays a list of snapshot aliases.

Syntax

isi snapshot aliases list
   [--limit <integer>]
   [--sort {id | name | target_id | target_name | created}]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]

Options

{--limit | -l} <integer>
   Displays no more than the specified number of items.

--sort <attribute>
   Sorts output displayed by the specified attribute.
   The following values are valid:
   id
      Sorts output by the ID of the snapshot alias.
   name
      Sorts output by the name of the snapshot alias.
   target_id
      Sorts output by the ID of the snapshot that the snapshot alias is assigned to.
   target_name
      Sorts output by the name of the snapshot that the snapshot alias is assigned to.
   created
      Sorts output by the date the snapshot alias was created.

{--descending | -d}
   Displays output in reverse order.

--format <output-format>
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

```
{--no-header | -a}
  Displays table and CSV output without headers.
{--no-footer | -z}
  Displays table output without footers.
{--verbose | -v}
  Displays more detailed information.
```

**isi snapshot aliases view**

Displays detailed information about a snapshot alias.

**Syntax**

```
isi snapshot aliases view <alias>
```

**Options**

```
<alias>
  Displays detailed information about the specified snapshot alias. Specify as a snapshot-alias name or ID.
```
Snapshots
CHAPTER 15

Deduplication with SmartDedupe

This section contains the following topics:

- Deduplication overview .................................................. 624
- Deduplication jobs ............................................................. 624
- Data replication and backup with deduplication ................ 625
- Snapshots with deduplication .......................................... 625
- Deduplication considerations ......................................... 626
- Shadow-store considerations .......................................... 626
- SmartDedupe license functionality ................................. 627
- Managing deduplication ............................................... 627
- Deduplication commands ............................................... 631
Deduplication overview

SmartDedupe enables you to save storage space on your cluster by reducing redundant data. Deduplication maximizes the efficiency of your cluster by decreasing the amount of storage required to store multiple files with identical blocks.

The SmartDedupe software module deduplicates data by scanning an Isilon cluster for identical data blocks. Each block is 8 KB. If SmartDedupe finds duplicate blocks, SmartDedupe moves a single copy of the blocks to a hidden file called a shadow store. SmartDedupe then deletes the duplicate blocks from the original files and replaces the blocks with pointers to the shadow store.

Deduplication is applied at the directory level, targeting all files and directories underneath one or more root directories. SmartDedupe not only deduplicates identical blocks in different files, it also deduplicates identical blocks within a single file.

You can first assess a directory for deduplication and determine the estimated amount of space you can expect to save. You can then decide whether to deduplicate the directory. After you begin deduplicating a directory, you can monitor how much space is saved by deduplication in real time.

For two or more files to be deduplicated, the files must have the same disk pool policy ID and protection policy. If one or both of these attributes differs between two or more identical files, or files with identical 8K blocks, the files are not deduplicated.

Because it is possible to specify protection policies on a per-file or per-directory basis, deduplication can further be impacted. Consider the example of two files, /ifs/data/projects/alpha/logo.jpg and /ifs/data/projects/beta/logo.jpg. Even though the logo.jpg files in both directories are identical, if one has a different protection policy from the other, the two files would not be deduplicated.

In addition, if you have activated a SmartPools license on your cluster, you can specify custom file pool policies. These file pool policies might cause files that are identical or have identical 8K blocks to be stored in different node pools. Consequently, those files would have different disk pool policy IDs and would not be deduplicated.

SmartDedupe also does not deduplicate files that are 32 KB or smaller, because doing so would consume more cluster resources than the storage savings are worth. The default size of a shadow store is 2 GB. Each shadow store can contain up to 256,000 blocks. Each block in a shadow store can be referenced up to 32,000 times.

Deduplication jobs

Deduplication is performed by a system maintenance job referred to as a deduplication job. You can monitor and control deduplication jobs as you would any other maintenance job on the cluster. Although the overall performance impact of deduplication is minimal, the deduplication job consumes 400 MB of memory per node.

When a deduplication job runs for the first time on a cluster, SmartDedupe samples blocks from each file and creates index entries for those blocks. If the index entries of two blocks match, SmartDedupe scans the blocks adjacent to the matching pair and then deduplicates all duplicate blocks. After a deduplication job samples a file once, new deduplication jobs will not sample the file again until the file is modified.

The first deduplication job that you run might take significantly longer to complete than subsequent deduplication jobs. The first deduplication job must scan all files under the specified directories to generate the initial index. If subsequent
deduplication jobs take a long time to complete, this most likely indicates that a large amount of data is being deduplicated. However, it can also indicate that users are storing large amounts of new data on the cluster. If a deduplication job is interrupted during the deduplication process, the job will automatically restart the scanning process from where the job was interrupted.

Note

You should run deduplication jobs when users are not modifying data on the cluster. If users are continually modifying files on the cluster, the amount of space saved by deduplication is minimal because the deduplicated blocks are constantly removed from the shadow store.

How frequently you should run a deduplication job on your Isilon cluster varies, depending on the size of your data set, the rate of changes, and opportunity. For most clusters, we recommend that you start a deduplication job every 7-10 days. You can start a deduplication job manually or schedule a recurring job at specified intervals. By default, the deduplication job is configured to run at a low priority. However, you can specify job controls, such as priority and impact, on deduplication jobs that run manually or by schedule.

The permissions required to modify deduplication settings are not the same as those needed to run a deduplication job. Although a user must have the maintenance job permission to run a deduplication job, the user must have the deduplication permission to modify deduplication settings. By default, the root user and SystemAdmin user have the necessary permissions for all deduplication operations.

Data replication and backup with deduplication

When deduplicated files are replicated to another Isilon cluster or backed up to a tape device, the deduplicated files no longer share blocks on the target Isilon cluster or backup device. However, although you can deduplicate data on a target Isilon cluster, you cannot deduplicate data on an NDMP backup device.

Shadow stores are not transferred to target clusters or backup devices. Because of this, deduplicated files do not consume less space than non-deduplicated files when they are replicated or backed up. To avoid running out of space, you must ensure that target clusters and tape devices have enough free space to store deduplicated data as if the data had not been deduplicated. To reduce the amount of storage space consumed on a target Isilon cluster, you can configure deduplication for the target directories of your replication policies. Although this will deduplicate data on the target directory, it will not allow SyncIQ to transfer shadow stores. Deduplication is still performed by deduplication jobs running on the target cluster.

The amount of cluster resources required to backup and replicate deduplicated data is the same as for non-deduplicated data. You can deduplicate data while the data is being replicated or backed up.

Snapshots with deduplication

You cannot deduplicate the data stored in a snapshot. However, you can create snapshots of deduplicated data.

If you create a snapshot for a deduplicated directory, and then modify the contents of that directory, the references to shadow stores will be transferred to the snapshot over time. Therefore, if you enable deduplication before you create snapshots, you will save more space on your cluster. If you implement deduplication on a cluster that
already has a significant amount of data stored in snapshots, it will take time before the snapshot data is affected by deduplication. Newly created snapshots can contain deduplicated data, but snapshots created before deduplication was implemented cannot.

If you plan on reverting a snapshot, it is best to revert the snapshot before running a deduplication job. Restoring a snapshot can overwrite many of the files on the cluster. Any deduplicated files are reverted back to normal files if they are overwritten by a snapshot revert. However, after the snapshot revert is complete, you can deduplicate the directory and the space savings persist on the cluster.

**Deduplication considerations**

Deduplication can significantly increase the efficiency at which you store data. However, the effect of deduplication varies depending on the cluster.

You can reduce redundancy on a cluster by running SmartDedupe. Deduplication creates links that can impact the speed at which you can read from and write to files. In particular, sequentially reading chunks smaller than 512 KB of a deduplicated file can be significantly slower than reading the same small, sequential chunks of a non-deduplicated file. This performance degradation applies only if you are reading non-cached data. For cached data, the performance for deduplicated files is potentially better than non-deduplicated files. If you stream chunks larger than 512 KB, deduplication does not significantly impact the read performance of the file. If you intend on streaming 8 KB or less of each file at a time, and you do not plan on concurrently streaming the files, it is recommended that you do not deduplicate the files.

Deduplication is most effective when applied to static or archived files and directories. The less files are modified, the less negative effect deduplication has on the cluster. For example, virtual machines often contain several copies of identical files that are rarely modified. Deduplicating a large number of virtual machines can greatly reduce consumed storage space.

**Shadow-store considerations**

Shadow stores are hidden files that are referenced by cloned and deduplicated files. Files that reference shadow stores behave differently than other files.

- Reading shadow-store references might be slower than reading data directly. Specifically, reading non-cached shadow-store references is slower than reading non-cached data. Reading cached shadow-store references takes no more time than reading cached data.
- When files that reference shadow stores are replicated to another Isilon cluster or backed up to a Network Data Management Protocol (NDMP) backup device, the shadow stores are not transferred to the target Isilon cluster or backup device. The files are transferred as if they contained the data that they reference from shadow stores. On the target Isilon cluster or backup device, the files consume the same amount of space as if they had not referenced shadow stores.
- When OneFS creates a shadow store, OneFS assigns the shadow store to a storage pool of a file that references the shadow store. If you delete the storage pool that a shadow store resides on, the shadow store is moved to a pool occupied by another file that references the shadow store.
- OneFS does not delete a shadow-store block immediately after the last reference to the block is deleted. Instead, OneFS waits until the ShadowStoreDelete job is
run to delete the unreferenced block. If a large number of unreferenced blocks exist on the cluster, OneFS might report a negative deduplication savings until the ShadowStoreDelete job is run.

- Shadow stores are protected at least as much as the most protected file that references it. For example, if one file that references a shadow store resides in a storage pool with +2 protection and another file that references the shadow store resides in a storage pool with +3 protection, the shadow store is protected at +3.
- Quotas account for files that reference shadow stores as if the files contained the data referenced from shadow stores; from the perspective of a quota, shadow-store references do not exist. However, if a quota includes data protection overhead, the quota does not account for the data protection overhead of shadow stores.

### SmartDedupe license functionality

You can deduplicate data only if you activate a SmartDedupe license on a cluster. However, you can assess deduplication savings without activating a SmartDedupe license.

If you activate a SmartDedupe license, and then deduplicate data, the space savings are not lost if the license becomes inactive. You can also still view deduplication savings while the license is inactive. However, you will not be able to deduplicate additional data until you re-activate the SmartDedupe license.

### Managing deduplication

You can manage deduplication on a cluster by first assessing how much space you can save by deduplicating individual directories. After you determine which directories are worth deduplicating, you can configure SmartDedupe to deduplicate those directories specifically. You can then monitor the actual amount of disk space you are saving.

### Assess deduplication space savings

You can assess the amount of disk space you will save by deduplicating a directory.

**Procedure**

1. Specify which directory to assess by running the `isi dedupe settings modify` command.

   The following command configures SmartDedupe to assess deduplication savings for `/ifs/data/archive`:

   ```
   isi dedupe settings modify --assess-paths /ifs/data/archive
   ```

   If you assess multiple directories, disk savings will not be differentiated by directory in the deduplication report.

2. Start the assessment job by running the following command:

   ```
   isi job jobs start dedupeassessment
   ```
3. Identify the ID of the assessment report by running the following command:

   
   ```
   isi dedupe reports list
   ```

4. View prospective space savings by running the `isi dedupe reports view` command:

   The following command displays the prospective savings recorded in a deduplication report with an ID of 46:

   ```
   isi dedupe reports view 46
   ```

### Specify deduplication settings

You can specify which directories you want to deduplicate.

**Procedure**

1. Specify which directories you want to deduplicate by running the `isi dedupe settings modify` command.

   The following command targets `/ifs/data/archive` and `/ifs/data/media` for deduplication:

   ```
   isi dedupe settings modify --paths /ifs/data/media,/ifs/data/archive
   ```

2. (Optional) To modify the settings of the deduplication job, run the `isi job types modify` command.

   The following command configures the deduplication job to be run every Friday at 10:00 PM:

   ```
   isi job types Dedupe --schedule "Every Friday at 10:00 PM"
   ```

### View deduplication space savings

You can view the amount of disk space that you are currently saving with deduplication.

**Procedure**

1. Run the following command:

   ```
   isi dedupe stats
   ```
View a deduplication report

After a deduplication job completes, you can view information about the job in a deduplication report.

Procedure

1. (Optional) To identify the ID of the deduplication report you want to view, run the following command:

   ```
   isi dedupe reports list
   ```

2. View a deduplication report by running the `isi dedupe reports view` command.

   The following command displays a deduplication report with an ID of 44:

   ```
   isi dedupe reports view 44
   ```

Deduplication job report information

You can view the following deduplication specific information in deduplication job reports:

**Start time**

The time the deduplication job started.

**End time**

The time the deduplication job ended.

**Iteration Count**

The number of times that SmartDedupe interrupted the sampling process. If SmartDedupe is sampling a large amount of data, SmartDedupe might interrupt sampling in order to start deduplicating the data. After SmartDedupe finishes deduplicating the sampled data, SmartDedupe will continue sampling the remaining data.

**Scanned blocks**

The total number of blocks located underneath the specified deduplicated directories.

**Sampled blocks**

The number of blocks that SmartDedupe created index entries for.

**Deduped blocks**

The number of blocks that were deduplicated.

**Dedupe percent**

The percentage of scanned blocks that were deduplicated.

**Created dedupe requests**

The total number of deduplication requests created. A deduplication request is created for each matching pair of data blocks. For example, if you have 3 data blocks that all match, SmartDedupe creates 2 requests. One of the requests
could pair file1 and file2 together and the other request could pair file2 and file3 together.

**Successful dedupe requests**
The number of deduplication requests that completed successfully.

**Failed dedupe requests**
The number of deduplication requests that failed. If a deduplication request fails, it doesn't mean that the job failed too. A deduplication request can fail for any number of reasons. For example, the file might have been modified since it was sampled.

**Skipped files**
The number of files that were not scanned by the deduplication job. SmartDedupe skips files for a number of reasons. For example, SmartDedupe skips files that have already been scanned and haven't been modified since. SmartDedupe also skips all files that are smaller than 4 KB.

**Index entries**
The number of entries that currently exist in the index.

**Index lookup attempts**
The total number of lookups that have been done by earlier deduplication jobs plus the number of lookups done by this deduplication job. A lookup is when the deduplication job attempts to match a block that was indexed with a block that hasn't been indexed.

**Index lookup hits**
The number of blocks that matched index entries.

**Deduplication information**
You can view information about how much disk space is being saved by deduplication. The following information is displayed in the output of the `isi dedupe stats` command:

**Cluster Physical Size**
The total amount of physical disk space on the cluster.

**Cluster Used Size**
The total amount of disk space currently occupied by data on the cluster.

**Logical Size Deduplicated**
The amount of disk space that has been deduplicated in terms of reported file sizes. For example, if you have three identical files that are all 5 GB, the logical size deduplicated is 15 GB.

**Logical Saving**
The amount of disk space saved by deduplication in terms of reported file sizes. For example, if you have three identical files that are all 5 GB, the logical saving is 10 GB.

**Estimated Size Deduplicated**
The total amount of physical disk space that has been deduplicated, including protection overhead and metadata. For example, if you have three identical files
that are all 5 GB, the estimated size deduplicated would be greater than 15 GB, because of the disk space consumed by file metadata and protection overhead.

**Estimated Physical Saving**
The total amount of physical disk space saved by deduplication, including protection overhead and metadata. For example, if you have three identical files that are all 5 GB, the estimated physical saving would be greater than 10 GB, because deduplication saved space that would have been occupied by file metadata and protection overhead.

**Deduplication commands**

You can control data deduplication through the deduplication commands. Deduplication commands are available only if you activate a SmartDedupe license.

**isi dedupe settings modify**

Modifies the settings of deduplication jobs.

**Syntax**

```bash
isi dedupe settings modify

[|--paths <path>]* | --clear-paths]
|--add-paths <path>]*
|--remove-paths <path>]*

[|--assess-paths <path>]* | --clear-assess-paths]
|--add-assess-paths <path>]*
|--remove-assess-paths <path>]*

|--verbose
```

**Options**

|--paths <path>
Deduplicates files located under the specified root directories.

|--clear-paths
Stops deduplication for all previously specified root directories. If you run the `isi dedupe settings modify` command with this option, you must run the command again with either `--paths` or `--add-path` to resume deduplication.

|--add-paths <path>
Deduplicates files located under the specified root directory in addition to directories that are already being deduplicated.

|--remove-paths <path>
Stops deduplicating the specified root directory.

|--assess-paths <path>
Assesses how much space will be saved if files located under the specified root directories are deduplicated.

|--clear-assess-paths
Stops assessing how much space will be saved if previously specified root directories are deduplicated. If you run the `isi dedupe settings modify`
command with this option, you must run the command again with either --paths or --add-path to resume deduplication.

--add-assess-paths <path>
Assesses how much space will be saved if the specified root directories are deduplicated in addition to directories that are already being assessed.

--remove-assess-paths <path>
Stops assessing how much space will be saved if the specified root directories are deduplicated.

|----verbose | -v|
Displays more detailed information.

Examples
The following command starts deduplicating /ifs/data/active and /ifs/data/media:

isi dedupe settings modify --add-paths /ifs/data/active,/ifs/data/media

The following command stops deduplicating /ifs/data/active and /ifs/data/media:

isi dedupe settings modify --remove-paths /ifs/data/active,/ifs/data/media

**isi dedupe settings view**
Displays current deduplication settings.

**Syntax**

isi dedupe settings view

**Options**
There are no options for this command.

**isi dedupe stats**
Displays information about how much data is being saved by deduplication.

**Syntax**

isi dedupe stats

**Options**
There are no options for this command.
Examples
To view information about deduplication space savings, run the following command:

```bash
isi dedupe stats
```

The system displays output similar to the following example:

```
Cluster Physical Size: 17.019G
Cluster Used Size: 4.994G
Logical Size Deduplicated: 13.36M
  Logical Saving: 11.13M
Estimated Size Deduplicated: 30.28M
  Estimated Physical Saving: 25.23M
```

**isi dedupe reports list**

Displays a list of deduplication reports.

**Syntax**

```bash
isi dedupe reports list
  [--limit <integer>]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]
```

**Options**

```bash
{--limit | -l} <integer>
  Displays no more than the specified number of items.

  --format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

  {--no-header | -a}
  Displays table output without headers.

  {--no-footer | -z}
  Displays table output without footers. Footers display snapshot totals, such as the total amount of storage space consumed by snapshots.

  {--verbose | -v}
  Displays more detailed information.
```

**Examples**

To view a list of deduplication reports, run the following command:

```bash
isi dedupe reports list
```
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Time</th>
<th>Job ID</th>
<th>Job Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-05-09T11:03:37</td>
<td>4</td>
<td>Dedupe</td>
</tr>
<tr>
<td>2013-05-10T00:02:27</td>
<td>8</td>
<td>Dedupe</td>
</tr>
<tr>
<td>2013-05-16T00:02:32</td>
<td>16</td>
<td>Dedupe</td>
</tr>
<tr>
<td>2013-05-17T00:02:32</td>
<td>19</td>
<td>Dedupe</td>
</tr>
<tr>
<td>2013-05-09T16:14:04</td>
<td>5</td>
<td>DedupeAssessment</td>
</tr>
</tbody>
</table>

Total: 6

**isi dedupe reports view**

Displays a deduplication report.

**Syntax**

```
isi dedupe reports view <job-id>
```

**Options**

- `<job-id>`

  Displays the deduplication report for the deduplication job of the specified ID.

**Examples**

The following command displays a deduplication job:

```
isi dedupe reports view 12
```

The system displays output similar to the following example:

```
Time: 2013-10-14T09:39:22
Job ID: 52
Job Type: Dedupe
Reports
  Time : 2013-10-14T09:39:22
  Results :
  Dedupe job report:{
    Start time = 2013-Oct-14:09:33:34
    End time = 2013-Oct-14:09:39:22
    Iteration count = 1
    Scanned blocks = 1716
    Sampled blocks = 78
    Dedumed blocks = 1425
    Dedupe percent = 83.042
    Created dedupe requests = 65
    Successful dedupe requests = 65
    Failed dedupe requests = 0
    Skipped files = 0
    Index entries = 38
    Index lookup attempts = 38
    Index lookup hits = 0
  }
  Elapsed time:                      347 seconds
  Aborts:                              0
  Errors:                              0
  Scanned files:                       6
  Directories:                         2
  2 paths:
```
<table>
<thead>
<tr>
<th>Directory</th>
<th>CPU usage:</th>
<th>Virtual memory size:</th>
<th>Resident memory size:</th>
<th>Read:</th>
<th>Write:</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ifs/data/dir2</td>
<td>max 29% (dev 2),</td>
<td>max 128388K (dev 1), min 106628K</td>
<td>max 27396K (dev 1), min 9980K</td>
<td>2160 ops, 124437504 bytes (118.7M)</td>
<td>30570 ops, 222851584 bytes (212.5M)</td>
</tr>
<tr>
<td>/ifs/data/dir1</td>
<td>min 0% (dev 1),</td>
<td>avg 107617K</td>
<td>avg 11585K</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>avg 6%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Deduplication with SmartDedupe
CHAPTER 16
Data replication with SyncIQ

This section contains the following topics:

- SyncIQ data replication overview ................................................................. 638
- Replication policies and jobs ........................................................................ 638
- Replication snapshots .................................................................................. 644
- Data failover and failback with SyncIQ ...................................................... 645
- Recovery times and objectives for SyncIQ .................................................. 646
- Replication policy priority ............................................................................ 647
- SyncIQ license functionality ......................................................................... 647
- Creating replication policies ........................................................................ 647
- Managing replication to remote clusters ..................................................... 653
- Initiating data failover and failback with SyncIQ .......................................... 655
- Performing disaster recovery for SmartLock directories ............................. 658
- Managing replication policies ...................................................................... 660
- Managing replication to the local cluster ..................................................... 663
- Managing replication performance rules ...................................................... 665
- Managing replication reports ....................................................................... 668
- Managing failed replication jobs .................................................................. 670
- Data replication commands ........................................................................ 672
SyncIQ data replication overview

OneFS enables you to replicate data from one Isilon cluster to another through the SyncIQ software module. You must activate a SyncIQ license on both Isilon clusters before you can replicate data between them.

You can replicate data at the directory level while optionally excluding specific files and sub-directories from being replicated. SyncIQ creates and references snapshots to replicate a consistent point-in-time image of a root directory. Metadata such as access control lists (ACL) and alternate data streams (ADS) are replicated along with data.

SyncIQ enables you to maintain a consistent backup copy of your data on another Isilon cluster. SyncIQ offers automated failover and failback capabilities that enable you to continue operations on another Isilon cluster if a primary cluster becomes unavailable.

Accessing SyncIQ with IsilonSD Edge

The SyncIQ software module is available only with a purchased license of IsilonSD Edge. It is not packaged with the free license of this product. Therefore, you must purchase a license of IsilonSD Edge to access the SyncIQ backup and replication functions.

Replication policies and jobs

Data replication is coordinated according to replication policies and replication jobs. Replication policies specify what data is replicated, where the data is replicated to, and how often the data is replicated. Replication jobs are the operations that replicate data from one Isilon cluster to another. SyncIQ generates replication jobs according to replication policies.

A replication policy specifies two clusters: the source and the target. The cluster on which the replication policy exists is the source cluster. The cluster that data is being replicated to is the target cluster. When a replication policy starts, SyncIQ generates a replication job for the policy. When a replication job runs, files from a directory tree on the source cluster are replicated to a directory tree on the target cluster; these directory trees are known as source and target directories.

After the first replication job created by a replication policy finishes, the target directory and all files contained in the target directory are set to a read-only state, and can be modified only by other replication jobs belonging to the same replication policy. We recommend that you do not create more than 1,000 policies on a cluster.

Note

To prevent permissions errors, make sure that ACL policy settings are the same across source and target clusters.

You can create two types of replication policies: synchronization policies and copy policies. A synchronization policy maintains an exact replica of the source directory on the target cluster. If a file or sub-directory is deleted from the source directory, the file or directory is deleted from the target cluster when the policy is run again.

You can use synchronization policies to fail over and fail back data between source and target clusters. When a source cluster becomes unavailable, you can fail over data on
a target cluster and make the data available to clients. When the source cluster becomes available again, you can fail back the data to the source cluster.

A copy policy maintains recent versions of the files that are stored on the source cluster. However, files that are deleted on the source cluster are not deleted from the target cluster. Failback is not supported for copy policies. Copy policies are most commonly used for archival purposes.

Copy policies enable you to remove files from the source cluster without losing those files on the target cluster. Deleting files on the source cluster improves performance on the source cluster while maintaining the deleted files on the target cluster. This can be useful if, for example, your source cluster is being used for production purposes and your target cluster is being used only for archiving.

After creating a job for a replication policy, SyncIQ must wait until the job completes before it can create another job for the policy. Any number of replication jobs can exist on a cluster at a given time; however, no more than 50 replication jobs can run on a source cluster at the same time. If more than 50 replication jobs exist on a cluster, the first 50 jobs run while the others are queued to run.

There is no limit to the number of replication jobs that a target cluster can support concurrently. However, because more replication jobs require more cluster resources, replication will slow down as more concurrent jobs are added.

When a replication job runs, OneFS generates workers on the source and target cluster. Workers on the source cluster read and send data while workers on the target cluster receive and write data. OneFS generates no more than 8 workers per node per replication job. For example, in a five node cluster, OneFS would create no more than 40 workers for a replication job.

You can replicate any number of files and directories with a single replication job. You can prevent a large replication job from overwhelming the system by limiting the amount of cluster resources and network bandwidth that data synchronization is allowed to consume. Because each node in a cluster is able to send and receive data, the speed at which data is replicated increases for larger clusters.

Automated replication policies

You can manually start a replication policy at any time, but you can also configure replication policies to start automatically based on source directory modifications or schedules.

You can configure a replication policy to run according to a schedule, so that you can control when replication is performed. You can also configure policies to replicate the data captured in snapshots of a directory. You can also configure a replication policy to start when SyncIQ detects a modification to the source directory, so that SyncIQ maintains a more current version of your data on the target cluster.

Scheduling a policy can be useful under the following conditions:

- You want to replicate data when user activity is minimal
- You can accurately predict when modifications will be made to the data

If a policy is configured to run according to a schedule, you can configure the policy not to run if no changes have been made to the contents of the source directory since the job was last run. However, if changes are made to the parent directory of the source directory or a sibling directory of the source directory, and then a snapshot of the parent directory is taken, SyncIQ will create a job for the policy, even if no changes have been made to the source directory. Also, if you monitor the cluster through the File System Analytics (FSA) feature of InsightIQ, the FSA job will create
snapshots of /ifs, which will most likely cause a replication job to start whenever the FSA job is run.

Replicating data contained in snapshots of a directory can be useful under the following conditions:

- You want to replicate data according to a schedule, and you are already generating snapshots of the source directory through a snapshot schedule
- You want to maintain identical snapshots on both the source and target cluster
- You want to replicate existing snapshots to the target cluster
  
  To do this, you must enable archival snapshots on the target cluster. This setting can only be enabled when the policy is created.

If a policy is configured to replicate snapshots, you can configure SyncIQ to replicate only snapshots that match a specified naming pattern.

Configuring a policy to start when changes are made to the source directory can be useful under the following conditions:

- You want to retain a up-to-date copy of your data at all times
- You are expecting a large number of changes at unpredictable intervals

For policies that are configured to start whenever changes are made to the source directory, SyncIQ checks the source directories every ten seconds. SyncIQ checks all files and directories underneath the source directory, regardless of whether those files or directories are excluded from replication, so SyncIQ might occasionally run a replication job unnecessarily. For example, assume that newPolicy replicates /ifs/data/media but excludes /ifs/data/media/temp. If a modification is made to /ifs/data/media/temp/file.txt, SyncIQ will run newPolicy, even though /ifs/data/media/temp/file.txt will not be replicated.

If a policy is configured to start whenever changes are made to the source directory, and a replication job fails, SyncIQ waits one minute before attempting to run the policy again. SyncIQ increases this delay exponentially for each failure up to a maximum of eight hours. You can override the delay by running the policy manually at any time.

After a job for the policy completes successfully, SyncIQ will resume checking the source directory every ten seconds.

If a policy is configured to start whenever changes are made to the source directory, you can configure SyncIQ to wait a specified period of time after the source directory is modified before starting a job.

---

**Note**

To avoid frequent synchronization of minimal sets of changes, and overtaxing system resources, we strongly advise against configuring continuous replication when the source directory is highly active. In such cases, it is often better to configure continuous replication with a change-triggered delay of several hours to consolidate groups of changes.

---

**Source and target cluster association**

SyncIQ associates a replication policy with a target cluster by marking the target cluster when the job runs for the first time. Even if you modify the name or IP address of the target cluster, the mark persists on the target cluster. When a replication policy is run, SyncIQ checks the mark to ensure that data is being replicated to the correct location.

On the target cluster, you can manually break an association between a replication policy and target directory. Breaking the association between a source and target
cluster causes the mark on the target cluster to be deleted. You might want to 
manually break a target association if an association is obsolete. If you break the 
association of a policy, the policy is disabled on the source cluster and you cannot run 
the policy. If you want to run the disabled policy again, you must reset the replication 
policy.

Breaking a policy association causes either a full replication or differential replication 
to occur the next time you run the replication policy. During a full or differential 
replication, SyncIQ creates a new association between the source and target clusters. 
Depending on the amount of data being replicated, a full or differential replication can 
take a very long time to complete.

**CAUTION**

Changes to the configuration of the target cluster outside of SyncIQ can 
introduce an error condition that effectively breaks the association between the 
source and target cluster. For example, changing the DNS record of the target 
cluster could cause this problem. If you need to make significant configuration 
changes to the target cluster outside of SyncIQ, make sure that your SyncIQ 
policies can still connect to the target cluster.

---

**Configuring SyncIQ source and target clusters with NAT**

Source and target clusters can use NAT (network address translation) for SyncIQ 
failover and fallback purposes, but must be configured appropriately.

In this scenario, source and target clusters are typically at different physical locations, 
use private, non-routable address space, and do not have direct connections to the 
Internet. Each cluster typically is assigned a range of private IP addresses. For 
example, a cluster with 12 nodes might be assigned IP addresses 192.168.10.11 to 
192.168.10.22.

To communicate over the public Internet, source and target clusters must have all 
incoming and outgoing data packets appropriately translated and redirected by a NAT-enabled 
firewall or router.

**CAUTION**

SyncIQ data is not encrypted. Running SyncIQ jobs over the public Internet 
provides no protection against data theft.

SyncIQ enables you to limit replication jobs to particular nodes within your cluster. For 
extreme example, if your cluster was made up of 12 nodes, you could limit replication jobs to 
just three of those nodes. For NAT support, you would need to establish a one-for-one 
association between the source and target clusters. So, if you are limiting replication 
jobs to three nodes on your source cluster, you must associate three nodes on your 
target cluster.

In this instance, you would need to configure static NAT, sometimes referred to as 
inbound mapping. On both the source and target clusters, for the private address 
assigned to each node, you would associate a static NAT address. For example:

<table>
<thead>
<tr>
<th>Source cluster</th>
<th>Target Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node name</td>
<td>Private address</td>
</tr>
<tr>
<td>source-1</td>
<td>192.168.10.11</td>
</tr>
</tbody>
</table>
To configure static NAT, you would need to edit the `/etc/local/hosts` file on all six nodes, and associate them with their counterparts by adding the appropriate NAT address and node name. For example, in the `/etc/local/hosts` file on the three nodes of the source cluster, the entries would look like:

```
10.1.2.11 target-1
10.1.2.12 target-2
10.1.2.13 target-3
```

Similarly, on the three nodes of the target cluster, you would edit the `/etc/local/hosts` file, and insert the NAT address and name of the associated node on the source cluster. For example, on the three nodes of the target cluster, the entries would look like:

```
10.8.8.201 source-1
10.8.8.202 source-2
10.8.8.203 source-3
```

When the NAT server receives packets of SyncIQ data from a node on the source cluster, the NAT server replaces the packet headers and the node's port number and internal IP address with the NAT server's own port number and external IP address. The NAT server on the source network then sends the packets through the Internet to the target network, where another NAT server performs a similar process to transmit the data to the target node. The process is reversed when the data fails back.

With this type of configuration, SyncIQ can determine the correct addresses to connect with, so that SyncIQ can send and receive data. In this scenario, no SmartConnect zone configuration is required.

For information about the ports used by SyncIQ, see the OneFS Security Configuration Guide for your OneFS version.

### Full and differential replication

If a replication policy encounters an issue that cannot be fixed (for example, if the association was broken on the target cluster), you might need to reset the replication policy. If you reset a replication policy, SyncIQ performs either a full replication or a differential replication the next time the policy is run. You can specify the type of replication that SyncIQ performs.

During a full replication, SyncIQ transfers all data from the source cluster regardless of what data exists on the target cluster. A full replication consumes large amounts of network bandwidth and can take a very long time to complete. However, a full replication is less strenuous on CPU usage than a differential replication.
During a differential replication, SyncIQ first checks whether a file already exists on the target cluster and then transfers only data that does not already exist on the target cluster. A differential replication consumes less network bandwidth than a full replication; however, differential replications consume more CPU. Differential replication can be much faster than a full replication if there is an adequate amount of available CPU for the replication job to consume.

Controlling replication job resource consumption

You can create rules that limit the network traffic created by replication jobs, the rate at which files are sent by replication jobs, the percent of CPU used by replication jobs, and the number of workers created for replication jobs.

If you limit the percentage of total workers that SyncIQ can create, the limit is applied to the total amount of workers that SyncIQ could create, which is determined by cluster hardware. Workers on the source cluster read and send data while workers on the target cluster receive and write data.

Note

File-operation rules might not work accurately for files that can take more than a second to transfer and for files that are not predictably similar in size.

Replication policy priority

When creating a replication policy, you can configure a policy to have priority over other jobs.

If multiple replication jobs are queued to be run because the maximum number of jobs are already running, jobs created by policies with priority will be run before jobs without priorities. For example, assume that 50 jobs are currently running. A job without priority is the created and queued to run; next, a job with priority is created and queued to run. The job with priority will run next, even though the job without priority has been queued for a longer period of time.

SyncIQ will also pause replication jobs without priority to allow jobs with priority to run. For example, assume that 50 jobs are already running, and one of them does not have priority. If a replication job with priority is created, SyncIQ will pause the replication job without priority and run the job with priority.

Replication reports

After a replication job completes, SyncIQ generates a replication report that contains detailed information about the job, including how long the job ran, how much data was transferred, and what errors occurred.

If a replication report is interrupted, SyncIQ might create a subreport about the progress of the job so far. If the job is then restarted, SyncIQ creates another subreport about the progress of the job until the job either completes or is interrupted again. SyncIQ creates a subreport each time the job is interrupted until the job completes successfully. If multiple subreports are created for a job, SyncIQ combines the information from the subreports into a single report.

SyncIQ routinely deletes replication reports. You can specify the maximum number of replication reports that SyncIQ retains and the length of time that SyncIQ retains replication reports. If the maximum number of replication reports is exceeded on a cluster, SyncIQ deletes the oldest report each time a new report is created.

You cannot customize the content of a replication report.
Note

If you delete a replication policy, SyncIQ automatically deletes any reports that were generated for that policy.

Replication snapshots

SyncIQ generates snapshots to facilitate replication, failover, and failback between Isilon clusters. Snapshots generated by SyncIQ can also be used for archival purposes on the target cluster.

Source cluster snapshots

SyncIQ generates snapshots on the source cluster to ensure that a consistent point-in-time image is replicated and that unaltered data is not sent to the target cluster.

Before running a replication job, SyncIQ creates a snapshot of the source directory. SyncIQ then replicates data according to the snapshot rather than the current state of the cluster, allowing users to modify source directory files while ensuring that an exact point-in-time image of the source directory is replicated.

For example, if a replication job of /ifs/data/dir/ starts at 1:00 PM and finishes at 1:20 PM, and /ifs/data/dir/file is modified at 1:10 PM, the modifications are not reflected on the target cluster, even if /ifs/data/dir/file is not replicated until 1:15 PM.

You can replicate data according to a snapshot generated with the SnapshotIQ software module. If you replicate data according to a SnapshotIQ snapshot, SyncIQ does not generate another snapshot of the source directory. This method can be useful if you want to replicate identical copies of data to multiple Isilon clusters.

SyncIQ generates source snapshots to ensure that replication jobs do not transfer unmodified data. When a job is created for a replication policy, SyncIQ checks whether it is the first job created for the policy. If it is not the first job created for the policy, SyncIQ compares the snapshot generated for the earlier job with the snapshot generated for the new job.

SyncIQ replicates only data that has changed since the last time a snapshot was generated for the replication policy. When a replication job is completed, SyncIQ deletes the previous source-cluster snapshot and retains the most recent snapshot until the next job is run.

Target cluster snapshots

When a replication job is run, SyncIQ generates a snapshot on the target cluster to facilitate failover operations. When the next replication job is created for the replication policy, the job creates a new snapshot and deletes the old one.

If a SnapshotIQ license has been activated on the target cluster, you can configure a replication policy to generate additional snapshots that remain on the target cluster even as subsequent replication jobs run.

SyncIQ generates target snapshots to facilitate failover on the target cluster regardless of whether a SnapshotIQ license has been configured on the target cluster. Failover snapshots are generated when a replication job completes. SyncIQ retains only one failover snapshot per replication policy, and deletes the old snapshot after the new snapshot is created.
If a SnapshotIQ license has been activated on the target cluster, you can configure SyncIQ to generate archival snapshots on the target cluster that are not automatically deleted when subsequent replication jobs run. Archival snapshots contain the same data as the snapshots that are generated for failover purposes. However, you can configure how long archival snapshots are retained on the target cluster. You can access archival snapshots the same way that you access other snapshots generated on a cluster.

Data failover and failback with SyncIQ

SyncIQ enables you to perform automated data failover and failback operations between Isilon clusters. If a cluster is rendered unusable, you can fail over to another Isilon cluster, enabling clients to continue accessing their data. If the unusable cluster becomes accessible again, you can fail back to the original Isilon cluster.

For the purposes of explaining failover and failback procedures, the cluster originally accessed by clients is referred to as the primary cluster, and the cluster that client data is replicated to is referred to as the secondary cluster. Failover is the process that allows clients to modify data on a secondary cluster. Failback is the process that allows clients to access data on the primary cluster again. If changes were made to data on the secondary cluster, those changes are replicated back to the primary cluster during failback.

Failover and failback can be useful in disaster recovery procedures. For example, if a primary cluster is damaged by a natural disaster, you can migrate clients to a secondary cluster until the primary cluster is repaired and then migrate the clients back to the primary cluster.

You can fail over and fail back to facilitate scheduled cluster maintenance. For example, if you are upgrading the primary cluster, you might want to migrate clients to a secondary cluster until the upgrade is complete and then migrate clients back to the primary cluster.

Note

Data failover and failback is not supported for compliance SmartLock directories. However, data failover and failback is supported for enterprise SmartLock directories.

Data failover

Data failover is the process of preparing data on a secondary cluster to be modified by clients. After you fail over to a secondary cluster, you can redirect clients to modify their data on the secondary cluster.

Before failover is performed, you must create and run a replication policy on the primary cluster. You initiate the failover process on the secondary cluster. Failover is performed per replication policy; to migrate data that is spread across multiple replication policies, you must initiate failover for each replication policy.

You can use any replication policy to fail over. However, if the action of the replication policy is set to copy, any file that was deleted on the primary cluster will be present on the secondary cluster. When the client connects to the secondary cluster, all files that were deleted on the primary cluster will be available to the client.

If you initiate failover for a replication policy while an associated replication job is running, the failover operation completes but the replication job fails. Because data might be in an inconsistent state, SyncIQ uses the snapshot generated by the last successful replication job to revert data on the secondary cluster to the last recovery point.
If a disaster occurs on the primary cluster, any modifications to data that were made after the last successful replication job started are not reflected on the secondary cluster. When a client connects to the secondary cluster, their data appears as it was when the last successful replication job was started.

Data failback

Data failback is the process of restoring clusters to the roles they occupied before a failover operation. After data failback is complete, the primary cluster hosts clients and replicates data to the secondary cluster for backup.

The first step in the failback process is updating the primary cluster with all of the modifications that were made to the data on the secondary cluster. The next step in the failback process is preparing the primary cluster to be accessed by clients. The final step in the failback process is resuming data replication from the primary to the secondary cluster. At the end of the failback process, you can redirect users to resume accessing their data on the primary cluster.

To update the primary cluster with the modifications that were made on the secondary cluster, SyncIQ must create a SyncIQ domain for the source directory.

You can fail back data with any replication policy that meets all of the following criteria:

- The source directory is not a compliance SmartLock directory.
- The policy has been failed over.
- The policy is a synchronization policy.
- The policy does not exclude any files or directories from replication.

Recovery times and objectives for SyncIQ

The Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) are measurements of the impacts that a disaster can have on business operations. You can calculate your RPO and RTO for a disaster recovery with replication policies.

RPO is the maximum amount of time for which data is lost if a cluster suddenly becomes unavailable. For an Isilon cluster, the RPO is the amount of time that has passed since the last completed replication job started. The RPO is never greater than the time it takes for two consecutive replication jobs to run and complete.

If a disaster occurs while a replication job is running, the data on the secondary cluster is reverted to the state it was in when the last replication job completed. For example, consider an environment in which a replication policy is scheduled to run every three hours, and replication jobs take two hours to complete. If a disaster occurs an hour after a replication job begins, the RPO is four hours, because it has been four hours since a completed job began replicating data.

RTO is the maximum amount of time required to make backup data available to clients after a disaster. The RTO is always less than or approximately equal to the RPO, depending on the rate at which replication jobs are created for a given policy.

If replication jobs run continuously, meaning that another replication job is created for the policy before the previous replication job completes, the RTO is approximately equal to the RPO. When the secondary cluster is failed over, the data on the cluster is reset to the state it was in when the last replication job completed; resetting the data takes an amount of time proportional to the time it took users to modify the data.

If replication jobs run on a scheduled interval, meaning that there is a period of time after a replication job completes before the next replication job for the policy starts, the relationship between RTO and RPO depends on whether a replication job is running.
when the disaster occurs. If a job is in progress when a disaster occurs, the RTO is roughly equal to the RPO. However, if a job is not running when a disaster occurs, the RTO is negligible because the secondary cluster was not modified since the last replication job ran, and the failover process is almost instantaneous.

**RPO Alerts**

You can configure SyncIQ to create OneFS events that alert you to the fact that a specified Recovery Point Objective (RPO) has been exceeded. You can view these events through the same interface as other OneFS events.

The events have an event ID of 400040020. The event message for these alerts follows the following format:

```
SW_SIQ_RPO_EXCEEDED: SyncIQ RPO exceeded for policy <replication_policy>
```

For example, assume you set an RPO of 5 hours; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ will create a OneFS event.

**Replication policy priority**

When creating a replication policy, you can configure a policy to have priority over other jobs.

If multiple replication jobs are queued to be run because the maximum number of jobs are already running, jobs created by policies with priority will be run before jobs without priorities. For example, assume that 50 jobs are currently running. A job without priority is the created and queued to run; next, a job with priority is created and queued to run. The job with priority will run next, even though the job without priority has been queued for a longer period of time.

SyncIQ will also pause replication jobs without priority to allow jobs with priority to run. For example, assume that 50 jobs are already running, and one of them does not have priority. If a replication job with priority is created, SyncIQ will pause the replication job without priority and run the job with priority.

**SyncIQ license functionality**

You can replicate data to another Isilon cluster only if you activate a SyncIQ license on both the local cluster and the target cluster.

If a SyncIQ license becomes inactive, you cannot create, run, or manage replication policies. Also, all previously created replication policies are disabled. Replication policies that target the local cluster are also disabled. However, data that was previously replicated to the local cluster is still available.

**Creating replication policies**

You can create replication policies that determine when data is replicated with SyncIQ.
Excluding directories in replication

You can exclude directories from being replicated by replication policies even if the directories exist under the specified source directory.

Note

Failback is not supported for replication policies that exclude directories.

By default, all files and directories under the source directory of a replication policy are replicated to the target cluster. However, you can prevent directories under the source directory from being replicated.

If you specify a directory to exclude, files and directories under the excluded directory are not replicated to the target cluster. If you specify a directory to include, only the files and directories under the included directory are replicated to the target cluster; any directories that are not contained in an included directory are excluded.

If you both include and exclude directories, any excluded directories must be contained in one of the included directories; otherwise, the excluded-directory setting has no effect. For example, consider a policy with the following settings:

- The root directory is /ifs/data
- The included directories are /ifs/data/media/music and /ifs/data/media/movies
- The excluded directories are /ifs/data/archive and /ifs/data/media/music/working

In this example, the setting that excludes the /ifs/data/archive directory has no effect because the /ifs/data/archive directory is not under either of the included directories. The /ifs/data/archive directory is not replicated regardless of whether the directory is explicitly excluded. However, the setting that excludes the /ifs/data/media/music/working directory does have an effect, because the directory would be replicated if the setting was not specified.

In addition, if you exclude a directory that contains the source directory, the exclude-directory setting has no effect. For example, if the root directory of a policy is /ifs/data, explicitly excluding the /ifs directory does not prevent /ifs/data from being replicated.

Any directories that you explicitly include or exclude must be contained in or under the specified root directory. For example, consider a policy in which the specified root directory is /ifs/data. In this example, you could include both the /ifs/data/media and the /ifs/data/users/ directories because they are under /ifs/data.

Excluding directories from a synchronization policy does not cause the directories to be deleted on the target cluster. For example, consider a replication policy that synchronizes /ifs/data on the source cluster to /ifs/data on the target cluster. If the policy excludes /ifs/data/media from replication, and /ifs/data/media/file exists on the target cluster, running the policy does not cause /ifs/data/media/file to be deleted from the target cluster.

Excluding files in replication

If you do not want specific files to be replicated by a replication policy, you can exclude them from the replication process through file-matching criteria statements.
You can configure file-matching criteria statements during the replication-policy creation process.

---

**Note**

You cannot fail back replication policies that exclude files.

A file-criteria statement can include one or more elements. Each file-criteria element contains a file attribute, a comparison operator, and a comparison value. You can combine multiple criteria elements in a criteria statement with Boolean "AND" and "OR" operators. You can configure any number of file-criteria definitions.

Configuring file-criteria statements can cause the associated jobs to run slowly. It is recommended that you specify file-criteria statements in a replication policy only if necessary.

Modifying a file-criteria statement will cause a full replication to occur the next time that a replication policy is started. Depending on the amount of data being replicated, a full replication can take a very long time to complete.

For synchronization policies, if you modify the comparison operators or comparison values of a file attribute, and a file no longer matches the specified file-matching criteria, the file is deleted from the target the next time the job is run. This rule does not apply to copy policies.

### File criteria options

You can configure a replication policy to exclude files that meet or do not meet specific criteria.

You can specify file criteria based on the following file attributes:

- **Date created**
  
  Includes or excludes files based on when the file was created. This option is available for copy policies only. You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

- **Date accessed**
  
  Includes or excludes files based on when the file was last accessed. This option is available for copy policies only, and only if the global access-time-tracking option of the cluster is enabled. You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

- **Date modified**
  
  Includes or excludes files based on when the file was last modified. This option is available for copy policies only. You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

- **File name**
  
  Includes or excludes files based on the file name. You can specify to include or exclude full or partial names that contain specific text. The following wildcard characters are accepted:
Note

Alternatively, you can filter file names by using POSIX regular-expression (regex) text. Isilon clusters support IEEE Std 1003.2 (POSIX.2) regular expressions. For more information about POSIX regular expressions, see the BSD man pages.

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, m* matches movies and m123.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Matches any characters contained in the brackets, or a range of characters separated by a dash. For example, b[aei]t matches bat, bet, and bit. For example, 1[4-7]2 matches 142, 152, 162, and 172. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, b[!ie] matches bat but not bit or bet. You can match a bracket within a bracket if it is either the first or last character. For example, [[c]at matches cat and [at. You can match a dash within a bracket if it is either the first or last character. For example, car[-s] matches cars and car-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, t?p matches tap, tip, and top.</td>
</tr>
</tbody>
</table>

Path

Includes or excludes files based on the file path. This option is available for copy policies only. You can specify to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters *, ?, and [ ].

Size

Includes or excludes files based on their size.
Note

File sizes are represented in multiples of 1024, not 1000.

Type
Includes or excludes files based on one of the following file-system object types:
- Soft link
- Regular file
- Directory

Configure default replication policy settings

You can configure default settings for replication policies. If you do not modify these settings when creating a replication policy, the specified default settings are applied.

Procedure
1. Run the `isi sync settings modify` command.

   The following command configures SyncIQ to delete replication reports that are older than 2 years:

   ```
   isi sync settings modify --report-max-age 2Y
   ```

Create a replication policy

You can create a replication policy with SyncIQ that defines how and when data is replicated to another Isilon cluster. A replication policy specifies the target cluster, source and target directories, and directories and files to be excluded during replication.

CAUTION

In a SyncIQ replication policy, OneFS enables you to specify a source directory that is a target directory, or is contained within a target directory, from a different replication policy. Referred to as cascading replication, this use case is specifically for backup purposes, and should be configured carefully. OneFS does not allow failback in such cases.

If you modify any of the following policy settings after a policy is run, OneFS performs either a full or differential replication the next time the policy is run.

- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster name or address

This applies only if you modify a replication policy to specify a different target cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed. Note also that SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would cause the job to fail.
Target directory

Note

If you create a replication policy for a SmartLock compliance directory, the SyncIQ and SmartLock compliance domains must be configured at the same root directory level. A SmartLock compliance directory cannot be nested inside a SyncIQ directory.

Procedure

1. Run the `isi sync policies create` command.

   The following command creates a policy that replicates the directory `/ifs/data/source` on the source cluster to `/ifs/data/target` on target cluster `10.1.99.36` every week. The command also creates archival snapshots on the target cluster:

   ```
   isi sync policies create mypolicy sync /ifs/data/source 10.1.99.36 /ifs/data/target --schedule "Every Sunday at 12:00 AM" --target-snapshot-archive on --target-snapshot-expiration 1Y --target-snapshot-pattern "%{PolicyName}-%{SrcCluster}-%Y-%m-%d"
   ```

Create a SyncIQ domain

You can create a SyncIQ domain to increase the speed at which failback is performed for a replication policy. Because you can fail back only synchronization policies, it is not necessary to create SyncIQ domains for copy policies.

Failing back a replication policy requires that a SyncIQ domain be created for the source directory. OneFS automatically creates a SyncIQ domain during the failback process. However, if you intend on failing back a replication policy, it is recommended that you create a SyncIQ domain for the source directory of the replication policy while the directory is empty. Creating a domain for a directory that contains less data takes less time.

Procedure

1. Run the `isi job jobs start` command.

   The following command creates a SyncIQ domain for `/ifs/data/source`:

   ```
   isi job jobs start domainmark --root /ifs/data/media --dm-type SyncIQ
   ```

Assess a replication policy

Before running a replication policy for the first time, you can view statistics on the files that would be affected by the replication without transferring any files. This can be useful if you want to preview the size of the data set that will be transferred if you run the policy.

You can assess only replication policies that have never been run before.

Procedure

1. Run the `isi sync jobs start` command with the `--test` option.
The following command creates a report about how much data will be transferred when weeklySync is run:

```plaintext
isi sync jobs start weeklySync --test
```

2. To view the assessment report, run the `isi sync reports view` command. The following command displays the assessment report for weeklySync:

```plaintext
isi sync reports view weeklySync 1
```

### Managing replication to remote clusters

You can manually run, view, assess, pause, resume, cancel, resolve, and reset replication jobs that target other clusters.

After a policy job starts, you can pause the job to suspend replication activities. Afterwards, you can resume the job, continuing replication from the point where the job was interrupted. You can also cancel a running or paused replication job if you want to free the cluster resources allocated for the job. A paused job reserves cluster resources whether or not the resources are in use. A cancelled job releases its cluster resources and allows another replication job to consume those resources. No more than five running and paused replication jobs can exist on a cluster at a time. However, an unlimited number of canceled replication jobs can exist on a cluster. If a replication job remains paused for more than a week, SyncIQ automatically cancels the job.

### Start a replication job

You can manually start a replication job for a replication policy at any time. You can also replicate data according to a snapshot created by SnapshotIQ. You cannot replicate data according to a snapshot generated by SyncIQ.

**Procedure**

1. Run the `isi sync jobs start` command.

   The following command starts weeklySync:

   ```plaintext
   isi sync jobs start weeklySync
   ```

   The following command replicates the source directory of weeklySync according to the snapshot HourlyBackup_07-15-2013_23:00:

   ```plaintext
   isi sync jobs start weeklySync \
   --source-snapshot HourlyBackup_07-15-2013_23:00
   ```

### Pause a replication job

You can pause a running replication job and then resume the job later. Pausing a replication job temporarily stops data from being replicated, but does not free the cluster resources replicating the data.

**Procedure**

1. Run the `isi sync jobs pause` command.
The following command pauses weeklySync:

```
isi sync jobs pause weeklySync
```

**Resume a replication job**

You can resume a paused replication job.

**Procedure**

1. Run the `isi sync jobs resume` command.

The following command resumes weeklySync:

```
isi sync jobs resume weeklySync
```

**Cancel a replication job**

You can cancel a running or paused replication job. Cancelling a replication job stops data from being replicated and frees the cluster resources that were replicating data. You cannot resume a cancelled replication job; to restart replication, you must start the replication policy again.

**Procedure**

1. Run the `isi sync jobs cancel` command.

The following command cancels weeklySync:

```
isi sync jobs cancel weeklySync
```

**View active replication jobs**

You can view information about replication jobs that are currently running or paused.

**Procedure**

1. View all active replication jobs by running the following command:

```
isi sync jobs list
```

2. To view detailed information about a specific replication job, run the `isi sync jobs view` command.

The following command displays detailed information about a replication job created by weeklySync:

```
isi sync jobs view weeklySync
```

The system displays output similar to the following example:

```
Policy Name: weeklySync
   ID: 3
   State: running
   Action: run
   Duration: 5s
   Start Time: 2013-07-16T23:12:00
```
Replication job information

You can view information about replication jobs.

The following information is displayed in the output of the `isi snapshot settings view` command:

- **Policy Name**
  - The name of the associated replication policy.
- **ID**
  - The ID of the replication job.
- **State**
  - The status of the job.
- **Action**
  - The type of replication policy.

Initiating data failover and failback with SyncIQ

You can fail over from one Isilon cluster to another if, for example, your primary cluster becomes unavailable. You can fail back when the primary cluster becomes available again. You can revert failover if you decide that the failover was unnecessary, or if you failed over for testing purposes.

Note

Data failover and failback are not supported for compliance SmartLock directories. However, failover and failback are supported for enterprise SmartLock directories. Although you cannot fail over compliance SmartLock directories, you can recover them on a target cluster. Also, although you cannot fail back compliance SmartLock directories, you can migrate them back to the source cluster.

Fail over data to a secondary cluster

You can fail over to a secondary Isilon cluster if, for example, your primary cluster becomes unavailable.

**Before you begin**

You must have created and successfully run a replication policy on the primary cluster. This action replicated data to the secondary cluster.

Note

Data failover is not supported for compliance SmartLock directories. However, data failover is supported for enterprise SmartLock directories.

Complete the following procedure for each replication policy that you want to fail over.

**Procedure**

1. If your primary cluster is still online, complete the following steps:
   a. Stop all writes to the replication policy’s path.
      This ensures that new data will not be written to the policy path.
b. Modify the replication policy so that it is set to run only manually.

This prevents the policy on the primary cluster from automatically running a replication job. If the policy on the primary cluster runs a replication job while writes are allowed to the target directory, the job will fail and the replication policy will be deactivated. If this happens, modify the policy so that it is set to run only manually, resolve the policy, and complete the failback process. After you complete the failback process, you can modify the policy to run according to a schedule again.

The following command ensures that the policy weeklySync runs only manually:

```
isi sync policies modify weeklySync --schedule ""
```

2. On the secondary cluster, run the `isi sync recovery allow-write` command.

The following command enables replicated directories and files specified in the weeklySync policy to be writable:

```
isi sync recovery allow-write weeklySync
```

3. Direct your users to use the secondary cluster.

### Revert a failover operation

Failover reversion undoes a failover operation on a secondary cluster, enabling you to replicate data from the primary cluster to the secondary cluster again. Failover reversion is useful if the primary cluster becomes available before data is modified on the secondary cluster or if you failed over to a secondary cluster for testing purposes.

**Before you begin**

Fail over a replication policy.

Reverting a failover operation does not migrate modified data back to the primary cluster. To migrate data that clients have modified on the secondary cluster, you must fail back to the primary cluster.

**Note**

Failover reversion is not supported for SmartLock directories.

Complete the following procedure for each replication policy that you want to fail over.

**Procedure**

1. Run the `isi sync recovery allow-write` command with the `--revert` option.

   For example, the following command reverts a failover operation for `newPolicy`:

   ```
   isi sync recovery allow-write newPolicy --revert
   ```
Fail back data to a primary cluster

After you fail over to a secondary cluster, you can fail back to the primary cluster.

Before you begin

Fail over by executing a replication policy from the primary cluster. Also, ensure that your primary cluster is back online.

Procedure

1. Create mirror policies on the secondary cluster by running the `isi sync recovery resync-prep` command on the primary cluster.
   
   The following command creates a mirror policy for `weeklySync`:
   
   ```
   isi sync recovery resync-prep weeklySync
   ```
   
   SyncIQ names mirror policies according to the following pattern:
   
   `<replication-policy-name>_mirror`

2. Before beginning the failback process, prevent clients from accessing the secondary cluster.
   
   This action ensures that SyncIQ fails back the latest data set, including all changes that users made to data on the secondary cluster while the primary cluster was out of service. We recommend that you wait until client activity is low before preventing access to the secondary cluster.

3. On the secondary cluster, run the `isi sync jobs start` command to run the mirror policy and replicate data to the primary cluster.
   
   The following command runs a mirror policy named `weeklySync_mirror` immediately:
   
   ```
   isi sync jobs start weeklySync_mirror
   ```
   
   Alternatively, you can modify the mirror policy to run on a particular schedule. The following command schedules a mirror policy named `weeklySync_mirror` to run daily at 12:01 AM:
   
   ```
   isi sync modify weeklySync_mirror --enabled yes --schedule "every day at 12:01 AM"
   ```
   
   If specifying a schedule for the mirror policy, you need only allow the mirror policy to run once at the scheduled time. After that, you should set the mirror policy back to a manual schedule.

4. On the primary cluster, allow writes to the target directories of the mirror policy by running the `isi sync recovery allow-write` command.
   
   The following command allows writes to the directories specified in the `weeklySync_mirror` policy:
   
   ```
   isi sync recovery allow-write weeklySync_mirror
   ```
5. On the secondary cluster, complete the failback process by running the `isi sync recovery resync-prep` command for the mirror policy.

   The following command completes the failback process for `weeklySync_mirror` by placing the secondary cluster back into read-only mode and ensuring that the data sets are consistent on both the primary and secondary clusters:

   ```bash
   isi sync recovery resync-prep weeklySync_mirror
   ```

   After you finish

   Redirect clients to begin accessing the primary cluster. Although not required, it is safe to remove a mirror policy after failback has completed successfully.

   **Performing disaster recovery for SmartLock directories**

   Although you cannot fail over or fail back compliance SmartLock directories, you can recover compliance directories on a target cluster and migrate them back to the source cluster.

   **Note**

   Data failover and failback is supported for SmartLock enterprise directories.

   **Recover SmartLock compliance directories on a target cluster**

   You can recover compliance SmartLock directories that you have replicated to a target cluster.

   Create and successfully run a replication policy.

   Complete the following procedure for each SmartLock directory that you want to recover.

   **Procedure**

   1. On the target cluster, enable writes to the target SmartLock directories.

      • If the last replication job completed successfully and a replication job is not currently running, run the `isi sync recovery allow-write` command.

      For example, the following command enables writes to the target directory of SmartLockSync:

      ```bash
      isi sync recovery allow-write SmartLockSync
      ```

      • If a replication job is currently running, wait until the replication job completes, and then run the `isi sync recovery allow-write` command.

      For example, the following command enables writes to the target directory of SmartLockSync:

      ```bash
      isi sync recovery allow-write SmartLockSync
      ```

      • If the primary cluster became unavailable while a replication job was running, select run the `isi sync target break` command.
For example, the following command enables writes to the target directory of SmartLockSync:

```bash
isi sync target break SmartLockSync
```

2. If you ran `isi sync target break`, restore any files that are left in an inconsistent state.
   
   a. Delete all files that are not committed to a WORM state from the target directory.
   
   b. Copy all files from the failover snapshot to the target directory.

   Failover snapshots are named according to the following naming pattern:

   ```text
   SIQ-Failover-<policy-name>-<year>-<month>-<day>_<hour>-<minute>-<second>
   ```

   Snapshots are located under the hidden `/ifs/.snapshot` directory.

3. If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directory of the replication policy, apply those settings to the target directory.

   Because autocommit information is not transferred to the target cluster, files that were scheduled to be committed to a WORM state on the source cluster will not be scheduled to be committed at the same time on the target cluster. To ensure that all files are retained for the appropriate time period, you can commit all files in target SmartLock directories to a WORM state. For example, the following command automatically commits all files in `/ifs/data/smartlock` to a WORM state after one minute.

   ```bash
   isi worm domains modify --domain /ifs/data/smartlock --autocommit-offset 1m
   ```

### Migrate SmartLock compliance directories

You might want to migrate SmartLock compliance directories if you restored the compliance directories on a target cluster and want to transfer those directories either back to the source cluster or to a new cluster.

**Procedure**

1. On a cluster, create a replication policy for each directory that you want to migrate.

   The policies must meet the following requirements:

   - The source directory is the SmartLock directory that you are migrating.
   - The target directory must be an empty SmartLock directory. The directory must be of the same SmartLock type as the source directory of a policy you are failing back. For example, if the target directory is a compliance directory, the source must also be a compliance directory.

2. Replicate data to the target cluster by running the policies you created.

   You can replicate data either by manually starting the policies or by specifying a policy schedule.
3. (Optional) To ensure that SmartLock protection is enforced for all files, commit all files in the SmartLock directory to a WORM state.

Because autocommit information is not transferred to the target cluster, files that were scheduled to be committed to a WORM state on the source cluster will not be scheduled to be committed at the same time on the target cluster. To ensure that all files are retained for the appropriate time period, you can commit all files in target SmartLock directories to a WORM state.

For example, the following command automatically commits all files in /ifs/data/smartlock to a WORM state after one minute:

```bash
isi worm domains modify --domain /ifs/data/smartlock --autocommit-offset 1m
```

This step is necessarily only if you have configured an autocommit time period for the SmartLock directory.

4. Prevent clients from accessing the source cluster and run the policy that you created.

To minimize impact to clients, it is recommended that you wait until client access is low before preventing client access to the cluster.

5. On the target cluster, enable writes to the target directories of the replication policies by running the `isi sync recovery allow-writes` command.

For example, the following command enables writes to the target directory of SmartLockSync:

```bash
isi sync recovery allow-writes SmartLockSync
```

6. If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directories of the replication policies, apply those settings to the target directories.

7. Delete the copy of your SmartLock data on the source cluster.

If the SmartLock directories are compliance directories or enterprise directories with the privileged delete functionality permanently disabled, you cannot recover the space consumed by the source SmartLock directories until all files are released from a WORM state. If you want to free the space before files are released from a WORM state, contact Isilon Technical Support for information about reformatting your cluster.

### Managing replication policies

You can modify, view, enable, and disable replication policies.

### Modify a replication policy

You can modify the settings of a replication policy.

If you modify any of the following policy settings after the policy runs, OneFS performs either a full or differential replication the next time the policy runs:

- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster
  This applies only if you target a different cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed.
- Target directory

Procedure

1. Run the `isi sync policies modify` command.

   Assuming that weeklySync has been reset and has not been run since it was reset, the following command causes a differential replication to be performed the next time weeklySync is run:

   ```bash
   isi sync policies modify weeklySync --target-compare-initial-sync on
   ```

   **Delete a replication policy**

   You can delete a replication policy. Once a policy is deleted, SyncIQ no longer creates replication jobs for the policy. Deleting a replication policy breaks the target association on the target cluster, and allows writes to the target directory.

   If you want to temporarily suspend a replication policy from creating replication jobs, you can disable the policy, and then enable the policy again later.

   Procedure

   1. Run the `isi sync policies delete` command.

      The following command deletes weeklySync from the source cluster and breaks the target association on the target cluster:

      ```bash
      isi sync policies delete weeklySync
      ```

      **Note**

      The operation will not succeed until SyncIQ can communicate with the target cluster; until then, the policy will still appear in the output of the `isi sync policies list` command. After the connection between the source cluster and target cluster is reestablished, SyncIQ will delete the policy the next time that the job is scheduled to run; if the policy is configured to run only manually, you must manually run the policy again. If SyncIQ is permanently unable to communicate with the target cluster, run the `isi sync policies delete` command with the `--local-only` option. This will delete the policy from the local cluster only and not break the target association on the target cluster.
Enable or disable a replication policy

You can temporarily suspend a replication policy from creating replication jobs, and then enable it again later.

Note

If you disable a replication policy while an associated replication job is running, the running replication job is not interrupted. However, the policy will not create another job until the policy is enabled.

Procedure

1. Run either the `isi sync policies enable` or the `isi sync policies disable` command.

   The following command enables weeklySync:

   ```
   isi sync policies enable weeklySync
   ```

   The following command disables weeklySync:

   ```
   isi sync policies disable weeklySync
   ```

View replication policies

You can view information about replication policies.

Procedure

1. View information about all replication policies by running the following command:

   ```
   isi sync policies list
   ```

2. (Optional) To view detailed information about a specific replication policy, run the `isi sync policies view` command.

   The following command displays detailed information about weeklySync:

   ```
   isi sync policies view weeklySync
   ```

   The system displays output similar to the following example:

   ```
   ID: dd16d277ff995a78e9affbba6f6e2919
   Name: weeklySync
   Path: /ifs/data/archive
   Action: sync
   Enabled: No
   Target: localhost
   Description: Check Integrity: Yes
   Source Include Directories: -
   Source Exclude Directories: -
   Source Subnet: -
   Source Pool: -
   Source Match Criteria: -
   ```
Replication policy information

You can view information about replication policies through the output of the `isi sync policies list` command.

**Name**

The name of the policy.

**Path**

The path of the source directory on the source cluster.

**Action**

The type of replication policy.

**Enabled**

Whether the policy is enabled or disabled.

**Target**

The IP address or fully qualified domain name of the target cluster.

Managing replication to the local cluster

You can interrupt replication jobs that target the local cluster.

You can cancel a currently running job that targets the local cluster, or you can break the association between a policy and its specified target. Breaking a source and target cluster association causes SyncIQ to perform a full replication the next time the policy is run.
Cancel replication to the local cluster

You can cancel a replication job that is targeting the local cluster.

Procedure

1. Run the `isi sync target cancel` command.
   - To cancel a job, specify a replication policy. For example, the following command cancels a replication job created according to `weeklySync`:
     
     ```bash
     isi sync target cancel weeklySync
     ```
   - To cancel all jobs targeting the local cluster, run the following command:
     
     ```bash
     isi sync target cancel --all
     ```

Break local target association

You can break the association between a replication policy and the local cluster. Breaking this association requires you to reset the replication policy before you can run the policy again.

Note

After a replication policy is reset, SyncIQ performs a full or differential replication the next time the policy is run. Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete.

Procedure

1. Run the `isi sync target break` command.
   The following command breaks the association between `weeklySync` and the local cluster:
     
     ```bash
     isi sync target break weeklySync
     ```

View replication policies targeting the local cluster

You can view information about replication policies that are currently replicating data to the local cluster.

Procedure

1. View information about all replication policies that are currently targeting the local cluster by running the following command:
     
     ```bash
     isi sync target list
     ```

2. To view detailed information about a specific replication policy, run the `isi sync target view` command.
   The following command displays detailed information about `weeklySync`:
     
     ```bash
     isi sync target view weeklySync
     ```
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Name</th>
<th>weeklySync</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>cluster</td>
</tr>
<tr>
<td>Target Path</td>
<td>/ifs/data/sometarget</td>
</tr>
<tr>
<td>Last Job State</td>
<td>finished</td>
</tr>
<tr>
<td>FOFB State</td>
<td>writes_disabled</td>
</tr>
<tr>
<td>Source Cluster GUID</td>
<td>000c295159ae74fcde517c1b85adc03daff9</td>
</tr>
<tr>
<td>Last Source Coordinator IP</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>Legacy Policy</td>
<td>No</td>
</tr>
<tr>
<td>Last Update</td>
<td>2013-07-17T15:39:51</td>
</tr>
</tbody>
</table>

Remote replication policy information

You can view information about replication policies that are currently targeting the local cluster through the output of the `isi sync target list` command.

- **Name**
  - The name of the replication policy.

- **Source**
  - The name of the source cluster.

- **Target Path**
  - The path of the target directory on the target cluster.

- **Last Job State**
  - The state of the most recent replication job for the policy.

- **FOFB State**
  - The failover-failback state of the target directory.

Managing replication performance rules

You can manage the impact of replication on cluster performance by creating rules that limit the network traffic created and the rate at which files are sent by replication jobs.

Create a network traffic rule

You can create a network traffic rule that limits the amount of network traffic that replication policies are allowed to generate during a specified time period.

**Procedure**

1. Run the `isi sync rules create` command.

   The following command creates a network traffic rule that limits bandwidth consumption to 100 KB per second from 9:00 AM to 5:00 PM every weekday:

   ```
   isi sync rules create bandwidth 9:00-17:00 M-F 100
   ```
Create a file operations rule

You can create a file-operations rule that limits the number of files that replication jobs can send per second.

Procedure
1. Run the `isi sync rules create` command.

   The following command creates a file-operations rule that limits the file-send rate to 3 files per second from 9:00 AM to 5:00 PM every weekday:

   ```
   isi sync rules create file_count 9:00-17:00 M-F 3
   ```

Modify a performance rule

You can modify a performance rule.

Procedure
1. (Optional) To identify the ID of the performance rule you want to modify, run the following command:

   ```
   isi sync rules list
   ```

2. Modify a performance rule by running the `isi sync rules modify` command.

   The following command causes a performance rule with an ID of bw-0 to be enforced only on Saturday and Sunday:

   ```
   isi sync rules modify bw-0 --days X,S
   ```

Delete a performance rule

You can delete a performance rule.

Procedure
1. (Optional) To identify the ID of the performance rule you want to modify, run the following command:

   ```
   isi sync rules list
   ```

2. Delete a performance rule by running the `isi sync rules delete` command.

   The following command deletes a performance rule with an ID of bw-0:

   ```
   isi sync rules delete bw-0
   ```
Enable or disable a performance rule

You can disable a performance rule to temporarily prevent the rule from being enforced. You can also enable a performance rule after it has been disabled.

Procedure

1. (Optional) To identify the ID of the performance rule you want to enable or disable, run the following command:
   
   ```
   isi sync rules list
   ```

2. Run the `isi sync rules modify` command.
   
The following command enables a performance rule with an ID of bw-0:
   
   ```
   isi sync rules modify bw-0 --enabled true
   ```

   The following command disables a performance rule with an ID of bw-0:
   
   ```
   isi sync rules modify bw-0 --enabled false
   ```

View performance rules

You can view performance rules.

Procedure

1. View information about all performance rules by running the following command:
   
   ```
   isi sync rules list
   ```

2. (Optional) To view detailed information about a specific performance rule, run the `isi sync rules view` command.
   
The following command displays detailed information about a performance rule with an ID of bw-0:
   
   ```
   isi sync rules view --id bw-0
   ```

The system displays output similar to the following example:

```
ID: bw-0
   Enabled: Yes
   Type: bandwidth
   Limit: 100 kbps
   Days: Sun,Sat
   Schedule
     Begin : 09:00
     End : 17:00
   Description: Bandwidth rule for weekdays
```
Managing replication reports

In addition to viewing replication reports, you can configure how long reports are retained on the cluster. You can also delete any reports that have passed their expiration period.

Configure default replication report settings

You can configure the default amount of time that SyncIQ retains replication reports for. You can also configure the maximum number of reports that SyncIQ retains for each replication policy.

Procedure

1. Run the `isi sync settings modify` command.

   The following command causes OneFS to delete replication reports that are older than 2 years:

   ```
   isi sync settings modify --report-max-age 2Y
   ```

Delete replication reports

Replication reports are routinely deleted by SyncIQ after the expiration date for the reports has passed. SyncIQ also deletes reports after the number of reports exceeds the specified limit. Excess reports are periodically deleted by SyncIQ; however, you can manually delete all excess replication reports at any time. This procedure is available only through the command-line interface (CLI).

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster, and log in.
2. Delete excess replication reports by running the following command:

   ```
   isi sync reports rotate
   ```

View replication reports

You can view replication reports and subreports.

Procedure

1. View a list of all replication reports by running the following command:

   ```
   isi sync reports list
   ```

2. View a replication report by running the `isi sync reports view` command.

   The following command displays a replication report for weeklySync:

   ```
   isi sync reports view weeklySync 2
   ```

3. (Optional) To view a list of subreports for a report, run the `isi sync reports subreports list` command.
The following command displays subreports for weeklySync:

```shell
isi sync reports subreports list weeklySync 1
```

4. **(Optional) To view a subreport, run the** `isi sync reports subreports view` **command.**

The following command displays a subreport for weeklySync:

```shell
isi sync reports subreports view weeklySync 1 2
```

The system displays output similar to the following example:

```
Policy Name: weeklySync
  Job ID: 1
  Subreport ID: 2
  Start Time: 2013-07-17T21:59:10
  End Time: 2013-07-17T21:59:15
  Action: run
  State: finished
  Policy ID: a358db8b248bf432c71543e0f02df64e
  Sync Type: initial
  Duration: 5s
  Errors: -
  Source Directories Visited: 0
  Source Directories Deleted: 0
  Target Directories Deleted: 0
  Source Directories Created: 0
  Target Directories Created: 0
  Source Directories Linked: 0
  Target Directories Linked: 0
  Source Directories Unlinked: 0
  Target Directories Unlinked: 0
  Num Retransmitted Files: 0
  Retransmitted Files: -
  Total Files: 0
    Files New: 0
  Source Files Deleted: 0
  Files Changed: 0
  Target Files Deleted: 0
  Up To Date Files Skipped: 0
  User Conflict Files Skipped: 0
  Error Io Files Skipped: 0
  Error Net Files Skipped: 0
  Error Checksum Files Skipped: 0
  Bytes Transferred: 245
  Total Network Bytes: 245
  Total Data Bytes: 20
  File Data Bytes: 20
  Sparse Data Bytes: 0
  Target Snapshots: SIQ-Failover-
  Total Phases: 2
  Phases
    Phase : STF_PHASE_IDMAP_SEND
      Start Time : 2013-07-17T21:59:11
```

---

View replication reports
Replication report information

You can view information about replication jobs through the Reports table.

Policy Name
The name of the associated policy for the job. You can view or edit settings for the policy by clicking the policy name.

Status
Displays the status of the job. The following job statuses are possible:

- **Running**
  The job is currently running without error.

- **Paused**
  The job has been temporarily paused.

- **Finished**
  The job completed successfully.

- **Failed**
  The job failed to complete.

Started
Indicates when the job started.

Ended
Indicates when the job ended.

Duration
Indicates how long the job took to complete.

Transferred
The total number of files that were transferred during the job run, and the total size of all transferred files. For assessed policies, Assessment appears.

Source Directory
The path of the source directory on the source cluster.

Target Host
The IP address or fully qualified domain name of the target cluster.

Action
Displays any report-related actions that you can perform.

Managing failed replication jobs

If a replication job fails due to an error, SyncIQ might disable the corresponding replication policy. For example SyncIQ might disable a replication policy if the IP or
hostname of the target cluster is modified. If a replication policy is disabled, the policy cannot be run.

To resume replication for a disabled policy, you must either fix the error that caused the policy to be disabled, or reset the replication policy. It is recommended that you attempt to fix the issue rather than reset the policy. If you believe you have fixed the error, you can return the replication policy to an enabled state by resolving the policy. You can then run the policy again to test whether the issue was fixed. If you are unable to fix the issue, you can reset the replication policy. However, resetting the policy causes a full or differential replication to be performed the next time the policy is run.

Note
Depending on the amount of data being synchronized or copied, full and differential replications can take a very long time to complete.

Resolve a replication policy
If SyncIQ disables a replication policy due to a replication error, and you fix the issue that caused the error, you can resolve the replication policy. Resolving a replication policy enables you to run the policy again. If you cannot resolve the issue that caused the error, you can reset the replication policy.

Procedure
1. Run the `isi sync policies resolve` command.
   
   The following command resolves weeklySync:

   ```
   isi sync policies resolve weeklySync
   ```

Reset a replication policy
If a replication job encounters an error that you cannot resolve, you can reset the corresponding replication policy. Resetting a policy causes OneFS to perform a full or differential replication the next time the policy is run.

Resetting a replication policy deletes the source-cluster snapshot.

Note
Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete. Reset a replication policy only if you cannot fix the issue that caused the replication error. If you fix the issue that caused the error, resolve the policy instead of resetting the policy.

Procedure
1. Run the `isi sync policies reset` command.

   The following command resets weeklySync:

   ```
   isi sync policies reset weeklySync
   ```
Perform a full or differential replication

After you reset a replication policy, you must perform either a full or differential replication. You can do this only from the CLI.

Before you begin
Reset a replication policy.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in through the root or compliance administrator account.
2. Specify the type of replication you want to perform by running the `isi sync policies modify` command.
   - To perform a full replication, disable the `--target-compare-initial-sync` option.
     For example, the following command disables differential synchronization for newPolicy:

     ```bash
     isi sync policies modify newPolicy \
     --target-compare-initial-sync off
     ```
   - To perform a differential replication, enable the `--target-compare-initial-sync` option.
     For example, the following command enables differential synchronization for newPolicy:

     ```bash
     isi sync policies modify newPolicy \
     --target-compare-initial-sync on
     ```
3. Run the policy by running the `isi sync jobs start` command.
   For example, the following command runs newPolicy:

     ```bash
     isi sync jobs start newPolicy
     ```

Data replication commands

You can control data replication to other Isilon clusters through the data replication commands. Data replication commands apply specifically to the SyncIQ software module and are available only if you activate a SyncIQ license.

isi sync policies create

Creates a replication policy.

Syntax

```bash
isi sync policies create <name> <action> 
<source-root-path> <target-host> <target-path> 
[--description <string>] 
[|--password <password> | --set-password]] 
[|--source-includes-directories <string>]... 
[|--source-excludes-directories <string>]... 
[|--begin-filter {<predicate> <operator> <link}>...] --end-filter]
```
**Data replication with SyncIQ**

```bash
[--schedule {<schedule> | when-source-modified
    | when-snapshot-taken}]
[--skip-when-source-unmodified {true | false}]
[--rpo-alert <duration>]
[--job-delay <duration>]
[--snapshot-sync-pattern <pattern>]
[--snapshot-sync-existing {yes | no}]
[--enabled {true | false}]
[--check-integrity {true | false}]
[--log-level <level>]
[--log-removed-files {yes | no}]
[--workers-per-node <integer>]
[--target-snapshot-archive {on | off}]
[--target-snapshot-pattern <naming-pattern>]
[--target-snapshot-expiration <duration>]
[--target-snapshot-alias <naming-pattern>]
[--target-detect-modifications {on | off}]
[--source-snapshot-archive {on | off}]
[--source-snapshot-pattern <naming-pattern>]
[--source-snapshot-expiration <duration>]
[--report-max-age <duration>]
[--report-max-count <integer>]
[--resolve {enable | disable}]
[--restrict-target-network {on | off}]
[--source-subnet <subnet> --source-pool <pool>]
[--target-compare-initial-sync {on | off}]
[--accelerated-failback {yes | no}]
[--priority {0 | 1}]
[--cloud-deep-copy {deny | allow | force}]
[--verbose]
```

**Options**

**<name>**

Specifies a name for the replication policy. Specify as any string.

**<action>**

Specifies the type of replication policy. The following types of replication policy are valid:

- **copy**
  
  Creates a copy policy that adds copies of all files from the source to the target.

- **sync**
  
  Creates a synchronization policy that synchronizes data on the source cluster to the target cluster and deletes all files on the target cluster that are not present on the source cluster.

**<source-root-path>**

Specifies the directory on the local cluster that files are replicated from. Specify as a full directory path.

**<target-host>**

Specifies the cluster that the policy replicates data to. Specify as one of the following:

- The fully qualified domain name of any node in the target cluster.
- The host name of any node in the target cluster.
- The name of a SmartConnect zone in the target cluster.
- The IPv4 or IPv6 address of any node in the target cluster.
- localhost
  This will replicate data to another directory on the local cluster.

**Note**

SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

```
<target-path>
  Specifies the directory on the target cluster that files are replicated to.
  Specify as a full directory path.

--description <string>
  Specifies a description of the replication policy.

--password <password>
  Specifies a password to access the target cluster. If the target cluster requires a password for authentication purposes, you must specify this parameter or --set-password.

--set-password
  Prompts you to specify a password for the target cluster after the command is run. This can be useful if you do not want other users on the cluster to see the password you specify. If the target cluster requires a password for authentication purposes, you must specify this parameter or --password.

{--source-include-directories | -i} <path>
  Includes only the specified directories in replication.
  Specify as any directory path contained in the root directory. You can specify multiple directories by specifying --source-include-directories multiple times within a command. For example, if the root directory is /ifs/data, you could specify the following:

  ```
  --source-include-directories /ifs/data/music --source-include-directories /ifs/data/movies
  ```

{--source-exclude-directories | -e} <path>
  Does not include the specified directories in replication. Specify as any directory path contained in the root directory. If --source-include-directories is specified, --source-exclude-directories directories must be contained in the included directories. You can specify multiple directories by specifying --source-exclude-directories multiple times within a command. For example, you could specify the following:

  ```
  --source-exclude-directories /ifs/data/music --source-exclude-directories /ifs/data/movies
  --exclude /ifs/data/music/working
  ```
Specifies the file-matching criteria that determines which files are replicated. Files that do not match the file-matching criteria are not replicated. A file matching criterion consists of a predicate, an operator, and a link. The predicate specifies an attribute to filter by (for example, the size of a file). The following predicates are valid:

--size <integer> [{B | KB | MB | GB | TB | PB}]
Selects files according to the specified size.

--file-type <value>
Selects only the specified file-system object type.
The following values are valid:

f
Specifies regular files
d
Specifies directories
l
Specifies soft links

--name <value>
Selects only files whose names match the specified string.
You can include the following wildcard characters:

• *
• [ ]
• ?

--accessed-after '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that have been accessed since the specified time. This predicate is valid only for copy policies.

--accessed-before '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that have not been accessed since the specified time. This predicate is valid only for copy policies.

--accessed-time '<integer> {days | weeks | months | years} ago'
Selects files that were accessed during the specified time interval. This predicate is valid only for copy policies.

--birth-after '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that were created after the specified time. This predicate is valid only for copy policies.

--birth-before '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that were created before the specified time. This predicate is valid only for copy policies.
--birth-time `<integer> {days | weeks | months | years} ago`

Selects files that were created during the specified time interval. This predicate is valid only for copy policies.

--changed-after `'{<mm>/<dd>/<yyyy> [<HH>:<mm>]} | <integer> {days | weeks | months | years} ago}'`

Selects files that have been modified since the specified time. This predicate is valid only for copy policies.

--changed-before `'{<mm>/<dd>/<yyyy> [<HH>:<mm>]} | <integer> {days | weeks | months | years} ago}'`

Selects files that have not been modified since the specified time. This predicate is valid only for copy policies.

--changed-time `<integer> {days | weeks | months | years} ago`

Selects files that were modified during the specified time interval. This predicate is valid only for copy policies.

--no-group

Selects files based on whether they are owned by a group.

--no-user

Selects files based on whether they are owned by a user.

--posix-regex-name `<value>`

Selects only files whose names match the specified POSIX regular expression. IEEE Std 1003.2 (POSIX.2) regular expressions are supported.

--user-id `<id>`

Selects files based on whether they are owned by the user of the specified ID.

--user-name `<name>`

Selects files based on whether they are owned by the user of the specified name.

--group-id `<id>`

Selects files based on whether they are owned by the group of the specified ID.

--group-name `<name>`

Selects files based on whether they are owned by the group of the specified name.

The operator specifies which files are selected in relationship to the attribute (for example, all files smaller than the given size). Specify operators in the following form:

```
--operator <value>
```

The following operator values are valid:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>Equal. This is the default value.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal</td>
</tr>
<tr>
<td>lt</td>
<td>Less than</td>
</tr>
<tr>
<td>le</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td>gt</td>
<td>Greater than</td>
</tr>
<tr>
<td>ge</td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td>not</td>
<td>Not</td>
</tr>
</tbody>
</table>

The link specifies how the criterion relates to the one that follows it (for example, the file is selected only if it meets both criteria). The following links are valid:

`--and`  
Selects files that meet the criteria of the options that come before and after this value.

`--or`  
Selects files that meet either the criterion of the option that comes before this value or the criterion of the option that follows this value.

```bash
|--schedule | -S| <schedule> | when-source-modified | when-snapshot-taken
```

Specifies how often data will be replicated. Specifying `when-source-modified` causes OneFS to replicate data every time that the source directory of the policy is modified. Specifying `when-snapshot-taken` causes OneFS to replicate data every time that a snapshot is taken of the source directory. Specify in the following format:

```
"<interval> [<frequency>]"
```

Specify `<interval>` in one of the following formats:

- Every `{other | <integer>}` `{weekday | day}`
- Every `{other | <integer>}` week [on `<day>`]
- Every `{other | <integer>}` month [on the `<integer>`]
- Every `<day>[, ...]` [of every `{other | <integer>}` week]
- The last `{day | weekday | <day>}` of every `{other | <integer>}` month
- The `<integer>` `{weekday | <day>}` of every `{other | <integer>}` month
- Yearly on `<month>` `<integer>`
- Yearly on the `{last | <integer>}` `{weekday | <day>}` of `<month>`

Specify `<frequency>` in one of the following formats:
Data replication with SyncIQ

- at `<hh>[:<mm>] [{AM | PM}]`
- every `<integer>` {hours | minutes} [between `<hh>[:<mm>] [{AM | PM}]` and `<hh>[:<mm>] [{AM | PM}]`
- every `<integer>` {hours | minutes} [from `<hh>[:<mm>] [{AM | PM}]` to `<hh>[:<mm>] [{AM | PM}]`

You can optionally append "st", "th", or "rd" to `<integer>`. For example, you can specify "Every 1st month"

Specify `<day>` as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

--skip-when-source-unmodified {true | false}
Causes the policy not to be run if the contents of the source directory have not been modified since the last time the policy has been run. If `--schedule` of this replication policy is set to `<schedule>`, and the policy is scheduled to run before changes have been made to the contents of the source directory, the policy will not be run.

--rpo-alert `<duration>`
Creates a OneFS event if the specified Recovery Point Objective (RPO) is exceeded. For example, assume you set an RPO of 5 hours; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ will create a OneFS event.

The default value is 0, which will not generate events. This option is valid only if `--schedule` is set to `<schedule>`.

Note
This option is valid only if RPO alerts have been globally enabled through SyncIQ settings. The events have an event ID of 400040020.

--job-delay `<duration>`
Specifies the amount of time after the source directory is modified that SyncIQ waits before starting a replication job. If the `--schedule` of this replication policy is set to when-source-modified, and the contents of the source directory are modified, SyncIQ will wait the specified amount of time before starting a replication job.

The default value is 0 seconds.

--snapshot-sync-pattern `<pattern>`
Specifies the naming pattern for snapshots to be synced. If the `--schedule` of this replication policy is set to when-snapshot-taken, and a snapshot is taken of the source directory, and the snapshot name matches the specified naming pattern, SyncIQ will replicate the snapshot to the target cluster.

The default value is "*", which causes all snapshots of the source directory to be replicated if the `--schedule` of the policy is set to when-snapshot-taken.

--snapshot-sync-existing {yes | no}
Determines whether the policy replicates data contained in snapshots taken before the policy was created. If the `--schedule` of this replication policy is set to when-snapshot-taken, SyncIQ will replicate all existing snapshots of the
source directory that match the naming pattern specified by the \texttt{--snapshot-sync-pattern} option.  
The default value is \texttt{no}.

\textbf{Note}

In order to create identical snapshots on the target cluster, you must also specify \texttt{--target-snapshot-archive on}.

\texttt{--enabled \{true | false\}}

Determine whether the policy is enabled or disabled.
The default value is \texttt{true}.

\texttt{--check-integrity \{true | false\}}

Specifies whether to perform a checksum on each file data packet that is affected by the SyncIQ job. If this option is set to \texttt{true}, and the checksum values do not match, SyncIQ retransmits the file data packet.
The default value is \texttt{true}.

\texttt{--log-level \{level\}}

Specifies the amount of data recorded in logs.
The following values are valid, organized from least to most information:

- fatal
- error
- notice
- info
- copy
- debug
- trace

The default value is \texttt{info}.

\texttt{--log-removed-files \{yes | no\}}

Determines whether SyncIQ retains a log of all files that are deleted when a synchronization policy is run. This parameter has no effect for copy policies.
The default value is \texttt{no}.

\texttt{--workers-per-node \{ --workers-per-node | -w \} \{integer\}}

Specifies the number of workers per node that are generated by SyncIQ to perform each replication job for the policy.
The default value is \texttt{3}.

\textbf{Note}

This option has been deprecated and will not be recognized if configured.

\texttt{--target-snapshot-archive \{on | off\}}

Determines whether archival snapshots are generated on the target cluster. If this option is set to \texttt{off}, SyncIQ will still maintain exactly one snapshot at a time on the target cluster to facilitate failback. You must activate a SnapshotIQ license on the target cluster to generate archival snapshots on the target cluster.
--target-snapshot-pattern <naming-pattern>
Specifies the snapshot naming pattern for snapshots that are generated by replication jobs on the target cluster.
The default naming pattern is the following string:

\[SIQ-%{SrcCluster}--%{PolicyName}-%Y-%m-%d_%H-%M\]

--target-snapshot-expiration <duration>
Specifies an expiration period for archival snapshots on the target cluster.
If this option is not specified, archival snapshots will remain indefinitely on the target cluster.
Specify in the following format:

\[<integer><units>\]

The following <units> are valid:

Y
  Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours

--target-snapshot-alias <naming-pattern>
Specifies a naming pattern for the most recent archival snapshot generated on the target cluster.
The default alias is the following string:

\[SIQ-%{SrcCluster}--%{PolicyName}-latest\]

--target-detect-modifications {on | off}
Determines whether SyncIQ checks the target directory for modifications before replicating files.

⚠️ CAUTION
Specifying off could result in data loss. It is recommended that you consult Isilon Technical Support before specifying off.

--source-snapshot-archive {on | off}
Determines whether archival snapshots are retained on the source cluster. If this option is set to `off`, SyncIQ will still maintain one snapshot at a time for the policy to facilitate replication.

`--source-snapshot-pattern <naming-pattern>`

Specifies a naming pattern for the most recent archival snapshot generated on the source cluster.

For example, the following pattern is valid:

```
SIQ-source-%{PolicyName}-%Y-%m-%d_%H-%M
```

`--source-snapshot-expiration <duration>`

Specifies an expiration period for archival snapshots retained on the source cluster.

If this option is not specified, archival snapshots will exist indefinitely on the source cluster.

Specify in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- `Y` Specifies years
- `M` Specifies months
- `W` Specifies weeks
- `D` Specifies days
- `H` Specifies hours

`--report-max-age <duration>`

Specifies how long replication reports are retained before they are automatically deleted by SyncIQ.

Specify in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- `Y` Specifies years
- `M` Specifies months
W
Specifies weeks

D
Specifies days

H
Specifies hours

--report-max-count <integer>
Specifies the maximum number of reports to retain for the replication policy.

--resolve {enable | disable}
Determines whether users can manually resolve the policy if the policy encounters an error and becomes unrunnable.

--restrict-target-network {on | off}
If you specify on, and you specify the target cluster as a SmartConnect zone, replication jobs connect only to nodes in the specified zone. If off is specified, does not restrict replication jobs to specific nodes on the target cluster.

--source-subnet <subnet>
Restricts replication jobs to running only on nodes in the specified subnet on the local cluster. If you specify this option, you must also specify --source-pool.

--source-pool <pool>
Restricts replication jobs to running only on nodes in the specified pool on the local cluster. If you specify this option, you must also specify --source-subnet.

--target-compare-initial-sync {on | off}
Determines whether the full or differential replications are performed for this policy. Full or differential replications are performed the first time a policy is run and after a policy has been reset. If set to on, performs a differential replication. If set to off, performs a full replication.
If differential replication is enabled the first time a replication policy is run, the policy will run slower without any benefit.
The default value is off.

--accelerated-failback {enable | disable}
If enabled, SyncIQ will perform failback configuration tasks the next time that a job is run, rather than waiting to perform those tasks during the failback process. Performing these tasks ahead of time will increase the speed of failback operations.

--priority {0 | 1}
Determines whether the policy has priority.
The default value is 0, which means that the policy does not have priority.

--cloud-deep-copy {deny | allow | force}
Determines how the policy replicates CloudPools smartlinks. If set to deny, SyncIQ replicates all CloudPools smartlinks to the target cluster as smartlinks; if the target cluster does not support the smartlinks, the job will fail. If set to
force, SyncIQ replicates all smartlinks to the target cluster as regular files. If set to allow, SyncIQ will attempt to replicate smartlinks to the target cluster as smartlinks; if the target cluster does not support the smartlinks, SyncIQ will replicate the smartlinks as regular files.

`{--verbose | -v}` Displays a message confirming that the snapshot schedule was created.

isi sync policies modify

Modifies existing replication policies.

Syntax

```
isi sync policies modify <policy>
    [--name <new-policy-name>]
    [--action <policy-type>]
    [--target-host <target-cluster>]
    [--target-path <target-path>]
    [--source-root-path <root-path>]
    [--description <string>]
    [--password <password>]
    [--set-password]
    [--source-include-directories <string>]
    [--clear-source-include-directories]
    [--add-source-include-directories <string>]
    [--remove-source-include-directories <string>]
    [--source-exclude-directories <string>]
    [--clear-source-exclude-directories]
    [--add-source-exclude-directories <string>]
    [--remove-source-exclude-directories <string>]
    [--begin-filter <predicate> --operator <value> ... --end-filter]
    [--schedule {<schedule> | when-source-modified}]
    [--skip-when-source-unmodified {true | false}]
    [--rpo-alert <duration>]
    [--job-delay <duration>]
    [--clear-job-delay]
    [--snapshot-sync-pattern <pattern>]
    [--clear-snapshot-sync-existing {yes | no}]
    [--snapshot-sync-existing {yes | no}]
    [--check-integrity {true | false}]
    [--log-level <level>]
    [--log-removed-files {yes | no}]
    [--workers-per-node <integer>]
    [--target-snapshot-archive {on | off}]
    [--target-snapshot-pattern <naming-pattern>]
    [--clear-target-snapshot-pattern <naming-pattern>]
    [--target-snapshot-expiration <duration>]
    [--target-snapshot-include-directories <string>]
    [--clear-target-snapshot-include-directories]
    [--add-target-snapshot-include-directories <string>]
    [--remove-target-snapshot-include-directories <string>]
    [--target-snapshot-pattern <naming-pattern>]
    [--target-snapshot-expiration <duration>]
    [--report-max-age <duration>]
    [--report-max-count <integer>]
    [--restrict-target-network {on | off}]
    [--source-subnet <subnet> --source-pool <pool>]
    [--clear-source-network]
    [--target-compare-initial-sync {on | off}]
    [--accelerated-failback {yes | no}]
    [--priority {0 | 1}]
    [--cloud-deep-copy {deny | allow | force}]
    [--verbose]
    [--force]
```
Options

<policy>
Identifies the policy to modify, either by current policy ID or name.

{name | -n} <new-policy-name>
Specifies a new name for this replication policy.

--action <policy-type>
Specifies the type of replication policy.
The following types of replication policy are valid:

  copy
  Creates a copy policy that adds copies of all files from the source to the
target.

  sync
  Creates a synchronization policy that synchronizes data on the source
  cluster to the target cluster and deletes all files on the target cluster that are
  not present on the source cluster.

--target-host | -C <target-cluster>
Specifies the cluster that the policy replicates data to.
Specify as one of the following:

  • The fully qualified domain name of any node in the target cluster.
  • The host name of any node in the target cluster.
  • The name of a SmartConnect zone in the target cluster.
  • The IPv4 or IPv6 address of any node in the target cluster.
  • localhost
    This will replicate data to another directory on the local cluster.

Note
SyncIQ does not support dynamically allocated IP address pools. If a replication
job connects to a dynamically allocated IP address, SmartConnect might reassign
the address while a replication job is running, which would disconnect the job and
cause it to fail.

--target-path | -p <target-path>
Specifies the directory on the target cluster that files are replicated to.
Specify as a full directory path.

--source-root-path <root-path>
Specifies the directory on the local cluster that files are replicated from.
Specify as a full directory path.

--description <string>
Specifies a description of this replication policy.

--password <password>
Specifies a password to access the target cluster. If the target cluster requires a password for authentication purposes, you must specify this parameter or --set-password.

--set-password
Prompts you to specify a password for the target cluster after the command is run. This can be useful if you do not want other users on the cluster to see the password you specify. If the target cluster requires a password for authentication purposes, you must specify this parameter or --password.

{--source-include-directories | -i} <path>
Includes only the specified directories in replication. Specify as any directory path contained in the root directory. You can specify multiple directories by specifying --source-include-directories multiple times within a command. For example, if the root directory is /ifs/data, you could specify the following:

```
--source-include-directories /ifs/data/music --source-include-directories /ifs/data/movies
```

--clear-source-include-directories
Clears the list of included directories.

--add-source-include-directories <path>
Adds the specified directory to the list of included directories.

--remove-source-include-directories <path>
Removes the specified directory from the list of included directories.

{--source-exclude-directories | -e} <path>
Does not include the specified directories in replication. Specify as any directory path contained in the root directory. If --source-include-directories is specified, --source-exclude-directories directories must be contained in the included directories. You can specify multiple directories by specifying --source-exclude-directories multiple times within a command. For example, you could specify the following:

```
--source-exclude-directories /ifs/data/music --source-exclude-directories /ifs/data/movies --exclude /ifs/data/music/working
```

--clear-source-exclude-directories
Clears the list of excluded directories.

--add-source-exclude-directories <path>
Adds the specified directory to the list of excluded directories.

--remove-source-exclude-directories <path>
Removes the specified directory from the list of excluded directories.

--begin-filter <predicate> --operator <value> [ <predicate> --operator <value> ]...
--end-filter
Specifies the file-matching criteria that determines which files are replicated. Specify <predicate> as one or more of the following options:

The following options are valid for both copy and synchronization policies:

- `--size <integer> [{B | KB | MB | GB | TB | PB}]`
  Selects files according to the specified size.

- `--file-type <value>`
  Selects only the specified file-system object type.
  The following values are valid:
  
  - `f`
    Specifies regular files
  
  - `d`
    Specifies directories
  
  - `l`
    Specifies soft links

- `--name <value>`
  Selects only files whose names match the specified string.
  You can include the following wildcards:
  
  - `*`
  
  - `[ ]`
  
  - `?`

The following options are valid only for copy policies:

- `--accessed-after '{<mm>/<dd>/<yyyy> [HH]:<mm>] | <integer> {days | weeks | months | years} ago}'`
  Selects files that have been accessed since the specified time. This predicate is valid only for copy policies.

- `--accessed-before '{<mm>/<dd>/<yyyy> [HH]:<mm>] | <integer> {days | weeks | months | years} ago}'`
  Selects files that have not been accessed since the specified time. This predicate is valid only for copy policies.

- `--accessed-time '{<mm>/<dd>/<yyyy> [HH]:<mm>] | <integer> {days | weeks | months | years} ago}'`
  Selects files that were accessed at the specified time. This predicate is valid only for copy policies.

- `--birth-after '{<mm>/<dd>/<yyyy> [HH]:<mm>] | <integer> {days | weeks | months | years} ago}'`
  Selects files that were created after the specified time. This predicate is valid only for copy policies.

- `--birth-before '{<mm>/<dd>/<yyyy> [HH]:<mm>] | <integer> {days | weeks | months | years} ago}'`
  Selects files that were created before the specified time. This predicate is valid only for copy policies.
--birth-time '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that were created at the specified time. This predicate is valid only for copy policies.

--changed-after '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that have been modified since the specified time. This predicate is valid only for copy policies.

--changed-before '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that have not been modified since the specified time. This predicate is valid only for copy policies.

--changed-time '{<mm>/<dd>/<yyyy> [<HH>:<mm>] | <integer> {days | weeks | months | years} ago}'
Selects files that were modified at the specified time. This predicate is valid only for copy policies.

--no-group
Selects files based on whether they are owned by a group.

--no-user
Selects files based on whether they are owned by a user.

--posix-regex-name <value>
Selects only files whose names match the specified POSIX regular expression. IEEE Std 1003.2 (POSIX.2) regular expressions are supported.

--user-id <id>
Selects files based on whether they are owned by the user of the specified ID.

--user-name <name>
Selects files based on whether they are owned by the user of the specified name.

--group-id <id>
Selects files based on whether they are owned by the group of the specified ID.

--group-name <name>
Selects files based on whether they are owned by the group of the specified name.

The following <operator> values are valid:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>Equal. This is the default value.</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal</td>
</tr>
<tr>
<td>lt</td>
<td>Less than</td>
</tr>
<tr>
<td>le</td>
<td>Less than or equal to</td>
</tr>
</tbody>
</table>
You can use the following <link> values to combine and alter the options available for predicates:

---and

Selects files that meet the criteria of the options that come before and after this value.

---or

Selects files that meet either the criterion of the option that comes before this value or the criterion of the option that follows this value.

{--schedule | -S} {<schedule> | when-source-modified}

Specifies how often data will be replicated. Specifying when-source-modified causes OneFS to replicate data every time that the source directory of the policy is modified. Specify <schedule> in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every {{other | <integer>}} {weekday | day}
- Every {{other | <integer>}} week [on <day>]
- Every {{other | <integer>}} month [on the <integer>]
- Every <day>[, ...] [of every {{other | <integer>}} week]
- The last {day | weekday | <day>} of every {{other | <integer>}} month
- The <integer> {weekday | <day>} of every {{other | <integer>}} month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>[:<mm>] {{AM | PM}}
- every <integer> {hours | minutes} [between <hh>[:<mm>] {{AM | PM}} and <hh>[:<mm>] {{AM | PM}}]
You can optionally append "st", "nd", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

To configure a policy to be run only manually, specify the following option:

```
--schedule ""
```

```
--skip-when-source-unmodified {true | false}
```

Causes the policy not to be run if the contents of the source directory have not been modified since the last time the policy has been run. If --schedule of this replication policy is set to <schedule>, and the policy is scheduled to run before changes have been made to the contents of the source directory, the policy will not be run.

```
--rpo-alert <duration>
```

Creates a OneFS event if the specified Recovery Point Objective (RPO) is exceeded. For example, assume you set an RPO of 5 hours; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ will create a OneFS event. The default value is 0, which will not generate events. This option is valid only if --schedule is set to <schedule>.

---

**Note**

This option is valid only if RPO alerts have been globally enabled through SyncIQ settings. The events have an event ID of 400040020.

```
--job-delay <duration>
```

Specifies the amount of time after the source directory is modified that SyncIQ waits before starting a replication job. If the --schedule of this replication policy is set to when-source-modified, and the contents of the source directory are modified, SyncIQ will wait the specified amount of time before starting a replication job. The default value is 0 seconds.

```
--clear-job-delay
```

Clears the amount of time after the source directory is modified that SyncIQ waits before starting a replication job.

```
--snapshot-sync-pattern <pattern>
```

Specifies the naming pattern for snapshots to be synced. If the --schedule of this replication policy is set to when-snapshot-taken, and a snapshot is taken of the source directory, and the snapshot name matches the specified naming pattern, SyncIQ will replicate the snapshot to the target cluster. The default value is ", which causes all snapshots of the source directory to be replicated if the --schedule of the policy is set to when-snapshot-taken.
--snapshot-sync-existing {yes | no}
Determines whether the policy replicates the data contained snapshots taken before the policy was created.

---

Note
Because this setting cannot be modified after the policy is initially created, this option cannot be specified with isi sync policies modify.

--enabled {true | false}
Determines whether the policy is enabled or disabled.

--check-integrity {true | false}
Specifies whether to perform a checksum on each file data packet that is affected by the SyncIQ job. If this option is set to true and the checksum values do not match, SyncIQ retransmits the file data packet. The default value is true.

--log-level <level>
Specifies the amount of data recorded in logs. The following values are valid, organized from least to most information:
- fatal
- error
- notice
- info
- copy
- debug
- trace
The default value is info.

--log-removed-files {yes | no}
Determines whether SyncIQ retains a log of all files that are deleted when a synchronization policy is run. If the policy is a copy policy, this parameter has no effect. The default value is no.

{--workers-per-node | -w} <integer>
Specifies the number of workers per node that are generated by SyncIQ to perform each replication job for the policy. The default value is 3.

---

Note
This option has been deprecated and will not be recognized if configured.

--target-snapshot-archive {on | off}
Determines whether archival snapshots are generated on the target cluster. If this option is set to off, SyncIQ will still maintain exactly one snapshot at a time on the target cluster to facilitate failback. You must activate a SnapshotIQ license on the target cluster to generate archival snapshots on the target cluster.
--target-snapshot-pattern <naming-pattern>
Specifies the snapshot naming pattern for snapshots that are generated by
replication jobs on the target cluster.
The default naming pattern is the following string:

```
SIQ-%{SrcCluster}- %{PolicyName}- %Y-%m-%d_%H-%M
```

--target-snapshot-expiration <duration>
Specifies an expiration period for archival snapshots on the target cluster.
If this option is not specified, archival snapshots will remain indefinitely on the
target cluster.
Specify in the following format:

```
<integer><units>
```

The following <units> are valid:

- **Y**
  Specifies years
- **M**
  Specifies months
- **W**
  Specifies weeks
- **D**
  Specifies days
- **H**
  Specifies hours

--target-snapshot-alias <naming-pattern>
Specifies a naming pattern for the most recent archival snapshot generated on
the target cluster.
The default alias is the following string:

```
SIQ-%{SrcCluster}- %{PolicyName}-latest
```

--target-detect-modifications {on | off}
Determines whether SyncIQ checks the target directory for modifications before
replicating files.

⚠️ **CAUTION**

Specifying **off** could result in data loss. It is recommended that you consult
Isilon Technical Support before specifying off.

--source-snapshot-archive {on | off}
Determines whether archival snapshots are retained on the source cluster. If this option is set to `off`, SyncIQ will still maintain one snapshot at a time for the policy to facilitate replication.

```bash
--source-snapshot-pattern <naming-pattern>
```

Specifies a naming pattern for the most recent archival snapshot generated on the source cluster.

For example, the following pattern is valid:

```
SIQ-source-%{PolicyName}-%Y-%m-%d_%H-%M
```

```bash
--source-snapshot-expiration <duration>
```

Specifies an expiration period for archival snapshots retained on the source cluster.

If this option is not specified, archival snapshots will exist indefinitely on the source cluster.

Specify in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- `Y` Specifies years
- `M` Specifies months
- `W` Specifies weeks
- `D` Specifies days
- `H` Specifies hours

```bash
--report-max-age <duration>
```

Specifies how long replication reports are retained before they are automatically deleted by SyncIQ.

Specify in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- `Y` Specifies years
- `M` Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours

--report-max-count <integer>
  Specifies the maximum number of reports to retain for the replication policy.

--restrict-target-network {on | off}
  If you specify on, and you specify the target cluster as a SmartConnect zone,
  replication jobs connect only to nodes in the specified zone. If off is specified,
  does not restrict replication jobs to specific nodes on the target cluster.

--source-subnet <subnet>
  Restricts replication jobs to running only on nodes in the specified subnet on the
  local cluster.

--source-pool <pool>
  Restricts replication jobs to running only on nodes in the specified pool on the
  local cluster.

--clear-source-network
  Runs replication jobs on any nodes in the cluster, instead of restricting the jobs to
  a specified subnet.

--target-compare-initial-sync {on | off}
  Determines whether the full or differential replications are performed for this
  policy. Full or differential replications are performed the first time a policy is run
  and after a policy has been reset. If set to on, performs a differential replication.
  If set to off, performs a full replication.
  If differential replication is enabled the first time a replication policy is run, the
  policy will run slower without any benefit.
  The default value is off.

--accelerated-failback {enable | disable}
  If enabled, SyncIQ will perform failback configuration tasks the next time that a
  job is run, rather than waiting to perform those tasks during the failback process.
  Performing these tasks ahead of time will increase the speed of failback
  operations.

--priority {0 | 1}
  Determines whether the policy has priority.

--cloud-deep-copy {deny | allow | force}
  Determines how the policy replicates CloudPools smartlinks. If set to deny,
  SyncIQ replicates all CloudPools smartlinks to the target cluster as smartlinks; if
  the target cluster does not support the smartlinks, the job will fail. If set to
  force, SyncIQ replicates all smartlinks to the target cluster as regular files. If set
  to allow, SyncIQ will attempt to replicate smartlinks to the target cluster as
smartlinks; if the target cluster does not support the smartlinks, SyncIQ will replicate the smartlinks as regular files.

|--verbose | -v|
Displays a confirmation message.

|--force | -f|
Does not prompt you to confirm modifications.

**isi sync policies delete**

Deletes a replication policy.

The command will not succeed until SyncIQ can communicate with the target cluster; until then, the policy will still appear in the output of the `isi sync policies list` command. After the connection between the source cluster and target cluster is reestablished, SyncIQ will delete the policy the next time that the job is scheduled to run; if the policy is configured to run only manually, you must manually run the policy again. If SyncIQ is permanently unable to communicate with the target cluster, specify the `--local-only` option. This will delete the policy from the local cluster only and not break the target association on the target cluster.

**Syntax**

```
isi sync policies delete {<policy> | --all}  
[--local-only]  
[--force]  
[--verbose]
```

**Options**

**<policy>**
Deletes the specified replication policy.

**--all**
Deletes all replication policies.

**--local-only**
Does not break the target association on the target cluster. Not deleting a policy association on the target cluster will cause the target directory to remain in a read-only state.

---

**Note**

If SyncIQ is unable to communicate with the target cluster, you must specify this option to successfully delete the policy.

---

**{|--force | -f|**
Deletes the policy, even if an associated job is currently running. Also, does not prompt you to confirm the deletion.

---

**CAUTION**

Forcing a policy to delete might cause errors if an associated replication job is currently running.
{--verbose | -v}
  Displays a confirmation message.

**isi sync policies list**

Displays a list of replication policies.

**Syntax**

```bash
isi sync policies list
  [--limit <integer>]
  [--sort <attribute>]
  [--descending]
  [--format (table | json | csv | list)]
  [--no-header]
  [--no-footer]
  [--verbose]
```

**Options**

If no options are specified, displays a table of all replication policies.

{--limit | -l} <integer>
  Displays no more than the specified number of items.

--sort <attribute>
  Sorts output displayed by the specified attribute.
  The following values are valid:
  
  name
    Sorts output by the name of the replication policy.
  
  target_path
    Sorts output by the path of the target directory.
  
  action
    Sorts output by the type of replication policy.
  
  description
    Sorts output by the policy description.
  
  enabled
    Sorts output by whether the policies are enabled or disabled.
  
  target_host
    Sorts output by the target cluster.
  
  check_integrity
    Sorts output by whether the policy is configured to perform a checksum on each file data packet that is affected by a replication job.
  
  source_root_path
    Sorts output by the path of the source directory.
  
  source_include_directories
    Sorts output by directories that have been explicitly included in replication.
source_exclude_directories
Sorts output by directories that have been explicitly excluded in replication.

file_matching_pattern
Sorts output by the predicate that determines which files are replicated.

target_snapshot_archive
Sorts output by whether archival snapshots are generated on the target cluster.

target_snapshot_pattern
Sorts output by the snapshot naming pattern for snapshots that are generated by replication jobs on the target cluster.

target_snapshot_expiration
Sorts output by the expiration period for archival snapshots on the target cluster.

target_detect_modifications
Sorts output by whether full or differential replications are performed for this policy.

source_snapshot_archive
Sorts output by whether archival snapshots are retained on the source cluster.

source_snapshot_pattern
Sorts output by the naming pattern for the most recent archival snapshot generated on the source cluster.

source_snapshot_expiration
Sorts output by the expiration period for archival snapshots retained on the source cluster.

schedule
Sorts output by the schedule of the policy.

log_level
Sorts output by the amount of data that is recorded in logs.

log_removed_files
Sorts output by whether OneFS retains a log of all files that are deleted when the replication policy is run.

workers_per_node
Sorts output by the number of workers per node that are generated by OneFS to perform each replication job for the policy.

report_max_age
Sorts output by how long replication reports are retained before they are automatically deleted by OneFS

report_max_count
Sorts output by the maximum number of reports that are retained for the replication policy.
force_interface
Sorts output by whether data is sent over only the default interface of the subnet specified by the --source-network option of the isi sync policies create or isi sync policies modify commands.

restrict_target_network
Sorts output by whether replication jobs are restricted to connecting to nodes in a specified zone on the target cluster.

target_compare_initial_sync
Sorts output by whether full or differential replications are performed for the policies.

last_success
Sorts output by the last time that a replication job completed successfully.

password_set
Sorts output by whether the policy specifies a password for the target cluster.

source_network
Sorts output by the subnet on the local cluster that the replication policy is restricted to.

source_interface
Sorts output by the pool on the local cluster that the replication policy is restricted to.

|--descending | -d
Displays output in reverse order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

|--no-header | -a
Displays table and CSV output without headers.

|--no-footer | -z
Displays table output without footers.

|--verbose | -v
Displays more detailed information.

isi sync policies reset
Resets a replication policy after the policy encounters an error and the cause of the error cannot be identified or fixed. If you fix the cause of the error, run isi sync policies resolve instead.

Resetting a replication policy causes either a full replication or a differential replication to be performed the next time the policy is run.
Syntax

`isi sync policies reset {<policy> | --all} [--verbose]`

Options

 `<policy>`
  Resets the specified replication policy.
  Specify as a replication policy name or ID

  `--all`
  Resets all replication policies

  `{--verbose | -v}`
  Displays more detailed information.

**isi sync policies resolve**

Resolves a conflicted replication policy after the policy encounters an error and the cause of the error is fixed. If the cause of the error cannot be fixed, run the `isi sync policies reset` command instead.

Syntax

`isi sync policies resolve <policy> [--force]`

Options

 `<policy>`
  Resolves the specified replication policy.
  Specify as a replication policy name or ID.

  `{--force | -f}`
  Suppresses command-line prompts and messages.

**isi sync policies view**

Displays information about a replication policy.

Syntax

`isi sync policies view <policy>`

Options

 `<policy>`
  Displays information about the specified replication policy.
  Specify as a replication policy name or ID.
isi sync policies disable

Temporarily disables a replication policy. If a replication policy is disabled, the policy will not create replication jobs. However, if a replication job is currently running for a replication policy, disabling the policy will not pause or stop the job.

Syntax

```
isi sync policies disable {<policy> | --all} [--verbose]
```

Options

- `<policy>`
  - Enables the specified replication policy. Specify as a replication policy name or a replication policy ID.
- `--all`
  - Enables all replication policies on the cluster.
- `--verbose`
  - Displays more detailed information.

isi sync policies enable

Enables a disabled replication policy.

Syntax

```
isi sync policies enable {<policy> | --all} [--verbose]
```

Options

- `<policy>`
  - Enables the specified replication policy. Specify as a replication policy name or a replication policy ID.
- `--all`
  - Enables all replication policies on the cluster.
- `--verbose`
  - Displays more detailed information.

isi sync jobs start

Starts a replication job for a replication policy.

Syntax

```
isi sync jobs start <policy-name> [--test]
```
Options

<policy-name>

Starts a replication job for the specified replication policy.

--test

Creates a replication policy report that reflects the number of files and directories that would be replicated if the specified policy was run. You can test only policies that have not been run before.

--source-snapshot <snapshot>

Replicates data according to the specified SnapshotIQ snapshot. If specified, a snapshot is not generated for the replication job. Replicating data according to snapshots generated by the SyncIQ tool is not supported. Specify as a snapshot name or ID. The source directory of the policy must be contained in the specified snapshot. This option is valid only if the last replication job completed successfully or if you are performing a full or differential replication. If the last replication job completed successfully, the specified snapshot must be more recent than the snapshot referenced by the last replication job.

{--verbose | -v}

Displays more detailed information.

isi sync jobs pause

Pauses a running replication job.

Syntax

isi sync jobs pause {<policy-name> | --all} [--verbose]

Options

<policy-name>

Pauses a job that was created according to the specified replication policy. Specify as a replication policy name.

--all

Pauses all currently running replication jobs.

{--verbose | -v}

Displays more detailed information.
isi sync jobs resume

Resumes paused replication jobs.

Syntax

```
isi sync jobs resume {<policy-name> | --all} [--verbose]
```

Options

<policy-name>
Resumes a paused job that was created by the specified policy. Specify as a replication policy name.

--all
Resumes all currently running replication jobs.

{--verbose | -v}
Displays more detailed information.

isi sync jobs cancel

Cancels a running or paused replication job.

Syntax

```
isi sync jobs cancel {<policy-name> | --all} [--verbose]
```

Options

<policy-name>
Cancels a job that was created according to the specified replication policy. Specify as a replication policy name or ID.

--all
Cancels all currently running replication jobs.

--verbose
Displays more detailed information.

isi sync jobs list

Displays information about the most recently completed and next scheduled replication jobs of replication policies.

Syntax

```
isi sync jobs list [--state <state>] [--limit <integer>] [--format {table | json | csv | list}]
```
Options
If no options are specified, displays information about replication jobs for all policies.

--state <state>
Displays only jobs in the specified state. The following values are valid:
  scheduled
  Displays jobs that are scheduled to run.
  running
  Displays running jobs.
  paused
  Displays jobs that were paused by a user.
  finished
  Displays jobs that have completed successfully.
  failed
  Displays jobs that failed during the replication process.
  canceled
  Displays jobs that were cancelled by a user.
  needs_attention
  Displays jobs that require user intervention before they can continue.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.

isi sync jobs view
Displays information about a running replication job.

Syntax

isi sync jobs view <policy>
Options

<policy>
Displays information about a running replication job created according to the specified policy.
Specify as a replication policy name or ID.

isi sync jobs reports list
Displays information about running replication jobs targeting the local cluster.
Syntax

`isi sync jobs reports list [--limit <integer>] [--format {table | json | csv | list}] [--no-header] [--no-footer] [--verbose]`

Options

`{--limit | -l} <integer>`
Displays no more than the specified number of items.

`--format {table | json | csv | list}`
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`
Displays table and CSV output without headers.

`{--no-footer | -z}`
Displays table output without footers.

`{--verbose | -v}`
Displays more detailed information.

isi sync jobs reports view
Displays information about a running replication job targeting the local cluster.
Syntax

`isi sync jobs reports view <policy>`

Options

<policy>
Displays information about a replication job created according to the specified replication policy.
Specify as a replication policy name or ID.
isi sync settings modify

Manages global replication settings.

Syntax

```
isi sync settings modify
   [--service {on | off | paused}]
   [--source-subnet <subnet>]
   [--source-pool <pool>]
   [--restrict-target-network {on | off}]
   [--report-max-age <duration>]
   [--report-max-count <integer>]
   [--report-email <email-address>]
   [--clear-report-email]
   [--add-report-email <email-address>]
   [--remove-report-email <email-address>]
   [--verbose]
```

Options

If no options are specified, displays current default replication report settings.

--service {on | off | paused}
   Determines the state of the SyncIQ tool.

--source-subnet <subnet>
   Restricts replication jobs to running only on nodes in the specified subnet on the local cluster.

--source-pool <pool>
   Restricts replication jobs to running only on nodes in the specified pool on the local cluster.

--restrict-target-network {on | off}
   If you specify on, and you specify the target cluster as a SmartConnect zone, replication jobs connect only to nodes in the specified zone. If off is specified, does not restrict replication jobs to specific nodes on the target cluster.

Note

SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

--report-max-age <duration>
   Specifies the default amount of time that SyncIQ retains reports before automatically deleting them.
   Specify in the following format:

   `<integer><units>`

   The following `<units>` are valid:
Y
  Specifies years
M
  Specifies months
D
  Specifies days
H
  Specifies hours

--report-max-count <integer>
  Specifies the default maximum number of reports to retain for a replication policy.

{---verbose | -v}
  Displays more detailed information.

isi sync settings view
Displays global replication settings.
Syntax

isi sync settings view

Options
There are no options for this command.

isi sync target cancel
Cancels running replication jobs targeting the local cluster.
Syntax

isi sync target cancel {<policy> | --target-path <path> | --all} [--verbose]

Options
<policy>
  Cancels a replication job created according to the specified replication policy.
  Specify as a replication policy name or ID.

--target-path <path>
  Cancels a replication job targeting the specified directory.

--all
  Cancels all running replication jobs targeting the local cluster.

--verbose
  Displays more detailed information.
isi sync target list

Displays a list of replication policies targeting the local cluster.

Syntax

```
isi sync target list
   [--target-path <path>]
   [--limit <integer>]
   [--sort <attribute>]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

If no options are specified, displays a table of all replication policies currently targeting
the local cluster.

```
--target-path <path>
   Displays information about the replication policy targeting the specified directory.

{--limit | -l} <integer>
   Displays no more than the specified number of items.

--sort <attribute>
   Sorts output displayed by the specified attribute.
   The following values are valid:
   
   **name**
   
   Sorts output by the name of the replication policy.

   **source_host**
   
   Sorts output by the name of the source cluster.

   **target_path**
   
   Sorts output by the path of the target directory.

   **last_job_status**
   
   Sorts output by the status of the last replication job created according to the
   policy.

   **failover_failback_state**
   
   Sorts output by whether the target directory is read only.

{--descending | -d}
   Displays output in reverse order.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-
   separated value (CSV), or list format.

{--no-header | -a}
   Displays table and CSV output without headers.
Displays table output without footers.

Displays more detailed information.

### isi sync target view

Displays information about a replication policy that is targeting the local cluster.

#### Syntax

```
isi sync target view {<policy-name> | --target-path <path>}
```

#### Options

- **<policy-name>**
  - Displays information about the specified policy.

- **--target-path <path>**
  - Displays information about the policy targeting the specified directory.

### isi sync target break

Breaks the association between a local cluster and a target cluster for a replication policy.

#### Note

Breaking a source and target association requires you to reset the replication policy before you can run the policy again. Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete.

#### Syntax

```
isi sync target break {<policy> | --target-path <path>}
[--force]
[--verbose]
```

#### Options

- **<policy>**
  - Removes the association of the specified replication policy targeting this cluster. Specify as a replication policy name, a replication policy ID, or the path of a target directory.

- **--target-path <path>**
  - Removes the association of the replication policy targeting the specified directory path.

- **{--force | -f}**
  - Forces the replication policy association to be removed, even if an associated job is currently running.
CAUTION

Forcing a target break might cause errors if an associated replication job is currently running.

```
{--verbose | -v}
```

Displays more detailed information.

isi sync target reports list

Displays information about completed replication jobs targeting the local cluster.

Syntax

```
isi sync target reports list
   [--state <state>]
   [--limit <integer>]
   [--sort <attribute>]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

If no options are specified, displays basic information about all completed replication jobs.

```
--state <state>
```

Displays information about only replication jobs in the specified state. The following states are valid:

- scheduled
- running
- paused
- finished
- failed
- canceled
- needs_attention
- unknown

```
{--limit | -l} <integer>
```

Displays no more than the specified number of items.

```
--sort <attribute>
```

Sorts output displayed by the specified attribute. The following values are valid:

- `start_time`
  Sorts output by when the replication job started.

- `end_time`
  Sorts output by when the replication job ended.
action
Sorts output by the action that the replication job performed.

state
Sorts output by the progress of the replication job.

id
Sorts output by the ID of the replication subreport.

policy_id
Sorts output by the ID of the replication policy.

policy_name
Sorts output by the name of the replication policy.

job_id
Sorts output by the ID of the replication job.

total_files
Sorts output by the total number of files that were modified by the replication job.

files_transferred
Sorts output by the total number of files that were transferred to the target cluster.

bytes_transferred
Sorts output by the total number of files that were transferred to the target cluster.

duration
Sorts output by how long the replication job ran.

errors
Sorts output by errors that the replication job encountered.

warnings
Sorts output by warnings that the replication job triggered.

{--descending | -d}
Displays output in reverse order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information.
### isi sync target reports view

Displays information about a completed replication job that targeted the local cluster.

**Syntax**

```
isi sync target reports view <policy> <job-id>
```

**Options**

- `<policy>`
  
  Displays a replication report about the specified replication policy.

- `<job-id>`
  
  Displays a replication report about the job with the specified ID.

### isi sync target reports subreports list

Displays subreports about completed replication jobs targeting the local cluster.

**Syntax**

```
```

**Options**

- `<policy>`
  
  Displays subreports about the specified policy.

- `<job-id>`
  
  Displays subreports about the job of the specified ID.

- `--limit | -l <integer>`
  
  Displays no more than the specified number of items.

- `--sort <attribute>`
  
  Sorts output displayed by the specified attribute.
  
  The following values are valid:

  - `start_time`
    
    Sorts output by when the replication job started.
  
  - `end_time`
    
    Sorts output by when the replication job ended.
  
  - `action`
    
    Sorts output by the action that the replication job performed.
  
  - `state`

  Sorts output by the specified attribute.
Sorts output by the progress of the replication job.

**id**
Sorts output by the ID of the replication report.

**policy_id**
Sorts output by the ID of the replication policy.

**policy_name**
Sorts output by the name of the replication policy.

**job_id**
Sorts output by the ID of the replication job.

**total_files**
Sorts output by the total number of files that were modified by the replication job.

**files_transferred**
Sorts output by the total number of files that were transferred to the target cluster.

**bytes_transferred**
Sorts output by the total number of files that were transferred to the target cluster.

**duration**
Sorts output by how long the replication job ran.

**errors**
Sorts output by errors that the replication job encountered.

**warnings**
Sorts output by warnings that the replication job triggered.

```bash
{--descending | -d}
Displays output in reverse order.
```

```bash
--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
```

```bash
{--no-header | -a}
Displays table and CSV output without headers.
```

```bash
{--no-footer | -z}
Displays table output without footers.
```

```bash
{--verbose | -v}
Displays more detailed information.
```
isi sync target reports subreports view

Displays a subreport about a completed replication job targeting the local cluster.

Syntax

```
isi sync target reports subreports view <policy> <job-id> <subreport-id>
```

Options

- `<policy>`
  Displays a sub report about the specified replication policy. Specify as a replication policy name.

- `<job-id>`
  Displays a sub report about the specified replication job. Specify as a replication job ID.

- `<subreport-id>`
  Displays the subreport with the specified ID.

isi sync reports list

Displays information about completed replication jobs targeting a remote cluster.

Syntax

```
isi sync reports list
   [--policy-name <policy>]
   [--state <state>]
   [--reports-per-policy <integer>]
   [--limit <integer>]
   [--sort <attribute>]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

- `--policy-name <policy>`
  Displays only replication reports that were created for the specified policy.

- `--state <state>`
  Displays only replication reports whose jobs are in the specified state.

- `--reports-per-policy <integer>`
  Displays no more than the specified number of reports per policy. The default value is 10.

- `--limit | -l <integer>`
  Displays no more than the specified number of items.

- `--sort <attribute>`
Sorts output displayed by the specified attribute. The following values are valid:

- **start_time**
  Sorts output by when the replication job started.

- **end_time**
  Sorts output by when the replication job ended.

- **action**
  Sorts output by the action that the replication job performed.

- **state**
  Sorts output by the progress of the replication job.

- **id**
  Sorts output by the ID of the replication subreport.

- **policy_id**
  Sorts output by the ID of the replication policy

- **policy_name**
  Sorts output by the name of the replication policy.

- **job_id**
  Sorts output by the ID of the replication job.

- **total_files**
  Sorts output by the total number of files that were modified by the replication job.

- **files_transferred**
  Sorts output by the total number of files that were transferred to the target cluster.

- **bytes_transferred**
  Sorts output by the total number of files that were transferred to the target cluster.

- **duration**
  Sorts output by how long the replication job ran.

- **errors**
  Sorts output by errors that the replication job encountered.

- **warnings**
  Sorts output by warnings that the replication job triggered.

```
{--descending | -d}
```
Displays output in reverse order.

```
--format {table | json | csv | list}
```
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

```
{--no-header | -a}
```
Displays table and CSV output without headers.

\{--no-footer | -z\}

Displays table output without footers.

\{--verbose | -v\}

Displays more detailed information.

**isi sync reports view**

Displays information about a completed replication job that targeted a remote cluster.

**Syntax**

```
isi sync reports view <policy> <job-id>
```

**Options**

\(<policy>\)

Displays a replication report about the specified replication policy.

\(<job-id>\)

Displays a replication report about the job with the specified ID.

**isi sync reports rotate**

If the number of replication reports has exceeded the maximum, deletes replication reports. The system intermittently deletes excess reports automatically. However, this command causes excess reports to be deleted immediately.

**Syntax**

```
isi sync reports rotate
\[--verbose\]
```

**Options**

\{--verbose | -v\}

Displays more detailed information.

**isi sync reports subreports list**

Displays subreports about completed replication jobs targeting remote clusters.

**Syntax**

```
isi sync reports subreports list <policy> <job-id>
\[--limit\]
\[--sort <attribute>\]
\[--descending\]
\[--format {table | json | csv | list}\]
\[--no-header\]
\[--no-footer\]
\[--verbose\]
```
Options
<policy>
Displays subreports about the specified policy.

<job-id>
Displays subreports about the job of the specified ID.

|--limit | -l <integer>
Displays no more than the specified number of items.

--sort <attribute>
Sorts output displayed by the specified attribute.
The following values are valid:
  start_time
  Sorts output by when the replication job started.
  end_time
  Sorts output by when the replication job ended.
  action
  Sorts output by the action that the replication job performed.
  state
  Sorts output by the progress of the replication job.
  id
  Sorts output by the ID of the replication report.
  policy_id
  Sorts output by the ID of the replication policy
  policy_name
  Sorts output by the name of the replication policy.
  job_id
  Sorts output by the ID of the replication job.
  total_files
  Sorts output by the total number of files that were modified by the replication job.
  files_transferred
  Sorts output by the total number of files that were transferred to the target cluster.
  bytes_transferred
  Sorts output by the total number of files that were transferred to the target cluster.
  duration
  Sorts output by how long the replication job ran.
  errors
  Sorts output by errors that the replication job encountered.
**warnings**

Sorts output by warnings that the replication job triggered.

`{--descending | -d}`

Displays output in reverse order.

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{--no-header | -a}`

Displays table and CSV output without headers.

`{--no-footer | -z}`

Displays table output without footers.

`{--verbose | -v}`

Displays more detailed information.

**isi sync reports subreports view**

Displays a subreport about a completed replication job that targeted a remote cluster.

**Syntax**

```bash
isi sync reports subreports view <policy> <job-id> <subreport-id>
```

**Options**

`<policy>`

Displays a sub report about the specified replication policy. Specify as a replication policy name.

`<job-id>`

Displays a sub report about the specified replication job. Specify as a replication job ID.

`<subreport-id>`

Displays the subreport of the specified ID.

**isi sync recovery allow-write**

Allows modifications to data in a target directory of a replication policy without breaking the association between the local cluster and the policy. The `isi sync target allow_write` command is most commonly used in failover and failback operations.

**Syntax**

```bash
isi sync recovery allow-write <policy-name> [--revert] [--log-level <level>]
```
Options

<policy-name>
Allows writes for the target directory of the specified replication policy. Specify as a replication policy name, a replication policy ID, or the path of a target directory.

--revert
Reverts an allow-writes operation on the local cluster only. This action does not affect the source cluster of the replication policy.

--log-level <level>
Specifies the amount of data recorded in logs. The following values are valid, organized from least to most information:
- fatal
- error
- notice
- info
- copy
- debug
- trace
The default value is info.

{--workers-per-node | -w}<integer>
Specifies the number of workers per node that are generated by SyncIQ to perform the allow-writes job. The default value is 3.

{--verbose | -v}
Displays more detailed information.

isi sync recovery resync-prep
Disables the specified policy, reverts the source directory of the policy to the last recovery point, and creates a mirror policy on the target cluster. The isi sync resync prep command is most commonly used in failback operations.

Syntax

isi sync recovery resync-prep <policy-name>
[--verbose]
Specify as a replication policy name or ID. The replication policy must be a synchronization policy.

--verbose
Displays more detailed information.

**isi sync rules create**

Creates a replication performance rule.

**Syntax**

```
isid sync rules create <type> <interval> <days> <limit>
[--description <string>]
[--verbose]
```

**Options**

**<type>**
Specifies the type of performance rule. The following values are valid:

- **file_count**
  Creates a performance rule that limits the number of files that can be sent by replication jobs per second.

- **bandwidth**
  Creates a performance rule that limits the amount of bandwidth that replication jobs are allowed to consume.

**<interval>**
Enforces the performance rule on the specified hours of the day. Specify in the following format:

```
<hh>:<mm>-<hh>:<mm>
```

**<days>**
Enforces the performance rule on the specified days of the week. The following values are valid:

- X
  Specifies Sunday

- M
  Specifies Monday

- T
  Specifies Tuesday

- W
  Specifies Wednesday

- R
  Specifies Thursday
F
  Specifies Friday
S
  Specifies Saturday

You can include multiple days by specifying multiple values separated by commas.
You can also include a range of days by specifying two values separated by a
  dash.

<limit>
  Specifies the maximum number of files that can be sent or KBs that can be
  consumed per second by replication jobs.

--description <string>
  Specifies a description of this performance rule.

--verbose
  Displays more detailed information.

isi sync rules modify

Modifies a replication performance rule.

Syntax

isi sync rules modify <id>
  |--interval <interval>
  |--days <days>
  |--limit <integer>
  |--enabled {true | false}
  |--description <string>
  |--verbose

Options

<id>
  Modifies the replication performance rule of the specified ID.

|--interval |--i <interval>
  Specifies which hours of the day to enforce the performance rule. Specify in the
  following format:

  <hh>:<mm>-<hh>:<mm>

|--days |--d <days>
  Specifies which days of the week to enforce the performance rule.
The following values are valid:

  X
    Specifies Sunday

  M
    Specifies Monday
T
  Specifies Tuesday
W
  Specifies Wednesday
R
  Specifies Thursday
F
  Specifies Friday
S
  Specifies Saturday

You can include multiple days by specifying multiple values separated by commas. You can also include a range of days by specifying two values separated by a dash.

--limit <limit>
  Specifies the maximum number of files that can be sent or KBs that can be consumed per second by replication jobs.

--enabled {true | false}
  Determines whether the policy is enabled or disabled.

--description <string>
  Specifies a description of this performance rule.

{--verbose | -v}
  Displays more detailed information.

**isi sync rules delete**

Deletes a replication performance rule.

**Syntax**

```
isi sync rules delete {<id> | --all | --type <type>}
[--force]
[--verbose]
```

**Options**

{id>
  Deletes the performance rule of the specified ID.

--all
  Deletes all performance rules.

--type <type>
  Deletes all performance rules of the specified type. The following values are valid:
  file_count
Deletes all performance rules that limit the number of files that can be sent by replication jobs per second.

**bandwidth**
Deletes all performance rules that limit the amount of bandwidth that replication jobs are allowed to consume.

**--force**
Does not prompt you to confirm that you want to delete the performance rule.

**--verbose**
Displays more detailed information.

**isi sync rules list**
Displays a list of replication performance rules.

**Syntax**

```
isi sync rules list
    [--type <type>]
    [--limit]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

**--type <type>**
Displays only performance rules of the specified type. The following values are valid:

**file_count**
Displays only performance rules that limit the number of files that can be sent by replication jobs per second.

**bandwidth**
Displays only performance rules that limit the amount of bandwidth that replication jobs are allowed to consume.

**--limit | -l** `<integer>`
Displays no more than the specified number of items.

**--format {table | json | csv | list}**
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

**--no-header | -a**
Displays table and CSV output without headers.

**--no-footer | -z**
Displays table output without footers.

**--verbose | -v**
Displays more detailed information.

**isi sync rules view**

Displays information about a replication performance rule.

**Syntax**

```
isi sync rules view <id>
```

**Options**

`<id>`

Displays information about the replication performance rule with the specified ID.
CHAPTER 17

Data layout with FlexProtect

This section contains the following topics:

- FlexProtect overview ................................................................. 724
- File striping .................................................................................. 724
- Requested data protection ......................................................... 724
- FlexProtect data recovery ......................................................... 725
- Requesting data protection ....................................................... 726
- Requested protection settings ................................................... 726
- Requested protection disk space usage ........................................ 727
FlexProtect overview

An Isilon cluster is designed to continuously serve data, even when one or more components simultaneously fail. OneFS ensures data availability by striping or mirroring data across the cluster. If a cluster component fails, data stored on the failed component is available on another component. After a component failure, lost data is restored on healthy components by the FlexProtect proprietary system.

Data protection is specified at the file level, not the block level, enabling the system to recover data quickly. Because all data, metadata, and parity information is distributed across all nodes, the cluster does not require a dedicated parity node or drive. This ensures that no single node limits the speed of the rebuild process.

File striping

OneFS uses the internal network to automatically allocate and stripe data across nodes and disks in the cluster. OneFS protects data as the data is being written. No separate action is necessary to stripe data.

OneFS breaks files into smaller logical chunks called stripes before writing the files to disk; the size of each file chunk is referred to as the stripe unit size. Each OneFS block is 8 KB, and a stripe unit consists of 16 blocks, for a total of 128 KB per stripe unit.

During a write, OneFS breaks data into stripes and then logically places the data in a stripe unit. As OneFS stripes data across the cluster, OneFS fills the stripe unit according to the number of nodes and protection level.

OneFS can continuously reallocate data and make storage space more usable and efficient. As the cluster size increases, OneFS stores large files more efficiently.

Requested data protection

The requested protection of data determines the amount of redundant data created on the cluster to ensure that data is protected against component failures. OneFS enables you to modify the requested protection in real time while clients are reading and writing data on the cluster.

OneFS provides several data protection settings. You can modify these protection settings at any time without rebooting or taking the cluster or file system offline.

When planning your storage solution, keep in mind that increasing the requested protection reduces write performance and requires additional storage space for the increased number of nodes.

OneFS uses the Reed Solomon algorithm for N+M protection. In the N+M data protection model, N represents the number of data-stripe units, and M represents the number of simultaneous node or drive failures—or a combination of node and drive failures—that the cluster can withstand without incurring data loss. N must be larger than M.

In addition to N+M data protection, OneFS also supports data mirroring from 2x to 8x, allowing from two to eight mirrors of data. In terms of overall cluster performance and resource consumption, N+M protection is often more efficient than mirrored protection. However, because read and write performance is reduced for N+M protection, data mirroring might be faster for data that is updated often and is small in size. Data mirroring requires significant overhead and might not always be the best data-protection method. For example, if you enable 3x mirroring, the specified content...
is duplicated three times on the cluster; depending on the amount of content mirrored, this can consume a significant amount of storage space.

**FlexProtect data recovery**

OneFS uses the FlexProtect proprietary system to detect and repair files and directories that are in a degraded state due to node or drive failures.

OneFS protects data in the cluster based on the configured protection policy. OneFS rebuilds failed disks, uses free storage space across the entire cluster to further prevent data loss, monitors data, and migrates data off of at-risk components.

OneFS distributes all data and error-correction information across the cluster and ensures that all data remains intact and accessible even in the event of simultaneous component failures. Under normal operating conditions, all data on the cluster is protected against one or more failures of a node or drive. However, if a node or drive fails, the cluster protection status is considered to be in a degraded state until the data is protected by OneFS again. OneFS reprotects data by rebuilding data in the free space of the cluster. While the protection status is in a degraded state, data is more vulnerable to data loss.

Because data is rebuilt in the free space of the cluster, the cluster does not require a dedicated hot-spare node or drive in order to recover from a component failure. Because a certain amount of free space is required to rebuild data, it is recommended that you reserve adequate free space through the virtual hot spare feature.

As you add more nodes, the cluster gains more CPU, memory, and disks to use during recovery operations. As a cluster grows larger, data restriping operations become faster.

**Smartfail**

OneFS protects data stored on failing nodes or drives through a process called smartfailing.

During the smartfail process, OneFS places a device into quarantine. Data stored on quarantined devices is read only. While a device is quarantined, OneFS reprotects the data on the device by distributing the data to other devices. After all data migration is complete, OneFS logically removes the device from the cluster, the cluster logically changes its width to the new configuration, and the node or drive can be physically replaced.

OneFS smartfails devices only as a last resort. Although you can manually smartfail nodes or drives, it is recommended that you first consult Isilon Technical Support.

Occasionally a device might fail before OneFS detects a problem. If a drive fails without being smartfailed, OneFS automatically starts rebuilding the data to available free space on the cluster. However, because a node might recover from a failure, if a node fails, OneFS does not start rebuilding data unless the node is logically removed from the cluster.

**Node failures**

Because node loss is often a temporary issue, OneFS does not automatically start reprotecting data when a node fails or goes offline. If a node reboots, the file system does not need to be rebuilt because it remains intact during the temporary failure.

If you configure N+1 data protection on a cluster, and one node fails, all of the data is still accessible from every other node in the cluster. If the node comes back online, the node rejoins the cluster automatically without requiring a full rebuild.
To ensure that data remains protected, if you physically remove a node from the 
cluster, you must also logically remove the node from the cluster. After you logically 
remove a node, the node automatically reformats its own drives, and resets itself to 
the factory default settings. The reset occurs only after OneFS has confirmed that all 
data has been reprotected. You can logically remove a node using the smartfail 
process. It is important that you smartfail nodes only when you want to permanently 
remove a node from the cluster.

If you remove a failed node before adding a new node, data stored on the failed node 
must be rebuilt in the free space in the cluster. After the new node is added, OneFS 
distributes the data to the new node. It is more efficient to add a replacement node to 
the cluster before failing the old node because OneFS can immediately use the 
replacement node to rebuild the data stored on the failed node.

### Requesting data protection

You can specify the protection of a file or directory by setting its requested 
protection. This flexibility enables you to protect distinct sets of data at higher than 
default levels.

Requested protection of data is calculated by OneFS and set automatically on storage 
pools within your cluster. The default setting is referred to as suggested protection, 
and provides the optimal balance between data protection and storage efficiency. For 
example, a suggested protection of N+2:1 means that two drives or one node can fail 
without causing any data loss.

For best results, we recommend that you accept at least the suggested protection for 
data on your cluster. You can always specify a higher protection level than suggested 
protection on critical files, directories, or node pools.

OneFS allows you to request protection that the cluster is currently incapable of 
matching. If you request an unmatchable protection, the cluster will continue trying to 
match the requested protection until a match is possible. For example, in a four-node 
cluster, you might request a mirror protection of 5x. In this example, OneFS would 
mirror the data at 4x until you added a fifth node to the cluster, at which point OneFS 
would reprotect the data at 5x.

If you set requested protection to a level below suggested protection, OneFS warns 
you of this condition.

---

**Note**

For 4U Isilon IQ X-Series and NL-Series nodes, and IQ 12000X/EX 12000 combination 
platforms, the minimum cluster size of three nodes requires a minimum protection of 
N+2:1.

### Requested protection settings

Requested protection settings determine the level of hardware failure that a cluster 
can recover from without suffering data loss.

<table>
<thead>
<tr>
<th>Requested protection setting</th>
<th>Minimum number of nodes required</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1n</td>
<td>3</td>
<td>The cluster can recover from one drive or node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>Requested protection setting</td>
<td>Minimum number of nodes required</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>[+2d:1n]</td>
<td>3</td>
<td>The cluster can recover from two simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+2n]</td>
<td>4</td>
<td>The cluster can recover from two simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3d:1n]</td>
<td>3</td>
<td>The cluster can recover from three simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3d:1n1d]</td>
<td>3</td>
<td>The cluster can recover from three simultaneous drive failures or simultaneous failures of one node and one drive without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3n]</td>
<td>6</td>
<td>The cluster can recover from three simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4d:1n]</td>
<td>3</td>
<td>The cluster can recover from four simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4d:2n]</td>
<td>4</td>
<td>The cluster can recover from four simultaneous drive failures or two node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4n]</td>
<td>8</td>
<td>The cluster can recover from four simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>Nx (Data mirroring)</td>
<td>N</td>
<td>For example, 5x requires a minimum of five nodes. The cluster can recover from N - 1 drive or node failures without sustaining any data loss. For example, 5x protection means that the cluster can recover from four drive or node failures.</td>
</tr>
</tbody>
</table>

**Requested protection disk space usage**

Increasing the requested protection of data also increases the amount of space consumed by the data on the cluster.

The parity overhead for N + M protection depends on the file size and the number of nodes in the cluster. The percentage of parity overhead declines as the cluster gets larger.
The following table describes the estimated percentage of overhead depending on the requested protection and the size of the cluster or node pool. The table does not show recommended protection levels based on cluster size.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>[+1n]</th>
<th>[+2d:1n]</th>
<th>[+2n]</th>
<th>[+3d:1n]</th>
<th>[+3d:1n1d]</th>
<th>[+3n]</th>
<th>[+4d:1n]</th>
<th>[+4d:2n]</th>
<th>[+4n]</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2 +1</td>
<td>4 + 2</td>
<td>—</td>
<td>6 + 3</td>
<td>—</td>
<td>3 + 3</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>(33%)</td>
<td>(33%)</td>
<td>—</td>
<td>(33%)</td>
<td>—</td>
<td>(50%)</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>3 +1</td>
<td>6 + 2</td>
<td>2 + 2</td>
<td>9 + 3</td>
<td>5 + 3</td>
<td>—</td>
<td>12 + 4</td>
<td>4 + 4</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>(25%)</td>
<td>(25%)</td>
<td>(50%)</td>
<td>(25%)</td>
<td>(38%)</td>
<td>—</td>
<td>(25%)</td>
<td>(50%)</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>4 +1</td>
<td>8 + 2</td>
<td>3 + 2</td>
<td>12 + 3</td>
<td>7 + 3</td>
<td>—</td>
<td>16 + 4</td>
<td>6 + 4</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>(20%)</td>
<td>(20%)</td>
<td>(40%)</td>
<td>(20%)</td>
<td>(30%)</td>
<td>—</td>
<td>(20%)</td>
<td>(40%)</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>5 +1</td>
<td>10 + 2</td>
<td>4 + 2</td>
<td>15 + 3</td>
<td>9 + 3</td>
<td>3 + 3</td>
<td>16 + 4</td>
<td>8 + 4</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>(17%)</td>
<td>(17%)</td>
<td>(33%)</td>
<td>(17%)</td>
<td>(25%)</td>
<td>(50%)</td>
<td>(20%)</td>
<td>(33%)</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>6 +1</td>
<td>12 + 2</td>
<td>5 + 2</td>
<td>15 + 3</td>
<td>11 + 3</td>
<td>4 + 3</td>
<td>16 + 4</td>
<td>10 + 4</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>(14%)</td>
<td>(14%)</td>
<td>(29%)</td>
<td>(17%)</td>
<td>(21%)</td>
<td>(43%)</td>
<td>(20%)</td>
<td>(29%)</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>7 +1</td>
<td>14 + 2</td>
<td>6 + 2</td>
<td>15 + 3</td>
<td>13 + 3</td>
<td>5 + 3</td>
<td>16 + 4</td>
<td>12 + 4</td>
<td>4 + 4</td>
</tr>
<tr>
<td></td>
<td>(13%)</td>
<td>(12.5%)</td>
<td>(25%)</td>
<td>(17%)</td>
<td>(19%)</td>
<td>(38%)</td>
<td>(20%)</td>
<td>(25%)</td>
<td>(50%)</td>
</tr>
<tr>
<td>9</td>
<td>8 +1</td>
<td>16 + 2</td>
<td>7 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>6 + 3</td>
<td>16 + 4</td>
<td>14 + 4</td>
<td>5 + 4</td>
</tr>
<tr>
<td></td>
<td>(11%)</td>
<td>(11%)</td>
<td>(22%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(33%)</td>
<td>(20%)</td>
<td>(22%)</td>
<td>(44%)</td>
</tr>
<tr>
<td>10</td>
<td>9 +1</td>
<td>16 + 2</td>
<td>8 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>7 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>6 + 4</td>
</tr>
<tr>
<td></td>
<td>(10%)</td>
<td>(11%)</td>
<td>(20%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(30%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(40%)</td>
</tr>
<tr>
<td>12</td>
<td>11 +1</td>
<td>16 + 2</td>
<td>10 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>9 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>8 + 4</td>
</tr>
<tr>
<td></td>
<td>(8%)</td>
<td>(11%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(25%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(33%)</td>
</tr>
<tr>
<td>14</td>
<td>13 + 1</td>
<td>16 + 2</td>
<td>12 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>11 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>10 + 4</td>
</tr>
<tr>
<td></td>
<td>(7%)</td>
<td>(11%)</td>
<td>(14%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(21%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(29%)</td>
</tr>
<tr>
<td>16</td>
<td>15 + 1</td>
<td>16 + 2</td>
<td>14 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>13 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>12 + 4</td>
</tr>
<tr>
<td></td>
<td>(6%)</td>
<td>(11%)</td>
<td>(13%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(19%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(25%)</td>
</tr>
<tr>
<td>18</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>15 + 3</td>
<td>15+3</td>
<td>15 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>14 + 4</td>
</tr>
<tr>
<td></td>
<td>(6%)</td>
<td>(11%)</td>
<td>(11%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(17%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(22%)</td>
</tr>
<tr>
<td>20</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>16 + 3</td>
<td>16 +3</td>
<td>16 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>16 + 4</td>
</tr>
<tr>
<td></td>
<td>(6%)</td>
<td>(11%)</td>
<td>(11%)</td>
<td>(16%)</td>
<td>(16%)</td>
<td>(16%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(20%)</td>
</tr>
<tr>
<td>30</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>16 + 3</td>
<td>16 +3</td>
<td>16 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>16 + 4</td>
</tr>
<tr>
<td></td>
<td>(6%)</td>
<td>(11%)</td>
<td>(11%)</td>
<td>(16%)</td>
<td>(16%)</td>
<td>(16%)</td>
<td>(20%)</td>
<td>(20%)</td>
<td>(20%)</td>
</tr>
</tbody>
</table>

The parity overhead for mirrored data protection is not affected by the number of nodes in the cluster. The following table describes the parity overhead for requested mirrored protection.

<table>
<thead>
<tr>
<th></th>
<th>2x</th>
<th>3x</th>
<th>4x</th>
<th>5x</th>
<th>6x</th>
<th>7x</th>
<th>8x</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>67%</td>
<td>75%</td>
<td>80%</td>
<td>83%</td>
<td>86%</td>
<td>88%</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 18

NDMP backup and recovery overview

This section contains the following topics:

- NDMP backup and recovery overview .............................................................. 730
- NDMP two-way backup ................................................................................... 730
- NDMP three-way backup ................................................................................ 731
- NDMP multi-stream backup and recovery ........................................................ 731
- Snapshot-based incremental backups ............................................................... 731
- NDMP protocol support ................................................................................... 732
- Supported DMAs .............................................................................................. 733
- NDMP hardware support .................................................................................. 733
- NDMP backup limitations ................................................................................ 733
- NDMP performance recommendations ............................................................ 734
- Excluding files and directories from NDMP backups ........................................ 735
- Configuring basic NDMP backup settings ......................................................... 736
- Managing NDMP user accounts ....................................................................... 738
- Managing NDMP backup devices .................................................................... 739
- Managing NDMP Fibre Channel ports .............................................................. 740
- Managing NDMP sessions ............................................................................... 741
- Managing NDMP restartable backups ............................................................. 743
- Managing file list backups ............................................................................... 745
- NDMP restore operations ............................................................................... 748
- Sharing tape drives between clusters ............................................................... 748
- Managing default NDMP variables ................................................................. 749
- Managing snapshot based incremental backups .............................................. 756
- View NDMP backup logs ............................................................................... 757
- NDMP backup commands .............................................................................. 757
NDMP backup and recovery overview

In OneFS, you can back up and recover file-system data through the Network Data Management Protocol (NDMP). From a backup server, you can direct backup and recovery processes between an EMC Isilon cluster and backup devices such as tape devices, media servers, and virtual tape libraries (VTLs).

OneFS supports both three-way and two-way NDMP backup models.

Two-way NDMP backup is significantly faster than the three-way NDMP backup. It is also the most efficient method in terms of cluster resource consumption. However, a two-way NDMP backup requires that you attach one or more Backup Accelerator nodes to the cluster.

In both the two-way and three-way NDMP backup models, file history data is transferred from the cluster to the backup server. Before a backup begins, OneFS creates a snapshot of the targeted directory, then backs up the snapshot, which ensures that the backup image represents a specific point in time.

You do not need to activate a SnapshotIQ license on the cluster to perform NDMP backups. If you have activated a SnapshotIQ license on the cluster, you can generate a snapshot through the SnapshotIQ tool, and then back up the same snapshot. If you back up a SnapshotIQ snapshot, OneFS does not create another snapshot for the backup.

---

**Note**

If you are recovering SmartLock directories, we recommend that you do not specify autocommit time periods for them.

You can also back up WORM domains through NDMP.

NDMP backup and recovery for IsilonSD Edge

IsilonSD Edge supports only the three-way NDMP backup model. Two-way NDMP backups require a Backup Accelerator node on the IsilonSD cluster which is not supported.

NDMP two-way backup

The NDMP two-way backup is also known as the local or direct NDMP backup. To perform NDMP two-way backups, you must connect your EMC Isilon cluster to a Backup Accelerator node and attach a tape device to the Backup Accelerator node. You must then use OneFS to detect the tape device before you can back up to that device.

You can connect supported tape devices directly to the Fibre Channel ports of a Backup Accelerator node. Alternatively, you can connect Fibre Channel switches to the Fibre Channel ports on the Backup Accelerator node, and connect tape and media changer devices to the Fibre Channel switches. For more information, see your Fibre Channel switch documentation about zoning the switch to allow communication between the Backup Accelerator node and the connected tape and media changer devices.

If you attach tape devices to a Backup Accelerator node, the cluster detects the devices when you start or restart the node or when you re-scan the Fibre Channel.
ports to discover devices. If a cluster detects tape devices, the cluster creates an entry for the path to each detected device.

If you connect a device through a Fibre Channel switch, multiple paths can exist for a single device. For example, if you connect a tape device to a Fibre Channel switch, and then connect the Fibre Channel switch to two Fibre Channel ports, OneFS creates two entries for the device, one for each path.

---

**Note**

NDMP two-way backup is not supported with IsilonSD Edge.

---

### NDMP three-way backup

The NDMP three-way backup is also known as the remote NDMP backup.

During a three-way NDMP backup operation, a data management application (DMA) on a backup server instructs the cluster to start backing up data to a tape media server that is either attached to the LAN or directly attached to the DMA. The NDMP service runs on one NDMP Server and the NDMP tape service runs on a separate server. Both the servers are connected to each other across the network boundary.

### NDMP multi-stream backup and recovery

You can use the NDMP multi-stream backup feature, in conjunction with certain data management applications (DMAs), to speed up backups.

With multi-stream backup, you can use your DMA to specify multiple streams of data to back up concurrently. OneFS considers all streams in a specific multi-stream backup operation to be part of the same backup context. A multi-stream backup context is retained for five minutes after a backup operation completes.

If you used the NDMP multi-stream backup feature to back data up to tape drives, you can also recover that data in multiple streams, depending on the DMA. In OneFS 8.0.0, multi-stream backups are supported with CommVault Simpana version 11.0 Service Pack 3 and EMC NetWorker version 9.0.1. If you back up data using CommVault Simpana, a multi-stream context is created, but data is recovered one stream at a time.

---

**Note**

OneFS multi-stream backups are not supported by the NDMP restartable backup feature.

---

### Snapshot-based incremental backups

You can implement snapshot-based incremental backups to increase the speed at which these backups are performed.

During a snapshot-based incremental backup, OneFS checks the snapshot taken for the previous NDMP backup operation and compares it to a new snapshot. OneFS then backs up all files that was modified since the last snapshot was made.

If the incremental backup does not involve snapshots, OneFS must scan the directory to discover which files were modified. OneFS can perform incremental backups significantly faster if the change rate is low.
You can perform incremental backups without activating a SnapshotIQ license on the cluster. Although SnapshotIQ offers a number of useful features, it does not enhance snapshot capabilities in NDMP backup and recovery.

Set the `BACKUP_MODE` environment variable to `SNAPSHOT` to enable snapshot-based incremental backups. If you enable snapshot-based incremental backups, OneFS retains each snapshot taken for NDMP backups until a new backup of the same or lower level is performed. However, if you do not enable snapshot-based incremental backups, OneFS automatically deletes each snapshot generated after the corresponding backup is completed or canceled.

After setting the `BACKUP_MODE` environment variable, snapshot-based incremental backup works with certain data management applications (DMAs) as listed in the next table.

**Table 3 DMA support for snapshot-based incremental backups**

<table>
<thead>
<tr>
<th>DMA</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec NetBackup</td>
<td>Yes</td>
</tr>
<tr>
<td>EMC Networker</td>
<td>Yes</td>
</tr>
<tr>
<td>EMC Avamar</td>
<td>Yes</td>
</tr>
<tr>
<td>CommVault Simpana</td>
<td>No</td>
</tr>
<tr>
<td>IBM Tivoli Storage Manager</td>
<td>No</td>
</tr>
<tr>
<td>Symantec Backup Exec</td>
<td>No</td>
</tr>
<tr>
<td>Dell NetVault</td>
<td>No</td>
</tr>
<tr>
<td>ASG-Time Navigator</td>
<td>No</td>
</tr>
</tbody>
</table>

**NDMP protocol support**

You can back up the EMC Isilon cluster data through version 3 or 4 of the NDMP protocol.

OneFS supports the following features of NDMP versions 3 and 4:

- Full (level 0) NDMP backups
- Incremental (levels 1-9) NDMP backups and Incremental Forever (level 10)

**Note**

In a level 10 NDMP backup, only data changed since the most recent incremental (level 1-9) backup or the last level 10 backup is copied. By repeating level 10 backups, you can be assured that the latest versions of files in your data set are backed up without having to run a full backup.

- Token-based NDMP backups
- NDMP TAR backup type
- Dump backup type
- Path-based and dir/node file history format
- Direct Access Restore (DAR)
- Directory DAR (DDAR)
• Including and excluding specific files and directories from backup
• Backup of file attributes
• Backup of Access Control Lists (ACLs)
• Backup of Alternate Data Streams (ADSs)
• Backup Restartable Extension (BRE)

OneFS supports connecting to clusters through IPv4 or IPv6.

Supported DMAs

NDMP backups are coordinated by a data management application (DMA) that runs on a backup server.

OneFS supports all the DMAs that are listed in the Isilon Third-Party Software and Hardware Compatibility Guide.

Note

All supported DMAs can connect to an EMC Isilon cluster through the IPv4 protocol. However, only some of the DMAs support the IPv6 protocol for connecting to an EMC Isilon cluster.

NDMP hardware support

OneFS can back up data to and recover data from tape devices and virtual tape libraries (VTLs).

Supported tape devices

See the OneFS and NDMP hardware compatibility section in the Isilon Third-Party Software and Hardware Compatibility Guide for a list of supported tape devices for two-way NDMP backups. For NDMP three-way backups, the data management application (DMA) determines the tape devices that are supported.

Supported tape libraries

For both the two-way and three-way NDMP backups, OneFS supports all of the tape libraries that are supported by the DMA.

Supported virtual tape libraries

See the OneFS and NDMP hardware compatibility section in the Isilon Third-Party Software and Hardware Compatibility Guide for a list of supported virtual tape libraries. For three-way NDMP backups, the DMA determines the virtual tape libraries that will be supported.

NDMP backup limitations

NDMP backups have the following limitations.

• Does not support more than 4 KB path length.
• Does not back up file system configuration data, such as file protection level policies and quotas.
• Does not back up tape blocks larger than 256 KB.
• Does not support recovering data from a file system other than OneFS. However, you can migrate data through the NDMP protocol from a NetApp or EMC VNX.
NDMP performance recommendations

Consider the following recommendations to optimize OneFS NDMP backups.

**General performance recommendations**

- Install the latest patches for OneFS and your data management application (DMA).
- Run a maximum of eight NDMP concurrent sessions per A100 Backup Accelerator node and four NDMP concurrent sessions per Isilon IQ Backup Accelerator node to obtain optimal throughput per session.
- NDMP backups result in very high Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). You can reduce your RPO and RTO by attaching one or more Backup Accelerator nodes to the cluster and then running two-way NDMP backups.
- The throughput for an Isilon cluster during the backup and recovery operations is dependent on the dataset and is considerably reduced for small files.
- If you are backing up large numbers of small files, set up a separate schedule for each directory.
- If you are performing NDMP three-way backups, run multiple NDMP sessions on multiple nodes in your Isilon cluster.
- Recover files through Direct Access Restore (DAR), especially if you recover files frequently. However, it is recommended that you do not use DAR to recover a full backup or a large number of files, as DAR is better suited to restoring smaller numbers of files.
- Recover files through Directory DAR (DDAR) if you recover large numbers of files frequently.
- Use the largest tape record size available for your version of OneFS to increase throughput.
- If possible, do not include or exclude files from backup. Including or excluding files can affect backup performance, due to filtering overhead.
- Limit the depth of nested subdirectories in your file system.
- Limit the number of files in a directory. Distribute files across multiple directories instead of including a large number of files in a single directory.

**SmartConnect recommendations**

- A two-way NDMP backup session with SmartConnect requires backup accelerators for backup and recovery operations. However, a three-way NDMP session with SmartConnect does not require backup accelerators for these operations.
- For a NDMP two-way backup session with SmartConnect, connect to the NDMP session through a dedicated SmartConnect zone consisting of a pool of Network Interface Cards (NICs) on the backup accelerator nodes.
- For a two-way NDMP backup session without SmartConnect, initiate the backup session through a static IP address or fully qualified domain name of the backup accelerator node.
- For a three-way NDMP backup operation, the front-end Ethernet network or the interfaces of the nodes are used to serve the backup traffic. Therefore, it is recommended that you configure a DMA to initiate an NDMP session only using the nodes that are not already overburdened serving other workloads or connections.

- For a three-way NDMP backup operation with or without SmartConnect, initiate the backup session using the IP addresses of the nodes that are identified for running the NDMP sessions.

**Backup Accelerator recommendations**

- Assign static IP addresses to Backup Accelerator nodes.

- Attach more Backup Accelerator nodes to larger clusters. The recommended number of Backup Accelerator nodes is listed in the following table.

  **Table 4 Nodes per Backup Accelerator node**

<table>
<thead>
<tr>
<th>Node type</th>
<th>Recommended number of nodes per Backup Accelerator node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Series</td>
<td>3</td>
</tr>
<tr>
<td>NL-Series</td>
<td>3</td>
</tr>
<tr>
<td>S-Series</td>
<td>3</td>
</tr>
<tr>
<td>HD-Series</td>
<td>3</td>
</tr>
</tbody>
</table>

- Attach more Backup Accelerator nodes if you are backing up to more tape devices.

**DMA-specific recommendations**

- Enable parallelism for the DMA if the DMA supports this option. This allows OneFS to back up data to multiple tape devices at the same time.

---

**Excluding files and directories from NDMP backups**

You can exclude files and directories from NDMP backup operations by specifying NDMP environment variables through a data management application (DMA). If you include a file or directory, all other files and directories are automatically excluded from backup operations. If you exclude a file or directory, all files and directories except the excluded one are backed up.

You can include or exclude files and directories by specifying the following character patterns. The examples given in the table are valid only if the backup path is `/ifs/data`.

**Table 5 NDMP file and directory matching wildcards**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Includes or excludes the following directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Takes the place of any character or characters</td>
<td>archive*</td>
<td>/ifs/data/archive1/src/archive42_a/media</td>
</tr>
<tr>
<td>[]</td>
<td>Takes the place of a range of letters or numbers</td>
<td>data_store_[a-f] data_store_[0-9]</td>
<td>/ifs/data/data_store_a data_store_c</td>
</tr>
</tbody>
</table>
Table 5 NDMP file and directory matching wildcards (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Includes or excludes the following directories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>/ifs/data/data_store_8</td>
</tr>
<tr>
<td>?</td>
<td>Takes the place of any single character</td>
<td>user_?</td>
<td>/ifs/data/user_1 /ifs/data/user_2</td>
</tr>
<tr>
<td>\</td>
<td>Includes a blank space</td>
<td>user\ 1</td>
<td>/ifs/data/user 1</td>
</tr>
<tr>
<td>//</td>
<td>Takes the place of a single slash (/)</td>
<td>ifs//data//archive</td>
<td>/ifs/data/archive</td>
</tr>
<tr>
<td>***</td>
<td>Takes the place of a single asterisk (*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td>Ignores the pattern if it is at the beginning of a path</td>
<td>../home/john</td>
<td>home/john</td>
</tr>
</tbody>
</table>

Note

" " are required for Symantec NetBackup when multiple patterns are specified. The patterns are not limited to directories.

Unanchored patterns such as home or user1 target a string of text that might belong to many files or directories. If a pattern contains "/", it is an anchored pattern. An anchored pattern is always matched from the beginning of a path. A pattern in the middle of a path is not matched. Anchored patterns target specific file pathnames, such as ifs/data/home. You can include or exclude either types of patterns.

If you specify both the include and exclude patterns, the include pattern is first processed followed by the exclude pattern.

If you specify both the include and exclude patterns, any excluded files or directories under the included directories would not be backed up. If the excluded directories are not found in any of the included directories, the exclude specification would have no effect.

Note

Specifying unanchored patterns can degrade the performance of backups. It is recommended that you avoid unanchored patterns whenever possible.

Configuring basic NDMP backup settings

You can configure NDMP backup settings to control how these backups are performed on the EMC Isilon cluster. You can also configure OneFS to interact with a specific data management application (DMA) for NDMP backups.
Configure and enable NDMP backup

OneFS prevents NDMP backups by default. Before you can perform NDMP backups, you must enable NDMP backups and configure NDMP settings.

Procedure

1. Enable NDMP backup by running the following command:

   ```bash
   isi ndmp settings global modify --service=yes
   ```

2. Configure NDMP backup by running the `isi ndmp settings set` command.

   The following command configures OneFS to interact with EMC NetWorker:

   ```bash
   isi ndmp settings global modify --dma=emc
   ```

Disable NDMP backup

You can disable NDMP backup if you no longer want to back up data through NDMP.

Procedure

- Run the following command:

  ```bash
  isi ndmp settings global modify service=no
  ```

NDMP backup settings

You can configure settings that control how NDMP backups are performed on the cluster.

The following information is displayed in the output of the `isi ndmp settings global view` command:

- **port**
  The number of the port through which data management applications (DMAs) can connect to the cluster.

- **dma**
  The DMA vendor that the cluster is configured to interact with.

View NDMP backup settings

You can view current NDMP backup settings, which indicate whether the service is enabled, the port through which data management applications (DMAs) connect to the cluster, and the DMA vendor that OneFS is configured to interact with.

Procedure

- Run the `isi ndmp settings global view` command:
The system displays the NDMP settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>True</td>
</tr>
<tr>
<td>Port</td>
<td>10000</td>
</tr>
<tr>
<td>Dma</td>
<td>generic</td>
</tr>
<tr>
<td>Bre Max Num Contexts</td>
<td>64</td>
</tr>
<tr>
<td>Mab Context Retention Duration</td>
<td>300</td>
</tr>
<tr>
<td>Msr Context Retention Duration</td>
<td>600</td>
</tr>
</tbody>
</table>

Managing NDMP user accounts

You can create, delete, and modify the passwords of NDMP user accounts.

Create an NDMP user account

Before you can perform NDMP backups, you must create an NDMP user account through which a data management application (DMA) can access the cluster.

Procedure

- Run the `isi ndmp users create` command.

  The following command creates an NDMP user account called NDMPuser with a password of 1234:

  ```
  isi ndmp users create NDMPuser --password=1234
  ```

Modify the password of an NDMP user account

You can modify the password for an NDMP user account.

Procedure

- Run the `isi ndmp users modify` command.

  The following command modifies the password of a user named NDMPuser to 5678:

  ```
  isi ndmp users modify NDMPuser --password=5678
  ```

Delete an NDMP user account

You can delete an NDMP user account.

Procedure

- Run the `isi ndmp users delete` command.

  The following command deletes a user named NDMPuser:

  ```
  isi ndmp users delete NDMPuser
  ```
View NDMP user accounts

You can view information about NDMP user accounts.

Procedure

- Run the `isi ndmp users view` command

  The following command displays information about the account for a user named NDMPuser:

  ```bash
  isi ndmp users view NDMPuser
  ```

Managing NDMP backup devices

After you attach a tape or media changer device to a Backup Accelerator node, you must configure OneFS to detect and establish a connection to the device. After the connection between the cluster and the backup device is established, you can modify the name that the cluster has assigned to the device, or disconnect the device from the cluster.

In case the device has multiple LUNs, you must configure LUN0 so that all the LUNs are detected properly.

Detect NDMP backup devices

If you connect devices to a Backup Accelerator node, you must configure OneFS to detect the devices before OneFS can back up data to and restore data from the devices. You can scan a specific node, a specific port, or all ports on all nodes.

Procedure

- Run the `isi tape rescan` command.

  The following command detects devices on node 18:

  ```bash
  isi tape rescan --node=18
  ```

Modify an NDMP backup device entry name

You can modify the name of an NDMP device entry.

Procedure

- Run the `isi tape modify` command.

  The following command renames tape003 to tape005:

  ```bash
  isi tape modify tape003 --new-name=tape005
  ```

Delete a device entry for a disconnected NDMP backup device

If you physically remove an NDMP device from a cluster, OneFS retains the entry for the device. You can delete a device entry for a removed device. You can also remove
the device entry for a device that is still physically attached to the cluster; this causes OneFS to disconnect from the device.

If you remove a device entry for a device that is connected to the cluster, and you do not physically disconnect the device, OneFS will detect the device the next time it scans the ports. You cannot remove a device entry for a device that is currently being backed up to or restored from.

Procedure

- The following command disconnects tape001 from the cluster:

  ```
  isi tape delete --name=tape001
  ```

View NDMP backup devices

You can view information about tape and media changer devices that are currently attached to the cluster through a Backup Accelerator node.

Procedure

- Run the following command to list tape devices on node 18:

  ```
  isi tape list --node=18 --tape
  ```

Managing NDMP Fibre Channel ports

You can manage the Fibre Channel ports that connect tape and media changer devices to a Backup Accelerator node. You can also enable, disable, or modify the settings of an NDMP Fibre Channel port.

Modify NDMP backup port settings

You can modify the settings of an NDMP backup port.

Procedure

- Run the `isi fc settings modify` command.

  The following command configures port 1 on node 5 to support a point-to-point Fibre Channel topology:

  ```
  isi fc settings modify 5.1 --topology=ptp
  ```

Enable or disable an NDMP backup port

You can enable or disable an NDMP backup port.

Procedure

- Run the `isi fc settings modify` command:

  The following command disables port 1 on node 5:

  ```
  isi fc settings modify 5.1 --state=disable
  ```
The following command enables port 1 on node 5:

```
isim fc settings modify 5.1 --state=enable
```

**View NDMP backup ports**

You can view information about Fibre Channel ports of Backup Accelerator nodes attached to a cluster.

**Procedure**

- Run the following command to view Fibre Channel port settings for port 1 on node 5:

```
isim fc settings view 5.1
```

**NDMP backup port settings**

OneFS assigns default settings to each port on each Backup Accelerator node attached to the cluster. These settings identify each port and specify how the port interacts with NDMP backup devices.

The following information is displayed in the output of the `isi fc list` command:

- **Port**
  The name of the Backup Accelerator node, and the number of the port.

- **WWNN**
  The world wide node name (WWNN) of the port. This name is the same for each port on a given node.

- **WWPN**
  The world wide port name (WWPN) of the port. This name is unique to the port.

- **State**
  Whether the port is enabled or disabled.

- **Topology**
  The type of Fibre Channel topology that the port is configured to support.

- **Rate**
  The rate at which data is sent through the port. The rate can be set to 1 Gb/s, 2 Gb/s, 4 Gb/s, 8 Gb/s, and Auto. 8 Gb/s is available for A100 nodes only. If set to Auto, OneFS automatically negotiates with the DMA to determine the rate. Auto is the recommended setting.

**Managing NDMP sessions**

You can view the status of NDMP sessions or terminate a session that is in progress.
End an NDMP session

You can interrupt an NDMP backup or restore operation by ending an NDMP session.

Procedure

1. To retrieve the ID of the NDMP session that you want to end, run the `isi ndmp sessions list` command.
2. Run the `isi ndmp sessions delete` command.

   The following command ends an NDMP session with an ID of 4.36339 and skips the confirmation prompt:

   ```bash
   isi ndmp sessions delete 4.36339 --force
   ```

View NDMP sessions

You can view information about NDMP sessions that exist between the cluster and data management applications (DMAs).

Procedure

- Run the `isi ndmp sessions view` command. The following command displays information about session 4.36339.

   ```bash
   isi ndmp sessions view 4.36339
   ```

NDMP session information

You can view information about active NDMP sessions.

The following information is displayed in the output of the `isi ndmp list` command:

<table>
<thead>
<tr>
<th>Session</th>
<th>The unique identification number that OneFS assigned to the session.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>The current state of the data server. The data server is a component of OneFS that sends data during backups and receives information during restore operations.</td>
</tr>
<tr>
<td>A</td>
<td>Active. The data server is currently sending data.</td>
</tr>
<tr>
<td>I</td>
<td>Idle. The data server is not sending data.</td>
</tr>
<tr>
<td>L</td>
<td>Listen. The data server is waiting to connect to the data mover.</td>
</tr>
<tr>
<td>M</td>
<td>Mover. The current state of the data mover. The data mover is a component of the backup server that receives data during backups and sends data during restore operations.</td>
</tr>
</tbody>
</table>
A
Active. The data mover is currently receiving data.

I
Idle. The data mover is not receiving data.

L
Listen. The data mover is waiting to connect to the data server.

OP
The type of operation that is currently in progress. If no operation is in progress, this field is blank.

B (0-10)
Backup. Indicates that data is currently being backed up to a media server. The number indicates the level of NDMP backup.

R
Restore. Indicates that data is currently being restored from a media server.

Elapsed Time
How much time has elapsed since the session started.

Bytes Moved
The number of bytes that were transferred during the session.

Throughput
The average throughput of the session over the past five minutes.

Managing NDMP restartable backups

An NDMP restartable backup is a type of backup that you can enable in your data management application (DMA). If a restartable backup fails, for example, because of a power outage, you can restart the backup from a checkpoint close to the point of failure. In contrast, when a non-restartable backup fails, you must back up all data from the beginning, regardless of what was transferred during the initial backup process.

After you enable restartable backups from your DMA, you can manage restartable backup contexts from OneFS. These contexts are the data that OneFS stores to facilitate restartable backups. Each context represents a checkpoint that the restartable backup process can return to if a backup fails. There can be only one restartable backup context per restartable backup session. A backup restartable context contains working files in the state of the latest checkpoint.

Restartable backups are supported for EMC NetWorker 8.1 and later versions and CommVault Simpana DMAs.

Note

NDMP multi-stream backup does not support BRE.
Configure NDMP restartable backups for EMC NetWorker

You must configure EMC NetWorker to enable NDMP restartable backups and, optionally, define the checkpoint interval.

If you do not specify a checkpoint interval, NetWorker uses the default interval of 5 GB.

Procedure

1. Configure the client and the directory path that you want to back up as you would normally.
2. In the Client Properties dialog box, enable restartable backups.
   a. On the General page, click the Checkpoint enabled checkbox.
   b. In the Checkpoint granularity drop-down list, select File.
3. In the Application information field, type any NDMP variables that you want to specify.
   The following variable setting specifies a checkpoint interval of 1 GB:
   `CHECKPOINT_INTERVAL_IN_BYTES=1GB`
4. Finish configuration and click OK in the Client Properties dialog box.
5. Start the backup.
6. If the backup is interrupted—for example, because of a power failure—restart it.
   a. On the Monitoring page, locate the backup process in the Groups list.
   b. Right-click the backup process and then, in the context menu, click Restart.
   NetWorker automatically restarts the backup from the last checkpoint.

View NDMP restartable backup contexts

You can view NDMP restartable backup contexts that have been configured.

Procedure

1. List all the restartable backup contexts by running the following command:

   ```bash
   isi ndmp contexts list --type bre
   ```

2. To view detailed information about a specific restartable backup context, run the `isi ndmp contexts view` command.
   The following command displays detailed information about a backup context with an ID of 792eeb8a-8784-11e2-aa70-0025904e91a4:

   ```bash
   isi ndmp contexts view bre_792eeb8a-8784-11e2-aa70-0025904e91a4
   ```
Delete an NDMP restartable backup context

After an NDMP restartable backup context is no longer needed, your data management application (DMA) automatically requests OneFS to delete the context. You can manually delete a restartable backup context before the DMA requests it.

Note

We recommend that you do not manually delete restartable backup contexts. Manually deleting a restartable backup context requires you to restart the corresponding NDMP backup from the beginning.

Procedure

- Run the `isi ndmp contexts delete` command.

  The following command deletes a restartable backup context with an ID of 792eeb8a-8784-11e2-aa70-0025904e91a4:

  ```bash
  isi ndmp contexts delete bre_792eeb8a-8784-11e2-aa70-0025904e91a4
  ```

Configure NDMP restartable backup settings

You can specify the number of restartable backup contexts that OneFS can retain at a time, up to a maximum of 1024 contexts.

Procedure

- Run the `isi ndmp settings global modify` command.

  The following command sets the maximum number of restartable backup contexts to 128:

  ```bash
  isi ndmp settings global modify --bre_max_num_contexts=128
  ```

View NDMP restartable backup settings

You can view the current limit of restartable backup contexts that OneFS retains at one time.

Procedure

- Run the following command:

  ```bash
  isi ndmp settings global view
  ```

Managing file list backups

If your data management application (DMA) can pass environment variables to OneFS, you can control backups by specifying a file list.

With a normal NDMP level 0 (full) backup, your DMA backs up an entire source directory. With an NDMP incremental (level 1-10) backup, your DMA backs up only those files that have been created or changed since the previous incremental backup of the same level.
When you specify a file list backup, only the listed files in a directory that are in a sorted order are backed up.

A backup level other than 0 triggers an incremental file list backup. In an incremental file list backup, only the listed files that were created or changed in the source directory since the last incremental backup of the same level are backed up.

To configure a file list backup, you must complete the following tasks:

- Create the file list in a sorted order and place it in OneFS.
- Specify the path of the source directory.
- Specify the file list location.

The file list is an ASCII text file that lists the pathnames of files to be backed up. The pathnames must be relative to the path specified in the `FILESYSTEM` environment variable. Absolute file paths in the file list are not supported. The pathnames of all files must be included, or they are not backed up.

To specify the full path of the source directory to be backed up, you must specify the `FILESYSTEM` environment variable in your DMA. For example:

```bash
FILESYSTEM=/ifs/data/projects
```

To specify the pathname of the file list, you must specify the environment variable, `BACKUP_FILE_LIST` in your DMA. The file list must be accessible from the node performing the backup. For example:

```bash
BACKUP_FILE_LIST=/ifs/data/proj_list.txt
```

### Format of a backup file list

You must create a file list to enable a file list backup.

A file list backup requires an ASCII text file in a particular format to identify the pathnames of files to be backed up. Following is an example of a file list with pathnames relative to `/ifs/data/projects`:

```plaintext
proj001/plan/\001File
proj001/plan/\002File
proj001/plan/\003File
proj001/plan/\004File
proj001/plan/\005File
proj001/plan/\006File
proj001/plan/\aFile
proj001/plan/\bFile
proj001/plan/\tFile
proj001/plan/\nFile
proj002/plan/\vFile
proj002/plan/\fFile
proj002/plan/\rFile
proj002/plan/\016File
proj002/plan/\017File
proj002/plan/\020File
proj002/plan/\023File
proj002/plan/\024File
proj005/plan/\036File
proj005/plan/\037File
proj005/plan/ File
proj005/plan/!File
proj005/plan/"File
proj005/plan/#File
proj005/plan/$File
proj005/plan/%File
```
As shown in the example, the pathnames are relative to the full path of the source directory, which you specify in the FILESYSTEM environment variable. Absolute file paths are not supported in the file list.

Also as shown, the directories and files must be in sorted order for the backup to be successful. A # at the beginning of a line in the file list indicates to skip the line.

The pathnames of all files must be included in the file list, or they are not backed up. For example, if you only include the pathname of a subdirectory, the subdirectory is backed up, but not the files the subdirectory contains. The exception is ADS (alternate data streams). All ADS associated with a file to be backed up are automatically backed up.

Placement of the file list

Before you can perform a file list backup, you must place the file list in OneFS.

For example, suppose the FILESYSTEM environment variable specifies the full path of the directory to be backed up as /ifs/data/projects. You can place the text file containing the file list anywhere within the /ifs path.

Start a file list backup

You can configure and start a file list backup from your data management application (DMA).

Before you begin

You should have already specified and saved the list of files to be backed up in an ASCII text file.

Configure a file list backup from your DMA as you would any backup, but with a few additional steps as described in the following procedure.

Procedure

1. Copy the file list to the OneFS file system on the EMC Isilon cluster containing the files to be backed up.

   For example, if the directory that you specify in the FILESYSTEM environment variable is /ifs/data/projects, you could place your file list at /ifs/data.

2. In your DMA, specify the BACKUP_FILE_LIST environment variable to be the full pathname of the file list that resides on the EMC Isilon cluster.

   For example, if the file list was named proj_backup.txt, and you placed it at /ifs/data, specify /ifs/data/proj_backup.txt as the full pathname of the file list.

3. Start your backup as you normally would.

Results

The files in your file list are backed up as specified.
NDMP restore operations

NDMP supports the following types of restore operations:

- NDMP parallel restore (multi-threaded process)
- NDMP serial restore (single-threaded process)

NDMP parallel restore operation

Parallel (multi-threaded) restore enables faster full or partial restore operations by writing data to the cluster as fast as the data can be read from the tape. Parallel restore is the default restore mechanism in OneFS.

You can restore multiple files concurrently through the parallel restore mechanism.

NDMP serial restore operation

For troubleshooting or for other purposes, you can run a serial restore operation which uses fewer system resources. The serial restore operation runs as a single-threaded process and restores one file at a time to the specified path.

Specify a NDMP serial restore operation

You can use the `RESTORE_OPTIONS` environment variable to specify a serial (single-threaded) restore operation.

Procedure

1. In your data management application, configure a restore operation as you normally would.
2. Make sure that the `RESTORE_OPTIONS` environment variable is set to 1 on your data management application.
   
   If the `RESTORE_OPTIONS` environment variable is not already set to 1, specify the `isi ndmp settings variables modify` command from the OneFS command line. The following command specifies serial restore for the `/ifs/data/projects` directory:

   ```bash
   isi ndmp settings variables modify /ifs/data/projects
   RESTORE_OPTIONS 1
   ```

   The value of the `path` option is the `FILESYTEM` environment variable set during the backup operation. The value that you specify for the `name` option is case sensitive.

3. Start the restore operation.

Sharing tape drives between clusters

Multiple Isilon clusters, or an EMC Isilon cluster and a third-party NAS system, can be configured to share a single tape drive. This helps to maximize the use of the tape infrastructure in your data center.

In your data management application (DMA), you must configure NDMP to control the tape drive and ensure that it is shared properly. The following configurations are supported.
Managing default NDMP variables

In OneFS, you can manage NDMP backup and recovery operations by specifying default NDMP environment variables. You can also override default NDMP environment variables through your data management application (DMA).

For more information about specifying NDMP environment variables through your DMA, see your DMA documentation.

Specify the default NDMP variable settings for a path

You can specify default NDMP variable settings for a path.

Procedure

1. Open a secure shell (SSH) connection to any node in the EMC Isilon cluster and log in.
2. Set default NDMP variables by running the `isi ndmp settings variables create` command.
   
   For example, the following command enables snapshot-based incremental backups for `/ifs/data/media`:

   ```bash
   isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
   ```

Modify the default NDMP variable settings for a path

You can modify the default NDMP variable settings for a path.

Procedure

1. Open a secure shell (SSH) connection to any node in the EMC Isilon cluster and log in.
2. Modify default NDMP variable settings by running the `isi ndmp settings variables modify` command.

   For example, the following command sets the default file history format to path-based format for `/ifs/data/media`:

   ```bash
   isi ndmp settings variables modify /ifs/data/media HIST F
   ```
3. (Optional) To remove a default NDMP variable setting for a path, run the `isi ndmp settings variables delete` command:

For example, the following command removes the default file history format for `/ifs/data/media`:

```
isi ndmp settings variables delete /ifs/data/media --name=HIST
```

**Note**

If you do not specify the `--name` option, all the variables for the specified path are deleted after a confirmation.

---

**View the default NDMP settings for a path**

You can view the default NDMP settings for a path.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the EMC Isilon cluster and log in.
2. View the default NDMP settings by running the following command:

```
isi ndmp settings variables list
```

---

**NDMP environment variables**

You can specify default settings of NDMP backup and recovery operations through NDMP environment variables. You can also specify NDMP environment variables through your data management application (DMA).

Symantec NetBackup and EMC NetWorker are the only two DMAs that allow you to directly set environment variables and propagate them to OneFS.

**Table 6 NDMP environment variables**

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP_FILE_LIST</td>
<td>&lt;file-path&gt;</td>
<td>None</td>
<td>Triggers a file list backup. Currently, only EMC NetWorker and Symantec NetBackup can pass environment variables to OneFS.</td>
</tr>
<tr>
<td>BACKUP_MODE</td>
<td>TIMESTAMP SNAPSHOT</td>
<td>TIMESTAMP</td>
<td>Enables or disables snapshot-based incremental backups. To enable snapshot-based incremental backups, specify SNAPSHOT.</td>
</tr>
<tr>
<td>BACKUP_OPTIONS</td>
<td>0x00000100 0x00000200</td>
<td>0</td>
<td>This environment variable is specific only to dataset</td>
</tr>
<tr>
<td>Environment variable</td>
<td>Valid values</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>0x00000400</td>
<td></td>
<td>containing CloudPools stub files. Controls the behavior of the backup. 0 Backs up modified cache data.</td>
</tr>
<tr>
<td></td>
<td>0x00000100</td>
<td></td>
<td>Reads stub file data from the cloud and backs up the stub files as regular files.</td>
</tr>
<tr>
<td></td>
<td>0x00000200</td>
<td></td>
<td>Backs up all the cached data that is stored in the stub files.</td>
</tr>
<tr>
<td></td>
<td>0x00000400</td>
<td></td>
<td>Recalls and backs up data stored in stub files.</td>
</tr>
<tr>
<td>BASE_DATE</td>
<td></td>
<td></td>
<td>Enables a token-based incremental backup. Dumpdates file will not be updated in this case.</td>
</tr>
<tr>
<td>DIRECT</td>
<td>Y N</td>
<td>N</td>
<td>Enables or disables Direct Access Restore (DAR) and Directory DAR (DDAR). The following values are valid: Y Enables DAR and DDAR. N Disables DAR and DDAR.</td>
</tr>
<tr>
<td>EXCLUDE</td>
<td>&lt;file-matching-pattern&gt;</td>
<td>None</td>
<td>If you specify this option, OneFS does not back up files and directories that meet the specified pattern. Separate multiple patterns with a space.</td>
</tr>
</tbody>
</table>
### Table 6 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILES</td>
<td><code>&lt;file-matching-pattern&gt;</code></td>
<td>None</td>
<td>If you specify this option, OneFS backs up only files and directories that meet the specified pattern. Separate multiple patterns with a space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>As a rule, files are matched first and then the EXCLUDE pattern is applied.</td>
</tr>
<tr>
<td>HIST</td>
<td><code>&lt;file-history-format&gt;</code></td>
<td>Y</td>
<td>Specifies the file history format. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies directory or node file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies path-based file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the default file history format determined by your NDMP backup settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disables file history.</td>
</tr>
<tr>
<td>LEVEL</td>
<td><code>&lt;integer&gt;</code></td>
<td>0</td>
<td>Specifies the level of NDMP backup to perform. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Performs a full NDMP backup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Performs an incremental backup at the specified level.</td>
</tr>
<tr>
<td>Environment variable</td>
<td>Valid values</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>Performs Incremental Forever backups.</td>
</tr>
<tr>
<td>MSB_RETENTION_PERIOD</td>
<td>Integer 300 sec</td>
<td></td>
<td>Specifies the backup context retention period.</td>
</tr>
<tr>
<td>MSR_RETENTION_PERIOD</td>
<td>0 through 60<em>60</em>24 600 sec</td>
<td></td>
<td>Specifies the recovery context retention period within which a recovery session can be retried.</td>
</tr>
<tr>
<td>RECURSIVE</td>
<td>Y / N Y</td>
<td></td>
<td>Specifies that the backup session is recursive.</td>
</tr>
<tr>
<td>RESTORE_BIRTHTIME</td>
<td>Y / N N</td>
<td></td>
<td>Specifies whether to recover the birth time for a recovery session.</td>
</tr>
</tbody>
</table>
| RESTORE_HARDLINK_BY_TABLE        | Y / N N                            |         | For a single-threaded restore session, determines whether OneFS recovers hard links by building a hard-link table during recovery operations. Specify this option if hard links are incorrectly backed up and recovery operations are failing. If a recovery operation fails because hard links were incorrectly backed up, the following message appears in the NDMP backup logs:  
  Bad hardlink path for <path>  

**Note**  
This variable is not effective for a parallel restore operation. |
| RESTORE_OPTIONS                  | 0 1 0x00000002 0x00000004            | 0       | The restore operation, by default, is multi-threaded to improve performance. To change the restore operation to single- |
### Table 6 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threaded, specify RESTORE_OPTIONS=1</td>
<td>0</td>
<td>0</td>
<td>The restore operation does not overwrite the permissions of the existing directories.</td>
</tr>
<tr>
<td>0x00000002</td>
<td>Forges the restore operation to overwrite the permissions of existing directories using the information from the restore stream. This option is applicable only to directories in nlist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00000004</td>
<td>In releases prior to OneFS 8.0.0, intermediate directories created during a restore operation have their default permissions set. In OneFS 8.0.0 and later releases, permissions of an intermediate directory is the same as the first file restored within that directory. 0x00000004 reverts back to the former restore method, and sets the permissions of the intermediate directories to 0700 and sets UID/GID to 0.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 6 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPDATE</td>
<td>Y, N</td>
<td>Y</td>
<td>Determines whether OneFS updates the dump dates file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Y: OneFS updates the dump dates file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N: OneFS does not update the dump dates file.</td>
</tr>
</tbody>
</table>

## Setting environment variables for backup operations

The `BASE_DATE`, `LEVEL`, `BACKUP_MODE`, and `BACKUP_OPTIONS` environment variables determine the type of the NDMP backup operations to perform and the level of those operations.

- If the `BASE_DATE` environment variable is set to any value and if you set the `BACKUP_MODE` environment variable to `SNAPSHOT`, the `LEVEL` environment variable is automatically set to `10` and an Incremental Forever backup is performed.
- If the `BASE_DATE` environment variable is set to `0`, a full backup is performed.
- If the `BASE_DATE` environment variable is not set to `0`, the entries in the dump dates file are read and compared with the `BASE_DATE` environment variable. If an entry is found and a prior valid snapshot is found, a faster incremental backup is performed.
- If the `BASE_DATE` environment variable is not set to `0` and if no entries are found in the dump dates file and no prior valid snapshots are found, a token-based backup is performed using the value of the `BASE_DATE` environment variable.
- If the `BASE_DATE` environment variable is set, the `BACKUP_OPTIONS` environment variable is set to `0x00000001` by default.
- If the `BACKUP_MODE` environment variable is set to `SNAPSHOT`, the `BACKUP_OPTIONS` environment variable is set to `0x00000002` by default.
- If the `BACKUP_OPTIONS` environment variable is set to `0x00000004`, the snapshot is saved and maintained by the application used for the backup process.
- In order to run an Incremental Forever backup with faster incremental backups, you must set the following environment variables:
  - `BASE_DATE=<time>`
  - `BACKUP_MODE=snapshot`
  - `BACKUP_OPTIONS=7`
Managing snapshot based incremental backups

After you enable snapshot-based incremental backups, you can view and delete the snapshots created for these backups.

Enable snapshot-based incremental backups for a directory

You can configure OneFS to perform snapshot-based incremental backups for a directory by default. You can also override the default setting in your data management application (DMA).

Procedure

- Run the `isi ndmp settings variable create` command.

  The following command enables snapshot-based incremental backups for `/ifs/data/media`:

  ```bash
  isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
  ```

Delete snapshots for snapshot-based incremental backups

You can delete snapshots created for snapshot-based incremental backups.

Note

It is recommended that you do not delete snapshots created for snapshot-based incremental backups. If all snapshots are deleted for a path, the next backup performed for the path is a full backup.

Procedure

- Run the `isi ndmp dumpdates delete` command.

  The following command deletes all snapshots created for backing up `/ifs/data/media`:

  ```bash
  isi ndmp dumpdates delete /ifs/data/media
  ```

View snapshots for snapshot-based incremental backups

You can view snapshots generated for snapshot-based incremental backups.

Procedure

- Run the following command:

  ```bash
  isi ndmp dumpdates list
  ```
View NDMP backup logs

You can view information about NDMP backup and restore operations through NDMP backup logs.

Procedure

1. View the contents of the `/var/log/isi_ndmp_d` directory by running the following command:

   ```bash
   more /var/log/isi_ndmp_d
   ```

NDMP backup commands

You can control Network Data Management Protocol (NDMP) backups through the NDMP backup commands.

**isi ndmp users create**

Creates a new NDMP user.

**Syntax**

```bash
isi ndmp users create <name> [--password <string>]
```

**Options**

- `<name>`
  - The name of the user.

- `--password <string>`
  - The password for the new NDMP user. If you do not specify a password, the new user will be prompted to enter a password, and will be prompted to confirm the password by entering it again. This command fails if the specified user already exists.

**Examples**

The following command creates an NDMP user account with username `ndmp_user` and password `1234`:

```bash
isi ndmp users create ndmp_user --password=1234
```
isi ndmp users delete

Deletes a specified NDMP user.

Syntax

```bash
isi ndmp users delete <name>
   [--force]
   [--verbose]
```

Options

- `<name>`
  - The name of the NDMP user to delete.

- `[--force | -f]`
  - Skips the confirmation prompt.

- `[--verbose | -v]`
  - Displays more detailed information.

isi ndmp users list

Lists all NDMP users.

Syntax

```bash
isi ndmp users list
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
```

Options

- `--format {table | json | csv | list}`
  - Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

- `[--no-header | -a]`
  - Displays table and CSV output without headers.

- `[--no-footer | -z]`
  - Displays table output without footers.

Example

This is an example of the output created by this command:

```
Name   
-------
ndmp_nick
ndmp_lisa
ndmp_jason
-------
Total: 3
```
isi ndmp users modify

Changes the password for the specified NDMP user.

Syntax

```bash
isi ndmp users delete <name>
   [--password <string>]
```

Options

- `<name>`
  The name of NDMP user you are modifying.

- `--password <string>`
  The password for the NDMP user you are modifying. If you do not specify a password, the user will be prompted to enter a password, and will be prompted to confirm the password by entering it again.

isi ndmp users view

View a specific NDMP user.

Syntax

```bash
isi ndmp users view <name>
   [--format {list | json}]
```

Output

- `<name>`
  The name of the NDMP user.

- `--format {list | json}`
  Lists the NDMP user in the specified format.

Example

The following is an example of the output created by this command, for an NDMP user named `ndmp_lisa`, and with JSON format specified:

```
["id": "ndmp_lisa", "name": "ndmp_lisa"]
```

isi ndmp contexts delete

Deletes an NDMP context.

Syntax

```bash
isi ndmp contexts delete <id>
   [--force]
   [--verbose]
```
Options

<id>
   The context ID string.

|--force | -f
   Skips the confirmation prompt.

|--verbose | -v
   Displays more detailed information.

isi ndmp contexts list

Lists NDMP contexts.

Syntax

isi ndmp contexts list
   [--type {bre | backup | restore}]
   [--format {table | json | csv | list}]

Options

|--type | -t {bre | backup | restore}
   Displays entries for the specified level: backup restartable extension (BRE), backup, or restore.

|--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

isi ndmp contexts view

Displays detailed information of an NDMP context.

Syntax

isi ndmp contexts view <id>
   [--format {list | json}]

Options

<id>
   The context ID string.

|--format {list | json}
   Lists the NDMP context in the specified format.
**isi ndmp dumpdates delete**

Deletes a snapshot created for a snapshot-based NDMP incremental backup.

**Syntax**

```
isi ndmp dumpdates delete <path>
   [--level <integer>]
   [--force]
   [--verbose]
```

**Options**

- `<path>`
  - The path of the NDMP dumpdate. Must be within the /ifs directory structure.

- `--level <integer>`
  - Deletes a dumpdate entry for a backup of the specified level for the given directory. If this option is not specified, deletes all dumpdate entries for the given directory.

**Examples**

The following command deletes the dumpdate entry for a level 0 backup of /ifs/data/media:

```
isi ndmp dumpdates delete /ifs/data/media --level=0
```

---

**isi ndmp dumpdates list**

Displays snapshots created for snapshot-based NDMP incremental backups.

**Syntax**

```
isi ndmp dumpdates list
   [--path <path>]
   [--level <integer>]
   [--limit <integer>]
   [--sort {path | level}]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

**Options**

- `--path <path>`
  - The path of the NDMP dumpdate. Must be within the /ifs directory structure.

- `--level <integer>`
  - Displays dumpdate entries for a backup of the specified level for the given directory path.

- `{--limit | -l}<integer>`
  - The number of NDMP dumpdates to display.
--sort {path | level}
    Sorts data by the specified field.

{--descending | -d}
    Sorts data in descending order.

--format {table | json | csv | list}
    Displays NDMP dumpdates in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
    Displays table and CSV output without headers.

{--no-footer | -z}
    Displays table output without footers.

{--verbose | -v}
    Displays more detailed information.

Examples
To view NDMP dumpdate entries, run the following command:

    isi ndmp dumpdates list

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Date</th>
<th>Level</th>
<th>SnapID</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri May 29 12:06:26 2015</td>
<td>0</td>
<td>18028</td>
<td>/ifs/tmp/backup</td>
</tr>
<tr>
<td>Fri May 29 12:20:56 2015</td>
<td>1</td>
<td>18030</td>
<td>/ifs/tmp/backup</td>
</tr>
</tbody>
</table>

If a snapshot was created for a non-snapshot-based incremental backup, the snapshot ID is 0.

isi ndmp sessions delete

Stops an NDMP session.

Syntax

    isi ndmp sessions delete <session>
        [--force]
        [--verbose]

Options

<session>
    The NDMP session identifier. The session ID consists of the logical node number (LNN) followed by a decimal point and then the process ID (PID), such as <lnn>.<pid>.

{--force | -f}
    Skips the confirmation prompt.

{verbose | -v}
Displays more detailed information.

Example
The following command ends an NDMP session with the session ID 4.36339:

```bash
isi ndmp sessions delete 4.36339
```

**isi ndmp sessions list**

Lists all or specified NDMP sessions.

**Syntax**

```bash
isi ndmp sessions list
[--node <integer>]
[--session <string>]
[--consolidate]
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

```
{--node | -n} <integer>
    Displays only sessions for the specified node.

{--session | -s} <string>
    The NDMP session identifier. The session ID consists of the logical node number (LNN) followed by a decimal point and then the process ID (PID), such as <lnn>.<pid>.

{--consolidate | -c}
    Consolidates sessions of a multi-stream context.

{--limit | -l} <integer>
    The number of NDMP sessions to display.

--format {table | json | csv | list}
    Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
    Displays table and CSV output without headers.

{--no-footer | -z}
    Displays table output without footers.

{verbose | -v}
    Displays more detailed information.
**isi ndmp sessions view**

Displays detailed information about an NDMP session.

**Syntax**

```
isi ndmp sessions view <session>
  [--probe]
  [--format {list | json}]
```

**Options**

- `<session>`
  - The NDMP session identifier. The session ID consists of the logical node number (LNN) followed by a decimal point and then the process ID (PID), such as `<lnn>.<pid>`.
- `--probe`
  - Displays probe information about the NDMP session.
- `--format {list | json}`
  - Displays NDMP session information in list or JSON format.

**isi ndmp settings diagnostics modify**

Modifies NDMP diagnostics settings.

**Syntax**

```
isi ndmp settings diagnostics modify
  [--diag-level <integer>]
  [--protocol-version <integer>]
  [--trace-level {none | standard | include-file-history | log-file-history}]
```

**Options**

- `--diag-level <integer>`
  - The diagnostics level for NDMP.
- `--protocol-version <integer>`
  - The NDMP protocol version (3 or 4).
- `--trace-level {none | standard | include-file-history | log-file-history}`
  - The NDMP trace log level. Select `none` for no log, `standard` for NDMP protocol tracing, `include-file-history` to log file history information into the trace file, or `log-file-history` to log file history into the file history log.
**isi ndmp settings diagnostics view**

Displays NDMP diagnostic settings.

**Syntax**

```bash
isi ndmp settings diagnostics view
   [--format {list | json}]
```

**Options**

`--format {list | json}`

Displays NDMP diagnostic settings information in list or JSON format.

**isi ndmp settings global modify**

Modifies NDMP global settings.

**Syntax**

```bash
isi ndmp settings global modify
   [--service {true | false}]
   [--dma {generic | atempo | bakbone | commvault | emc | symantec | tivoli | symantec-netbackup | symantec-backupexec}]
   [--port <integer>]
   [--bre-max-num-contexts <integer>]
   [--msb-context-retention-duration <integer>]
   [--msr-context-retention-duration <integer>]
```

**Options**

`{--service | -s}{yes | no}`

Enables or disables the NDMP service.

`{--dma | -d}{generic | atempo | bakbone | commvault | emc | symantec | tivoli | symantec-netbackup | symantec-backupexec}`

The data management application (DMA) that controls NDMP sessions.

`{--port | -p} <integer>`

Sets the TCP/IP port number on which the NDMP daemon listens for incoming connections. The default port is 10000.

`--bre-max-num-contexts <integer>`

Sets the maximum number of restartable backup contexts. The system maximum limit is 1024, and the default is 64. Set this option to zero (0) to disable restartable backups.

`--msb-context-retention-duration <integer>`

Sets the duration of multi-stream backup context retention. Express durations in YMWDHms integer format. The default duration is 5m (five minutes).

`--msr-context-retention-duration <integer>`

Sets the duration of multi-stream restore context retention. Express durations in YMWDHms integer format. The default duration is 10m (ten minutes).
**isi ndmp settings global view**

Displays NDMP global settings.

**Syntax**

```
isi ndmp settings global view
[--format {list | json}]
```

**Options**

`--format {list | json}`

Displays NDMP global settings in list or JSON format.

**Example**

The following is an example of the output generated by this command:

```
Service: True
Port: 10000
Dma: emc
Bre Max Num Contexts: 64
Msb Context Retention Duration: 300
Msr Context Retention Duration: 600
```

**isi ndmp settings variables create**

Sets the default value for an NDMP environment variable for a given path.

**Syntax**

```
isi ndmp settings variables create <path> <name> <value>
```

For a list of available environment variables, see [NDMP environment variables](#).

**Options**

`<path>`

Applies the default NDMP environment variable value to the specified path. The directory path must be within `/ifs`.

`<name>`

Specifies the NDMP environment variable to define.

`<value>`

Specifies the value to be applied to the NDMP environment variable.

**Examples**

The following command enables snapshot-based incremental backups to be performed for `/ifs/data/media` by default:

```
isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
```
**isi ndmp settings variables delete**

Deletes the default value for an NDMP environment variable for a given path.

**Syntax**

```bash
isi ndmp settings variables delete <path>  
    [--name <string>]
```

**Options**

For a list of available environment variables, see NDMP environment variables.

`<path>`

Applies the default NDMP-environment-variable value to the specified path. This must be a valid directory path within /ifs.

`--name <variable>`

The name of the variable to be deleted. If you do not specify a variable name, all environment variables are deleted for the specified path. If this option is not specified, deletes default values for all NDMP environment variables for the given directory.

**Examples**

The following command removes all default NDMP settings for /ifs/data/media:

```bash
isi ndmp settings variables delete /ifs/data/media
```

The following command removes the default file-history setting for backing up /ifs/data/media:

```bash
isi ndmp settings variables delete /ifs/data/media --name HIST
```

**isi ndmp settings variables list**

Lists all preferred NDMP environment variables.

**Syntax**

```bash
isi ndmp settings variables list  
    [--path <path>]  
    [--format {table | json | csv | list}]  
    [--no-header]  
    [--no-footer]
```

**Options**

`--path <path>`

Applies the default NDMP-environment-variable value to the specified path.

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
NDMP backup and recovery overview

{--no-header | -a}
   Displays table and CSV output without headers.

{--no-footer | -z}
   Displays table output without footers.

**isi ndmp settings variables modify**

Modifies the default value for an NDMP environment variable for a given path.

Syntax

```
isi ndmp settings variables modify <path> <name> <value>
```

Options

For a list of available environment variables, see NDMP environment variables.

<path>
   Applies the default NDMP-environment-variable value to the specified path. This
   must be a valid directory path within /ifs.

<name>
   Specifies the NDMP environment variable to be defined.

<value>
   Specifies the value to be applied to the NDMP environment variable.

**isi fc settings list**

Lists Fibre Channel port settings.

Syntax

```
isi fc settings list
   [--format {table | json | csv | list}]
   [--no-header]
```

Options

--format {table | json | csv | list}
   Displays Fibre Channel port settings in table, JSON, CSV, or list format.

{--no-header | -a]}
   Does not display headers in table or CSV formats.

Examples

The following command displays all ports on node 5:

```
isi fc settings list
```
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Port</th>
<th>WWNN</th>
<th>WWPN</th>
<th>State</th>
<th>Topology</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>5:1</td>
<td>2000001b3214ccc3</td>
<td>2100001b3214ccc3</td>
<td>enabled</td>
<td>auto</td>
<td>auto</td>
</tr>
<tr>
<td>5:2</td>
<td>2000001b3234ccc3</td>
<td>2101001b3234ccc3</td>
<td>enabled</td>
<td>auto</td>
<td>auto</td>
</tr>
<tr>
<td>5:3</td>
<td>2000001b3254ccc3</td>
<td>2100001b3254ccc3</td>
<td>enabled</td>
<td>auto</td>
<td>auto</td>
</tr>
<tr>
<td>5:4</td>
<td>2000001b3234ccc3</td>
<td>2103001b3274ccc3</td>
<td>enabled</td>
<td>auto</td>
<td>auto</td>
</tr>
</tbody>
</table>

### isi fc settings modify

Modifies Fibre Channel settings for a specific port.

#### Syntax

```bash
isi fc settings modify <port>
[--wwnn <string>]
[--wwpn <string>]
[--state {enable | disable}]
[--topology {auto | loop | ptp}]
[--rate {auto | 1 | 2 | 4 | 8}]
```

#### Options

|--wwnn <string>  
  Specifies the world-wide node name (WWNN) of the port as a string of 16 hexadecimal numerals.

|--wwpn <string>  
  Specifies the world-wide port name (WWPN) of the port as a string of 16 hexadecimal numerals.

|--state {enable | disable}  
  Specifies whether the port is enabled or disabled.

|--topology {auto | loop | ptp}  
  Specifies the type of Fibre Channel topology that the port expects. The following settings are valid:
    
    **auto**
    
    Causes the port to detect the topology automatically. This is the recommended setting. Specify this setting if you are using a fabric topology.
    
    **loop**
    
    Causes the port to expect an arbitrated loop topology, with multiple backup devices connected to a single port in a circular formation.
    
    **ptp**
    
    Causes the port to expect a point-to-point topology, with one backup device or Fibre Channel switch directly connected to the port.

|--rate {auto | 1 | 2 | 4 | 8}  
  Specifies the rate that OneFS will attempt to send data through the port. The following rates are valid:
    
    **auto**
    
    OneFS automatically negotiates with the DMA to determine the rate. This is the recommended setting.
Attempts to send data through the port at a speed of 1 Gb per second.

Attempts to send data through the port at a speed of 2 Gb per second.

Attempts to send data through the port at a speed of 4 Gb per second.

Attempts to send data through the port at a speed of 8 Gb per second.

**isi fc settings view**

Displays settings for a specific Fibre Channel port.

**Syntax**

```
isi fc settings view <port>  
[--format {list | json}]
```

**Options**

- `--format {list | json}`
  Displays the Fibre Channel port settings in list or JSON format.

**isi tape delete**

Disconnects the cluster from an NDMP tape or media change device that is currently connected to a Backup Accelerator node on the cluster.

**Syntax**

```
isi tape delete  
[--name <string>]  
[--all]  
[--force]  
[--verbose]
```

**Options**

- `--name <string>`
  The name of the NDMP tape or media change device.

- `--all`
  Disconnects the cluster from all devices.

- `{--force | -f}`
  Skips the confirmation prompt.

- `{--verbose | -v}`
Displays more detailed information.

**Example**
The following command disconnects `tape001` from the cluster:

```bash
isi tape delete tape001
```

**isi tape list**

Displays a list of NDMP devices that are currently connected to the cluster.

**Syntax**

```
isi tape list
[--node <lnn>]
[--tape]
[--mc]
[--activepath]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

`--node <lnn>`
Displays only devices that are attached to the node of the specified logical node number (LNN).

`--tape`
Displays only tape devices.

`--mc`
Displays only media changer devices.

`--activepath`
Displays only the active paths of a device.

`--format {table | json | csv | list}`
Displays devices in table, JSON, CSV, or list format.

`{--no-header | -a}`
Does not display headers in table or CSV format.

`{--no-footer | -z}`
Does not display table summary footer information.

`{--verbose | -v}`
Displays more detailed information.
Examples
To view a list of all NDMP devices, run the following command:

```plaintext
isi tape list
```

**isi tape modify**

Modifies the name or state of a tape or media changer device.

**Syntax**

```plaintext
isi tape modify <name>
   [--new-name <string>]
   [--close-device]
```

**Options**

- `<name>`
  The current device name.

- `--new-name <string>`
  The new device name.

- `--close-device`
  Forces the device state to closed if the device is currently open. If an NDMP session unexpectedly stops, a tape or media changer device may be left in an open state, which prevents the device from being opened again.

**isi tape rescan**

Scans Fibre Channel ports for undetected NDMP backup devices that are attached to Backup Accelerator nodes. If the scan reveals new devices, the cluster creates entries for the new devices.

**Syntax**

```plaintext
isi tape rescan
   [--node <lnn>]
   [--port <integer>]
   [--reconcile]
```

**Options**

If no options are specified, scans all nodes and ports.

- `--node <lnn>`
  Scans only the node of the specified logical node number (LNN).

- `--port <integer>`
  Scans only the specified port. If you specify `--node`, scans only the specified port on the specified node. If you do not specify `--node`, scans the specified port on all nodes.

- `--reconcile`
Removes entries for devices or paths that have become inaccessible.

Example
To scan the entire cluster for NDMP devices, and remove entries for devices and paths that have become inaccessible, run the following command:

```
isitape rescan --reconcile
```

**isi tape view**

Displays information about a tape or media changer device.

**Syntax**

```
isitape view <name>  
 [--activepath]  
 [--format {list | json}]
```

**Options**

- `<name>`
  The name of the tape or media changer device.

- `--activepath`
  Displays only the active paths of the device.

- `--format {list | json}`
  Displays devices in list or JSON format.
CHAPTER 19

File retention with SmartLock

This section contains the following topics:

- SmartLock overview ................................................................. 776
- Compliance mode ........................................................................ 776
- SmartLock directories ................................................................. 776
- Accessing SmartLock with IsilonSD Edge .................................. 777
- Replication and backup with SmartLock ..................................... 777
- SmartLock license functionality .................................................. 779
- SmartLock considerations .......................................................... 779
- Set the compliance clock ............................................................. 779
- View the compliance clock .......................................................... 780
- Creating a SmartLock directory .................................................. 780
- Managing SmartLock directories ................................................ 782
- Managing files in SmartLock directories ..................................... 786
- SmartLock commands ................................................................. 790
SmartLock overview

With the SmartLock software module, you can prevent users from modifying and deleting files on an EMC Isilon cluster. To protect data in this manner, you must activate a SmartLock license.

With SmartLock, you can identify a directory in OneFS as a WORM domain. WORM stands for write once, read many. All files within the WORM domain will be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted.

After a file is removed from a WORM state, you can delete the file. However, you can never modify a file that has been committed to a WORM state, even after it is removed from a WORM state.

In OneFS, SmartLock can be configured as one of two modes: compliance mode or enterprise mode.

Compliance mode

SmartLock compliance mode enables you to protect your data in compliance with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4.

Note

You can upgrade an EMC Isilon cluster to SmartLock compliance mode only during the initial cluster configuration process, prior to activating a SmartLock license. A cluster cannot be converted to SmartLock compliance mode after the cluster is initially configured and put into production.

If you upgrade a cluster to SmartLock compliance mode, the root user is removed and you are not able to log in to that cluster through the root user account. Instead, you can log in to the cluster through the compliance administrator account that is configured during initial cluster configuration.

When you are logged in to a SmartLock compliance mode cluster through the compliance administrator account, you can perform administrative tasks through the `sudo` command.

SmartLock directories

In a SmartLock directory, you can commit a file to a WORM state manually or you can configure SmartLock to automatically commit the file. Before you can create SmartLock directories, you must activate a SmartLock license on the cluster.

You can create two types of SmartLock directories: enterprise and compliance. However, you can create compliance directories only if the EMC Isilon cluster has been set up in SmartLock compliance mode during initial configuration.

Enterprise directories enable you to protect your data without restricting your cluster to comply with regulations defined by U.S. Securities and Exchange Commission rule 17a-4. If you commit a file to a WORM state in an enterprise directory, the file can never be modified and cannot be deleted until the retention period passes.

However, if you own a file and have been assigned the `ISI_PRIV_IFS_WORM_DELETE` privilege, or you are logged in through the root user account, you can delete the file through the privileged delete feature before the...
The privileged delete feature is not available for compliance directories. Enterprise directories reference the system clock to facilitate time-dependent operations, including file retention.

Compliance directories enable you to protect your data in compliance with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4. If you commit a file to a WORM state in a compliance directory, the file cannot be modified or deleted before the specified retention period has expired. You cannot delete committed files, even if you are logged in to the compliance administrator account. Compliance directories reference the compliance clock to facilitate time-dependent operations, including file retention.

You must set the compliance clock before you can create compliance directories. You cannot set the compliance clock only once. After you set the compliance clock, you cannot modify the compliance clock time. The compliance clock is controlled by the compliance clock daemon. Because root and compliance administrator users can disable the compliance clock daemon, it is possible for those users to increase the retention period of WORM committed files in compliance mode. However, it is not possible to decrease the retention period of a WORM committed file.

**Accessing SmartLock with IsilonSD Edge**

The SmartLock software module is available only with a purchased license of IsilonSD Edge. It is not packaged with the free license of this product.

Make note of the following considerations before using SmartLock with IsilonSD Edge:

- IsilonSD Edge supports SmartLock in both enterprise and compliance modes. However, an IsilonSD cluster might not comply with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4, even though it might comply with this regulation on hardware appliances.
- When an IsilonSD cluster is placed in compliance mode, you cannot add new nodes to the cluster. Therefore, you must add as many nodes as necessary before upgrading the cluster to SmartLock compliance mode.

**Replication and backup with SmartLock**

You must ensure that SmartLock directories on the EMC Isilon cluster remain protected during replication and backup operations.

If you are replicating SmartLock directories with SyncIQ, it is recommended that you configure all nodes on the source and target clusters into Network Time Protocol (NTP) peer mode to ensure that the node clocks are synchronized. For compliance clusters, it is recommended that you configure all nodes on the source and target clusters into NTP peer mode before you set the compliance clock to ensure that the compliance clocks are initially set to the same time.

**Note**

If you replicate data to a SmartLock directory, do not configure SmartLock settings for that directory until you are no longer replicating data to the directory. Configuring an autocommit time period for a SmartLock directory that you are replicating to can cause replication jobs to fail. If the target directory commits a file to a WORM state, and the file is modified on the source cluster, the next replication job will fail because it cannot update the file.
SmartLock replication and backup limitations

Be aware of the limitations of replicating and backing up SmartLock directories with SyncIQ and NDMP.

If the source directory or target directory of a SyncIQ policy is a SmartLock directory, replication might not be allowed. For more information, see the following table:

<table>
<thead>
<tr>
<th>Source directory type</th>
<th>Target directory type</th>
<th>Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SmartLock</td>
<td>Non-SmartLock</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock compliance</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>Non-SmartLock</td>
<td>Yes; however, retention dates and commit status of files will be lost.</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock compliance</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>Non-SmartLock</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock enterprise</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock compliance</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If you are replicating a SmartLock directory to another SmartLock directory, you must create the target SmartLock directory prior to running the replication policy. Although OneFS will create a target directory automatically if a target directory does not already exist, OneFS will not create a target SmartLock directory automatically. If you attempt to replicate an enterprise directory before the target directory has been created, OneFS will create a non-SmartLock target directory and the replication job will succeed. If you replicate a compliance directory before the target directory has been created, the replication job will fail.

If you replicate SmartLock directories to another EMC Isilon cluster with SyncIQ, the WORM state of files is replicated. However, SmartLock directory configuration settings are not transferred to the target directory.

For example, if you replicate a directory that contains a committed file that is set to expire on March 4th, the file is still set to expire on March 4th on the target cluster. However, if the directory on the source cluster is set to prevent files from being committed for more than a year, the target directory is not automatically set to the same restriction.

If you back up data to an NDMP device, all SmartLock metadata relating to the retention date and commit status is transferred to the NDMP device. If you recover data to a SmartLock directory on the cluster, the metadata persists on the cluster. However, if the directory that you recover data to is not a SmartLock directory, the metadata is lost. You can recover data to a SmartLock directory only if the directory is empty.
SmartLock license functionality

You must activate a SmartLock license on an EMC Isilon cluster before you can create SmartLock directories and commit files to a WORM state.

If a SmartLock license becomes inactive, you will not be able to create new SmartLock directories on the cluster, modify SmartLock directory configuration settings, or delete files committed to a WORM state in enterprise directories before their expiration dates. However, you can still commit files within existing SmartLock directories to a WORM state.

If a SmartLock license becomes inactive on a cluster that is running in SmartLock compliance mode, root access to the cluster is not restored.

SmartLock considerations

- If a file is owned exclusively by the root user, and the file exists on an EMC Isilon cluster that is in SmartLock compliance mode, the file will be inaccessible, because the root user account is disabled in compliance mode. For example, this can happen if a file is assigned root ownership on a cluster that has not been configured in compliance mode, and then the file is replicated to a cluster in compliance mode. This can also occur if a root-owned file is restored onto a compliance cluster from a backup.

- It is recommended that you create files outside of SmartLock directories and then transfer them into a SmartLock directory after you are finished working with the files. If you are uploading files to a cluster, it is recommended that you upload the files to a non-SmartLock directory, and then later transfer the files to a SmartLock directory. If a file is committed to a WORM state while the file is being uploaded, the file will become trapped in an inconsistent state.

- Files can be committed to a WORM state while they are still open. If you specify an autocommit time period for a directory, the autocommit time period is calculated according to the length of time since the file was last modified, not when the file was closed. If you delay writing to an open file for more than the autocommit time period, the file is automatically committed to a WORM state, and you will not be able to write to the file.

- In a Microsoft Windows environment, if you commit a file to a WORM state, you can no longer modify the hidden or archive attributes of the file. Any attempt to modify the hidden or archive attributes of a WORM committed file generates an error. This can prevent third-party applications from modifying the hidden or archive attributes.

Set the compliance clock

Before you can create SmartLock compliance directories, you must set the compliance clock.

Setting the compliance clock configures the clock to the same time as the cluster system clock. Before you set the compliance clock, ensure that the system clock is set to the correct time. If the compliance clock later becomes unsynchronized with the system clock, the compliance clock will slowly correct itself to match the system clock. The compliance clock corrects itself at a rate of approximately one week per year.
Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in through the compliance administrator account.
2. Set the compliance clock by running the following command:

   `isi worm cdate set`

View the compliance clock

You can view the current time of the compliance clock.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in through the compliance administrator account.
2. View the compliance clock by running the following command:

   `isi worm cdate view`

Creating a SmartLock directory

You can create a SmartLock directory and configure settings that control how long files are retained in a WORM state and when files are automatically committed to a WORM state. You cannot move or rename a directory that contains a SmartLock directory.

Retention periods

A retention period is the length of time that a file remains in a WORM state before being released from a WORM state. You can configure SmartLock directory settings that enforce default, maximum, and minimum retention periods for the directory.

If you manually commit a file, you can optionally specify the date that the file is released from a WORM state. You can configure a minimum and a maximum retention period for a SmartLock directory to prevent files from being retained for too long or too short a time period. It is recommended that you specify a minimum retention period for all SmartLock directories.

For example, assume that you have a SmartLock directory with a minimum retention period of two days. At 1:00 PM on Monday, you commit a file to a WORM state, and specify the file to be released from a WORM state on Tuesday at 3:00 PM. The file will be released from a WORM state two days later on Wednesday at 1:00 PM, because releasing the file earlier would violate the minimum retention period.

You can also configure a default retention period that is assigned when you commit a file without specifying a date to release the file from a WORM state.

Autocommit time periods

You can configure an autocommit time period for SmartLock directories. An autocommit time period causes files that have been in a SmartLock directory for a
period of time without being modified to be automatically committed to a WORM state.

If you modify the autocommit time period of a SmartLock directory that contains uncommitted files, the new autocommit time period is immediately applied to the files that existed before the modification. For example, consider a SmartLock directory with an autocommit time period of 2 hours. If you modify a file in the SmartLock directory at 1:00 PM, and you decrease the autocommit time period to 1 hour at 2:15 PM, the file is instantly committed to a WORM state.

If a file is manually committed to a WORM state, the read-write permissions of the file are modified. However, if a file is automatically committed to a WORM state, the read-write permissions of the file are not modified.

Create an enterprise directory for a non-empty directory

You can make a non-empty directory into a SmartLock enterprise directory. This procedure is available only through the command-line interface (CLI).

Before creating a SmartLock directory, be aware of the following conditions and requirements:

- You cannot create a SmartLock directory as a subdirectory of an existing SmartLock directory.
- Hard links cannot cross SmartLock directory boundaries.
- Creating a SmartLock directory causes a corresponding SmartLock domain to be created for that directory.

Procedure

1. Run the `isi job jobs start` command.

   The following command creates a SmartLock enterprise domain for `/ifs/data/smartlock`:

   ```bash
   isi job jobs start DomainMark --root /ifs/data/smartlock --dm-type Worm
   ```

Create a SmartLock directory

You can create a SmartLock directory and commit files in that directory to a WORM state.

Before creating a SmartLock directory, be aware of the following conditions and requirements:

- You cannot create a SmartLock directory as a subdirectory of an existing SmartLock directory.
- Hard links cannot cross SmartLock directory boundaries.
- Creating a SmartLock directory causes a corresponding SmartLock domain to be created for that directory.

Procedure

1. Run the `isi worm domains create` command.

   If you specify the path of an existing directory, the directory must be empty.
The following command creates a compliance directory with a default retention period of four years, a minimum retention period of three years, and a maximum retention period of five years:

```
isi worm domains create /ifs/data/SmartLock/directory1 \ 
  --compliance --default-retention 4Y --min-retention 3Y \ 
  --max-retention 5Y --mkdir
```

The following command creates an enterprise directory with an autocommit time period of thirty minutes and a minimum retention period of three months:

```
isi worm domains create /ifs/data/SmartLock/directory2 \ 
  --autocommit-offset 30m --min-retention 3M --mkdir
```

### Managing SmartLock directories

You can modify SmartLock directory settings, including the default, minimum, maximum retention period and the autocommit time period.

A SmartLock directory can be renamed only if the directory is empty.

### Modify a SmartLock directory

You can modify the SmartLock configuration settings for a SmartLock directory.

**Note**

You can modify SmartLock directory settings only 32 times per directory. It is recommended that you set SmartLock configuration settings only once and do not modify the settings after files are added to the SmartLock directory.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Modify SmartLock configuration settings by running the `isi worm modify` command.

The following command sets the default retention period to one year:

```
isi worm domains modify /ifs/data/SmartLock/directory1 \ 
  --default-retention 1Y
```

### View SmartLock directory settings

You can view the SmartLock directory settings for SmartLock directories.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the EMC Isilon cluster and log in.
2. View all SmartLock domains by running the following command:

```
isi worm domains list
```
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Path</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>65536</td>
<td>/ifs/data/SmartLock/directory1 enterprise</td>
<td>enterprise</td>
</tr>
<tr>
<td>65537</td>
<td>/ifs/data/SmartLock/directory2 enterprise</td>
<td>enterprise</td>
</tr>
<tr>
<td>65538</td>
<td>/ifs/data/SmartLock/directory3 enterprise</td>
<td>enterprise</td>
</tr>
</tbody>
</table>

3. (Optional) To view detailed information about a specific SmartLock directory, run the `isi worm domains view` command.

The following command displays detailed information about `/ifs/data/SmartLock/directory2`:

```
isi worm domains view /ifs/data/SmartLock/directory2
```

The system displays output similar to the following example:

```
ID: 65537
Path: /ifs/data/SmartLock/directory2
Type: enterprise
LIN: 4295426060
Autocommit Offset: 30m
Override Date: -
Privileged Delete: off
Default Retention: 1Y
  Min Retention: 3M
  Max Retention: -
Total Modifies: 3/32 Max
```

**SmartLock directory configuration settings**

You can configure SmartLock directory settings that determine when files are committed to and how long files are retained in a WORM state.

**ID**

The numerical ID of the corresponding SmartLock domain.

**Path**

The path of the directory.

**Type**

The type of SmartLock directory.

**LIN**

The inode number of the directory.

**Autocommit offset**

The autocommit time period for the directory. After a file exists in this SmartLock directory without being modified for the specified time period, the file is automatically committed to a WORM state.

Times are expressed in the format "<integer> <time>", where `<time>` is one of the following values:

- **Y**
  
  Specifies years
M
  Specifies months

W
  Specifies weeks

D
  Specifies days

H
  Specifies hours

m
  Specifies minutes

s
  Specifies seconds

Override date
  The override retention date for the directory. Files committed to a WORM state are not released from a WORM state until after the specified date, regardless of the maximum retention period for the directory or whether a user specifies an earlier date to release a file from a WORM state.

Privileged delete
  Indicates whether files committed to a WORM state in the directory can be deleted through the privileged delete functionality. To access the privilege delete functionality, you must either be assigned the ISI_PRIVIFS_WORM_DELETE privilege and own the file you are deleting. You can also access the privilege delete functionality for any file if you are logged in through the root or compadmin user account.

  on
    Files committed to a WORM state can be deleted through the isi worm files delete command.

  off
    Files committed to a WORM state cannot be deleted, even through the isi worm files delete command.

  disabled
    Files committed to a WORM state cannot be deleted, even through the isi worm files delete command. After this setting is applied, it cannot be modified.

Default retention period
  The default retention period for the directory. If a user does not specify a date to release a file from a WORM state, the default retention period is assigned. Times are expressed in the format "<integer> <time>", where <time> is one of the following values:

  Y
    Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours
m
  Specifies minutes
s
  Specifies seconds

*Forever* indicates that WORM committed files are retained permanently by default. Use *Min* indicates that the default retention period is equal to the minimum retention date. Use *Max* indicates that the default retention period is equal to the maximum retention date.

**Minimum retention period**

The minimum retention period for the directory. Files are retained in a WORM state for at least the specified amount of time, even if a user specifies an expiration date that results in a shorter retention period.

Times are expressed in the format "<integer> <time>"; where <time> is one of the following values:

Y
  Specifies years
M
  Specifies months
W
  Specifies weeks
D
  Specifies days
H
  Specifies hours
m
  Specifies minutes
s
  Specifies seconds

*Forever* indicates that all WORM committed files are retained permanently.
Maximum retention period

The maximum retention period for the directory. Files cannot be retained in a WORM state for more than the specified amount of time, even if a user specifies an expiration date that results in a longer retention period.

Times are expressed in the format "<integer> <time>", where <time> is one of the following values:

- Y
  - Specifies years
- M
  - Specifies months
- W
  - Specifies weeks
- D
  - Specifies days
- H
  - Specifies hours
- m
  - Specifies minutes
- s
  - Specifies seconds

_Forever_ indicates that there is no maximum retention period.

Managing files in SmartLock directories

You can commit files in SmartLock directories to a WORM state by removing the read-write privileges of the file. You can also set a specific date at which the retention period of the file expires. Once a file is committed to a WORM state, you can increase the retention period of the file, but you cannot decrease the retention period of the file. You cannot move a file that has been committed to a WORM state, even after the retention period for the file has expired.

The retention period expiration date is set by modifying the access time of a file. In a UNIX command line, the access time can be modified through the `touch` command. Although there is no method of modifying the access time through Windows Explorer, you can modify the access time through Windows Powershell. Accessing a file does not set the retention period expiration date.

If you run the `touch` command on a file in a SmartLock directory without specifying a date on which to release the file from a SmartLock state, and you commit the file, the retention period is automatically set to the default retention period specified for the SmartLock directory. If you have not specified a default retention period for the SmartLock directory, the file is assigned a retention period of zero seconds. It is recommended that you specify a minimum retention period for all SmartLock directories.
Set a retention period through a UNIX command line

You can specify when a file will be released from a WORM state through a UNIX command line.

Procedure

1. Open a connection to any node in the EMC Isilon cluster through a UNIX command line and log in.
2. Set the retention period by modifying the access time of the file through the `touch` command.

The following command sets an expiration date of June 1, 2015 for `/ifs/data/test.txt`:

```
touch -at 201506010000 /ifs/data/test.txt
```

Set a retention period through Windows Powershell

You can specify when a file will be released from a WORM state through Microsoft Windows Powershell.

Procedure

1. Open the Windows PowerShel command prompt.
2. (Optional) Establish a connection to the EMC Isilon cluster by running the `net use` command.

   The following command establishes a connection to the `/ifs` directory on `cluster.ip.address.com`:

   ```
   net use "\cluster.ip.address.com\ifs" /user:root password
   ```

3. Specify the name of the file you want to set a retention period for by creating an object.

   The file must exist in a SmartLock directory.

   The following command creates an object for `/smartlock/file.txt`:

   ```
   $file = Get-Item "\cluster.ip.address.com\ifs\smartlock\file.txt"
   ```

4. Specify the retention period by setting the last access time for the file.

   The following command sets an expiration date of July 1, 2015 at 1:00 PM:

   ```
   $file.LastAccessTime = Get-Date "2015/7/1 1:00 pm"
   ```

Commit a file to a WORM state through a UNIX command line

You can commit a file to a WORM state through a UNIX command line.

To commit a file to a WORM state, you must remove all write privileges from the file. If a file is already set to a read-only state, you must first add write privileges to the file, and then return the file to a read-only state.
Procedure

1. Open a connection to the EMC Isilon cluster through a UNIX command line interface and log in.

2. Remove write privileges from a file by running the `chmod` command.

   The following command removes write privileges of `/ifs/data/smartlock/file.txt`:

   ```sh
   chmod ugo-w /ifs/data/smartlock/file.txt
   ```

Commit a file to a WORM state through Windows Explorer

You can commit a file to a WORM state through Microsoft Windows Explorer. This procedure describes how to commit a file through Windows 7.

To commit a file to a WORM state, you must apply the read-only setting. If a file is already set to a read-only state, you must first remove the file from a read-only state and then return it to a read-only state.

Procedure

1. In Windows Explorer, navigate to the file you want to commit to a WORM state.

2. Right-click the folder and then click **Properties**.

3. In the **Properties** window, click the **General** tab.

4. Select the **Read-only** check box, and then click **OK**.

Override the retention period for all files in a SmartLock directory

You can override the retention period for files in a SmartLock directory. All files committed to a WORM state within the directory will remain in a WORM state until after the specified day.

If files are committed to a WORM state after the retention period is overridden, the override date functions as a minimum retention date. All files committed to a WORM state do not expire until at least the given day, regardless of user specifications.

Procedure

1. Open a secure shell (SSH) connection to any node in the EMC Isilon cluster and log in.

2. Override the retention period expiration date for all WORM committed files in a SmartLock directory by running the `isi worm modify` command.

   For example, the following command overrides the retention period expiration date of `/ifs/data/SmartLock/directory1` to June 1, 2014:

   ```sh
   isi worm domains modify /ifs/data/SmartLock/directory1 --override-date 2014-06-01
   ```
Delete a file committed to a WORM state

You can delete a WORM committed file before the expiration date through the privileged delete functionality. This procedure is available only through the command-line interface (CLI).

**Before you begin**

- Privileged delete functionality must not be permanently disabled for the SmartLock directory that contains the file.
- You must either be the owner of the file and have the ISI_PRIV_IFS_WORM_DELETE and ISI_PRIV_NS_IFS_ACCESS privileges, or be logged in through the root user account.

**Procedure**

1. Open a connection to the EMC Isilon cluster through a UNIX command line and log in.
2. If privileged delete functionality was disabled for the SmartLock directory, modify the directory by running the `isi worm domains modify` command with the `-privileged-delete` option.
   
   The following command enables privileged delete for `/ifs/data/SmartLock/directory1`:
   ```bash
   isi worm domains modify /ifs/data/SmartLock/directory1 \
   --privileged-delete true
   ```
3. Delete the WORM committed file by running the `isi worm files delete` command.
   
   The following command deletes `/ifs/data/SmartLock/directory1/file`:
   ```bash
   isi worm files delete /ifs/data/SmartLock/directory1/file
   ```
   
   The system displays output similar to the following:
   ```
   Are you sure? [yes, [no]]:
   ```
4. Type `yes` and then press ENTER.

View WORM status of a file

You can view the WORM status of an individual file. This procedure is available only through the command-line interface (CLI).

**Procedure**

1. Open a connection to the EMC Isilon cluster through a UNIX command line.
2. View the WORM status of a file by running the `isi worm files view` command.
   
   For example, the following command displays the WORM status of a file:
   ```bash
   isi worm files view /ifs/data/SmartLock/directory1/file
   ```
The system displays output similar to the following:

<table>
<thead>
<tr>
<th>ID</th>
<th>Root Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>65539</td>
<td>/ifs/data/SmartLock/directory1</td>
</tr>
</tbody>
</table>

WORM State: COMMITTED
Expires: 2015-06-01T00:00:00

SmartLock commands

You can control file retention through the WORM commands. WORM commands apply specifically to the SmartLock tool, and are available only if you have activated a SmartLock license on the cluster.

isi worm domains create

Creates a SmartLock directory.

Syntax

isi worm domains create <path>

|--compliance
|--autocommit-offset <duration>
|--override-date <timestamp>
|--privileged-delete {true | false}
|--default-retention {<duration> | forever | use_min | use_max}
|--min-retention {<duration> | forever}
|--max-retention <duration>
|--mkdir
|--force
|--verbose

Options

<path>

Creates a SmartLock directory at the specified path. Specify as a directory path.

|--compliance | -C

Specifies the SmartLock directory as a SmartLock compliance directory. This option is valid only on clusters running in SmartLock compliance mode.

|--autocommit-offset | -a <duration>

Specifies an autocommit time period. After a file exists in a SmartLock directory without being modified for the specified length of time, the file automatically committed to a WORM state. Specify <duration> in the following format:

<integer><units>

Specify <units> are valid:

Y

Specifies years

File retention with SmartLock

OneFS 8.0.0 CLI Administration Guide
Specifies months

W
Specifies weeks

D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds

To specify no autocommit time period, specify none. The default value is none.

{--override-date | -o} <timestamp>
Specifies an override retention date for the directory. Files committed to a
WORM state are not released from a WORM state until after the specified date,
regardless of the maximum retention period for the directory or whether a user
specifies an earlier date to release a file from a WORM state.
Specify <timestamp> in the following format:

<YYYY>-<MM>-<DD>[T<hh>:<mm>[:<ss>]]

{--privileged-delete | -p}{true | false}
Determines whether files in the directory can be deleted through the isi worm
files delete command. This option is available only for SmartLock enterprise
directories.
The default value is false.

--disable-privileged-delete
Permanently prevents WORM committed files from being deleted from the
SmartLock directory.

Note
If you specify this option, you can never enable the privileged delete functionality
for the directory. If a file is then committed to a WORM state in the directory,
you will not be able to delete the file until the retention period has passed.

{--default-retention | -d}{<duration> | forever | use_min | use_max}
Specifies a default retention period. If a user does not explicitly assign a retention
period expiration date, the default retention period is assigned to the file when it
is committed to a WORM state.
Specify `<duration>` in the following format:

```markdown
<integer><units>
```

Specify `<units>` are valid:

Y
  Specifies years

M
  Specifies months

W
  Specifies weeks

D
  Specifies days

H
  Specifies hours

m
  Specifies minutes

s
  Specifies seconds

To permanently retain WORM committed files by default, specify `forever`. To assign the minimum retention period as the default retention period, specify `use_min`. To assign the maximum retention period as the default retention period, specify `use_max`.

```ruby
{--min-retention | -m} {<duration> | forever}
```

Specifies a minimum retention period. Files are retained in a WORM state for at least the specified amount of time.

Specify `<duration>` in the following format:

```markdown
<integer><units>
```

Specify `<units>` as one of the following values:

Y
  Specifies years

M
  Specifies months

W
  Specifies weeks
D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds

To permanently retain all WORM committed files, specify \texttt{forever}.

{\texttt{--max-retention} \mid \texttt{-x}} {\texttt{<duration>}} \mid \texttt{forever}

Specifies a maximum retention period. Files cannot be retained in a WORM state for more than the specified amount of time, even if a user specifies an expiration date that results in a longer retention period.

Specify \texttt{<duration>} in the following format:

\begin{verbatim}
<integer><units>
\end{verbatim}

Specify \texttt{<units>} as one of the following values:

Y
Specifies years

M
Specifies months

W
Specifies weeks

D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds

To specify no maximum retention period, specify \texttt{forever}.

{\texttt{--mkdir} \mid \texttt{-M}}

Creates the specified directory if it does not already exist.

{\texttt{--force} \mid \texttt{-f}}
Does not prompt you to confirm the creation of the SmartLock directory.

```bash
|--verbose | -v
```
Displays more detailed information.

### isi worm domains modify

Modifies SmartLock settings of a SmartLock directory.

**Syntax**

```bash
isi worm domains modify <domain>
 [|--compliance | -C]
 [|--autocommit-offset <duration> | --clear-autocommit-offset]
 [|--override-date <timestamp> | --clear-override-date]
 [|--privileged-delete [true | false]]
 [|--default-retention [<duration> | forever | use_min | use_max] | --clear-default-retention]
 [|--min-retention [<duration> | forever] | --clear-min-retention]
 [|--max-retention <duration> | --clear-max-retention]
 [|--force]
 [|--verbose]
```

**Options**

**<domain>**

Modifies the specified SmartLock directory.

Specify as a directory path, ID, or LIN of a SmartLock directory.

**|--compliance | -C**

Specifies the SmartLock directory as a SmartLock compliance directory. This option is valid only on clusters running in SmartLock compliance mode.

**|--autocommit-offset | -a <duration>**

Specifies an autocommit time period. After a file exists in a SmartLock directory without being modified for the specified length of time, the file automatically committed to a WORM state.

Specify `<duration>` in the following format:

```bash
<integer><units>
```

Specify `<units>` are valid:

- `Y`
  - Specifies years

- `M`
  - Specifies months

- `W`
  - Specifies weeks
D
  Specifies days

H
  Specifies hours

m
  Specifies minutes

s
  Specifies seconds

To specify no autocommit time period, specify none. The default value is none.

--clear-autocommit-offset
  Removes the autocommit time period for the given SmartLock directory.

{--override-date | -o} <timestamp>
  Specifies an override retention date for the directory. Files committed to a
  WORM state are not released from a WORM state until after the specified date,
  regardless of the maximum retention period for the directory or whether a user
  specifies an earlier date to release a file from a WORM state.
  Specify <timestamp> in the following format:

  <YYYY>-<MM>-<DD>[T<hh>]<mm>[<ss>]]

--clear-override-date
  Removes the override retention date for the given SmartLock directory.

{--privileged-delete | -p} {true | false}
  Determines whether files in the directory can be deleted through the isi worm
  files delete command. This option is available only for SmartLock enterprise
  directories.
  The default value is false.

--disable-privileged-delete
  Permanently prevents WORM committed files from being deleted from the
  SmartLock directory.

Note
  If you specify this option, you can never enable the privileged delete functionality
  for the SmartLock directory. If a file is then committed to a WORM state in the
  directory, you will not be able to delete the file until the retention period
  expiration date has passed.

{--default-retention | -d} {<duration> | forever | use_min | use_max}
  Specifies a default retention period. If a user does not explicitly assign a retention
  period expiration date, the default retention period is assigned to the file when it
  is committed to a WORM state.
Specify `<duration>` in the following format:

```
<integer><units>
```

Specify `<units>` are valid:

- Y
  - Specifies years
- M
  - Specifies months
- W
  - Specifies weeks
- D
  - Specifies days
- H
  - Specifies hours
- m
  - Specifies minutes
- s
  - Specifies seconds

To permanently retain WORM committed files by default, specify `forever`. To assign the minimum retention period as the default retention period, specify `use_min`. To assign the maximum retention period as the default retention period, specify `use_max`.

```
--clear-default-retention
```

Removes the default retention period for the given SmartLock directory.

```
{--min-retention | -m} {<duration> | forever}
```

Specifies a minimum retention period. Files are retained in a WORM state for at least the specified amount of time.

Specify `<duration>` in the following format:

```
<integer><units>
```

Specify `<units>` as one of the following values:

- Y
  - Specifies years
- M
  - Specifies months
Specifies weeks

D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds

To permanently retain all WORM committed files, specify `forever`.

`--clear-min-retention`
Removes the minimum retention period for the given SmartLock directory.

 `{--max-retention | -x} \{<duration> | forever\}`
Specifies a maximum retention period. Files cannot be retained in a WORM state for more than the specified amount of time, even if a user specifies an expiration date that results in a longer retention period.

Specify `<duration>` in the following format:

 `<integer><units>`

Specify `<units>` as one of the following values:

Y
Specifies years

M
Specifies months

W
Specifies weeks

D
Specifies days

H
Specifies hours

m
Specifies minutes

s
Specifies seconds
To specify no maximum retention period, specify `forever`.

`--clear-max-retention`
Removes the maximum retention period for the given SmartLock directory.

`{--force | -f}`
Does not prompt you to confirm the creation of the SmartLock directory.

`{--verbose | -v}`
Displays more detailed information.

**isi worm domains list**
Displays a list of WORM directories.

**Syntax**

```
isi worm domains list
[--limit <integer>]
[--sort <attribute>]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

`{--limit | -l} <integer>`
Displays no more than the specified number of items.

`--sort <attribute>`
Sorts output displayed by the specified attribute.
The following values are valid:

- `id`
  Sorts output by the SmartLock directory ID.

- `path`
  Sorts output by the path of the SmartLock directory.

- `type`
  Sorts output based on whether the SmartLock directory is a compliance directory.

- `lin`
  Sorts output by the inode number of the SmartLock directory.

- `autocommit_offset`
  Sorts output by the autocommit time period of the SmartLock directory.

- `override_date`
  Sorts output by the override retention date of the SmartLock directory.

- `privileged_delete`
  Sorts output based on whether the privileged delete functionality is enabled for the SmartLock directory.
default_retention
Sorts output by the default retention period of the SmartLock directory.

min_retention
Sorts output by the minimum retention period of the SmartLock directory.

max_retention
Sorts output by the maximum retention period of the SmartLock directory.

total_modifies
Sorts output by the total number of times that the SmartLock directory has been modified.

{--descending | -d}
Displays output in reverse order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table output without headers.

{--no-footer | -z}
Displays table output without footers. Footers display snapshot totals, such as the total amount of storage space consumed by snapshots.

{--verbose | -v}
Displays more detailed information.

**isi worm domains view**
Displays WORM information about a specific directory or file.

**Syntax**

```bash
isi worm domains view <domain>
```

**Options**

<domain>
Displays information about the specified SmartLock directory.
Specify as a directory path, ID, or LIN of a SmartLock directory.

**isi worm cdate set**
Sets the SmartLock compliance clock to the current time on the system clock.

⚠️ **CAUTION**
You can set the compliance clock only once. After the compliance clock has been set, you cannot modify the compliance clock time.
Syntax

isi worm cdate set

Options
There are no options for this command.

**isi worm cdate view**

Displays whether or not the SmartLock compliance clock is set. If the compliance clock is set, displays the current time on the compliance clock.

Syntax

isi worm cdate view

Options
There are no options for this command.

**isi worm files delete**

Deletes a file committed to a WORM state. This command can be run only by the root user or compliance administrator.

Syntax

isi worm files delete <path>
    [--force]
    [--verbose]

Options

<path>
    Deletes the specified file. The file must exist in a SmartLock enterprise directory with the privileged delete functionality enabled.
    Specify as a file path.

--force
    Does not prompt you to confirm that you want to delete the file.

--verbose
    Displays more detailed information.

**isi worm files view**

Displays information about a file committed to a WORM state.

Syntax

isi worm files view <path>
    [--no-symlinks]
Options

<path>
Displays information about the specified file. The file must be committed to a WORM state.
Specify as a file path.

--no-symlinks
If <path> refers to a file, and the given file is a symbolic link, displays WORM information about the symbolic link. If this option is not specified, and the file is a symbolic link, displays WORM information about the file that the symbolic link refers to.
File retention with SmartLock
CHAPTER 20

Protection domains

This section contains the following topics:

- Protection domains overview ................................................................. 804
- Protection domain considerations .......................................................... 804
- Create a protection domain ................................................................... 805
- Delete a protection domain .................................................................... 805
Protection domains overview

Protection domains are markers that prevent modifications to files and directories. If a domain is applied to a directory, the domain is also applied to all of the files and subdirectories under the directory. You can specify domains manually; however, OneFS usually creates domains automatically.

There are three types of domains: SyncIQ domains, SmartLock domains, and SnapRevert domains. SyncIQ domains can be assigned to source and target directories of replication policies. OneFS automatically creates a SyncIQ domain for the target directory of a replication policy the first time that the policy is run. OneFS also automatically creates a SyncIQ domain for the source directory of a replication policy during the failback process. You can manually create a SyncIQ domain for a source directory before you initiate the failback process by configuring the policy for accelerated failback, but you cannot delete a SyncIQ domain that marks the target directory of a replication policy.

SmartLock domains are assigned to SmartLock directories to prevent committed files from being modified or deleted. OneFS automatically creates a SmartLock domain when a SmartLock directory is created. You cannot delete a SmartLock domain. However, if you delete a SmartLock directory, OneFS automatically deletes the SmartLock domain associated with the directory.

SnapRevert domains are assigned to directories that are contained in snapshots to prevent files and directories from being modified while a snapshot is being reverted. OneFS does not automatically create SnapRevert domains. You cannot revert a snapshot until you create a SnapRevert domain for the directory that the snapshot contains. You can create SnapRevert domains for subdirectories of directories that already have SnapRevert domains. For example, you could create SnapRevert domains for both /ifs/data and /ifs/data/archive. You can delete a SnapRevert domain if you no longer want to revert snapshots of a directory.

Protection domains for IsilonSD Edge

With a purchased license of IsilonSD Edge, you can access the SyncIQ and SmartLock protection domains.

Protection domain considerations

You can manually create protection domains before they are required by OneFS to perform certain actions. However, manually creating protection domains can limit your ability to interact with the data marked by the domain.

- Copying a large number of files into a protection domain might take a very long time because each file must be marked individually as belonging to the protection domain.

- You cannot move directories in or out of protection domains. However, you can move a directory contained in a protection domain to another location within the same protection domain.

- Creating a protection domain for a directory that contains a large number of files will take more time than creating a protection domain for a directory with fewer files. Because of this, it is recommended that you create protection domains for directories while the directories are empty, and then add files to the directory.
If a domain is currently preventing the modification or deletion of a file, you cannot create a protection domain for a directory that contains that file. For example, if `/ifs/data/smartlock/file.txt` is set to a WORM state by a SmartLock domain, you cannot create a SnapRevert domain for `/ifs/data/`.

---

**Note**

If you use SyncIQ to create a replication policy for a SmartLock compliance directory, the SyncIQ and SmartLock compliance domains must be configured at the same root directory level. A SmartLock compliance domain cannot be nested inside a SyncIQ domain.

---

**Create a protection domain**

You can create replication or snapshot revert domains to facilitate snapshot revert and failover operations. You cannot create a SmartLock domain. OneFS automatically creates a SmartLock domain when you create a SmartLock directory.

**Procedure**

1. Run the `isi job jobs start` command.

   The following command creates a SyncIQ domain for `/ifs/data/source`:

   ```
   isi job jobs start domainmark --root /ifs/data/media \
   --dm-type SyncIQ
   ```

---

**Delete a protection domain**

You can delete a replication or snapshot revert domain if you want to move directories out of the domain. You cannot delete a SmartLock domain. OneFS automatically deletes a SmartLock domain when you delete a SmartLock directory.

**Procedure**

1. Run the `isi job jobs start` command.

   The following command deletes a SyncIQ domain for `/ifs/data/source`:

   ```
   isi job jobs start domainmark --root /ifs/data/media \
   --dm-type SyncIQ --delete
   ```
Protection domains
CHAPTER 21
Data-at-rest-encryption

This section contains the following topics:

- Data-at-rest encryption overview ................................................................. 808
- Self-encrypting drives .................................................................................. 808
- Data security on self-encrypted drives .......................................................... 808
- Data migration to a cluster with self-encrypted drives ................................. 809
- Chassis and drive states ............................................................................... 809
- Smartfailed drive REPLACE state ................................................................. 813
- Smartfailed drive ERASE state ................................................................. 814
Data-at-rest encryption overview

You can enhance data security with a EMC Isilon cluster that contains only self-encrypting-drive nodes, providing data-at-rest protection.

The OneFS system is available as a cluster that is composed of Isilon OneFS nodes that contain only self-encrypting drives (SEDs). The system requirements and management of data at rest on self-encrypting nodes are identical to that of nodes that do not contain self-encrypting drives. Clusters of mixed node types are not supported.

Data-at-rest encryption for IsilonSD Edge

IsilonSD Edge does not support data-at-rest encryption because the IsilonSD nodes do not support the self-encrypting drive type.

Self-encrypting drives

Self-encrypting drives store data on a EMC Isilon cluster that is specially designed for data-at-rest encryption.

Data-at-rest- encryption on self-encrypted drives occurs when data that is stored on a device is encrypted to prevent unauthorized data access. All data written to the storage device is encrypted when it is stored, and all data read from the storage device is decrypted when it is read. The stored data is encrypted with a 256-bit data AES encryption key and decrypted in the same manner. OneFS controls data access by combining the drive authentication key with on-disk data-encryption keys.

Note

All nodes in a cluster must be of the self-encrypting drive type. Mixed nodes are not supported.

Data security on self-encrypted drives

Smartfailing self-encrypted drives guarantees data security after removal.

Data on self-encrypted drives is protected from unauthorized access by authenticating encryption keys. Encryption keys never leave the drive. When a drive is locked, successful authentication unlocks the drive for data access.

The data on self-encrypted drives is rendered inaccessible in the following conditions:

- When a self-encrypting drive is smartfailed, drive authentication keys are deleted from the node. The data on the drive cannot be decrypted and is therefore unreadable, which secures the drive.
- When a drive is smartfailed and removed from a node, the encryption key on the drive is removed. Because the encryption key for reading data from the drive must be the same key that was used when the data was written, it is impossible to decrypt data that was previously written to the drive. When you smartfail and then remove a drive, it is cryptographically erased.
Note
Smartfailing a drive is the preferred method for removing a self-encrypted drive. Removing a node that has been smartfailed guarantees that data is inaccessible.

- When a self-encrypting drive loses power, the drive locks to prevent unauthorized access. When power is restored, data is again accessible when the appropriate drive authentication key is provided.

Data migration to a cluster with self-encrypted drives

You can have data from your existing cluster migrated to a cluster of nodes made up of self-encrypted drives (SEDs). As a result, all migrated and future data on the new cluster will be encrypted.

Note
Data migration to a cluster with SEDs must be performed by Isilon Professional Services. For more information, contact your EMC Isilon representative.

Chassis and drive states

You can view chassis and drive state details.

In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work. A cluster can lose write quorum but keep read quorum. OneFS provides details about the status of chassis and drives in your cluster. The following table describes all the possible states that you may encounter in your cluster.

Note
If you are running IsilonSD Edge, you can view and manage the chassis and drive state details through the IsilonSD Management Plug-in. For more information, see the IsilonSD Edge Installation and Administration Guide.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHY</td>
<td>All drives in the node are functioning correctly.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td>A solid state drive (SSD) was deployed as level 3 (L3) cache to increase the size of cache memory and improve throughput speeds.</td>
<td>Command-line interface</td>
<td></td>
</tr>
<tr>
<td>SMARTFAIL or Smartfail or restripe in progress</td>
<td>The drive is in the process of being removed safely from the file system, either because of an I/O</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>error or by user request. Nodes or drives in a smartfail or read-only state affect only write quorum.</td>
<td>Command-line interface, web administration interface</td>
<td>X</td>
</tr>
<tr>
<td>NOT AVAILABLE</td>
<td>A drive is unavailable for a variety of reasons. You can click the bay to view detailed information about this condition.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state includes the <code>ERASE</code> and <code>SED_ERROR</code> command-line interface states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSPENDED</td>
<td>This state indicates that drive activity is temporarily suspended and the drive is not in use. The state is manually initiated and does not occur during normal cluster activity.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>NOT IN USE</td>
<td>A node in an offline state affects both read and write quorum.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>REPLACE</td>
<td>The drive was smartfailed successfully and is ready to be replaced.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>STALLED</td>
<td>The drive is stalled and undergoing stall evaluation. Stall evaluation is the process of checking drives that are slow or having other issues. Depending on the outcome of the evaluation, the drive may return to service or be smartfailed. This is a transient state.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NEW</td>
<td>The drive is new and blank. This is the state that a drive is in when you run the <code>isi dev</code> command with the <code>-a add</code> option.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>USED</td>
<td>The drive was added and contained an Isilon GUID but the drive is not from this node. This drive likely will be formatted into the cluster.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>PREPARING</td>
<td>The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>EMPTY</td>
<td>No drive is in this bay.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>WRONG_TYPE</td>
<td>The drive type is wrong for this node. For example, a non-SED drive in a SED node, SAS instead of the expected SATA drive type.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>BOOT_DRIVE</td>
<td>Unique to the A100 drive, which has boot drives in its bays.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>SED_ERROR</td>
<td>The drive cannot be acknowledged by the OneFS system.</td>
<td>Command-line interface only</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state is included in Not available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERASE</td>
<td>The drive is ready for removal but needs your attention because the data has not been erased. You can erase the drive</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Insecure</td>
<td>Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td>Command-line interface only</td>
<td>X</td>
</tr>
<tr>
<td>Unencrypted SED</td>
<td>Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td>Web administration interface only</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: In the web administration interface, this state is labeled **Unencrypted SED**.

Note: In the command-line interface, this state is labeled **INSECURE**.
Smartfailed drive REPLACE state

You can see different drive states during the smartfail process.

If you run the `isi dev` command while the drive in bay 1 is being smartfailed, the system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Node 1, [ATTN]</th>
<th>Bay 1</th>
<th>Lnum 11</th>
<th>SMARTFAIL</th>
<th>SN:Z296M8HK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 2</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8N5</td>
</tr>
<tr>
<td>Bay 3</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296LB5P4</td>
</tr>
<tr>
<td>Bay 4</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296LCJW</td>
</tr>
<tr>
<td>Bay 5</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296MBX</td>
</tr>
<tr>
<td>Bay 6</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z295LXT7</td>
</tr>
<tr>
<td>Bay 7</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8Z7</td>
</tr>
<tr>
<td>Bay 8</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8SQ</td>
</tr>
<tr>
<td>Bay 9</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8BA</td>
</tr>
<tr>
<td>Bay 10</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8Q7</td>
</tr>
<tr>
<td>Bay 11</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8SP</td>
</tr>
<tr>
<td>Bay 12</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8QZ</td>
</tr>
<tr>
<td>Bay 12</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8QZ</td>
</tr>
</tbody>
</table>

If you run the `isi dev` command after the smartfail completes successfully, the system displays output similar to the following example, showing the drive state as REPLACE:

<table>
<thead>
<tr>
<th>Node 1, [ATTN]</th>
<th>Bay 1</th>
<th>Lnum 11</th>
<th>REPLACE</th>
<th>SN:Z296M8HK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 2</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8N5</td>
</tr>
<tr>
<td>Bay 3</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296LB5P4</td>
</tr>
<tr>
<td>Bay 4</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296LCJW</td>
</tr>
<tr>
<td>Bay 5</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296MBX</td>
</tr>
<tr>
<td>Bay 6</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z295LXT7</td>
</tr>
<tr>
<td>Bay 7</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8Z7</td>
</tr>
<tr>
<td>Bay 8</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8SQ</td>
</tr>
<tr>
<td>Bay 9</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8BA</td>
</tr>
<tr>
<td>Bay 10</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8Q7</td>
</tr>
<tr>
<td>Bay 11</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8SP</td>
</tr>
<tr>
<td>Bay 12</td>
<td></td>
<td></td>
<td>HEALTHY</td>
<td>SN:Z296M8QZ</td>
</tr>
</tbody>
</table>
If you run the `isi dev` command while the drive in bay 3 is being smartfailed, the system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Node 1, [ATTN]</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td>Inum 11</td>
<td>[REPLACE]</td>
<td>SN:Z296M8HK</td>
<td></td>
</tr>
<tr>
<td>000093172EY04</td>
<td>/dev/da1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 2</td>
<td>Inum 10</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8N5</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 3</td>
<td>Inum 9</td>
<td>[SMARTFAIL]</td>
<td>SN:Z296LBP4</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 4</td>
<td>Inum 8</td>
<td>[HEALTHY]</td>
<td>SN:Z296LCJW</td>
<td></td>
</tr>
<tr>
<td>00009327BYE03</td>
<td>/dev/da4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 5</td>
<td>Inum 7</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8XB</td>
<td></td>
</tr>
<tr>
<td>00009330KYE03</td>
<td>/dev/da5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 6</td>
<td>Inum 6</td>
<td>[HEALTHY]</td>
<td>SN:Z295LXT7</td>
<td></td>
</tr>
<tr>
<td>000093172EY04</td>
<td>/dev/da6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 7</td>
<td>Inum 5</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8ZF</td>
<td></td>
</tr>
<tr>
<td>00009330KYE03</td>
<td>/dev/da7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 8</td>
<td>Inum 4</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8SD</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 9</td>
<td>Inum 3</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8QA</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 10</td>
<td>Inum 2</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8Q7</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 11</td>
<td>Inum 1</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8SP</td>
<td></td>
</tr>
<tr>
<td>00009330EYE04</td>
<td>/dev/da11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 12</td>
<td>Inum 0</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8QZ</td>
<td></td>
</tr>
<tr>
<td>00009330JYE03</td>
<td>/dev/da12</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Smartfailed drive ERASE state

At the end of a smartfail process, OneFS attempts to delete the authentication key on a drive if it is unable to reset the key.

**Note**

- To securely delete the authentication key on a single drive, smartfail the individual drive.
- To securely delete the authentication key on a single node, smartfail the node.
- To securely delete the authentication keys on an entire cluster, smartfail each node and run the `isi_reformat_node` command on the last node.

Upon running the `isi dev` command, the system displays output similar to the following example, showing the drive state as ERASE:

<table>
<thead>
<tr>
<th>Node 1, [ATTN]</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td>Inum 11</td>
<td>[REPLACE]</td>
<td>SN:Z296M8HK</td>
<td></td>
</tr>
<tr>
<td>000093172EY04</td>
<td>/dev/da1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 2</td>
<td>Inum 10</td>
<td>[HEALTHY]</td>
<td>SN:Z296M8N5</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay 3</td>
<td>Inum 9</td>
<td>[ERASE]</td>
<td>SN:Z296LBP4</td>
<td></td>
</tr>
<tr>
<td>00009330EYE03</td>
<td>/dev/da3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Drives showing the ERASE state can be safely retired, reused, or returned.

Any further access to a drive showing the ERASE state requires the authentication key of the drive to be set to its default manufactured security ID (MSID). This action erases the data encryption key (DEK) on the drive and renders any existing data on the drive permanently unreadable.
CHAPTER 22
SmartQuotas

This section contains the following topics:

- SmartQuotas overview ................................................................. 816
- Quota types .............................................................................. 816
- Default quota type ................................................................. 817
- Usage accounting and limits ................................................ 819
- Disk-usage calculations ......................................................... 820
- Quota notifications ................................................................. 821
- Quota notification rules ......................................................... 822
- Quota reports .......................................................................... 822
- Creating quotas ..................................................................... 823
- Managing quotas ................................................................. 824
- Quota commands ................................................................. 838
SmartQuotas overview

The SmartQuotas module is an optional quota-management tool that monitors and enforces administrator-defined storage limits. Using accounting and enforcement quota limits, reporting capabilities, and automated notifications, SmartQuotas manages storage use, monitors disk storage, and issues alerts when disk-storage limits are exceeded.

Quotas help you manage storage usage according to criteria that you define. Quotas are used for tracking—and sometimes limiting—the amount of storage that a user, group, or project consumes. Quotas help ensure that a user or department does not infringe on the storage that is allocated to other users or departments. In some quota implementations, writes beyond the defined space are denied, and in other cases, a simple notification is sent.

**Note**

Do not apply quotas to `/ifs/.ifsvar/` or its subdirectories. If you limit the size of the `/ifs/.ifsvar/` directory through a quota, and the directory reaches its limit, jobs such as File-System Analytics fail. A quota blocks older job reports from being deleted from the `/ifs/.ifsvar/` subdirectories to make room for newer reports.

The SmartQuotas module requires a separate license. For more information about the SmartQuotas module or to activate the module, contact your EMC Isilon sales representative.

Quota types

OneFS uses the concept of quota types as the fundamental organizational unit of storage quotas. Storage quotas comprise a set of resources and an accounting of each resource type for that set. Storage quotas are also called storage domains.

Storage quotas creation requires three identifiers:

- The directory to monitor
- Whether snapshots are tracked against the quota limit
- The quota type (directory, user, or group)

**Note**

Do not create quotas of any type on the OneFS root (`/ifs`). A root-level quota may significantly degrade performance.

You can choose a quota type from the following entities:

- **Directory**
  A specific directory and its subdirectories.

- **User**
  Either a specific user or default user (every user). Specific-user quotas that you configure take precedence over a default user quota.

- **Group**
  All members of a specific group or all members of a default group (every group). Any specific-group quotas that you configure take precedence over a default
group quota. Associating a group quota with a default group quota creates a linked quota.

You can create multiple quota types on the same directory, but they must be of a different type or have a different snapshot option. You can specify quota types for any directory in OneFS and nest them within each other to create a hierarchy of complex storage-use policies.

Nested storage quotas can overlap. For example, the following quota settings ensure that the finance directory never exceeds 5 TB, while limiting the users in the finance department to 1 TB each:

- Set a 5 TB hard quota on /ifs/data/finance.
- Set 1 TB soft quotas on each user in the finance department.

**Default quota type**

Default quotas automatically create other quotas for users or groups in a specified directory.

A default quota specifies a policy for new entities that match a trigger. The default-user@/ifs/cs becomes specific-user@/ifs/cs for each specific-user that is not otherwise defined.

For example, you can create a default-user quota on the /ifs/dir-1 directory, where that directory is owned by the root user. The default-user type automatically creates a domain on that directory for root and adds the usage there:

```
my-OneFS-1# mkdir /ifs/dir-1
my-OneFS-1# isi quota quotas create /ifs/dir-1 default-user
my-OneFS-1# isi quota quotas ls --path=/ifs/dir-1

<table>
<thead>
<tr>
<th>Type</th>
<th>AppliesTo</th>
<th>Path</th>
<th>Snap</th>
<th>Hard</th>
<th>Soft</th>
<th>Adv</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-user</td>
<td>DEFAULT</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
<tr>
<td>user</td>
<td>root</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
</tbody>
</table>
```

Now add a file owned by a different user (admin):

```
my-OneFS-1# touch /ifs/dir-1/somefile
my-OneFS-1# chown admin /ifs/dir-1/somefile
my-OneFS-1# isi quota quotas ls --path=/ifs/dir-1

<table>
<thead>
<tr>
<th>Type</th>
<th>AppliesTo</th>
<th>Path</th>
<th>Snap</th>
<th>Hard</th>
<th>Soft</th>
<th>Adv</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-user</td>
<td>DEFAULT</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
<tr>
<td>user</td>
<td>root</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>26b</td>
</tr>
<tr>
<td>user</td>
<td>admin</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
</tbody>
</table>
```

In this example, the default-user type created a specific-user type automatically (user:admin) and added the new usage to it. Default-user does not have any usage because it is used only to generate new quotas automatically. Default-user enforcement is copied to a specific-user (user:admin), and the inherited quota is called a linked quota. In this way, each user account gets its own usage accounting.

Defaults can overlap. For example, default-user@/ifs/dir-1 and default-user@/ifs/cs both may be defined. If the default enforcement changes, OneFS storage quotas propagate the changes to the linked quotas asynchronously. Because the update is
asynchronous, there is some delay before updates are in effect. If a default type, such as every user or every group, is deleted, OneFS deletes all children that are marked as inherited. As an option, you can delete the default without deleting the children, but it is important to note that this action breaks inheritance on all inherited children.

Continuing with the example, add another file owned by the root user. Because the root type exists, the new usage is added to it.

```
my-OneFS-1# touch /ifs/dir-1/anotherfile
my-OneFS-1# isi quota ls -v --path=/ifs/dir-1 --format=list
  Type: default-user
  AppliesTo: DEFAULT
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 0
    With Overhead : 0.00b
    W/O Overhead : 0.00b
    Over: -
    Enforced: No
    Container: No
    Linked: -

  --
  Type: user
  AppliesTo: root
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 2
    With Overhead : 3.50K
    W/O Overhead : 55.00b
    Over: -
    Enforced: No
    Container: No
    Linked: Yes

  ---
  Type: user
  AppliesTo: admin
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 1
    With Overhead : 1.50K
    W/O Overhead : 0.00b
    Over: -
    Enforced: No
    Container: No
    Linked: Yes
```
The enforcement on default-user is copied to the specific-user when the specific-user allocates within the type, and the new inherited quota type is also a linked quota.

Note

Configuration changes for linked quotas must be made on the parent quota that the linked quota is inheriting from. Changes to the parent quota are propagated to all children. To override configuration from the parent quota, unlink the quota first.

Usage accounting and limits

Storage quotas support two usage types that you can create to manage storage space: usage accounting and enforcement limits.

You can configure OneFS quotas by usage type to track or limit storage use. The accounting option, which monitors disk-storage use, is useful for auditing, planning, and billing. Enforcement limits set storage limits for users, groups, or directories.

Accounting

The accounting option tracks but does not limit disk-storage use. Using the accounting option for a quota, you can monitor inode count and physical and logical space resources. Physical space refers to all of the space used to store files and directories, including data and metadata in the domain. Logical space refers to the sum of all files sizes, excluding file metadata and sparse regions. User data storage is tracked using logical-space calculations, which do not include protection overhead. As an example, by using the accounting option, you can do the following:

- Track the amount of disk space used by various users or groups to bill each user, group, or directory for only the disk space used.
- Review and analyze reports that help you identify storage usage patterns and define storage policies.
- Plan for capacity and other storage needs.

Enforcement limits

Enforcement limits include all of the functionality of the accounting option, plus the ability to limit disk storage and send notifications. Using enforcement limits, you can logically partition a cluster to control or restrict how much storage that a user, group, or directory can use. For example, you can set hard- or soft-capacity limits to ensure that adequate space is always available for key projects and critical applications and to ensure that users of the cluster do not exceed their allotted storage capacity. Optionally, you can deliver real-time email quota notifications to users, group managers, or administrators when they are approaching or have exceeded a quota limit.

Note

If a quota type uses the accounting-only option, enforcement limits cannot be used for that quota.

The actions of an administrator logged in as root may push a domain over a quota threshold. For example, changing the protection level or taking a snapshot has the potential to exceed quota parameters. System actions such as repairs also may push a quota domain over the limit.

The system provides three types of administrator-defined enforcement thresholds.
<table>
<thead>
<tr>
<th>Threshold type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Hard          | Limits disk usage to a size that cannot be exceeded. If an operation, such as a file write, causes a quota target to exceed a hard quota, the following events occur:  
  - the operation fails  
  - an alert is logged to the cluster  
  - a notification is issued to specified recipients.  
  Writes resume when the usage falls below the threshold. |
| Soft          | Allows a limit with a grace period that can be exceeded until the grace period expires. When a soft quota is exceeded, an alert is logged to the cluster and a notification is issued to specified recipients; however, data writes are permitted during the grace period.  
  If the soft threshold is still exceeded when the grace period expires, data writes fail, and a hard-limit notification is issued to the recipients you have specified.  
  Writes resume when the usage falls below the threshold. |
| Advisory      | An informational limit that can be exceeded. When an advisory quota threshold is exceeded, an alert is logged to the cluster and a notification is issued to specified recipients. Advisory thresholds do not prevent data writes. |

**Disk-usage calculations**

For each quota that you configure, you can specify whether data protection overhead is included in future disk usage calculations.

Most quota configurations do not need to include overhead calculations. If you do not include data protection overhead in usage calculations for a quota, future disk usage calculations for the quota include only the space that is required to store files and directories. Space that is required for the data protection setting of the cluster is not included.

Consider the same example user, who is now restricted by a 40 GB quota that does not include data protection overhead in its disk usage calculations. If your cluster is configured with a 2x data protection level and the user writes a 10 GB file to the cluster, that file consumes 20 GB of space but the 10GB for the data protection overhead is not counted in the quota calculation. In this example, the user has reached 25 percent of the 40 GB quota by writing a 10 GB file to the cluster. This method of disk usage calculation is recommended for most quota configurations.

If you include data protection overhead in usage calculations for a quota, future disk usage calculations for the quota include the total amount of space that is required to
store files and directories, in addition to any space that is required to accommodate your data protection settings, such as parity or mirroring. For example, consider a user who is restricted by a 40 GB quota that includes data protection overhead in its disk usage calculations. If your cluster is configured with a 2x data protection level (mirrored) and the user writes a 10 GB file to the cluster, that file actually consumes 20 GB of space: 10 GB for the file and 10 GB for the data protection overhead. In this example, the user has reached 50 percent of the 40 GB quota by writing a 10 GB file to the cluster.

**Note**

Cloned and deduplicated files are treated as ordinary files by quotas. If the quota includes data protection overhead, the data protection overhead for shared data is not included in the usage calculation.

You can configure quotas to include the space that is consumed by snapshots. A single path can have two quotas applied to it: one without snapshot usage, which is the default, and one with snapshot usage. If you include snapshots in the quota, more files are included in the calculation than are in the current directory. The actual disk usage is the sum of the current directory and any snapshots of that directory. You can see which snapshots are included in the calculation by examining the `.snapshot` directory for the quota path.

**Note**

Only snapshots created after the QuotaScan job finishes are included in the calculation.

### Quota notifications

Quota notifications are generated for enforcement quotas, providing users with information when a quota violation occurs. Reminders are sent periodically while the condition persists.

Each notification rule defines the condition that is to be enforced and the action that is to be executed when the condition is true. An enforcement quota can define multiple notification rules. When thresholds are exceeded, automatic email notifications can be sent to specified users, or you can monitor notifications as system alerts or receive emails for these events.

Notifications can be configured globally, to apply to all quota domains, or be configured for specific quota domains.

Enforcement quotas support the following notification settings. A given quota can use only one of these settings.

<table>
<thead>
<tr>
<th>Limit notification settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn Off Notifications for this Quota</td>
<td>Disables all notifications for the quota.</td>
</tr>
<tr>
<td>Use Default Notification Rules</td>
<td>Uses the global default notification for the specified type of quota.</td>
</tr>
<tr>
<td>Use Custom Notification Rules</td>
<td>Enables the creation of advanced, custom notifications that apply to the specific quota. Custom notifications can be configured for</td>
</tr>
</tbody>
</table>
Quota notification rules

You can write quota notification rules to generate alerts that are triggered by event thresholds.

When an event occurs, a notification is triggered according to your notification rule. For example, you can create a notification rule that sends an email when a disk-space allocation threshold is exceeded by a group.

You can configure notification rules to trigger an action according to event thresholds (a notification condition). A rule can specify a schedule, such as "every day at 1:00 AM," for executing an action or immediate notification of certain state transitions. When an event occurs, a notification trigger may execute one or more actions, such as sending an email or sending a cluster alert to the interface. The following examples demonstrate the types of criteria that you can use to configure notification rules.

- Notify when a threshold is exceeded; at most, once every 5 minutes
- Notify when allocation is denied; at most, once an hour
- Notify while over threshold, daily at 2 AM
- Notify while grace period expired weekly, on Sundays at 2 AM

Notifications are triggered for events grouped by the following categories:

**Instant notifications**

Includes the write-denied notification, triggered when a hard threshold denies a write, and the threshold-exceeded notification, triggered at the moment a hard, soft, or advisory threshold is exceeded. These are one-time notifications because they represent a discrete event in time.

**Ongoing notifications**

Generated on a scheduled basis to indicate a persisting condition, such as a hard, soft, or advisory threshold being over a limit or a soft threshold's grace period being expired for a prolonged period.

Quota reports

The OneFS SmartQuotas module provides reporting options that enable administrators to manage cluster resources and analyze usage statistics.

Storage quota reports provide a summarized view of the past or present state of the quota domains. After raw reporting data is collected by OneFS, you can produce data summaries by using a set of filtering parameters and sort types. Storage-quota reports include information about violators, grouped by threshold types. You can generate reports from a historical data sample or from current data. In either case, the reports are views of usage data at a given time. OneFS does not provide reports on data aggregated over time, such as trending reports, but you can use raw data to analyze trends. There is no configuration limit on the number of reports other than the space needed to store them.

OneFS provides the following data-collection and reporting methods:
Scheduled reports are generated and saved on a regular interval.

- Ad hoc reports are generated and saved at the request of the user.
- Live reports are generated for immediate and temporary viewing.

Scheduled reports are placed by default in the $/ifs/.isilon/smartquotas/reports$ directory, but the location is configurable to any directory under $/ifs$. Each generated report includes quota domain definition, state, usage, and global configuration settings. By default, ten reports are kept at a time, and older reports are purged. You can create ad hoc reports at any time to view the current state of the storage quotas system. These live reports can be saved manually. Ad hoc reports are saved to a location that is separate from scheduled reports to avoid skewing the timed-report sets.

Creating quotas

You can create two types of storage quotas to monitor data: accounting quotas and enforcement quotas. Storage quota limits and restrictions can apply to specific users, groups, or directories.

The type of quota that you create depends on your goal.

- **Enforcement quotas** monitor and limit disk usage. You can create enforcement quotas that use any combination of hard limits, soft limits, and advisory limits.

  **Note**

  Enforcement quotas are not recommended for snapshot-tracking quota domains.

- **Accounting quotas** monitor, but do not limit, disk usage.

  **Note**

  Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are running.

Create an accounting quota

You can create an accounting quota to monitor but not limit disk usage.

Optionally, you can include snapshot data, data-protection overhead, or both in the accounting quota.

For information about the parameters and options that you can use for this procedure, run the `isi quota quotas create --help` command.

**Procedure**

1. Run the `isi quota quotas create` command to create an accounting quota.

   The following command creates a quota for the `/quota_test_1` directory. The quota sets an advisory threshold that is informative rather than enforced.

   ```
   isi quota quotas create /ifs/data/quota_test_1 directory \ 
   --advisory-threshold=10M --enforced=false
   ```
After you finish

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by running the `isi job events list --job-type quotascan` command.

Create an enforcement quota

You can create an enforcement quota to monitor and limit disk usage.

You can create enforcement quotas that set hard, soft, and advisory limits.

For information about the parameters and options that you can use for this procedure, run the `isi quota quotas create --help` command.

Procedure

1. Run the `isi quota quotas create` command and set the `--enforced` parameter to `true`.

   The following command creates a quota for the `/ifs/data/quota_test_2` directory. The quota sets an advisory threshold that is enforced when the threshold specified is exceeded.

   ```
   isi quota quotas create /ifs/data/quota_test_2 directory \
   --advisory-threshold=100M --enforced=true
   ```

After you finish

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by running the `isi job events list --job-type quotascan` command.

Managing quotas

You can modify the configured values of a storage quota, and you can enable or disable a quota. You can also create quota limits and restrictions that apply to specific users, groups, or directories.

Quota management in OneFS is simplified by the quota search feature, which helps you locate a quota or quotas by using filters. You can unlink quotas that are associated with a parent quota, and configure custom notifications for quotas. You can also disable a quota temporarily and then enable it when needed.

Note

Moving quota directories across quota domains is not supported.

Search for quotas

You can search for a quota using a variety of search parameters.

For information about the parameters and options that you can use for this procedure, run the `isi quota quotas list --help` command.

Procedure

1. Run the `isi quota quotas list` command to search for quotas.
The following command finds all quotas that monitor the /ifs/data/quotas_test_1 directory:

```bash
isi quota quotas list --path=/ifs/data/quotas_test_1
```

## Manage quotas

Quotas help you monitor and analyze the current or historic use of disk storage. You can search for quotas, and modify, delete, and unlink quotas.

You must run an initial QuotaScan job for the default or scheduled quotas to prevent displaying incomplete data.

Before you modify a quota, consider how the changes will affect the file system and end users.

For information about the parameters and options that you can use for this procedure, run the `isi quota quotas list --help` command.

### Note

- You can edit or delete a quota report only when the quota is not linked to a default quota.
- You can unlink a quota only when the quota is linked to a default quota.

### Procedure

1. To monitor and analyze current disk storage, run the `isi quota quotas view` command.

   The following example provides current usage information for the root user on the specified directory and includes snapshot data. For more information about the parameters for this command, run the `isi quota quotas list --help` command.

   ```bash
   isi quota quotas list -v --path=/ifs/data/quotas_test_2 \ --include-snapshots="yes"
   ```

2. To view all information in the quota report, run the `isi quota reports list` command.

   To view specific information in a quota report, run the `isi quota quotas list --help` command to view the filter parameters. The following command lists all information in the quota report:

   ```bash
   isi quota reports list -v
   ```

3. (Optional) To delete a quota, run the `isi quota quotas delete` command.

   The following command deletes the specified directory-type quota. For information about parameters for this command, run the `isi quota quotas delete --help` command:

   ```bash
   isi quota quotas delete /ifs/data/quotas_test_2 directory
   ```

4. To unlink a quota, run the `isi quota quotas modify` command.
The following command example unlinks a user quota:

```
isi quota quotas modify /ifs/dir-1 user --linked=false --
user=admin
```

**Note**

Configuration changes for linked quotas must be made on the parent (default) quota that the linked quota is inheriting from. Changes to the parent quota are propagated to all children. If you want to override configuration from the parent quota, you must first unlink the quota.

### Export a quota configuration file

You can export quota settings as a configuration file, which can then be imported for reuse to another Isilon cluster. You can also store the exported quota configurations in a location outside of the cluster. This task may only be performed from the OneFS command line interface.

You can pipe the XML report to a file or directory. The file can then be imported to another cluster.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. At the command prompt, run the following command:

```
isi_classic quota list --export
```

The quota configuration file displays as raw XML.

### Import a quota configuration file

You can import quota settings in the form of a configuration file that has been exported from another Isilon cluster. This task can only be performed from the OneFS command-line interface.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Navigate to the location of the exported quota configuration file.
3. At the command prompt, run the following command, where `<filename>` is the name of an exported configuration file:

```
isi_classic quota import --from-file=<filename>
```

The system parses the file and imports the quota settings from the configuration file. Quota settings that you configured before importing the quota configuration file are retained, and the imported quota settings are effective immediately.
Managing quota notifications

Quota notifications can be enabled or disabled, modified, and deleted.
By default, a global quota notification is already configured and applied to all quotas.
You can continue to use the global quota notification settings, modify the global
notification settings, or disable or set a custom notification for a quota.

Enforcement quotas support four types of notifications and reminders:
- Threshold exceeded
- Over-quota reminder
- Grace period expired
- Write access denied

If a directory service is used to authenticate users, you can configure notification
mappings that control how email addresses are resolved when the cluster sends a
quota notification. If necessary, you can remap the domain that is used for quota email
notifications and you can remap Active Directory domains, local UNIX domains, or
both.

Configure default quota notification settings

You can configure default global quota notification settings that apply to all quotas of
a specified threshold type.

The custom notification settings that you configure for a quota take precedence over
the default global notification settings.

For information about the parameters and options that you can use for this procedure,
run the `isi quota settings notifications modify --help` command.

Procedure

1. Run the `isi quota settings notifications modify` command.

   The following command configures the default quota notification settings to
   generate an alert when the advisory threshold is exceeded:

   ```bash
   isi quota settings notifications modify advisory exceeded \
   --action-alert=true
   ```

   After you finish

   Before using quota data for analysis or other purposes, verify that no QuotaScan jobs
   are in progress by running the `isi job events list --job-type quotascan` command.

Configure custom quota notification rules

You can configure custom quota notification rules that apply only to a specified quota.

Before you begin

An enforcement quota must exist or be in the process of being created. To configure
notifications for an existing enforcement quota, follow the procedure to modify a
quota and then use these steps.

Quota-specific custom notification rules must be configured for that quota. If
notification rules are not configured for a quota, the default event notification
configuration is used.
For information about the parameters and options that you can use for this procedure, run the `isi quota quotas notifications create --help` command.

**Procedure**

1. To configure custom quota notification rules, run the `isi quota quotas notifications create` command.

   The following command creates an advisory quota notification rule for the `/ifs/data/quota_test_2` directory that uses the `--holdoff` parameter to specify the length of time to wait before generating a notification:

   ```
   isi quota quotas notifications create /ifs/data/quota_test_2 directory advisory exceeded --holdoff=10W
   ```

   **After you finish**

   Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by running the `isi job events list --job-type quotascan` command.

Map an email notification rule for a quota

Email notification mapping rules control how email addresses are resolved when the cluster sends a quota notification.

If necessary, you can remap the domain used for SmartQuotas email notifications. You can remap Active Directory Windows domains, local UNIX domains, or NIS domains.

**Note**

You must be logged in to the web administration interface to perform this task.

**Procedure**

1. Click File System Management > SmartQuotas > Settings.
2. (Optional) In the Email Mapping area, click Create an email mapping rule.
3. From the Provider Type list, select the authentication provider type for this notification rule. The default is Local. To determine which authentication providers are available on your cluster, navigate to Access > Authentication Providers.
4. From the Current Domain list, select the domain that you want to use for the mapping rule. If the list is blank, navigate to Cluster Management > Network Configuration, and then click Edit in the DNS Settings area to specify the domains that you want to use for mapping.
5. In the Map-to-Domain field, type the name of the domain that you want to map email notifications to. This can be the same domain name you selected from the Current Domain list. To specify multiple domains, separate the domain names with commas.
6. Click Save Rule.

**Email quota notification messages**

If email notifications for exceeded quotas are enabled, you can customize Isilon templates for email notifications or create your own.

There are three email notification templates provided with OneFS. The templates are located in `/etc/ifs` and are described in the following table:
If the default email notification templates do not meet your needs, you can configure your own custom email notification templates by using a combination of text and SmartQuotas variables. Whether you choose to create your own templates or modify the existing ones, make sure that the first line of the template file is a **Subject:** line. For example:

```
Subject: Disk quota exceeded
```

If you want to include information about the message sender, include a **From:** line immediately under the subject line. If you use an email address, include the full domain name for the address. For example:

```
From: administrator@abcd.com
```

In this example of the `quota_email_template.txt` file, a **From:** line is included. Additionally, the default text "Contact your system administrator for details" at the end of the template is changed to name the administrator:

```
Subject: Disk quota exceeded
From: administrator@abcd.com

The `<ISI_QUOTA_TYPE>` disk quota on directory `<ISI_QUOTA_PATH>` owned by `<ISI_QUOTA_OWNER>` on `<ISI_QUOTA_NODE>` was exceeded.

The quota limit is `<ISI_QUOTA_THRESHOLD>`, and `<ISI_QUOTA_USAGE>` is currently in use. You may be able to free some disk space by deleting unnecessary files. If your quota includes snapshot usage, your administrator may be able to free some disk space by deleting one or more snapshots. Contact Jane Anderson (`janderson@abcd.com`) for details.
```

This is an example of what a user will see as an emailed notification (note that the SmartQuotas variables are resolved):

```
Subject: Disk quota exceeded
From: administrator@abcd.com

The advisory disk quota on directory `/ifs/data/sales_tools/collateral` owned by `jsmith` on production-Boris was exceeded.

The quota limit is 10 GB, and 11 GB is in use. You may be able to free some disk space by deleting unnecessary files. If your quota includes snapshot usage, your administrator may be able to free some disk space by deleting one or more snapshots. Contact Jane Anderson (`janderson@abcd.com`) for details.
```
Custom email notification template variable descriptions

An email template contains text, and, optionally, variables that represent values. You can use any of the SmartQuotas variables in your templates.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_QUOTA_PATH</td>
<td>Path of quota domain</td>
<td>/ifs/data</td>
</tr>
<tr>
<td>ISI_QUOTA_THRESHOLD</td>
<td>Threshold value</td>
<td>20 GB</td>
</tr>
<tr>
<td>ISI_QUOTA_USAGE</td>
<td>Disk space in use</td>
<td>10.5 GB</td>
</tr>
<tr>
<td>ISI_QUOTA_OWNER</td>
<td>Name of quota domain owner</td>
<td>jsmith</td>
</tr>
<tr>
<td>ISI_QUOTA_TYPE</td>
<td>Threshold type</td>
<td>Advisory</td>
</tr>
<tr>
<td>ISI_QUOTA_GRACE</td>
<td>Grace period, in days</td>
<td>5 days</td>
</tr>
<tr>
<td>ISI_QUOTA_EXPIRATION</td>
<td>Expiration date of grace period</td>
<td>Fri May 22 14:23:19 PST 2015</td>
</tr>
<tr>
<td>ISI_QUOTA_NODE</td>
<td>Hostname of the node on which the quota event occurred</td>
<td>someHost-prod-wf-1</td>
</tr>
</tbody>
</table>

Customize email quota notification templates

You can customize Isilon templates for email notifications. This task can be performed only from the OneFS command line interface.

This procedure assumes that you are using the Isilon templates, which are located in the /etc/ifs directory.

Note

We recommend that you do not edit the templates directly. Instead, copy them to another directory to edit and deploy them.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Copy one of the default templates to a directory in which you will edit the file and later access it through the OneFS web administration interface. For example:

   ```
   cp /etc/ifs/quota_email_template.txt /ifs/data/quotanotifiers/quota_email_template_copy.txt
   ```

3. Open the template file in a text editor. For example:

   ```
   edit /ifs/data/quotanotifiers/quota_email_template_copy.txt
   ```

   The template appears in the editor.

4. Edit the template. If you are using or creating a customized template, make sure the template has a Subject: line.

5. Save your changes. Template files must be saved as .txt files.
6. In the web administration interface, navigate to **File System > SmartQuotas > Quotas & Usage**.

7. Select the quota that you want to set a notification rule for.

8. Click the **Settings** tab.

9. Select the notification rule that you want to use with the template that you created (for example, **Advisory Limit Notification Rules**). For more information about setting notification rules, see the instructions for configuring default quota notification settings and configuring custom quota notification rules in this chapter.

10. Select the event for the template (for example, **Event: Advisory Limit Value Exceeded**).

11. In the **Send Email** area, select one of the owner notification type check boxes.

12. In the **Message Template** field, enter or browse to find the template that you copied or customized.

13. (Optional) In the **Event** area, select **Create Cluster Event** to generate an event notification in addition to the email notification.

14. (Optional) In the **Delay** area, select the desired amount of time to wait before generating a notification. The default is zero minutes.

   Repeat steps 9 through 14 to specify an email notification template for each notification rule you wish to create for the quota.

15. Click **Save**.

### Managing quota reports

You can configure and schedule reports to help you monitor, track, and analyze storage use on an Isilon cluster.

You can view and schedule reports and customize report settings to track, monitor, and analyze disk storage use. Quota reports are managed by configuring settings that give you control over when reports are scheduled, how they are generated, where and how many are stored, and how they are viewed. The maximum number of scheduled reports that are available for viewing in the web-administration interface can be configured for each report type. When the maximum number of reports are stored, the system deletes the oldest reports to make space for new reports as they are generated.

### Create a quota report schedule

You can configure quota report settings to generate the quota report on a specified schedule.

Quota report settings determine whether and when scheduled reports are generated, and where and how the reports are stored. If you disable a scheduled report, you can still run unscheduled reports at any time.

For information about the parameters and options that you can use for this procedure, run the `isi quota reports list --help` command.

**Procedure**

1. To configure a quota report schedule, run the `isi quota settings reports modify` command.
The following command creates a quota report schedule that runs every two
days. For more information about date pattern or other schedule parameters,
see man isi-schedule.

```
isi quota settings reports modify --schedule="Every 2 days"
```

**Results**
Reports are generated according to the criteria and can be viewed by running the `isi
quota reports list` command.

**Generate a quota report**
In addition to scheduled quota reports, you can generate a report to capture usage
statistics at any time.

**Before you begin**
Before you can generate a quota report, quotas must exist and no QuotaScan jobs can
be running.

For information about the parameters and options that you can use for this procedure,
run the `isi quota reports create --help` command.

**Procedure**
1. To generate a quota report, run the `isi quota reports create` command.
The following command creates an ad hoc quota report.

```
isi quota reports create -v
```

**Results**
You can view the quota report by running the `isi quota reports list -v` command.

**Locate a quota report**
You can locate quota reports, which are stored as XML files, and use your own tools
and transforms to view them. This task can only be performed from the OneFS
command-line interface.

**Procedure**
1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Navigate to the directory where quota reports are stored. The following path is
   the default quota report location:
   `/ifs/.isilon/smartquotas/reports`

   **Note**
   If quota reports are not in the default directory, you can run the `isi quota
   settings` command to find the directory where they are stored.

   3. At the command prompt, run the `ls` command.
      - To view a list of all quota reports in the directory, run the following
        command:

```
ls -a *.xml
```
To view a specific quota report in the directory, run the following command:

```
ls <filename>.xml
```

### Basic quota settings

When you create a storage quota, the following attributes must be defined, at a minimum. When you specify usage limits, additional options are available for defining your quota.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Path</td>
<td>The directory that the quota is on.</td>
</tr>
<tr>
<td>User Quota</td>
<td>Select to automatically create a quota for every current or future user that stores data in the specified directory.</td>
</tr>
<tr>
<td>Group Quota</td>
<td>Select to automatically create a quota for every current or future group that stores data in the specified directory.</td>
</tr>
<tr>
<td>Include Snapshot Data</td>
<td>Select to count all snapshot data in usage limits; cannot be changed after the quota is created.</td>
</tr>
<tr>
<td>Include Data-Protection Overhead</td>
<td>Select to count protection overhead in usage limits.</td>
</tr>
<tr>
<td>No Usage Limit</td>
<td>Select to account for usage only.</td>
</tr>
<tr>
<td>Specify Usage Limits</td>
<td>Select to enforce advisory, soft, or absolute limits.</td>
</tr>
</tbody>
</table>

### Advisory limit quota notification rules settings

You can configure custom quota notification rules for advisory limits for a quota. These settings are available when you select the option to use custom notification rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Exceeded</th>
<th>Remains exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send email</td>
<td>Specify the type of email to use.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another</td>
<td>Select to send an email notification to another recipient and type the recipient’s email address.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Soft limit quota notification rules settings

You can configure custom soft limit notification rules for a quota. These settings are available when you select the option to use custom notification rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Exceeded</th>
<th>Remains exceeded</th>
<th>Grace period expired</th>
<th>Write access denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send email</td>
<td>Specify the recipient of the email notification.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another</td>
<td>Select to send an email notification to another recipient and type</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Exceeded</td>
<td>Remains exceeded</td>
<td>Grace period expired</td>
<td>Write access denied</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the recipient's email address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can only enter one email address. If you want to notify more than one person, consider creating a distribution list and specifying that as the email address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Message template</strong></td>
<td>Select from the following template types for use in formatting email notifications:</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• Default (leave <strong>Message Template</strong> field blank to use default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Custom</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Create cluster event</strong></td>
<td>Select to generate an event notification for the quota.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Delay</strong></td>
<td>Specify the length of time (hours, days, weeks) to delay before generating a notification.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>Specify the notification and alert frequency: daily, weekly, monthly, yearly; depending on selection, specify intervals, day to send, time of day, multiple emails per rule.</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
# Hard limit quota notification rules settings

You can configure custom quota notification rules for hard limits for a quota. These settings are available when you select the option to use custom notification rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Write access denied</th>
<th>Exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send email</td>
<td>Specify the recipient of the email notification.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another</td>
<td>Select to send an email notification to another recipient and type the recipient's email address.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
|                   | **Note**
|                   | You can only type one email address. If you want to notify more than one person, consider creating a distribution list and specifying that as the email address. |                      |          |
| Message template  | Select from the following template types for use in formatting email notifications: | Yes                 | Yes      |
|                   | • Default (leave Message Template field blank to use default)               |                     |          |
|                   | • Custom                                                                    |                     |          |
| Create cluster event | Select to generate an event notification for the quota when exceeded.     | Yes                 | Yes      |
| Delay             | Specify the length of time (hours, days, weeks) to delay before generating a notification. | Yes                 | No       |
| Frequency         | Specify the notification and alert frequency: daily, weekly, monthly, yearly. Depending on selection, specify intervals, day to send, time of day, multiple email messages per rule. | No                  | Yes      |
Limit notification settings

You have three notification options when you create an enforcement quota: use default notification rules, turn off notifications, or use custom notification rules. Enforcement quotas support the following notification settings for each threshold type. A quota can use only one of these settings.

<table>
<thead>
<tr>
<th>Notification setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Notification Rules</td>
<td>Uses the default notification rules that you configured for the specified threshold type.</td>
</tr>
<tr>
<td>Turn Off Notifications for this Quota</td>
<td>Disables all notifications for the quota.</td>
</tr>
<tr>
<td>Use Custom Notification Rules</td>
<td>Provides settings to create basic custom notifications that apply to only this quota.</td>
</tr>
</tbody>
</table>

Quota report settings

You can configure quota report settings that track disk usage. These settings determine whether and when scheduled reports are generated, and where and how reports are stored. When the maximum number of reports are stored, the system deletes the oldest reports to make space for new reports as they are generated.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled reporting</td>
<td>Enables or disables the scheduled reporting feature.</td>
</tr>
<tr>
<td>• Off. Manually generated on-demand reports can be run at any time.</td>
<td></td>
</tr>
<tr>
<td>• On. Reports run automatically according to the schedule that you specify.</td>
<td></td>
</tr>
<tr>
<td>Report frequency</td>
<td>Specifies the interval for this report to run: daily, weekly, monthly, or yearly. You can use the following options to further refine the report schedule.</td>
</tr>
<tr>
<td>Generate report every</td>
<td>Specify the numeric value for the selected report frequency; for example, every 2 months.</td>
</tr>
<tr>
<td>Generate reports on</td>
<td>Select the day or multiple days to generate reports.</td>
</tr>
<tr>
<td>Select report day by</td>
<td>Specify date or day of the week to generate the report.</td>
</tr>
<tr>
<td>Generate one report per specified by</td>
<td>Set the time of day to generate this report.</td>
</tr>
<tr>
<td>Generate multiple reports per specified day</td>
<td>Set the intervals and times of day to generate the report for that day.</td>
</tr>
<tr>
<td>Scheduled report archiving</td>
<td>Determines the maximum number of scheduled reports that are available for viewing on the SmartQuotas Reports page.</td>
</tr>
<tr>
<td>Limit archive size</td>
<td>for scheduled reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep.</td>
</tr>
</tbody>
</table>
### Quota commands

You can configure quotas to track, limit, and manage disk usage by directory, user, or group. Quota commands that create and modify quotas are available only if you activate a SmartQuotas license on the cluster.

**isi quota quotas create**

Creates new file system quotas.

**Syntax**

```
isi quota quotas create <path> <type>
    |--user <name>
    |--group <name>
    |--gid <id>
    |--uid <id>
    |--wellknown <name>
    |--hard-threshold <size>
    |--advisory-threshold <size>
    |--soft-threshold <size>  [--soft-grace <duration>]
    |--soft-grace <duration>
    |--container {yes | no}
    |--include-snapshots {yes | no}
    |--thresholds-include-overhead {yes | no}
    |--zone <string>
    |--enforced {yes | no}  [--zone <zone>]
    |--verbose
```

**Options**

- `<path>`
  Specifies an absolute path within the /ifs file system.

- `<type>`
  {directory | user | group | default-user | default-group}

---

**Archive Directory.** Browse to the directory where you want to store quota reports for archiving.

**Manual report archiving**

Determines the maximum number of manually generated (on-demand) reports that are available for viewing on the SmartQuotas Reports page.

**Limit archive size** for live reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep.

**Archive Directory.** Browse to the directory where you want to store quota reports for archiving.
Specifies a quota type. The following values are valid:

directory
   Creates a quota for all data in the directory, regardless of owner.

user
   Creates a quota for one specific user. Requires specification of the --user,
       --uid, --sid, or --wellknown option.

group
   Creates a quota for one specific group. Requires specification of the --
       group, --gid, --sid, or --wellknown option.

default-user
   Creates a master quota that creates a linked quota for every user who has
       data in the directory.

default-group
   Creates a master quota that creates a linked quota for every group that owns
       data in the directory.

--user <name>
   Specifies a user name.

--group <name>
   Specifies a group name.

--gid <id>
   Specifies the numeric group identifier (GID).

--uid <id>
   Specifies a numeric user identifier (UID).

--sid <sid>
   Sets a security identifier (SID). For example, S-1-5-21-13.

--wellknown <name>
   Specifies a well-known user, group, machine, or account name.

--hard-threshold <size>
   Sets an absolute limit for disk usage. Attempts to write to disk are generally
       denied if the request violates the quota limit. Size is a capacity value formatted
       as<integer>{b | K | M | G | T | P}.

--advisory-threshold <size>
   Sets the advisory threshold. For notification purposes only. Does not enforce
       limitations on disk write requests. Size is a capacity value formatted
       as<integer>{b | K | M | G | T | P}.

--soft-threshold <size>
Specifies the soft threshold, which allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter. Size is a capacity value formatted as `<integer>\{b | K | M | G | T | P\}`.

`--soft-grace <duration>`

Specifies the soft threshold grace period, which is the amount of time to wait before disk write requests are denied.

Specify `<duration>` in the following format:

```
<integer><units>
```

The following `<units>` are valid:

Y

  Specifies years

M

  Specifies months

W

  Specifies weeks

D

  Specifies days

H

  Specifies hours

`--container {yes | no}`

Specifies that threshold be shown as the available space on the SMB share, instead of the whole cluster. The setting applies only to hard thresholds. When setting this value, you must specify `--enforced`.

`--include-snapshots {yes | no}`

Includes snapshots in the quota size.

`--thresholds-include-overhead {yes | no}`

Includes OneFS storage overhead in the quota threshold when set to `yes`.

`--enforced {yes | no}`

Enforces this quota when set to `yes`. Specifying any threshold automatically sets this value to `yes` on create.

`--zone <zone>`

Specifies an access zone.

`{--verbose | -v}`

Displays more detailed information.
# isi quota quotas delete

Deletes a file system quota or multiple quotas.

## Syntax

```plaintext
isi quota quotas delete <path> <type>
    [--uid <id>]
    [--user <name>]
    [--gid <id>]
    [--group <name>]
    [--sid <sid>]
    [--wellknown <name>]
    [--recurse-path-parents]
    [--recurse-path-children]
    [--include-snapshots {yes | no}]
    [--zone <zone>]
    [--verbose]
```

## Options

**<path>**
- Specifies an absolute path within the `/ifs` file system.

**<type>** `{directory | user | group | default-user | default-group | --all}`
- Deletes quotas of the specified type. Argument must be specified with the `<path>` variable. The following values are valid:
  - **directory**
    - Specifies a quota for all data in the directory, regardless of owner.
  - **user**
    - Specifies a quota for one specific user. Requires specification of `--user`, `--uid`, or `--sid`.
  - **group**
    - Specifies a quota for one specific group. Requires specification of the `--group`, `--gid`, or `--sid` option.
  - **default-user**
    - Specifies a master quota that creates a linked quota for every user who has data in the directory.
  - **default-group**
    - Specifies a master quota that creates a linked quota for every group that owns data in the directory.
  - **--all**
    - Deletes all quotas. Flag may not be specified with `<type>` or `<path>`.

**--uid <id>**
- Deletes a quota by the specified numeric user identifier (UID).

**--user <name>**
Deletes a quota associated with the user identified by name.

`--gid <id>`
Deletes a quota by the specified numeric group identifier (GID).

`--group <name>`
Deletes a quota associated with the group identified by name.

`--sid <sid>`
Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

`--wellknown <name>`
Deletes a quota associated with the wellknown persona.

`--recurse-path-parents`
Searches parent paths for quotas.

`--recurse-path-children`
Searches child paths for quotas.

`--include-snapshots {yes | no}`
Deletes quotas that include snapshot data usage.

`--zone <zone>`
Specifies an access zone.

`{--verbose | -v}`
Displays more detailed information.

**isi quota quotas modify**

Modifies a file system quota.

**Syntax**

```
isi quota quotas modify <path> <type>
[  --user <name> | --group <name> | --gid <id> | --uid <id>
   | --sid <sid> | --wellknown <name>]
[  --hard-threshold <size>]
[  --clear-hard-threshold]
[  --advisory-threshold <size>]
[  --clear-advisory-threshold]
[  --soft-threshold <size>]
[  --clear-soft-threshold]
[  --soft-grace <duration>]
[  --container {yes | no}]
[  --include-snapshots {yes | no}]
[  --thresholds-include-overhead {yes | no}]
[  --enforced {yes | no}]
[  --linked {yes | no}]
[  --zone <string>]
[   --verbose]
```

**Options**

`--path <path>`
Specifies an absolute path within the /ifs file system.
--type
Specifies a quota type. The following values are valid:
directory
    Creates a quota for all data in the directory, regardless of owner.
user
    Creates a quota for one specific user. Requires specification of the --user,
    --uid, or --sid option.
group
    Creates a quota for one specific group. Requires specification of the --
group, --gid, or --sid option.
default-user
    Creates a master quota that creates a linked quota for every user who has
data in the directory.
default-group
    Creates a master quota that creates a linked quota for every group that owns
data in the directory.

--user <name>
    Specifies a user name.
--group <name>
    Specifies a group name.
--gid <id>
    Specifies the numeric group identifier (GID).
--uid <id>
    Specifies a numeric user identifier (UID).
--sid <sid>
    Specifies a security identifier (SID) for selecting the quota that you want to
modify. For example, S-1-5-21-13.
--wellknown <name>
    Specifies a well-known user, group, machine, or account name.

--hard-threshold <size>
    Sets an absolute limit for disk usage. Attempts to write to disk are generally
denied if the request violates the quota limit. Size is a capacity value formatted
as<integer>({B | K | M | G | T | P}).
--clear-hard-threshold
    Clears an absolute limit for disk usage.

--advisory-threshold <size>
    Sets the advisory threshold. For notification purposes only. Does not enforce
limitations on disk write requests. Size is a capacity value formatted
as<integer>({B | K | M | G | T | P}).
--clear-advisory-threshold
Clears the advisory threshold.

**--soft-threshold <size>**  
Specifies the soft threshold, which allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.  
Size is a capacity value formatted as `<integer>([{\text{b}} | {\text{K}} | {\text{M}} | {\text{G}} | {\text{T}} | {\text{P}}}]`.

**--clear-soft-threshold**  
Clears the soft threshold.

**--soft-grace <duration>**  
Specifies the soft threshold grace period, which is the amount of time to wait before disk write requests are denied.  
Specify `<duration>` in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- **Y**  
  Specifies years

- **M**  
  Specifies months

- **W**  
  Specifies weeks

- **D**  
  Specifies days

- **H**  
  Specifies hours

- **m**  
  Specifies minutes

- **s**  
  Specifies seconds

**--container {yes | no}**  
Specifies that threshold be shown as the available space on the SMB share, instead of the whole cluster. The setting applies only to hard thresholds. When setting this value, you must specify **--enforced**.

**--include-snapshots {yes | no}**  
Includes snapshots in the quota size.

**--thresholds-include-overhead {yes | no}**  
Includes OneFS storage overhead in the quota threshold when set to yes.

**--enforced {yes | no}**  
Enforces this quota when set to yes. Specifying any threshold automatically sets this value to yes on create.
--linked {yes | no}
Unlinks a linked quota created automatically by a default-user or default-group quota. Unlinking allows the quota to be modified separately. To modify a linked quota, you must modify the original default-user or default-group quota it originated from, instead of the linked quota itself.

--zone <string>
The zone used by the quota. Use this parameter only to resolve personas used by the quota.

{--verbose | -v}
Displays more detailed information.

isi quota quotas list
Displays a list of quotas.

Syntax

```
isi quota quotas list
   [--user <name> | --group <name> | --gid <id> | --uid <id>
           | --sid <sid> | --wellknown <name>]
   [--type {directory | user | group | default-user
           | default-group}]
   [--path <path>]
   [--recurse-path-parents]
   [--recurse-path-children]
   [--include-snapshots {yes | no}]
   [--exceeded]
   [--enforced {yes | no}]
   [--zone <zone>]
   [--limit <integer>]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

--user <name>
Specifies a user name.

--group <name>
Specifies a group name.

--gid <id>
Specifies the numeric group identifier (GID).

--uid <id>
Specifies a numeric user identifier (UID).

--sid <sid>
Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

--wellknown <name>
Specifies a well-known user, group, machine, or account name.
<type>
  Specifies a quota type. The following values are valid:
  
directory
    Creates a quota for all data in the directory, regardless of owner.
  
user
    Creates a quota for one specific user. Requires specification of the --user,
    --uid, --sid, or --wellknown option.
  
group
    Creates a quota for one specific group. Requires specification of the --
    group, --gid, --sid, or --wellknown option.
  
default-user
    Creates a master quota that creates a linked quota for every user who has
    data in the directory.
  
default-group
    Creates a master quota that creates a linked quota for every group that owns
    data in the directory.
  
--path
  Specifies quotas on the specified path.

--recurse-path-parents
  Specifies parent paths for quotas.

--recurse-path-children
  Specifies child paths for quotas.

--include-snapshots {yes | no}
  Specifies quotas that include snapshot data usage.

--exceeded
  Specifies only quotas that have an exceeded threshold.

--enforced {yes | no}
  Specifies quotas that have an enforced threshold.

--zone <zone>
  Specifies quotas in the specified zone.

--limit <integer>
  Specifies the number of quotas to display.

--format
  Displays quotas in the specified format. The following values are valid:
  
  * table
  * json
  * csv
  * list

  {--no-header | -a}
Suppresses headers in CSV or table formats.

```
|--no-footer | -z
```
Suppresses table summary footer information.

```
|--verbose | -v
```
Displays more detailed information.

**isi quota quotas view**

Displays detailed properties of a single file system quota.

**Syntax**

```
isi quota quotas view
   --path <path>
   --type {directory | user | group | default-user | default-group}
   [|--user <name> | --group <name> | --gid <id> | --uid <id>
   | --sid <sid> | --wellknown <name>]
   [--include-snapshots {yes | no}]
   [--zone <string>]
```

**Options**

```
--path <path>
```
Specifies an absolute path within the /ifs file system.

```
--type
```
Specifies quotas of the specified type. Argument must be specified with the --path option. The following values are valid:

**directory**
Specifies a quota for all data in the directory, regardless of owner.

**user**
Specifies a quota for one specific user. Requires specification of --user, --uid, --sid, or --wellknown option.

**group**
Specifies a quota for one specific group. Requires specification of the --group, --gid, --sid, or --wellknown option.

**default-user**
Specifies a master quota that creates a linked quota for every user who has data in the directory.

**default-group**
Specifies a master quota that creates a linked quota for every group that owns data in the directory.

```
--user <name>
```
Specifies a quota associated with the user identified by name.
--group <name>
   Specifies a quota associated with the group identified by name.

--gid <id>
   Specifies a quota by the numeric group identifier (GID).

--uid <id>
   Specifies a quota by the specified numeric user identifier (UID).

--sid <sid>
   Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

--wellknown <name>
   Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
   Specifies quotas that include snapshot data usage.

--zone <zone>
   Specifies an access zone.

isi quota quotas notifications clear

Clears rules for a quota and uses system notification settings.

Note
Use the isi quota quotas notifications disable command to disable all notifications for a quota.

Syntax

```
isi quota quotas notifications clear <path> <type>
   [--user <name>]
   [--group <name>]
   [--gid <id>]
   [--uid <id>]
   [--sid <sid>]
   [--wellknown <name>]
   [--include-snapshots {yes | no}]
   [--force]
```

Options

<path>
   Specifies an absolute path within the /ifs file system.

<type>
   Specifies a quota type. The following values are valid:
   directory
      Creates a quota for all data in the directory, regardless of owner.
user
Creates a quota for one specific user. Requires specification of the --user, --uid, --sid, or --wellknown option.

group
Creates a quota for one specific group. Requires specification of the --group, --gid, --sid, or --wellknown option.
default-user
Creates a master quota that creates a linked quota for every user who has data in the directory.
default-group
Creates a master quota that creates a linked quota for every group that owns data in the directory.

--user <name>
Specifies a user name.

--group <name>
Specifies a group name.

--gid <id>
Specifies the numeric group identifier (GID).

--uid <id>
Specifies a numeric user identifier (UID).

--sid <sid>
Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

--wellknown <name>
Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
Includes snapshots in the quota size.

|--force | -f|
Skips the confirmation prompt.

isi quota quotas notifications create
Creates a notification rule for a quota.

Syntax

| isi quota quotas notifications create |
| --path <path> |
| --type {directory | user | group | default-user | default-group} |
| --threshold {hard | soft | advisory} |
| --condition {exceeded | denied | violated | expired} |
| [--user <name> | --group <name> | --gid <id> | --uid <id> |
| | --sid <sid> | --wellknown <name>] |
| [--include-snapshots {yes | no}] |
SmartQuotas

```
[--schedule <name>]
[--holdoff <duration>]
[--action-alert {yes | no}]
[--action-email-owner {yes | no}]
[--action-email-address <address>]
[--verbose]
```

Options

--path <path>
Specifies an absolute path within the /ifs file system.

--type
Specifies a quota type. The following values are valid:

- **directory**
  Creates a quota for all data in the directory, regardless of owner.

- **user**
  Creates a quota for one specific user. Requires specification of the --user, --uid, --gid, or --wellknown option.

- **group**
  Creates a quota for one specific group. Requires specification of the --group, --gid, --sid, or --wellknown option.

- **default-user**
  Creates a master quota that creates a linked quota for every user who has data in the directory.

- **default-group**
  Creates a master quota that creates a linked quota for every group that owns data in the directory.

--threshold
Specifies the threshold type. The following values are valid:

- **hard**
  Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.

- **soft**
  Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.

- **advisory**
  Sets the advisory threshold. For notification purposes only. Does not enforce limitations on disk write requests.

--condition
Specifies the quota condition on which to send a notification. The following values are valid:
denied
   Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.

exceeded
   Specifies a notification when disk usage exceeds the threshold.

violated
   Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

expired
   Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.

--user <name>
   Specifies a user name.

--group <name>
   Specifies a group name.

--gid <id>
   Specifies the numeric group identifier (GID).

--uid <id>
   Specifies a numeric user identifier (UID).

--sid <sid>
   Sets a security identifier (SID). For example, S-1-5-21-13.

--wellknown <name>
   Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
   Specifies quotas that include snapshot data usage.

--schedule <name>
   Specifies the date pattern at which recurring notifications are made. Specify in the following format:

   "<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>[, ...] [of every [{other | <integer>}] week]]
- The last {day | weekday | <day>} of every [[other | <integer>]] month
- The <integer> {weekday | <day>} of every [[other | <integer>]] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:
- at <hh>[:<mm>] [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>[:<mm>] [{AM | PM}] and <hh>[:<mm>] [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>[:<mm>] [{AM | PM}] to <hh>[:<mm>] [{AM | PM}]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

--holdoff <duration>
Specifies the length of time to wait before generating a notification.
Specify <duration> in the following format:

<integer><units>

The following <units> are valid:
- Y
  Specifies years
- M
  Specifies months
- W
  Specifies weeks
- D
  Specifies days
- H
  Specifies hours
- s
  Specifies seconds

--action-alert {yes | no}
Generates an alert when the notification condition is met.

--action-email-owner {yes | no}
Specifies that an email be sent to a user when the threshold is crossed. Requires
--action-email-address.

--action-email-address <address>
Specifies the email address of user to be notified.

{--verbose | -v}
Displays more detailed information.

isi quota quotas notifications delete
Deletes a quota notification rule.

Syntax

isi quota quotas notifications delete
  --path <path>
  --type {directory | user | group | default-user | default-group}
  --threshold {hard | soft | advisory}
  --condition {exceeded | denied | violated | expired}
  [--user <name> | --group <name> | --gid <id> | --uid <id>
   | --sid <sid> | --wellknown <name>]
  [--include-snapshots {yes | no}]
  [--verbose]

Options

--path <path>
Deletes quota notifications set on an absolute path within the /ifs file system.

--type
Deletes a quota notification by specified type. The following values are valid:

directory
  Specifies a quota for all data in the directory, regardless of owner.

user
  Specifies a quota for one specific user. Requires specification of the --
  user, --uid, --sid, or --wellknown option.

group
  Specifies a quota for one specific group. Requires specification of the --
  group, --gid, --sid, or --wellknown option.

default-user
  Specifies a master quota that creates a linked quota for every user who has
  data in the directory.

default-group
  Specifies a master quota that creates a linked quota for every group that
  owns data in the directory.

--threshold
Deletes a quota notification by specified threshold. The following values are valid:
**hard**
Specifies an absolute limit for disk usage.

**soft**
Specifies the soft threshold.

**advisory**
Specifies the advisory threshold.

**--condition**
Deletes a quote notification by the specified condition on which to send a notification. The following values are valid:

  **denied**
  Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.

  **exceeded**
  Specifies a notification when disk usage exceeds the threshold.

  **violated**
  Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

  **expired**
  Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.

**--user <name>**
Deletes a quota notification by the specified user name.

**--group <name>**
Deletes a quota notification by the specified group name.

**--gid <id>**
Deletes a quota notification by the specified numeric group identifier (GID).

**--uid <id>**
Deletes a quota notification by the specified numeric user identifier (UID).

**--sid <sid>**
Deletes a quota notification by the specified security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

**--wellKnown <name>**
Deletes a quota notification by the specified well-known user, group, machine, or account name.

**--include-snapshots {yes | no}**
Deletes a quota notification by the specified settings for Included snapshots in
the quota size.

```bash
|--verbose | -v

Displays more detailed information.
```

### isi quota quotas notifications disable

Disables all quota notifications.

⚠️ **CAUTION**

When you disable all quota notifications, system notification behavior is disabled
also. Use the `--clear` options to remove specific quota notification rules and fall
back to the system default.

#### Syntax

```bash
isi quota quotas notifications disable
   --path <path>
   --type {directory | user | group | default-user | default-group} 
   [--user <name> | --group <name> | --gid <id> | --uid <id> 
   | --sid <sid> | --wellknown <name>]
   [--include-snapshots {yes | no}]
```

#### Options

**--path <path>**

Specifies an absolute path within the /ifs file system.

**--type**

Disables quotas of the specified type. Argument must be specified with the `--
path` option. The following values are valid:

- **directory**
  
  Specifies a quota for all data in the directory, regardless of owner.

- **user**
  
  Specifies a quota for one specific user. Requires specification of `--user,--
  uid,--sid, or --wellknown` option.

- **group**
  
  Specifies a quota for one specific group. Requires specification of the `--
  group,--gid,--sid, or --wellknown` option.

- **default-user**
  
  Specifies a master quota that creates a linked quota for every user who has
data in the directory.

- **default-group**
  
  Specifies a master quota that creates a linked quota for every group that
owns data in the directory.
Disables a quota associated with the user identified by name.

Disables a quota by the specified numeric group identifier (GID).

Disables a quota by the specified numeric user identifier (UID).

Specifies a security identifier (SID) for selecting a quota. For example,
S-1-5-21-13.

Specifies a well-known user, group, machine, or account name.

Disables quotas that include snapshot data usage.

Displays a list of quota notification rules.

Specifies an absolute path within the /ifs file system.

Specifies a quota type. The following values are valid:

directory
   Creates a quota for all data in the directory, regardless of owner.

user
   Creates a quota for one specific user. Requires specification of the --user,
   --uid, --sid, or --wellknown option.
group
   Creates a quota for one specific group. Requires specification of the --group, --gid, --sid, or --wellknown option.

default-user
   Creates a master quota that creates a linked quota for every user who has data in the directory.

default-group
   Creates a master quota that creates a linked quota for every group that owns data in the directory.

--user <name>
   Specifies a user name.

--group <name>
   Specifies a group name.

--gid <id>
   Specifies the numeric group identifier (GID).

--uid <id>
   Specifies a numeric user identifier (UID).

--sid <sid>
   Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

--wellknown <name>
   Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
   Includes snapshots in the quota size.

{--limit | -l} <integer>
   Specifies the number of quota notification rules to display.

--format
   Displays quota notification rules in the specified format. The following values are valid:
   table
   json
   csv
   list

{--no-header | -a}
   Suppresses headers in CSV or table formats.
Suppresses table summary footer information.

Displays more detailed information.

 isi quota quotas notifications modify

Modifies a notification rule for a quota.

Syntax

```bash
isi quota quotas notifications modify
--path <path>
--type {directory | user | group | default-user | default-group}
--threshold {hard | soft | advisory}
--condition {exceeded | denied | violated | expired}
[--user <name> | --group <name> | --gid <id> | --uid <id>
  --sid <sid> | --wellknown <name>]
[--include-snapshots {yes | no}]
[--schedule <string>]
[--holdoff <duration>]
[--clear-holdoff]
[--action-alert {yes | no}]
[--action-email-owner {yes | no}]
[--action-email-address <address>]
[--email-template <path>]
[--clear-email-template]
[--verbose]
```

Options

`--path <path>`

Specifies an absolute path within the /ifs file system.

`--type`

Specifies a quota type. The following values are valid:

- directory
  
  Creates a quota for all data in the directory, regardless of owner.

- user
  
  Creates a quota for one specific user. Requires specification of the --user, --uid, --sid, or --wellknown option.

- group
  
  Creates a quota for one specific group. Requires specification of --group, --gid, --sid, or --wellknown option.

- default-user
  
  Creates a master quota that creates a linked quota for every user who has data in the directory.

- default-group
  
  Creates a master quota that creates a linked quota for every group that owns data in the directory.
--threshold
  Specifies the threshold type. The following values are valid:
    hard
      Sets an absolute limit for disk usage. Attempts to write to disk are generally
denied if the request violates the quota limit.
    soft
      Specifies the soft threshold. Allows writes to disk above the threshold until
the soft grace period expires. Attempts to write to disk are denied thereafter.
    advisory
      Sets the advisory threshold. For notification purposes only. Does not enforce
limitations on disk write requests.

--condition
  Specifies the quota condition on which to send a notification. The following values
are valid:
    denied
      Specifies a notification when a hard threshold or soft threshold outside of its
soft grace period causes a disk write operation to be denied.
    exceeded
      Specifies a notification when disk usage exceeds the threshold.
    violated
      Specifies a notification when disk usage exceeds a quota threshold but none
of the other conditions apply.
    expired
      Specifies a notification when disk usage exceeds the soft threshold and the
soft-grace period has expired.

--user <name>
  Specifies a user name.

--group <name>
  Specifies a group name.

--gid <id>
  Specifies the numeric group identifier (GID).

--uid <id>
  Specifies a numeric user identifier (UID).

--sid <sid>
  Sets a security identifier (SID). For example, S-1-5-21-13.

--wellknown <name>
  Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
  Includes snapshots in the quota size.
--schedule <name>

Specifies the date pattern at which recurring notifications are made.
Specify in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>[, ...] of every [{other | <integer>}] week]]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>[:<mm>] [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>[:<mm>] [{AM | PM}] and <hh>[:<mm>] [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>[:<mm>] [{AM | PM}] to <hh>[:<mm>] [{AM | PM}]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day.  
For example, both "saturday" and "sat" are valid.

--holdoff <duration>

Specifies the length of time to wait before generating a notification.
Specify <duration> in the following format:

<integer><units>

The following <units> are valid:

Y
- Specifies years
M
- Specifies months
Specifies weeks

D
Specifies days

H
Specifies hours

s
Specifies seconds

--clear-holdoff
Clears the value for the --holdoff duration.

--action-alert {yes | no}
Generates an alert when the notification condition is met.

--action-email-owner {yes | no}
Specifies that an email be sent to a user when the threshold is crossed. Requires --action-email-address.

--action-email-address <address>
Specifies the email address of user to be notified.

{--verbose | -v}
Displays more detailed information.

**isi quota quotas notifications view**

Displays the properties of a quota notification rule.

**Syntax**

```
isi quota quotas notifications view
--path <path>
--type {directory | user | group | default-user | default-group}
--threshold {hard | soft | advisory}
--condition {exceeded | denied | violated | expired}
[--user <name> | --group <name> | --gid <id> | --uid <id>
 | --sid <sid> | --wellknown <name>]
[--include-snapshots {yes | no}]
```

**Options**

--path <path>
Specifies an absolute path within the /ifs file system.

--type
Specifies a quota type. The following values are valid:

directory
Creates a quota for all data in the directory, regardless of owner.
user
Creates a quota for one specific user. Requires specification of the --user, --uid, --sid, or --wellknown option.

group
Creates a quota for one specific group. Requires specification of the --group, --gid, --sid, or --wellknown option.

default-user
Creates a master quota that creates a linked quota for every user who has data in the directory.

default-group
Creates a master quota that creates a linked quota for every group that owns data in the directory.

--threshold
Specifies the threshold type. The following values are valid:

  hard
  Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.

  soft
  Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.

  advisory
  Sets the advisory threshold. For notification purposes only. Does not enforce limitations on disk write requests.

--condition
Specifies the quota condition on which to send a notification. The following values are valid:

  denied
  Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.

  exceeded
  Specifies a notification when disk usage exceeds the threshold.

  violated
  Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

  expired
  Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.
--user <name>
    Specifies a user name.

--group <name>
    Specifies a group name.

--gid <id>
    Specifies the numeric group identifier (GID).

--uid <id>
    Specifies a numeric user identifier (UID).

--sid <sid>
    Specifies a security identifier (SID) for selecting the quota. For example, S-1-5-21-13.

--wellknown <name>
    Specifies a well-known user, group, machine, or account name.

--include-snapshots {yes | no}
    Includes snapshots in the quota size.

**isi quota reports create**

Generates a quota report.

**Syntax**

```bash
isi quota reports create
    [--verbose]
```

**Options**

```bash
--verbose | -v
```

Displays more detailed information.

**isi quota reports delete**

Deleting a specified report.

**Syntax**

```bash
isi quota reports delete
    --time <string>
    --generated {live | scheduled | manual}
    --type {summary | detail}
    [--verbose]
```

**Options**

```bash
--time <string>
```
Specifies the timestamp of the report.
Specify `<time-and-date>` in the following format:

```
<YYYY>-<MM>-<DD>[T<hh>:<mm>[;<ss>]]
```

Specify `<time>` as one of the following values.

Y
  Specifies years

M
  Specifies months

W
  Specifies weeks

D
  Specifies days

h
  Specifies hours

s
  Specifies seconds

`--generated`
  Specifies the method used to generate the report. The following values are valid:
  live
  scheduled
  manual

`--type`
  Specifies a report type. The following values are valid:
  summary
  detail

`{--verbose | -v}`
  Displays more detailed information.

**isi quota reports list**

Displays a list of quota reports.

**Syntax**

```
isi quota reports list
[--limit <integer>]
```
Options

--limit <integer>
  Specifies the number of quotas to display.

--format
  Displays quotas in the specified format. The following values are valid:
  table
  json
  csv
  list

{--no-header | -a}
  Suppresses headers in CSV or table formats.

{--no-footer | -z}
  Suppresses table summary footer information.

{--verbose | -v}
  Displays more detailed information.

isi quota settings mappings create

Creates a SmartQuotas email mapping rule.

Syntax

isi quota settings mappings create <type> <domain> <mapping>
  [--verbose]

Options

<type>{ad | local | nis | ldap}
  The authentication provider type for the source domain.

<domain>
  The fully-qualified domain name for the source domain you are mapping.

<mapping>
  The fully-qualified domain name for the destination domain you are mapping to.

{--verbose | -v}
  Displays more detailed information.
isi quota settings mappings delete

Deletes SmartQuotas email mapping rules.

Syntax

```
isi quota settings mappings delete <type> <domain>
  [--all]
  [--verbose]
  [--force]
```

Options

```
<type> {ad | local | nis | ldap}
  The authentication provider type for the source domain.

<domain>
  The fully-qualified domain name for the source domain you are mapping.

--all
  Deletes all mapping rules.

{--verbose | -v}
  Displays more detailed information.

{force | -f}
  Forces the deletion without displaying a confirmation prompt.
```

isi quota settings mappings list

Lists SmartQuotas email mapping rules.

Syntax

```
isi quota settings mappings list
  [--limit <integer>]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]
```

Options

```
{--limit | -l} <integer>
  The number of quota mapping settings to display.

--format {table | json | csv | list}
  Display quota mappings settings in table, JSON, CSV, or list format.

{--no-header | -a}
  Do not display headers in table or CSV formats.

{--no-footer | -z}
  Do not display table summary footer information.

{--verbose | -v}
```
**isi quota settings mappings modify**

Modifies an existing SmartQuotas email mapping rule.

**Syntax**

```
isi quota settings mappings modify <type> <domain> <mapping> [--verbose]
```

**Options**

- `<type>` {ad | local | nis | ldap}
  The authentication provider type for the source domain.

- `<domain>`
  The fully-qualified domain name for the source domain you are mapping.

- `<mapping>`
  The fully-qualified domain name for the destination domain you are mapping to.

- `[--verbose | -v]`
  Displays more detailed information.

**isi quota settings mappings view**

View a SmartQuotas email mapping rule.

**Syntax**

```
isi quota settings mappings view <type> <domain>
```

**Options**

- `<type>` {ad | local | nis | ldap}
  The authentication provider type for the source domain.

- `<domain>`
  The fully-qualified domain name for the source domain you are mapping.

**isi quota settings notifications clear**

Clears all default quota notification rules.

When you clear all default notification rules, the system reverts to system notification behavior. Use the `--disable` option to disable notification settings for a specific quota notification rule.

**Syntax**

```
isi quota settings notifications clear
```
isi quota settings notifications create

Creates a default notification rule.

Syntax

```
isi quota settings notifications create
   --threshold {hard | soft | advisory}
   --condition {exceeded | denied | violated | expired}
   --schedule <string>
   --holdoff <duration>
   [--action-alert {yes | no}]
   [--action-email-owner {yes | no}]
   [--action-email-address {yes | no}]
   [--email-template <path>]
   [--verbose]
```

Options

--threshold

Specifies the threshold type. The following values are valid:

- **hard**
  
  Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.

- **soft**
  
  Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.

- **advisory**
  
  Sets the advisory threshold. For notification purposes only. Does not enforce limitations on disk write requests.

--condition

Specifies the quota condition on which to send a notification. The following values are valid:

- **denied**
  
  Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.

- **exceeded**
  
  Specifies a notification when disk usage exceeds the threshold. Applies to only soft thresholds within the soft-grace period.

- **violated**
  
  Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

- **expired**
  
  Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.

--schedule <string>

Specifies the date pattern at which recurring notifications are made.
Specify in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>, ...] [of every [{other | <integer>}] week]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>[<mm>] [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>[<mm>] [{AM | PM}] and <hh>[<mm>] [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>[<mm>] [{AM | PM}] to <hh>[<mm>] [{AM | PM}]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month".

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

--holdoff <duration>
Specifies the length of time to wait before generating a notification.
Specify <duration> in the following format:

<integer> <units>

The following <units> are valid:

Y
- Specifies years

M
- Specifies months
**W**
Specifies weeks

**D**
Specifies days

**H**
Specifies hours

**s**
Specifies seconds

--action-alert \{yes | no\}
Generates an alert when the notification condition is met.

--action-email-owner \{yes | no\}
Specifies that an email be sent to a user when the threshold is crossed. Requires --action-email-address.

--action-email-address <address>
Specifies the email address of user to be notified.

--email-template <path>
Specifies the path in /ifs to the email template.

{--verbose | -v}
Displays more detailed information.

**isi quota settings notifications delete**
Delete a default quota notification rule.

**Syntax**

```bash
isi quota settings notifications delete
   --threshold \{hard | soft | advisory\}
   --condition \{exceeded | denied | violated | expired\}
   [--verbose]
```

**Options**

--threshold
Specifies the threshold type. The following values are valid:

**hard**
Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.

**soft**
Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.
advisory
Sets the advisory threshold. For notification purposes only. Does not enforce
limitations on disk write requests.

--condition
Specifies the quota condition on which to send a notification. The following values
are valid:

denied
Specifies a notification when a hard threshold or soft threshold outside of its
soft grace period causes a disk write operation to be denied.

exceeded
Specifies a notification when disk usage exceeds the threshold. Applies to
only soft thresholds within the soft-grace period.

violated
Specifies a notification when disk usage exceeds a quota threshold but none
of the other conditions apply.

expired
Specifies a notification when disk usage exceeds the soft threshold and the
soft-grace period has expired.

{--verbose | -v}
Displays more detailed information.

isi quota settings notifications list
Displays a list of global quota notification rules.

Syntax

isi quota settings notifications list
  [--limit <integer>]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]

Options

{--limit | -l} <integer>
  Specifies the number of quota notification rules to display.

--format
  Displays quotas in the specified format. The following values are valid:
  table
  json
  csv
list

|--no-header | -a
Suppresses headers in CSV or table formats.

|--no-footer | -z
Suppresses table summary footer information.

|--verbose | -v
Displays more detailed information.

isi quota settings notifications modify
Modifies a quota notification rule.

Syntax

```bash
isi quota settings notifications modify
   --threshold {hard | soft | advisory}
   --condition {exceeded | denied | violated | expired}
   [--schedule <string>]
   [--holdoff <duration>]
   [--clear-holdoff]
   [--action-alert {yes | no}]
   [--action-email-owner {yes | no}]
   [--action-email-address <address>]
   [--email-template <path>]
   [--clear-email-template]
   [--verbose]
```

Options

|--threshold
  Specifies the threshold type. The following values are valid:
  hard
  Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.
  soft
  Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.
  advisory
  Sets the advisory threshold. For notification purposes only. Does not enforce limitations on disk write requests.

|--condition
  Specifies the quota condition on which to send a notification. The following values are valid:
  denied
  Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.
exceeded
Specifies a notification when disk usage exceeds the threshold. Applies to only soft thresholds within the soft-grace period.

violated
Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

expired
Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.

--schedule <string>
Specifies the date pattern at which recurring notifications are made.

--holdoff <duration>
Specify in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>, ...] [of every [{other | <integer>}] week]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} {weekday | <day>} of <month>

Specify <frequency> in one of the following formats:

- at <hh>[:<mm>] [[AM | PM]]
- every [{<integer>}] {hours | minutes} [between <hh>[:<mm>] [[AM | PM]] and <hh>[:<mm>] [[AM | PM]]]
- every [{<integer>}] {hours | minutes} [from <hh>[:<mm>] [[AM | PM]] to <hh>[:<mm>] [[AM | PM]]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month".

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.
Specifies the length of time to wait before generating a notification. Specify `<duration>` in the following format:

```
<integer><units>
```

The following `<units>` are valid:

- **Y**
  - Specifies years
- **M**
  - Specifies months
- **W**
  - Specifies weeks
- **D**
  - Specifies days
- **H**
  - Specifies hours
- **s**
  - Specifies seconds

**--clear-holdoff**

Clears the value for the `--holdoff` duration.

**--action-alert {yes | no}**

Generates an alert when the notification condition is met.

**--action-email-owner {yes | no}**

Specifies that an email be sent to a user when the threshold is crossed. Requires `--action-email-address`.

**--action-email-address <address>**

Specifies the email address of user to be notified.

**{--verbose | -v}**

Displays more detailed information.

**--clear-email-template**

Clears the setting for the path to the email template.

### isi quota settings notifications view

Displays properties of a system default notification rule.

**Syntax**

```
isi quota settings notifications view
   --threshold {hard | soft | advisory}
   --condition {exceeded | denied | violated | expired}
```
Options

--threshold

Specifies the threshold type. The following values are valid:

hard

Sets an absolute limit for disk usage. Attempts to write to disk are generally denied if the request violates the quota limit.

soft

Specifies the soft threshold. Allows writes to disk above the threshold until the soft grace period expires. Attempts to write to disk are denied thereafter.

advisory

Sets the advisory threshold. For notification purposes only. Does not enforce limitations on disk write requests.

--condition

Specifies the quota condition on which to send a notification. The following values are valid:

denied

Specifies a notification when a hard threshold or soft threshold outside of its soft grace period causes a disk write operation to be denied.

exceeded

Specifies a notification when disk usage exceeds the threshold. Applies to only soft thresholds within the soft-grace period.

violated

Specifies a notification when disk usage exceeds a quota threshold but none of the other conditions apply.

expired

Specifies a notification when disk usage exceeds the soft threshold and the soft-grace period has expired.

isi quota settings reports modify

Modifies cluster-wide quota report settings.

Syntax

```
isi quota settings reports modify
   [--schedule <schedule>]
   [--revert-schedule]
   [--scheduled-dir <dir>]
   [--revert-scheduled-dir]
   [--scheduled-retain <integer>]
   [--revert-scheduled-retain]
   [--live-dir <dir> | --revert-live-dir]
   [--live-retain <integer> | --revert-live-retain]
   [--verbose]
```
Options

--schedule <schedule>

Specifies the date pattern at which recurring notifications are made.
Specify in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>[, ...] [of every [{other | <integer>}] week]]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>:<mm> [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>:<mm> [{AM | PM}] and <hh>:<mm> [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>:<mm> [{AM | PM}] to <hh>:<mm> [{AM | PM}]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "saturday" and "sat" are valid.

--revert-schedule

Sets the --schedule value to system default.

--scheduled-dir <dir>

Specifies the location where scheduled quota reports are stored.

--revert-scheduled-dir

Sets the --scheduled-dir value to system default.

--scheduled-retain <integer>

Specifies the maximum number of scheduled reports to keep.
--revert-scheduled-retain
Sets the --scheduled-retain value to system default.

--live-dir <dir>
Specifies the location where live quota reports are stored.

--revert-live-dir
Sets the --live-dir value to system default.

--live-retain <integer>
Specifies the maximum number of live quota reports to keep.

--revert-live-retain
Sets the --live-retain value to system default.

{--verbose | -v}
Displays more detailed information.

**isi quota settings reports view**
Displays cluster-wide quota report settings.

**Syntax**

```bash
isi quota settings reports view
```

**Options**
There are no options for this command.
SmartQuotas
CHAPTER 23

Storage Pools

This section contains the following topics:

- Storage pools overview ................................................................. 880
- Storage pool functions ................................................................. 880
- Autoprovisioning ........................................................................ 882
- Node pools .................................................................................. 883
- Virtual hot spare ........................................................................ 885
- Spillover ..................................................................................... 886
- Suggested protection ................................................................... 886
- Protection policies ........................................................................ 887
- SSD strategies ............................................................................ 887
- Global namespace acceleration .................................................. 888
- L3 cache overview ....................................................................... 889
- Tiers ........................................................................................... 891
- File pool policies .......................................................................... 891
- Managing node pools through the command-line interface ....... 892
- Managing L3 cache from the command-line interface .............. 901
- Managing tiers ............................................................................ 902
- Creating file pool policies .......................................................... 903
- Managing file pool policies ........................................................ 907
- Monitoring storage pools ............................................................ 910
- Storage pool commands ............................................................. 912
Storage pools overview

OneFS organizes different node types into separate node pools. In addition, you can organize these node pools into logical tiers of storage. By activating a SmartPools license, you can create file pool policies that store files in these tiers automatically, based on file-matching criteria that you specify.

Without an active SmartPools license, OneFS manages all node pools as a single pool of storage. File data and metadata is striped across the entire cluster so that data is protected, secure, and readily accessible. All files belong to the default file pool and are governed by the default file pool policy. In this mode, OneFS provides functions such as autoprovisioning, compatibilities, virtual hot spare (VHS), SSD strategies, global namespace acceleration (GNA), L3 cache, and storage tiers.

When you activate a SmartPools license, additional functions become available, including custom file pool policies and spillover management. With a SmartPools license, you can manage your data set with more granularity to improve the performance of your cluster.

The following table summarizes storage pool functions based on whether a SmartPools license is active.

<table>
<thead>
<tr>
<th>Function</th>
<th>Inactive SmartPools license</th>
<th>Active SmartPools license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic storage pool</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node class compatibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(node equivalency)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSD capacity compatibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSD count compatibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual hot spare</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSD strategies</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>L3 cache</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tiers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GNA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File pool policies</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Spillover management</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Storage pool functions

When a cluster is installed, and whenever nodes are added to the cluster, OneFS automatically groups nodes into node pools. Autoprovisioning of nodes into node pools enables OneFS to optimize performance, reliability, and data protection on the cluster.

Without an active SmartPools license, OneFS applies a default file pool policy to organize all data into a single file pool. With this policy, OneFS distributes data across the entire cluster so that data is protected and readily accessible. When you activate a SmartPools license, additional functions become available.
OneFS provides the following functions, with or without an active SmartPools license:

**Autoprovisioning of node pools**
Automatically groups equivalence-class nodes into node pools for optimal storage efficiency and protection. At least three nodes of an equivalence class are required for autoprovisioning to work.

**Node class compatibilities (node equivalency)**
Enables certain nodes that are not equivalence-class to join existing node pools. OneFS supports node class compatibilities between Isilon S200 and S210 nodes, X200 and X210 nodes, X400 and X410 nodes, and NL400 and NL410 nodes. L3 cache must be enabled on the node pools for node class compatibilities to work.

**SSD capacity compatibilities**
Enables nodes with different SSD capacities to be provisioned to an existing compatible node pool. Otherwise, compatible nodes that have different SSD capacities cannot join the same node pool. If you have fewer than three nodes with differences in SSD capacity, these nodes remain unprovisioned, and, therefore, not functional. L3 cache must be enabled on node pools for SSD capacity compatibilities to work.

**SSD count compatibilities**
Enables nodes with different numbers of SSDs to be provisioned to the same node pool. Otherwise, compatible nodes that have different SSD counts cannot join the same node pool. If you have fewer than three nodes with a particular SSD count, these nodes remain unprovisioned, and, therefore, not functional until you create an SSD count compatibility. L3 cache must be enabled on node pools for SSD count compatibilities to work.

**Tiers**
Groups node pools into logical tiers of storage. If you activate a SmartPools license for this feature, you can create custom file pool policies and direct different file pools to appropriate storage tiers.

**Default file pool policy**
Governs all file types and can store files anywhere on the cluster. Custom file pool policies, which require a SmartPools license, take precedence over the default file pool policy.

**Requested protection**
Specifies a requested protection setting for the default file pool, per node pool, or even on individual files. You can leave the default setting in place, or choose the suggested protection calculated by OneFS for optimal data protection.

**Virtual hot spare**
Reserves a portion of available storage space for data repair in the event of a disk failure.

**SSD strategies**
Defines the type of data that is stored on SSDs in the cluster. For example, storing metadata for read/write acceleration.

**L3 cache**
Specifies that SSDs in nodes are used to increase cache memory and speed up file system performance across larger working file sets.
Global namespace acceleration
Activates global namespace acceleration (GNA), which enables data stored on node pools without SSDs to access SSDs elsewhere in the cluster to store extra metadata mirrors. Extra metadata mirrors accelerate metadata read operations.

When you activate a SmartPools license, OneFS provides the following additional functions:

Custom file pool policies
Creates custom file pool policies to identify different classes of files, and stores these file pools in logical storage tiers. For example, you can define a high-performance tier of Isilon S-series node pools and an archival tier of high-capacity Isilon NL400 and HD400 node pools. Then, with custom file pool policies, you can identify file pools based on matching criteria, and you can define actions to perform on these pools. For example, one file pool policy can identify all JPEG files older than a year and store them in an archival tier. Another policy can move all files that were created or modified within the last three months to a performance tier.

Storage pool spillover
Enables automated capacity overflow management for storage pools. Spillover defines how to handle write operations when a storage pool is not writable. If spillover is enabled, data is redirected to a specified storage pool. If spillover is disabled, new data writes fail and an error message is sent to the client that is attempting the write operation.

Storage pool functions supported with IsilonSD Edge
IsilonSD Edge supports only the default file pool policy, requested protection, and virtual hot spare storage pool functions.

Make note of the following considerations before using storage pools with IsilonSD Edge:

- The drives on the IsilonSD nodes are always recognized by IsilonSD Edge as HDDs irrespective of the storage pool that they are hosted on.
- You cannot create heterogeneous nodes within the same IsilonSD cluster.

Autoprovisioning
When you add a node to an Isilon cluster, OneFS attempts to assign the node to a node pool. This process is known as autoprovisioning, which helps OneFS to provide optimal performance, load balancing, and file system integrity across a cluster.

A node is not autoprovisioned to a node pool and made writable until at least three nodes of the same equivalence class are added to the cluster. If you add only two nodes of an equivalence class, no data is stored on these nodes until a third node of the same class is added.

Similarly, if a node goes down or is removed from the cluster so that fewer than three equivalence-class nodes remain, the node pool becomes under-provisioned. In this case, the two remaining nodes are still writable. However, if only one node of an equivalence class remains, this node is not writable, but remains readable.

Over time, as you add new Isilon nodes to your cluster, the new nodes will likely be different from the older nodes in certain ways. For example, the new nodes can be of a different generation, or have different drive configurations. Unless you add three
new nodes of the same equivalence class each time you upgrade your cluster, the new
nodes will not be autoprovisioned.

To work around those restrictions, OneFS enables you to create three types of
compatibilities: node class, SSD capacity, and SSD count. With the appropriate
compatibilities in place, new node types can be provisioned to existing node pools. You
can add nodes one at a time to your cluster, and the new nodes can become fully
functioning peers within existing node pools.

For example, suppose a cluster had a node pool made up of three S200 nodes, and you
purchase an S210 node. In addition to being a different node generation, the S210
node could have a different number and capacity of SSDs. With the appropriate
compatibilities, the new S210 node can be provisioned to the S200 node pool.

Node pools

A node pool is a group of three or more Isilon nodes that forms a single pool of
storage. As you add nodes to your Isilon cluster, OneFS attempts to automatically
provision the new nodes into node pools.

To autoprovision a node, OneFS requires that the new node be of the same
equivalence class as the other nodes in the node pool. OneFS uses the following
criteria to determine if the new node is of the same equivalence class:

- Family code
- Chassis code
- Generation code
- Drive configuration
- RAM capacity

If the new node matches all criteria, OneFS provisions the new node to the node pool.
All nodes in a node pool are peers, and data is distributed across nodes in the pool.
Each provisioned node increases the aggregate disk, cache, CPU, and network
capacity of the cluster.

We strongly recommend that you let OneFS handle node provisioning. However, if you
have a special requirement or use case, you can move nodes from an autoprovisioned
node pool into a node pool that you define manually. The capability to create manually-
declared node pools is available only through the OneFS command-line interface, and
should be deployed only after consulting with EMC Isilon customer support.

If you try to remove a node from a node pool for the purpose of adding it to a manual
node pool, and the result would leave fewer than three nodes in the original node pool,
the removal fails. When you remove a node from a manually-defined node pool, OneFS
attempts to autoprovision the node back into a node pool of the same equivalence
class.

If you add fewer than three nodes of an equivalence class to your cluster, OneFS
cannot autoprovision these nodes. In these cases, you can often create one or more
compatibilities to enable OneFS to provision the newly added nodes to a compatible
node pool.

Types of compatibilities include node class, SSD capacity, and SSD count.

Node class compatibilities

To be autoprovisioned, a node must be of the same equivalence class as the other
nodes in the node pool. If a new node is not of the same equivalence class, you can
enable the node to be provisioned to an existing node pool often by defining a node class compatibility.

If you have existing S200, X200, X400, or NL400 node pools, and you add fewer than three Isilon S210, X210, X410, or NL410 nodes, you can create node class compatibilities to provision the new nodes and make them functional within the cluster. Only S210, X210, X410, and NL410 nodes are currently eligible for node class compatibility with older node generations.

To be provisioned, the new nodes should have the same drive configurations as their older-generation counterparts and must have compatible RAM amounts, as shown in the following table:

<table>
<thead>
<tr>
<th>S200/S210 Compatibility</th>
<th>X200/X210 Compatibility</th>
<th>X400/X410 Compatibility</th>
<th>NL400/NL410 Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>S200 RAM</td>
<td>S210 RAM</td>
<td>X200 RAM</td>
<td>X210 RAM</td>
</tr>
<tr>
<td>24 GB</td>
<td>32 GB</td>
<td>6 GB</td>
<td>Not available</td>
</tr>
<tr>
<td>48 GB</td>
<td>64 GB</td>
<td>12 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>96 GB</td>
<td>128 GB</td>
<td>24 GB</td>
<td>96 GB</td>
</tr>
<tr>
<td>256 GB</td>
<td>48 GB</td>
<td>48 GB</td>
<td>192 GB</td>
</tr>
</tbody>
</table>

If the new nodes have different drive configurations by virtue of having SSDs of varying capacities or counts, you need to create SSD capacity or SSD count compatibilities, in addition to node class compatibilities.

Note

After you have added three or more newer-generation nodes of a particular equivalence class to your cluster, you might want to remove the node class compatibilities that you have created. This step enables OneFS to autoprovision new S210, X210, X410, or NL410 nodes to their own node pools and take advantage of the higher performance specifications of the new node types. However, because larger node pools store data more efficiently, removing compatibilities can also reduce the amount of available storage on your cluster. If you are unsure whether to remove compatibilities, we recommend that you first consult with your EMC Isilon representative.

**SSD compatibilities**

For autoprovisioning to work, OneFS requires that all nodes in a node pool have the same HDD and SSD layouts. OneFS cannot autoprovision new nodes if they have different SSD capacities or SSD counts from the nodes in the existing node pool. To enable new nodes with different SSD capacities or counts to join a compatible node pool, you can create SSD compatibilities.

For example, if your cluster already has an S200 node pool, and you add a new S200 node, OneFS would attempt to autoprovision the new node to the S200 node pool. However, if the new S200 node has higher-capacity SSDs, or a different number of SSDs, than the older S200 nodes, OneFS cannot autoprovision the new node. To enable the new node to be autoprovisioned, you can create SSD compatibilities for the S200 node type.
As with node class compatibilities, SSD compatibilities require the nodes to be compatible, as shown in the following table:

<table>
<thead>
<tr>
<th>Existing node pool</th>
<th>SSD compatibilities that can be created</th>
</tr>
</thead>
<tbody>
<tr>
<td>S200</td>
<td>S200, S210*</td>
</tr>
<tr>
<td>X200</td>
<td>X200, X210*</td>
</tr>
<tr>
<td>X400</td>
<td>X400, X410*</td>
</tr>
<tr>
<td>NL400</td>
<td>NL400, NL410*</td>
</tr>
<tr>
<td>S210</td>
<td>S210, S200*</td>
</tr>
<tr>
<td>X210</td>
<td>X210, X200*</td>
</tr>
<tr>
<td>X410</td>
<td>X410, X400*</td>
</tr>
<tr>
<td>NL410</td>
<td>NL410, NL400*</td>
</tr>
</tbody>
</table>

* Also requires a node class compatibility with the existing node pool class.

Note

For SSD compatibilities to be created, all nodes must have L3 cache enabled. If you attempt to create a node class compatibility and appropriate SSD compatibilities, and the process fails with an error message, make sure that the existing node pool has L3 cache enabled. Then try again to create the compatibility. L3 cache can only be enabled on nodes that have fewer than 16 SSDs.

Manual node pools

If the node pools automatically provisioned by OneFS do not meet your needs, you can configure node pools manually. You do this by moving nodes from an existing node pool into the manual node pool.

This capability enables you to store data on specific nodes according to your purposes, and is available only through the OneFS command-line interface.

⚠️ CAUTION

It is recommended that you enable OneFS to provision nodes automatically. Manually created node pools might not provide the same performance and efficiency as automatically managed node pools, particularly if your changes result in fewer than 20 nodes in the manual node pool.

Virtual hot spare

Virtual hot spare (VHS) settings enable you to reserve disk space to rebuild the data in the event that a drive fails.

You can specify both a number of virtual drives to reserve and a percentage of total storage space. For example, if you specify two virtual drives and 15 percent, each node pool reserves virtual drive space equivalent to two drives or 15 percent of their total capacity (whichever is larger).

You can reserve space in node pools across the cluster for this purpose by specifying the following options:

- At least 1–4 virtual drives.
• At least 0–20% of total storage.

OneFS calculates the larger number of the two factors to determine the space that is allocated. When configuring VHS settings, be sure to consider the following information:

• If you deselect the option to **Ignore reserved space when calculating available free space** (the default), free-space calculations include the space reserved for VHS.

• If you deselect the option to **Deny data writes to reserved disk space** (the default), OneFS can use VHS for normal data writes. We recommend that you leave this option selected, or data repair can be compromised.

• If **Ignore reserved space when calculating available free space** is enabled while **Deny data writes to reserved disk space** is disabled, it is possible for the file system to report utilization as more than 100 percent.

---

**Note**

VHS settings affect spillover. If the VHS option **Deny data writes to reserved disk space** is enabled while **Ignore reserved space when calculating available free space** is disabled, spillover occurs before the file system reports 100% utilization.

---

**Spillover**

When you activate a SmartPools license, you can designate a node pool or tier to receive spillover data when the hardware specified by a file pool policy is full or otherwise not writable.

If you do not want data to spill over to a different location because the specified node pool or tier is full or not writable, you can disable this feature.

---

**Note**

Virtual hot spare reservations affect spillover. If the setting **Deny data writes to reserved disk space** is enabled, while **Ignore reserved space when calculating available free space** is disabled, spillover occurs before the file system reports 100% utilization.

---

**Suggested protection**

Based on the configuration of your Isilon cluster, OneFS automatically calculates the amount of protection that is recommended to maintain EMC Isilon's stringent data protection requirements.

OneFS includes a function to calculate the suggested protection for data to maintain a theoretical mean-time to data loss (MTTDL) of 5000 years. Suggested protection provides the optimal balance between data protection and storage efficiency on your cluster.

By configuring file pool policies, you can specify one of multiple requested protection settings for a single file, for subsets of files called file pools, or for all files on the cluster.

It is recommended that you do not specify a setting below suggested protection. OneFS periodically checks the protection level on the cluster, and alerts you if data falls below the recommended protection.
Protection policies

OneFS provides a number of protection policies to choose from when protecting a file or specifying a file pool policy.

The more nodes you have in your cluster, up to 20 nodes, the more efficiently OneFS can store and protect data, and the higher levels of requested protection the operating system can achieve. Depending on the configuration of your cluster and how much data is stored, OneFS might not be able to achieve the level of protection that you request. For example, if you have a three-node cluster that is approaching capacity, and you request +2n protection, OneFS might not be able to deliver the requested protection.

The following table describes the available protection policies in OneFS.

<table>
<thead>
<tr>
<th>Protection policy</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1n</td>
<td>Tolerate the failure of 1 drive or the failure of 1 node</td>
</tr>
<tr>
<td>+2d:1n</td>
<td>Tolerate the failure of 2 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+2n</td>
<td>Tolerate the failure of 2 drives or the failure of 2 nodes</td>
</tr>
<tr>
<td>+3d:1n</td>
<td>Tolerate the failure of 3 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+3d:1n1d</td>
<td>Tolerate the failure of 3 drives or the failure of 1 node and 1 drive</td>
</tr>
<tr>
<td>+3n</td>
<td>Tolerate the failure of 3 drives or the failure of 3 nodes</td>
</tr>
<tr>
<td>+4d:1n</td>
<td>Tolerate the failure of 4 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+4d:2n</td>
<td>Tolerate the failure of 4 drives or the failure of 2 nodes</td>
</tr>
<tr>
<td>+4n</td>
<td>Tolerate the failure of 4 drives or the failure of 4 nodes</td>
</tr>
<tr>
<td>Mirrors: 2x</td>
<td>Duplicates, or mirrors, data over the specified number of nodes. For example, 2x results in two copies of each data block.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>Mirrors can use more data than the other protection policies, but might be an effective way to protect files that are written non-sequentially or to provide faster access to important files.</td>
</tr>
<tr>
<td>Mirrors: 3x</td>
<td></td>
</tr>
<tr>
<td>Mirrors: 4x</td>
<td></td>
</tr>
<tr>
<td>Mirrors: 5x</td>
<td></td>
</tr>
<tr>
<td>Mirrors: 6x</td>
<td></td>
</tr>
<tr>
<td>Mirrors: 7x</td>
<td></td>
</tr>
<tr>
<td>Mirrors: 8x</td>
<td></td>
</tr>
</tbody>
</table>

SSD strategies

OneFS clusters can contain nodes that include solid-state drives (SSD). OneFS autoprovisions equivalence-class nodes with SSDs into one or more node pools. The SSD strategy defined in the default file pool policy determines how SSDs are used within the cluster, and can be set to increase performance across a wide range of workflows.

You can configure file pool policies to apply specific SSD strategies as needed. When you select SSD options during the creation of a file pool policy, you can identify the files in the OneFS cluster that require faster or slower performance. When the
SmartPools job runs, OneFS uses file pool policies to move this data to the appropriate storage pool and drive type.

The following SSD strategy options that you can set in a file pool policy are listed in order of slowest to fastest choices:

**Avoid SSDs**

Writes all associated file data and metadata to HDDs only.

---

**CAUTION**

Use this option to free SSD space only after consulting with Isilon Technical Support personnel. Using this strategy can negatively affect performance.

---

**Metadata read acceleration**

Writes both file data and metadata to HDDs. This is the default setting. An extra mirror of the file metadata is written to SSDs, if available. The SSD mirror is in addition to the number of mirrors, if any, required to satisfy the requested protection.

**Metadata read/write acceleration**

Writes file data to HDDs and metadata to SSDs, when available. This strategy accelerates metadata writes in addition to reads but requires about four to five times more SSD storage than the Metadata read acceleration setting. Enabling GNA does not affect read/write acceleration.

**Data on SSDs**

Uses SSD node pools for both data and metadata, regardless of whether global namespace acceleration is enabled. This SSD strategy does not result in the creation of additional mirrors beyond the normal requested protection but requires significantly increased storage requirements compared with the other SSD strategy options.

---

**Global namespace acceleration**

Global namespace acceleration (GNA) enables data on node pools without SSDs to have additional metadata mirrors on SSDs elsewhere in the cluster. Metadata mirrors on SSDs can improve file system performance by accelerating metadata read operations.

You can enable GNA only if 20 percent or more of the nodes in the cluster contain at least one SSD and 1.5 percent or more of total cluster storage is SSD-based. For best results, before enabling GNA, make sure that at least 2.0 percent of total cluster storage is SSD-based.

Even when enabled, GNA becomes inactive if the ratio of SSDs to HDDs falls below the 1.5 percent threshold, or if the percentage of nodes containing at least one SSD falls below 20 percent. GNA is reactivated when those requirements are met again. While GNA is inactive in such cases, existing SSD mirrors are readable, but newly written metadata does not get the extra SSD mirror.
Note
Node pools with L3 cache enabled are effectively invisible for GNA purposes. All ratio calculations for GNA are done exclusively for node pools without L3 cache enabled. So, for example, if you have six node pools on your cluster, and three of them have L3 cache enabled, GNA is applied only to the three remaining node pools without L3 cache enabled. On node pools with L3 cache enabled, metadata does not need an additional GNA mirror, because metadata access is already accelerated by L3 cache.

L3 cache overview

You can configure nodes with solid-state drives (SSDs) to increase cache memory and speed up file system performance across larger working file sets.

OneFS caches file data and metadata at multiple levels. The following table describes the types of file system cache available on an Isilon cluster.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Profile</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1 cache</td>
<td>RAM</td>
<td>Volatile</td>
<td>Local node</td>
<td>Also known as front-end cache, holds copies of file system metadata and data requested by the front-end network through NFS, SMB, HTTP, and so on.</td>
</tr>
<tr>
<td>L2 cache</td>
<td>RAM</td>
<td>Volatile</td>
<td>Global</td>
<td>Also known as back-end cache, holds copies of file system metadata and data on the node that owns the data.</td>
</tr>
<tr>
<td>SmartCache</td>
<td>Variable</td>
<td>Non-volatile</td>
<td>Local node</td>
<td>Holds any pending changes to front-end files waiting to be written to storage. This type of cache protects write-back data through a combination of RAM and stable storage.</td>
</tr>
<tr>
<td>L3 cache</td>
<td>SSD</td>
<td>Non-volatile</td>
<td>Global</td>
<td>Holds file data and metadata released from L2 cache, effectively increasing L2 cache capacity.</td>
</tr>
</tbody>
</table>

OneFS caches frequently accessed file and metadata in available random access memory (RAM). Caching enables OneFS to optimize data protection and file system performance. When RAM cache reaches capacity, OneFS normally discards the oldest cached data and processes new data requests by accessing the storage drives. This cycle is repeated each time RAM cache fills up.

You can deploy SSDs as L3 cache to reduce the cache cycling issue and further improve file system performance. L3 cache adds significantly to the available cache memory and provides faster access to data than hard disk drives (HDD).

As L2 cache reaches capacity, OneFS evaluates data to be released and, depending on your workflow, moves the data to L3 cache. In this way, much more of the most frequently accessed data is held in cache, and overall file system performance is improved.

For example, consider a cluster with 128GB of RAM. Typically the amount of RAM available for cache fluctuates, depending on other active processes. If 50 percent of RAM is available for cache, the cache size would be approximately 64GB. If this same cluster had three nodes, each with two 200GB SSDs, the amount of L3 cache would be 1.2TB, approximately 18 times the amount of available L2 cache.
L3 cache is enabled by default for new node pools. A node pool is a collection of nodes that are all of the same equivalence class, or for which compatibilities have been created. L3 cache applies only to the nodes where the SSDs reside. For the HD400 node, which is primarily for archival purposes, L3 cache is on by default and cannot be turned off. On the HD400, L3 cache is used only for metadata.

If you enable L3 cache on a node pool, OneFS manages all cache levels to provide optimal data protection, availability, and performance. In addition, in case of a power failure, the data on L3 cache is retained and still available after power is restored.

**Note**

Although some benefit from L3 cache is found in workflows with streaming and concurrent file access, L3 cache provides the most benefit in workflows that involve random file access.

**Migration to L3 cache**

L3 cache is enabled by default on new nodes. If you are upgrading your cluster from an older release (pre-OneFS 7.1.1), you must enable L3 cache manually on node pools that have SSDs. When you enable L3 cache, OneFS activates a process that migrates SSDs from storage disks to cache. File data currently on SSDs is moved elsewhere in the cluster.

You can enable L3 cache as the default for all new node pools or manually for a specific node pool, either through the command line or from the web administration interface. You can enable L3 cache only on node pools whose nodes have SSDs.

Depending on the amount of data stored in your SSDs, the migration process can take some time. OneFS displays a message informing you that the migration is about to begin:

**WARNING:** Changes to L3 cache configuration can have a long completion time. If this is a concern, please contact EMC Isilon Support for more information.

You must confirm whether OneFS should proceed with the migration. After you do, OneFS handles the migration intelligently as a background process. You can continue to administer your cluster during the migration.

If you choose to disable L3 cache on a node pool, the migration process is very fast.

**L3 cache on NL-series and HD-series node pools**

The HD-series and NL-series nodes are high-capacity units designed primarily for archival workflows. Archival workflows feature a higher percentage of data writes compared to data reads, and L3 cache with SSDs can improve significantly the speed of file system traversal activities such as directory lookup.

L3 cache is turned on by default on HD-series and NL-series node pools.

For NL-series nodes with hard-disk drives (HDD) smaller than 4 TB in capacity, L3 cache stores both data and metadata in SSDs by default. You can turn off L3 cache on NL-series nodes with 4 TB or smaller HDDs. However, we recommend that you leave L3 cache enabled, as NL-series nodes typically do not have large numbers of SSDs. From a performance perspective, the benefits of L3 cache outweigh the benefits of using SSDs as storage drives on these nodes.

For NL-series nodes with HDDs greater than 4 TB in capacity, and for all HD-series nodes, L3 cache stores metadata only in SSDs and cannot be disabled. L3 cache with
metadata only stored in SSDs provides the best performance for archiving data on these high-capacity nodes.

Tiers

A tier is a user-defined collection of node pools that you can specify as a storage pool for files. A node pool can belong to only one tier.

You can create tiers to assign your data to any of the node pools in the tier. For example, you can assign a collection of node pools to a tier specifically created to store data that requires high availability and fast access. In a three-tier system, this classification may be Tier 1. You can classify data that is used less frequently or that is accessed by fewer users as Tier-2 data. Tier 3 usually comprises data that is seldom used and can be archived for historical or regulatory purposes.

File pool policies

File pool policies define sets of files—file pools—and where and how they are stored on your cluster. You can configure multiple file pool policies with filtering rules that identify specific file pools and the requested protection and I/O optimization settings for these file pools. Creating custom file pool policies requires an active SmartPools license.

The initial installation of OneFS places all files into a single file pool, which is subject to the default file pool policy. Without an active SmartPools license, you can configure only the default file pool policy, which controls all files and stores them anywhere on the cluster.

With an active SmartPools license, OneFS augments basic storage functions by enabling you to create custom file pool policies that identify, protect, and control multiple file pools. With a custom file pool policy, for example, you can define and store a file pool on a specific node pool or tier for fast access or archival purposes.

When you create a file pool policy, flexible filtering criteria enable you to specify time-based attributes for the dates that files were last accessed, modified, or created. You can also define relative time attributes, such as 30 days before the current date. Other filtering criteria include file type, name, size, and custom attributes. The following examples demonstrate a few ways you can configure file pool policies:

- A file pool policy to set stronger protection on a specific set of important files.
- A file pool policy to store frequently accessed files in a node pool that provides the fastest reads or read/writes.
- A file pool policy to evaluate the last time files were accessed, so that older files are stored in a node pool best suited for regulatory archival purposes.

When the SmartPools job runs, typically once a day, it processes file pool policies in priority order. You can edit, reorder, or remove custom file pool policies at any time. The default file pool policy, however, is always last in priority order. Although you can edit the default file pool policy, you cannot reorder or remove it. When custom file pool policies are in place, the settings in the default file pool policy apply only to files that are not covered by another file pool policy.

When a new file is created, OneFS chooses a storage pool based on the default file pool policy, or, if it exists, a higher-priority custom file pool policy that matches the file. If a new file was originally matched by the default file pool policy, and you later create a custom file pool policy that matches the file, the file will be controlled by the
Managing node pools through the command-line interface

You can manage node pools through the command-line interface. You can work with node pools that are automatically provisioned, create and manage manual node pools, and create node class and SSD compatibilities for new nodes.

A node pool, whether automatically provisioned or manually created, must contain a minimum of three equivalent or compatible nodes. Nodes are provisioned when at least three equivalent or compatible nodes are added to the cluster. If you add only two equivalent or compatible nodes to a cluster, you cannot store data on the nodes until you add a third node.

OneFS provides node class compatibilities and SSD compatibilities, which you can create to enable compatible nodes to become members of an existing node pool. After you create a compatibility, any time a new compatible node is added to the cluster, OneFS provisions the new node to the appropriate node pool.

You can create a node pool manually only by selecting a subset of equivalence-class or compatible nodes from a single autoprovisioned node pool. You cannot create a manual node pool that takes some nodes from one node pool and some nodes from another.

You must have the ISI_PRIV_SMARTPOOLS or greater administrative privilege to manage node pools.

Create a node class compatibility

OneFS attempts to add new nodes to an existing node pool of the same equivalence class. For a new node that is not of the same equivalence class, you can create a node class compatibility, which enables a new node to be provisioned to a compatible node pool.

A new node must be provisioned to be functional within a cluster. The following compatibilities are currently supported: S200/S210, X200/X210, X400/X410, and NL400/NL410. For example, if you have a node pool made up of three or more S200 nodes, you can create a compatibility so that new S210 nodes will be provisioned to the S200 node pool.

Note

- New nodes must have compatible RAM and the same drive configurations as their older counterparts to be provisioned into those node pools. If drive configurations are not the same because of SSD capacity or SSD count differences, you can create SSD compatibilities, as well.
- You cannot create a node class compatibility if you are running IsilonSD Edge.

Procedure

1. Run the `isi storagepool compatibilities class active create` command.
The following command creates a compatibility between Isilon NL400 and NL410 nodes. Note that, in CLI commands, NL400 and NL410 nodes should be specified as N400 and N410.

```
isi storagepool compatibilities class active create N400 N410
```

OneFS provides a summary of the results of executing the command, and requires you to confirm the operation.

2. To proceed, type `yes`, and then press ENTER.

**Results**

OneFS attempts to add any unprovisioned NL410 nodes to the NL400 node pool. If the new nodes remain unprovisioned, either L3 cache is turned off for the targeted node pool, or you still need to create an SSD compatibility for the new nodes.

---

**Merge compatible node pools**

You can merge multiple compatible node pools to optimize storage efficiency on your cluster.

For example, if you have six S200 nodes in one node pool and three S210 nodes in a second node pool, you can create a compatibility to merge the two node pools into one pool of nine nodes. Larger node pools, up to approximately 20 nodes, enable OneFS to protect data more efficiently, therefore providing more storage space for new data.

**Note**

- Newer node types typically have better performance specifications than older node types, so merging them with older node types can reduce performance. Also, when two node pools are merged, OneFS restripes the data, which can take considerable time, depending on the size of your data set.
- You cannot merge multiple compatible node pools if you are running IsilonSD Edge.

**Procedure**

1. Run the `isi storagepool compatibilities class active create` command.

   The following command creates a compatibility between Isilon X400 and X410 node pools:

   ```
   isi storagepool compatibilities class active create X400 X410
   ```

   OneFS provides a summary of the results of executing the command, including the node pools that will be merged, and requires you to confirm the operation.

2. To proceed, type `yes`, and then press ENTER.

**Results**

The compatible node pools are merged into one node pool. If the node pools were not merged, either L3 cache is turned off for one of the node pools, or you still need to create an SSD compatibility between the two node pools.
Delete a node class compatibility

You can delete a node class compatibility. As a result, any nodes that were provisioned to a node pool because of this compatibility are removed from the node pool.

⚠️ CAUTION

Deleting a node class compatibility could result in unintended consequences. For example, if you delete a compatibility, and fewer than three compatible nodes are removed from the node pool, those nodes will be removed from your cluster's available pool of storage. The next time the SmartPools job runs, data on those nodes would be restriped elsewhere on the cluster, which could be a time-consuming process. If three or more compatible nodes are removed from the node pool, these nodes will form their own node pool, and data will be restriped. Any file pool policy pointing to the original node pool will now point to the node pool's tier, if one existed, or, otherwise, to a new tier created by OneFS.

Skip these steps if you are running IsilonSD Edge.

Procedure

1. Determine the ID number of the active compatibility that you intend to delete.
   The following command lists active compatibilities and their ID numbers:

   ```plaintext
   isi storagepool compatibilities class active list
   ```

2. Run the `isi storagepool compatibilities class active delete` command.
   The following command deletes a node class compatibility with an ID number of 1:

   ```plaintext
   isi storagepool compatibilities class active delete 1
   ```

   OneFS provides a summary of the results of executing the command, including the node pools that will be affected by the compatibility removal, and requires you to confirm the operation.

3. To proceed, type `yes`, and then press ENTER.

Results

OneFS splits any merged node pools, or unprovisions any previously compatible nodes that are fewer than three in number.

Create an SSD compatibility

You can create compatibilities both for SSD capacity and SSD count to enable new nodes to be provisioned to node pools with different SSD specifications. SSD compatibilities can be created for the following node types: S200, S210, X200, X210, X400, X410, NL400, and NL410.

For example, if you have a node pool made up of three S200 nodes with 100GB SSDs, and you install an S200 node with an equal number of 200GB SSDs, the new S200 node is not autoprovisioned to the S200 node pool until you create an SSD class compatibility. If the nodes of the S200 node pool each have six SSDs, and the new S200 node has eight SSDs, you must also create an SSD count compatibility to enable
the new S200 node to be provisioned to the S200 node pool. Similarly, if you have
different generation nodes that are class-compatible, such as S200 and S210 nodes,
you can create SSD compatibilities between those node types, as well.

Note
Skip this procedure if you are running IsilonSD Edge.

Procedure
1. Run the `isi storagepool compatibilities ssd active create` command.
   The following command creates an SSD class compatibility for Isilon S200
   nodes that have different capacity SSDs:
   ```
   isi storagepool compatibilities ssd active create S200
   ```
   The following command creates an SSD count compatibility for Isilon S200
   nodes that have a different number of SSDs:
   ```
   isi storagepool compatibilities ssd active create S200 --
   count true
   ```
   The following command creates both an SSD class compatibility and an SSD
   count compatibility between NL400 and NL410 nodes. Note that, in CLI
   commands, NL400 and NL410 are expressed as N400 and N410.
   ```
   isi storagepool compatibilities ssd active create N400 --
   class-2 N410 --count true
   ```
   OneFS provides a summary of the results of executing the command, and
   requires you to confirm the operation.
   2. To proceed with the operation, type `yes`, and then press ENTER.

Results
The SSD compatibility is created.

Delete an SSD compatibility
You can delete an SSD compatibility. If you do this, any nodes that are part of a node
pool because of this compatibility are removed from the node pool.

⚠️ CAUTION
Deleting an SSD compatibility could result in unintended consequences. For
example, if you delete an SSD compatibility, and fewer than three compatible
nodes are removed from a node pool as a result, these nodes are removed from
your cluster's available pool of storage. The next time the SmartPools job runs,
data on those nodes is restriped elsewhere on the cluster, which could be a time-
consuming process. If three or more compatible nodes are removed from the
node pool, these nodes form their own node pool, but data is restriped. Any file
pool policy pointing to the original node pool points instead to the node pool's
tier, if one existed, or, otherwise, to a new tier created by OneFS.

Skip this procedure if you are running IsilonSD Edge.
Procedure

1. Run the `isi storagepool compatibilities ssd active delete` command.

   You can run the `isi storagepool compatibilities ssd active list` command to determine the ID number of active compatibilities.

   The following command deletes an SSD compatibility with an ID number of 1:

   ```
   isi storagepool compatibilities ssd active delete 1
   ```

   The following command deletes an ssd compatibility between two different Isilon models:

   ```
   isi storagepool compatibilities ssd active delete 1 --id-2 2
   ```

   Before executing your command, OneFS provides a summary of the results and requires you to confirm the operation.

2. To proceed, type `yes`, and then press ENTER. To cancel, type `no`, and then press ENTER.

Results

If you proceed with the operation, OneFS splits any merged node pools, or unprovisions any previously compatible nodes fewer than three in number.

Create a node pool manually

You can create node pools manually if autoprosioning does not meet your requirements.

When you add new nodes to your cluster, OneFS places these nodes into node pools. This process is called autoprosioning. For some workflows, you might prefer to create node pools manually. A manually created node pool must have at least three nodes, identified by the logical node numbers (LNNs).

**CAUTION**

It is recommended that you enable OneFS to provision nodes automatically. Manually created node pools might not provide the same performance and efficiency as automatically managed node pools, particularly if your changes result in fewer than 20 nodes in the manual node pool.

Procedure

1. Run the `isi storagepool nodepools create` command.

   You can specify the nodes to be added to a nodepool by a comma-delimited list of LNNs (for example, `--lnns 1,2,5`) or by using ranges (for example, `--lnns 5-8`).

   The following command creates a node pool by specifying the LNNs of three nodes to be included.

   ```
   isi storagepool nodepools create PROJECT-1 --lnns 1,2,5
   ```
Add a node to a manually managed node pool

You can add a node to a manually managed node pool.

If you specify a node that is already part of another node pool, OneFS removes the node from the original node pool and adds it to the manually managed node pool.

Procedure

1. Run the `isi storagepool nodepools modify` command.

   The following command adds nodes with the LNNs (logical node numbers) of 3, 4, and 10 to an existing node pool:

   ```
   isi storagepool nodepools modify PROJECT-1 --lnns 3-4, 10
   ```

Change the name or protection policy of a node pool

You can change the name or protection policy of a node pool.

Procedure

1. Run the `isi storagepool nodepools modify` command.

   The following command changes the name and protection policy of a node pool:

   ```
   isi storagepool nodepools modify PROJECT-1 --set-name PROJECT-A --protection-policy +2:1
   ```

Remove a node from a manually managed node pool

You can remove a node from a manually managed node pool.

If you attempt to remove nodes from either a manually managed or automatically managed node pool so that the removal leaves only one or two nodes in the pool, the removal fails. You can, however, move all nodes from an autoprovisioned node pool into one that is manually managed.

When you remove a node from the manually managed node pool, OneFS autoprovisions the node into another node pool of the same equivalence class.

Procedure

1. Run the `isi storagepool nodepools modify` command.

   The following command removes two nodes, identified by its LNNs (logical node numbers) from a node pool.

   ```
   isi storagepool nodepools modify ARCHIVE_1 --remove-lnns 3,6
   ```

   LNN values can be specified as a range, for example, `--lnns=1-3`, or in a comma-separated list, for example, `--lnns=1,2,5,9`. 
Modify default storage pool settings

You can modify default storage pool settings for requested protection, I/O optimization, global namespace acceleration, virtual hot spare, and spillover.

Procedure

1. Run the `isi storagepool settings modify` command.

   The following command specifies automatic file protection and I/O optimization, disables global namespace acceleration, specifies a percentage of storage for a virtual hot spare, and enables L3 cache for node pools with SSDs:

   ```
   isi storagepool settings modify
   --automatically-manage-protection files_at_default
   --automatically-manage-io-optimization files_at_default
   --global-namespace-acceleration-enabled no
   --virtual-hot-spare-limit-percent 5
   --ssd-l3-cache-default-enabled yes
   ```

Results

OneFS applies your changes to any files managed by the default file pool policy the next time the SmartPools job runs.

SmartPools settings

SmartPools settings include directory protection, global namespace acceleration, L3 cache, virtual hot spare, spillover, requested protection management, and I/O optimization management.

<table>
<thead>
<tr>
<th>Settings in Web Admin</th>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Increase directory protection to a higher level than its contents</strong></td>
<td>--protect-directories-one-level-higher</td>
<td>Increases the amount of protection for directories at a higher level than the directories and files that they contain, so that data that is not lost can still be accessed. When device failures result in data loss (for example, three drives or two nodes in a +2:1 policy), enabling this setting ensures that intact data is still accessible.</td>
<td>This setting should be enabled (the default). When this setting is disabled, the directory that contains a file pool is protected according to your protection-level settings, but the devices used to store the directory and the file may not be the same. There is potential to lose nodes with file data intact but not be able to access the data because those nodes contained the directory. As an example, consider a cluster that has a +2 default file pool protection setting and no additional file pool policies. OneFS directories are always mirrored, so they are stored at 3x, which is the mirrored equivalent of the +2 default. This configuration can sustain a failure of two nodes before data...</td>
</tr>
<tr>
<td>Settings in Web Admin</td>
<td>Settings in CLI</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Enable global namespace acceleration</strong></td>
<td>--global-namespace-acceleration-enabled</td>
<td>Specifies whether to allow per-file metadata to use SSDs in the node pool.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When disabled, restricts per-file metadata to the storage pool policy of the file, except in the case of spillover. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, allows per-file metadata to use the SSDs in any node pool.</td>
<td></td>
</tr>
<tr>
<td><strong>Use SSDs as L3 Cache by default for new node pools</strong></td>
<td>--ssd-l3-cache-default-enabled</td>
<td>For node pools that include solid-state drives, deploy the SSDs as L3 cache. L3 cache extends L2 cache and speeds up file system performance across larger working file sets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>L3 cache is enabled by default on new node pools. When you enable L3 cache on an existing node pool, OneFS performs a migration, moving any existing data on the SSDs to other locations on the cluster. This setting is not applicable for IsilonSD Edge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OneFS manages all cache levels to provide optimal data protection, availability, and performance. In case of a power failure, the data on L3 cache is protected.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Node pools with L3 cache enabled are effectively invisible for GNA purposes. All ratio calculations for GNA are done exclusively for node pools without L3 cache enabled.
## Settings in Web
Admin

## Settings in CLI

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Virtual Hot Spare**| Reserves a minimum amount of space in the node pool that can be used for data repair in the event of a drive failure. To reserve disk space for use as a virtual hot spare, select from the following options:  
  - **Ignore reserved disk space when calculating available free space.** Subtracts the space reserved for the virtual hot spare when calculating available free space.  
  - **Deny data writes to reserved disk space.** Prevents write operations from using reserved disk space.  
  - **VHS Space Reserved.** You can reserve a minimum number of virtual drives (1-4), as well as a minimum percentage of total disk space (0-20%). If you configure both the minimum number of virtual drives and a minimum percentage of total disk space when you configure reserved VHS space, the enforced minimum value satisfies both requirements. If this setting is enabled and **Deny new data writes** is disabled, it is possible for the file system utilization to be reported at more than 100%. |
| **Enable global spillover** | Specifies how to handle write operations to a node pool that is not writable. | • When enabled, redirects write operations from a node pool that is not writable either to another node pool or anywhere on the cluster (the default).  
• When disabled, returns a disk space error for write operations to a node pool that is not writable. |
| **Spillover Data Target** | Specifies another storage pool to target when a storage pool is not writable. | When spillover is enabled, but it is important that data writes do not fail, select **anywhere** for the **Spillover Data Target** setting, even if file pool policies send data to specific pools. |
| **Manage protection settings** | When this setting is enabled, SmartPools manages requested protection levels automatically. | When **Apply to files with manually-managed protection** is enabled, |
### Settings in Web Admin

### Settings in CLI

<table>
<thead>
<tr>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>overwrites any protection settings that were configured through File System Explorer or the command-line interface.</td>
<td></td>
</tr>
</tbody>
</table>

| Manage I/O optimization settings | --automatically-manage-io-optimization | When enabled, uses SmartPools technology to manage I/O optimization. | When **Apply to files with manually-managed I/O optimization settings** is enabled, overwrites any I/O optimization settings that were configured through File System Explorer or the command-line interface. |

---

**Managing L3 cache from the command-line interface**

L3 cache can be administered globally or on specific node pools. If you choose to, you can also revert SSDs back to storage drives. In Isilon HD400 node pools, SSDs are exclusively for L3 cache purposes. On these nodes, L3 cache is turned on by default and cannot be turned off.

**Set L3 cache as the default for new node pools**

You can set L3 cache as the default, so that when new node pools are created, L3 cache is enabled automatically.

**Before you begin**

L3 cache is effective only on nodes that include SSDs. If none of your nodes has SSD storage, there is no need to enable L3 cache as the default.

**Procedure**

1. Run the `isi storagepool settings modify` command.

   The following command sets L3 cache enabled as the default for new node pools that are added.

   ```bash
   isi storagepool settings modify --ssd-l3-cache-default-enabled yes
   ```

2. Run the `isi storagepool settings view` command to confirm that the SSD L3 Cache Default Enabled attribute is set to **Yes**.

**Enable L3 cache on a specific node pool**

You can enable L3 cache for a specific node pool. This is useful when only some of your node pools are equipped with SSDs.

**Procedure**

1. Run the `isi storagepool nodepools modify` command on a specific node pool.
The following command enables L3 cache on a node pool named hq_datastore:

```
isi storagepool nodepools modify hq_datastore --l3 true
```

If the SSDs on the specified node pool previously were used as storage drives, a message appears asking you to confirm the change.

2. If prompted, type `yes`, and then press ENTER.

**Restore SSDs to storage drives for a node pool**

You can disable L3 cache for SSDs on a specific node pool and restore those SSDs to storage drives.

**Note**

On HD400 node pools, SSDs are used only for L3 cache, which is turned on by default and cannot be turned off. If you attempt to turn off L3 cache on an HD400 node pool through the command-line interface, OneFS generates this error message: Disabling L3 not supported for the given node type.

**Procedure**

1. Run the `isi storagepool nodepools modify` command on a specific node pool.

   The following command disables L3 cache on a node pool named hq_datastore:

   ```
   isi storagepool nodepools modify hq_datastore --l3 false
   ```

2. At the confirmation prompt, type `yes`, and then press ENTER.

**Managing tiers**

You can move node pools into tiers to optimize file and storage management.

Managing tiers requires `ISI_PRIV_SMARTPOOLS` or higher administrative privileges.

**Create a tier**

You can create a tier to group together one or more node pools for specific storage purposes.

Depending on the types of nodes in your cluster, you can create tiers for different categories of storage, for example, an archive tier, performance tier, or general-use tier. After creating a tier, you need to add the appropriate node pools to the tier.

**Procedure**

1. Run the `isi storagepool tiers create` command.

   The following command creates a tier named ARCHIVE_1, and adds node pools named hq_datastore1 and hq_datastore2 to the tier.

   ```
   isi storagepool tiers create ARCHIVE_1 --children
   hq_datastore1
   --children hq_datastore2
   ```
Add or move node pools in a tier

You can group node pools into tiers and move node pools from one tier to another.

Procedure

1. Run the `isi storagepool nodepools modify` command.

   The following example adds a node pool named PROJECT-A to a tier named ARCHIVE_1.

   ```bash
   isi storagepool nodepools modify PROJECT-A --tier ARCHIVE_1
   ```

   If the node pool, PROJECT-A, happened to be in another tier, the node pool would be moved to the ARCHIVE_1 tier.

Rename a tier

A tier name can contain alphanumeric characters and underscores but cannot begin with a number.

Procedure

1. Run the `isi storagepool tiers modify` command.

   The following command renames a tier from ARCHIVE_1 to ARCHIVE_A:

   ```bash
   isi storagepool tiers modify ARCHIVE_1 --set-name ARCHIVE_A
   ```

Delete a tier

When you delete a tier, its node pools remain available and can be added to other tiers.

Procedure

1. Run the `isi storagepool tiers delete` command.

   The following command deletes a tier named ARCHIVE_A:

   ```bash
   isi storagepool tiers delete ARCHIVE_A
   ```

Creating file pool policies

You can configure file pool policies to identify logical groups of files called file pools, and you can specify storage operations for these files.

Before you can create file pool policies, you must activate a SmartPools license, and you must have the SmartPools or higher administrative privilege.

File pool policies have two parts: file-matching criteria that define a file pool, and the actions to be applied to the file pool. You can define file pools based on characteristics, such as file type, size, path, birth, change, and access timestamps, and combine these criteria with Boolean operators (AND, OR).

In addition to file-matching criteria, you can identify a variety of actions to apply to the file pool. These actions include:

- Setting requested protection and data-access optimization parameters
• Identifying data and snapshot storage targets
• Defining data and snapshot SSD strategies
• Enabling or disabling SmartCache

For example, to free up disk space on your performance tier (S-series node pools), you could create a file pool policy to match all files greater than 25 MB in size, which have not been accessed or modified for more than a month, and move them to your archive tier (NL-series node pools).

You can configure and prioritize multiple file pool policies to optimize file storage for your particular work flows and cluster configuration. When the SmartPools job runs, by default once a day, it applies file pool policies in priority order. When a file pool matches the criteria defined in a policy, the actions in that policy are applied, and lower-priority custom policies are ignored for the file pool.

After the list of custom file pool policies is traversed, if any of the actions are not applied to a file, the actions in the default file pool policy are applied. In this way, the default file pool policy ensures that all actions apply to every file.

**Note**

You can reorder the file pool policy list at any time, but the default file pool policy is always last in the list of file pool policies.

OneFS also provides customizable template policies that you can copy to make your own policies. These templates, however, are only available from the OneFS web administration interface.

### Create a file pool policy

You can create a file pool policy to match specific files and apply SmartPools actions to the matched file pool. SmartPools actions include moving files to certain storage tiers, changing the requested protection levels, and optimizing write performance and data access.

**CAUTION**

If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies that match this data with anywhere for the --data-storage-target setting. Because the specified storage pool is included when you use anywhere, you should target specific storage pools to avoid unintentional file storage locations.

**Procedure**

1. Run the `isi filepool policies create` command.

   The following command creates a file pool policy that archives older files to a specific storage tier:

   ```
   isi filepool policies create ARCHIVE_OLD --description "Move older files to archive storage" --data-storage-target ARCHIVE_TIER --data-ssd-strategy metadata --begin-filter --file-type=file --and --birth-time=2013-09-01 --operator=lt --and --accessed-time=2013-12-01 --operator=lt --end-filter
   ```
Results

The file pool policy is applied when the next scheduled SmartPools job runs. By default, the SmartPools job runs once a day; however, you can also start the SmartPools job manually.

Valid wildcard characters

You can combine wildcard characters with file-matching options to define a file pool policy.

OneFS supports UNIX shell-style (glob) pattern matching for file name attributes and paths.

The following table lists the valid wildcard characters that you can combine with file-matching options to define a file pool policy.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, m* matches movies and m123.</td>
</tr>
<tr>
<td>[a-z]</td>
<td>Matches any characters contained in the brackets, or a range of characters separated by a hyphen. For example, b[aei]t matches bat, bet, and bit, and 1[4-7]2 matches 142, 152, 162, and 172. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, b[!ie] matches bat but not bit or bet. You can match a bracket within a bracket if it is either the first or last character. For example, [[c]at matches cat and [at. You can match a hyphen within a bracket if it is either the first or last character. For example, car[-s] matches cars and car-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, t?p matches tap, tip, and top.</td>
</tr>
</tbody>
</table>

Default file pool requested protection settings

Default protection settings include specifying the data storage target, snapshot storage target, requested protection, and SSD strategy for files that are filtered by the default file pool policy.

<table>
<thead>
<tr>
<th>Settings (Web Admin)</th>
<th>Settings (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Storage Target       | --data-storage-target --data-ssd-strategy | Specifies the storage pool (node pool or tier) that you want to target with this file pool policy. | Note
|                      |               |             | Use SSDs for metadata read acceleration writes |
|                      |               |             | If GNA is not enabled and the storage pool that you choose to target does not contain SSDs, you cannot define an SSD strategy. |

Valid wildcard characters 905
<table>
<thead>
<tr>
<th>Settings (Web Admin)</th>
<th>Settings (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAUTION</strong></td>
<td></td>
<td>If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies with anywhere for the Data storage target option. Because the specified storage pool is included when you use anywhere, target specific storage pools to avoid unintentional file storage locations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select one of the following options to define your SSD strategy:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Use SSDs for metadata read acceleration</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default. Write both file data and metadata to HDDs and metadata to SSDs. Accelerates metadata reads only. Uses less SSD space than the Metadata read/write acceleration setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Use SSDs for metadata read/write acceleration</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write metadata to SSD pools. Uses significantly more SSD space than Metadata read acceleration, but accelerates metadata reads and writes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Use SSDs for data &amp; metadata</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use SSDs for both data and metadata. Regardless of whether global namespace acceleration is enabled, any SSD blocks reside on the storage target if there is room.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Avoid SSDs</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write all associated file data and metadata to HDDs only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CAUTION</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this to free SSD space only after consulting with Isilon Technical Support personnel; the setting can negatively affect performance.</td>
<td></td>
</tr>
<tr>
<td>Snapshot storage target</td>
<td>--snapshot-storage-target --snapshot-ssd-strategy</td>
<td>Specifies the storage pool that you want to target for snapshot storage with this file pool policy. The settings are the same as those for data storage target, but apply to snapshot data.</td>
<td>Notes for data storage target apply to snapshot storage target</td>
</tr>
</tbody>
</table>
### Default file pool I/O optimization settings

You can manage the I/O optimization settings that are used in the default file pool policy, which can include files with manually managed attributes.

To allow SmartPools to overwrite optimization settings that were configured using File System Explorer or the `isi set` command, select the **Including files with manually-managed I/O optimization settings** option in the Default Protection Settings group. In the CLI, use the `--automatically-manage-io-optimization` option with the `isi storagepool settings modify` command.

<table>
<thead>
<tr>
<th>Setting (Web Admin)</th>
<th>Setting (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write Performance</td>
<td><code>--enable-coalescer</code></td>
<td>Enables or disables SmartCache (also referred to as the coalescer).</td>
<td><strong>Enable SmartCache</strong> is the recommended setting for optimal write performance. With asynchronous writes, the Isilon server buffers writes in memory. However, if you want to disable this buffering, we recommend that you configure your applications to use synchronous writes. If that is not possible, disable SmartCache.</td>
</tr>
<tr>
<td>Data Access Pattern</td>
<td><code>--data-access-pattern</code></td>
<td>Defines the optimization settings for accessing concurrent, streaming, or random data types.</td>
<td>Files and directories use a concurrent access pattern by default. To optimize performance, select the pattern dictated by your workflow. For example, a workflow heavy in video editing should be set to <strong>Optimize for streaming access</strong>. That workflow would suffer if the data access pattern was set to <strong>Optimize for random access</strong>.</td>
</tr>
</tbody>
</table>

### Managing file pool policies

You can perform a number of file pool policy management tasks.

File pool policy management tasks include:

- Modifying file pool policies
- Modifying the default file pool policy
- Creating a file pool policy from a template
- Reordering file pool policies
- Deleting file pool policies
Modify a file pool policy

You can modify the name, description, filter criteria, and the protection and I/O optimization settings applied by a file pool policy.

**CAUTION**

If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies with `anywhere` for the Data storage target option. Because the specified storage pool is included when you use `anywhere`, target specific storage pools to avoid unintentional file storage locations.

**Procedure**

1. Run the `isi filepool policies list` command to view a list of available file pool policies.
   
   A tabular list of policies and their descriptions appears.

2. Run the `isi filepool policies view` command to view the current settings of a file pool policy.
   
   The following example displays the settings of a file pool policy named `ARCHIVE_OLD`.

   ```
   isi filepool policies view ARCHIVE_OLD
   ```

3. Run the `isi filepool policies modify` command to change a file pool policy.
   
   The following example modifies the settings of a file pool policy named `ARCHIVE_OLD`.

   ```
   ```

**Results**

Changes to the file pool policy are applied when the next SmartPools job runs. However, you can also manually run the SmartPools job immediately.

Configure default file pool policy settings

Files that are not managed by custom file pool policies are managed by the default file pool policy. You can configure the default file pool policy settings.

**Procedure**

1. Run the `isi filepool default-policy view` command to display the current default file pool policy settings.
Output similar to the following example appears:

<table>
<thead>
<tr>
<th>Set Requested Protection: default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Access Pattern: random</td>
</tr>
<tr>
<td>Enable Coalescer: True</td>
</tr>
<tr>
<td>Data Storage Target: anywhere</td>
</tr>
<tr>
<td>Data SSD Strategy: metadata</td>
</tr>
<tr>
<td>Snapshot Storage Target: anywhere</td>
</tr>
<tr>
<td>Snapshot SSD Strategy: metadata</td>
</tr>
</tbody>
</table>

2. Run the `isi filepool default-policy modify` command to change default settings.

The following command modifies all default settings:

```
isi filepool default-policy modify --set-requested-protection +2 \ 
--data-access-pattern concurrency --enable-coalescer false \ 
--data-storage-target ARCHIVE_A --data-ssd-strategy avoid \ 
--snapshot-storage-target ARCHIVE_A --snapshot-ssd-strategy avoid
```

3. Run the `isi filepool default-policy view` command again to ensure that default file pool policy settings reflect your intentions.

**Results**

OneFS implements the new default file pool policy settings when the next scheduled SmartPools job runs and applies these settings to any files that are not managed by a custom file pool policy.

### Prioritize a file pool policy

You can change the priority order of a file pool policy.

File pool policies are evaluated in descending order according to their position in the file pool policies list. By default, when you create a new policy, it is inserted immediately above the default file pool policy. You can assign a policy a different priority by moving it up or down in the list. The default policy is always the last in priority, and applies to all files that are not matched by any other file pool policy.

**Procedure**

1. Run the `isi filepool policies list` command to view the list of available file pool policies and their priority order.

   Output similar to the following appears:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCHIVE_1</td>
<td>Move older files to archive tier</td>
</tr>
<tr>
<td>MOVE-LARGE</td>
<td>Move large files to archive tier</td>
</tr>
<tr>
<td>PERFORM_1</td>
<td>Move recent files to perf. tier</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
   Total: 3

2. Run the `isi filepool policies modify` command to change the priority of a file pool policy.

   The following example changes the priority of a file pool policy named `PERFORM_1`.

   ```
   isi filepool policies modify PERFORM_1 --apply-order 1
   ```
3. Run the `isi filepool policies list` command again to ensure that the policy list displays the correct priority order.

**Delete a file pool policy**

You can delete a file pool policy.

Delete a file pool policy only if you are aware of, or unconcerned with, the consequences.

**Procedure**

1. Run the `isi filepool policies delete` command.

   The following example deletes a file pool policy named ARCHIVE_1.

   ```
   isi filepool policies delete ARCHIVE_1
   ```

   The system asks you to confirm the deletion.

2. Type `yes`, then press ENTER.

**Results**

The file pool policy is removed. When you delete a policy, its file pool will be controlled either by another policy or by the default file pool policy the next time the SmartPools job runs.

**Monitoring storage pools**

You can access information on storage pool health and usage.

The following information is available:

- File pool policy health
- SmartPools health, including tiers, node pools, and subpools
- For each storage pool, percentage of HDD and SSD disk space usage
- SmartPools job status

**Monitor storage pools**

You can view storage pool status and details.

Details include the names of tiers and associated node pools, requested protection, HDD and SSD capacities and usage.

**Procedure**

1. Run the `isi storagepool list` command.

   Output similar to the following example appears:

   ```
   Name       Nodes  Protect  HDD    Total   %      SSD  Total %
   -----------------------------------------------
   PERF_TIER  1-3    -        12.94T 17.019T 26.99% 0.4T 1.2T
   33.00%
   - s-series 1-3 +2:1     12.94T 17.019T 26.99% 0.4T 1.2T
   33.00%
   ```
View the health of storage pools

You can view the health of storage pools.

Procedure

1. Run the `isi storagepool health` command.

   The following command, using the verbose option, displays a tabular description of storage pool health:

   `isi storagepool health --verbose`

View results of a SmartPools job

You can review detailed results from the last time the SmartPools job ran.

The SmartPools job, by default, runs once a day. It processes the file pool policies that you have created to manage storage on your cluster.

Procedure

1. Run the `isi job events list` command.

   A tabular listing of the most recent system jobs appears. The listing for the SmartPools job is similar to the following example:

   `2014-04-28T02:00:29 SmartPools [105] Succeeded`

2. Locate the SmartPools job in the listing, and make note of the number in square brackets.

   This is the job ID number.

3. Run the `isi job reports view` command, using the job ID number.

   The following example displays the report for a SmartPools job with the job ID of 105.

   `isi job reports view 105`

Results

The SmartPools report shows the outcome of all of the file pool policies that were run, including summaries for each policy, and overall job information such as elapsed time, LINs traversed, files and directories processed, and memory and I/O statistics.
Storage pool commands

You can monitor and manage node pools, tiers, and file pool policies and settings through the OneFS command-line interface. Some storage pool functions are available only if you activate a SmartPools license on the cluster.

isi filepool apply

Applies all file pool policies to the specified file or directory path. If no policy matches the file or directory path, OneFS applies the default file pool policy.

Syntax

```bash
isi filepool apply <path>
   [--path]<path>
   [--dont-restripe]
   [--nop]
   [--stats]
   [--quiet]
   [--recurse]
   [--verbose]
```

Options

--path <path>

Specifies the path to the file to be processed. This parameter is required.

--dont-restripe

Changes the per-file policies without restriping the file.

--nop

Calculates the specified settings without actually applying them. This option is best used with --verbose or --stats.

--stats

Displays statistics on the files processed.

--quiet

Suppresses warning messages.

--recurse

Specifies recursion through directories.

--verbose

Displays the configuration settings to be applied. We recommend using verbose mode. Otherwise the command would not display any screen output except for error messages.

Examples

These examples show the results of running `isi filepool apply` in verbose mode. In the examples, the output shows the results of comparing the path specified with each file pool policy. The `recurse` option is set so that all files in the /ifs/
data/projects path are matched against all file pool policies. The first policy listed is always the system default policy. In this example, the second match is to the file pool policy Technical Data.

```bash
isi filepool apply --path=/ifs/data/projects --verbose --recurse
```

Processing file /ifs/data/projects
Protection Level is DiskPool minimum
Layout policy is concurrent access
coalescer_enabled is true
data_disk_pool_policy_id is any pool group ID
data SSD strategy is metadata
snapshot_disk_pool_policy_id is any pool group ID
snapshot SSD strategy is metadata
cloud provider id is 0
New File Attributes
Protection Level is DiskPool minimum
Layout policy is concurrent access
coalescer_enabled is true
data_disk_pool_policy_id is any pool group ID
data SSD strategy is metadata
snapshot_disk_pool_policy_id is any pool group ID
snapshot SSD strategy is metadata
cloud provider id is 0

```
{'default':
{'Policy Number': -2,
'Files matched': {'head': 0, 'snapshot': 0},
'Directories matched': {'head': 1, 'snapshot': 0},
'ADS containers matched': {'head': 0, 'snapshot': 0},
'ADS streams matched': {'head': 0, 'snapshot': 0},
'Access changes skipped': 0,
'Protection changes skipped': 0,
'File creation templates matched': 1,
'File data placed on HDDs': {'head': 0, 'snapshot': 0},
'File data placed on SSDs': {'head': 0, 'snapshot': 0}},
'system':
{'Policy Number': 0,
'Files matched': {'head': 0, 'snapshot': 0},
'Directories matched': {'head': 0, 'snapshot': 0},
'ADS containers matched': {'head': 0, 'snapshot': 0},
'ADS streams matched': {'head': 0, 'snapshot': 0},
'Access changes skipped': 0,
'Protection changes skipped': 0,
'File creation templates matched': 0,
'File data placed on HDDs': {'head': 0, 'snapshot': 0},
'File data placed on SSDs': {'head': 0, 'snapshot': 0}},
```

This example shows the result of using the --nop option to calculate the results that would be produced by applying the file pool policy.

```bash
isi filepool apply --path=/ifs/data/projects --nop --verbose
```

Processing file /ifs/data/projects
Protection Level is DiskPool minimum
Layout policy is concurrent access
coalescer_enabled is true
data_disk_pool_policy_id is any pool group ID
data SSD strategy is metadata
snapshot_disk_pool_policy_id is any pool group ID
snapshot SSD strategy is metadata
cloud provider id is 0
New File Attributes
Protection Level is DiskPool minimum
Layout policy is concurrent access
coalescer_enabled is true
data_disk_pool_policy_id is any pool group ID
data SSD strategy is metadata
snapshot_disk_pool_policy_id is any pool group ID
snapshot SSD strategy is metadata
cloud provider id is 0

{"default":
  {'Policy Number': -2,
   'Files matched': {'head':0, 'snapshot': 0},
   'Directories matched': {'head':1, 'snapshot': 0},
   'ADS containers matched': {'head':0, 'snapshot': 0},
   'ADS streams matched': {'head':0, 'snapshot': 0},
   'Access changes skipped': 0,
   'Protection changes skipped': 0,
   'File creation templates matched': 1,
   'File data placed on HDDs': {'head':0, 'snapshot': 0},
   'File data placed on SSDs': {'head':0, 'snapshot': 0},
  },
  'system':
  {'Policy Number': -1,
   'Files matched': {'head':0, 'snapshot': 0},
   'Directories matched': {'head':0, 'snapshot': 0},
   'ADS containers matched': {'head':0, 'snapshot': 0},
   'ADS streams matched': {'head':0, 'snapshot': 0},
   'Access changes skipped': 0,
   'Protection changes skipped': 0,
   'File creation templates matched': 0,
   'File data placed on HDDs': {'head':0, 'snapshot': 0},
   'File data placed on SSDs': {'head':0, 'snapshot': 0},
  },
}

isi filepool default-policy modify

Modifies default file pool policy settings. The default file pool policy specifies storage settings for all files to which a higher-priority file pool policy does not apply.

Syntax

isi filepool default-policy modify
  [--data-access-pattern {random | concurrency | streaming}]
  [--set-requested-protection {default | +1 | +2:1 | +2 | +3:1 | +3 | +4 | 2x | 3x | 4x | 5x | 6x | 7x | 8x}]
  [--data-storage-target <string>]
  [--data-ssd-strategy {metadata | metadata-write | data | avoid}]
  [--snapshot-storage-target <string>]
  [--snapshot-ssd-strategy {metadata | metadata-write | data | avoid}]
  [--enable-coalescer {yes | no}]
  [--cloud-pool <string>]
  [--cloud-accessibility {cached | no-cache}]
  [--cloud-cache-expiration <duration>]
  [--cloud-cache-compression-enabled {yes | no}]
  [--cloud-data-retention <duration>]
  [--cloud-encryption-enabled {yes | no}]
  [--cloud-full-backup-retention <duration>]
  [--cloud-incremental-backup-retention <duration>]
  [--cloud-read-ahead <string>]
  [--cloud-writeback-frequency <duration>]
Options

--data-access-pattern <string>
  Specifies the preferred data access pattern, one of random, streaming, or concurrent.

--set-requested-protection <string>
  Specifies the requested protection for files that match this filepool policy (for example, +2:1).

--data-storage-target <string>
  Specifies the node pool or tier to which the policy moves files on the local cluster.

--data-ssd-strategy <string>
  Specifies how to use SSDs to store local data.
    
    avoid
    Writes all associated file data and metadata to HDDs only.
    
    metadata
    Writes both file data and metadata to HDDs. This is the default setting. An extra mirror of the file metadata is written to SSDs, if SSDs are available. The SSD mirror is in addition to the number required to satisfy the requested protection. Enabling global namespace acceleration (GNA) makes read acceleration available to files in node pools that do not contain SSDs.
    
    metadata-write
    Writes file data to HDDs and metadata to SSDs, when available. This strategy accelerates metadata writes in addition to reads but requires about four to five times more SSD storage than the metadata setting. Enabling GNA does not affect read/write acceleration.
    
    data
    Uses SSD node pools for both data and metadata, regardless of whether global namespace acceleration is enabled. This SSD strategy does not result in the creation of additional mirrors beyond the normal requested protection but requires significantly more storage space compared with the other SSD strategy options.

--snapshot-storage-target <integer>
  The ID of the node pool or tier chosen for storage of snapshots.

--snapshot-ssd-strategy <string>
  Specifies how to use SSDs to store snapshots. Valid options are metadata, metadata-write, data, avoid. The default is metadata.

--enable-coalescer {yes | no}
  Enable or disable the coalescer, also referred to as SmartCache. The coalescer protects write-back data through a combination of RAM and stable storage. It is
enabled by default, and should be disabled only in cooperation with EMC Isilon Customer Support.

--cloud-pool <string>
  Specifies the default CloudPool and, therefore, the cloud storage account where cloud data is to be archived.

--cloud-accessibility {cached | no-cache}
  Specifies whether, when a SmartLink file is accessed, cloud data is incrementally downloaded (cached) as needed, or fully downloaded (not cached).

--cloud-cache-expiration <duration>
  Specifies the minimum amount of time until the cache expires. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-compression-enabled {yes | no}
  Specifies whether data is to be compressed when archived to the cloud.

--cloud-data-retention <duration>
  Specifies the minimum amount of time that archived data will be retained in the cloud after a SmartLink file is deleted from the cluster. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-encryption-enabled {yes | no}
  Specifies whether data is to be encrypted when archived to the cloud.

--cloud-full-backup-retention <duration>
  Specifies the minimum amount of time that cloud files will be retained after the creation of a full backup. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-incremental-backup-retention <duration>
  Specifies the minimum amount of time that cloud files will be retained after the creation of an incremental backup. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-read-ahead {partial | full}
  Specifies the cache readahead strategy when SmartLink files are accessed. A partial strategy means that only the amount of data needed by the user is cached. A full strategy means that all file data will be cached when the user accesses a SmartLink file.

--cloud-writeback-frequency <duration>
  Specifies the minimum amount of time to wait before OneFS updates cloud data with local changes. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-archive-snapshot-files {yes | no}
  Whether or not policies should archive files with snapshots.

--verbose
Displays more detailed information.

Example
The command shown in the following example modifies the default file pool policy in several ways. The command sets the requested-protection-level to +2:1, sets the data-storage-target to anywhere (the system default), and changes the data--ssd-strategy to metadata-write.

```
isi filepool default-policy modify --set-requested-protection=+2:1
--data-storage-target=anywhere
--data-ssd-strategy=metadata-write
```

### isi filepool default-policy view

View default file pool policy settings. The default file pool policy specifies storage settings for all files to which a higher-priority file pool policy does not apply.

**Syntax**

```
isi filepool default-policy view
```

The following display shows sample output from the command:

```
Apply Order: -
File Matching Pattern: -
Set Requested Protection: default
Data Access Pattern: concurrency
Enable Coalescer: True
Data Storage Target: anywhere
Data SSD Strategy: metadata
Snapshot Storage Target: anywhere
Snapshot SSD Strategy: metadata
Cloud Pool: -
Cloud Compression Enabled: -
Cloud Encryption Enabled: -
Cloud Data Retention: -
Cloud Incremental Backup Retention: -
Cloud Full Backup Retention: -
Cloud Accessibility: -
Cloud Read Ahead: -
Cloud Cache Expiration: -
Cloud Writeback Frequency: -
Cloud Archive Snapshot Files: -
```

### isi filepool policies create

Create a custom file pool policy to identify a specific storage target and perform other actions on matched files and directories.

**Syntax**

```
isi filepool policies create <name>
[|--description <string>]
[|--begin-filter <predicate> <operator> <link>]<--end-filter]
[|--apply-order <integer>]
[|--data-access-pattern {random | concurrency | streaming}]
[|--set-requested-protection {default | +1 | +2:1 | +2 | +3:1 | +3}]
```
Options

Options

<name>

Specifies the name of the file pool policy to create.

--begin-filter {<predicate> <operator> <link>}, --end-filter

Specifies the file-matching criteria that determine the files to be managed by the filepool policy.

Each file matching criterion consists of three parts:

- Predicate. Specifies what attribute(s) to filter on. You can filter by path, name, file type, timestamp, or custom attribute, or use a combination of these attributes.
- Operator. Qualifies an attribute (for example, birth time) to describe a relationship to that attribute (for example, before).
- Link - Combines attributes using AND and OR statements.

The following predicates are valid:

--size=<nn>[(B | KB | MB | GB | TB | PB)]

Selects files according to the specified size.

--path=<pathname>

Selects files relative to the specified pathname.

--file-type= <value>

Selects only the specified file-system object type.

The following values are valid:

file

Specifies regular files.

directory

Specifies directories.
other
  Specifies links.

--name= <value>[--case-sensitive= {true | false}]
Selects only files whose names match the specified string. Use --case-
sensitive=true to enable case-sensitivity.

When forming the name, you can include the following wildcards:
  • *
  • [ ]
  • ?

--birth-time= <timestamp>
Selects files that were created relative to the specified date and time.
Timestamp arguments are formed as YYYY-MM-DDTHH:MM:SS. For example,
2013-09-01T08:00:00 specifies a timestamp of September 1, 2013 at 8:00
A.M. You can use --operator= with an argument of gt to mean after the
timestamp or lt to mean before the timestamp.

--changed-time= <timestamp>
Selects files that were modified relative to the specified date and time.

--metadata-changed-time= <timestamp>
Selects files whose metadata was modified relative to the specified date and
time.

--accessed-time= <timestamp>
Selects files that were accessed at the specified time interval.

--custom-attribute= <value>
Selects files based on a custom attribute.

You can use the operator= option to specify a qualifier for the file-matching
criterion. Specify operators in the following form:

--operator= <value>

The following operator values are valid:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>Equal. This is the default value.</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal</td>
</tr>
<tr>
<td>lt</td>
<td>Less than</td>
</tr>
<tr>
<td>le</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td>gt</td>
<td>Greater than</td>
</tr>
</tbody>
</table>
Link arguments can be used to specify multiple file-matching criteria. The following links are valid:

--and
Connects two file-matching criteria where files must match both criteria.

--or
Connects two file-matching criteria where files must match one or the other criteria.

--description <string>
Specifies a description of the filepool policy

--apply-order <integer>
Specifies the order index for execution of this policy.

--data-access-pattern <string>
Data access pattern random, streaming or concurrent.

--set-requested-protection <string>
Specifies a protection level for files that match this filepool policy (e.g., +3, +2:3, 8x).

--data-storage-target <string>
The name of the node pool or tier to which the policy moves files on the local cluster. If you do not specify a data storage target, the default is anywhere.

--data-ssd-strategy <string>
Specifies how to use SSDs to store local data.

  avoid
  Writes all associated file data and metadata to HDDs only.

  metadata
  Writes both file data and metadata to HDDs. This is the default setting. An extra mirror of the file metadata is written to SSDs, if SSDs are available. The SSD mirror is in addition to the number required to satisfy the requested protection. Enabling GNA makes read acceleration available to files in node pools that do not contain SSDs.

  metadata-write
  Writes file data to HDDs and metadata to SSDs, when available. This strategy accelerates metadata writes in addition to reads but requires about four to five times more SSD storage than the Metadata setting. Enabling GNA does not affect read/write acceleration.

  data
  Uses SSD node pools for both data and metadata, regardless of whether global namespace acceleration is enabled. This SSD strategy does not result
in the creation of additional mirrors beyond the normal requested protection 
but requires significantly increases storage requirements compared with the 
other SSD strategy options.

--snapshot-storage-target <string>
The name of the node pool or tier chosen for storage of snapshots. If you do not 
specify a snapshot storage target, the default is anywhere.

--snapshot-ssd-strategy <string>
Specifies how to use SSDs to store snapshots. Valid options are metadata,
data, avoid. The default is metadata.

--enable-coalescer {Yes | No}
Enable the coalescer.

--cloud-pool <string>
Specifies the default CloudPool and, therefore, the cloud storage account where 
cloud data is to be archived.

--cloud-accessibility {cached | no-cache}
Specifies whether, when a SmartLink file is accessed, cloud data is incrementally 
downloaded (cached) as needed, or fully downloaded (not cached).

--cloud-cache-expiration <duration>
Specifies the minimum amount of time until the cache expires. A number followed 
by a unit of time is accepted. For example, a setting of 9H would specify a nine-
hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-compression-enabled {yes | no}
Specifies whether data is to be compressed when archived to the cloud.

--cloud-data-retention <duration>
Specifies the minimum amount of time that archived data will be retained in the 
cloud after a SmartLink file is deleted from the cluster. A number followed by a 
unit of time is accepted. For example, a setting of 9H would specify a nine-hour 
duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-encryption-enabled {yes | no}
Specifies whether data is to be encrypted when archived to the cloud.

--cloud-full-backup-retention <duration>
Specifies the minimum amount of time that cloud files will be retained after the 
creation of a full backup. A number followed by a unit of time is accepted. For 
example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 
2D would specify a two-day duration.

--cloud-incremental-backup-retention <duration>
Specifies the minimum amount of time that cloud files will be retained after the 
creation of an incremental backup. A number followed by a unit of time is 
accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-read-ahead {partial | full}
Specifies the cache readahead strategy when SmartLink files are accessed. A partial strategy means that only the amount of data needed by the user is cached. A full strategy means that all file data will be cached when the user accesses a SmartLink file.

```bash
--cloud-writeback-frequency <duration>
```

Specifies the minimum amount of time to wait before OneFS updates cloud data with local changes. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

```bash
--cloud-archive-snapshot-files {yes | no}
```

Whether or not policies should archive files with snapshots.

```bash
--verbose
```

Displays more detailed information.

**Examples**

The following example creates a file pool policy that moves all files in directory `/ifs/data/chemical/arco/finance` to the local storage target named `Archive_2`.

```bash
isi filepool policies create Save_Fin_Data --begin-filter --path=/ifs/data/chemical/arco/finance --end-filter --data-storage-target Archive_2 --data-ssd-strategy=metadata
```

The following example matches older files that have not been accessed or modified later than specified dates, and moves the files to an archival tier of storage.

```bash
isi filepool policies create archive_old --data-storage-target ARCHIVE_1 --data-ssd-strategy avoid --begin-filter --file-type=file --and --birth-time=2013-09-01 --operator=lt --and --accessed-time=2013-12-01 --operator=lt --and --changed-time=2013-12-01 --operator=lt --end-filter
```

**isi filepool policies delete**

Delete a custom file pool policy. The default file pool policy cannot be deleted.

To list all file pool policies, run the `isi filepool policies list` command.

**Syntax**

```bash
isi filepool policies delete <name> [--force] [--verbose]
```

**Options**

`<name>`

Specifies the name of the file pool policy to be deleted.

`--force`

Deletes the file pool policy without asking for confirmation.

`--verbose`

Displays more detailed information.
Example
The following command deletes a file pool policy named ARCHIVE_OLD. The --force option circumvents the requirement to confirm the deletion.

    isi filepool policies delete ARCHIVE_OLD --force

isi filepool policies list
List all custom file pool policies configured on the system.

Syntax

    isi filepool policies list
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]

Options
--format
Output the list of file pool policies in a variety of formats. The following options are valid: table, json, csv, and list.

--no-header
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
The following example lists custom file pool policies in .csv format and outputs the list to a file in the OneFS file system.

    isi filepool policies list --format csv > /ifs/data/policy.csv

isi filepool policies modify
Modify a custom file pool policy.

Syntax

    isi filepool policies modify <name>
    [--description <string>]
    [--begin-filter{<predicate> <operator> <link>}...--end-filter]
    [--apply-order <integer>]
    [--data-access-pattern {random | concurrency | streaming}]
    [--set-requested-protection {default | +1 | +2:1 | +2 | +3:1 | +3 | +4 | 2x | 3x | 4x | 5x | 6x | 7x | 8x}]
    [--data-storage-target <string>]
Options

`<name>`

Specifies the name of the file pool policy to create.

`--begin-filter {<predicate> <operator> <link>}`...
`--end-filter`

Specifies the file-matching criteria that determine the files to be managed by the filepool policy.

Each file matching criterion consists of three parts:

- Predicate. Specifies what attribute(s) to filter on. You can filter by path, name, file type, timestamp, or custom attribute, or use a combination of these attributes.
- Operator. Qualifies an attribute (for example, birth time) to describe a relationship to that attribute (for example, before).
- Link - Combines attributes using AND and OR statements.

The following predicates are valid:

`--size=<nn>[{B | KB | MB | GB | TB | PB}]`

Selects files according to the specified size.

`--path=<pathname>`

Selects files relative to the specified pathname.

`--file-type= <value>`

Selects only the specified file-system object type.

The following values are valid:

- `file`
  
  Specifies regular files.

- `directory`

  Specifies directories.

- `other`

  Specifies links.
--name= <value> [--case-sensitive= {true | false}]
Selects only files whose names match the specified string. Use --case-sensitive=true to enable case-sensitivity.

When forming the name, you can include the following wildcards:

- *
- [ ]
- ?

--birth-time= <timestamp>
Selects files that were created relative to the specified date and time. Timestamp arguments are formed as YYYY-MM-DDTHH:MM:SS. For example, 2013-09-01T08:00:00 specifies a timestamp of September 1, 2013 at 8:00 A.M. You can use --operator= with an argument of gt to mean after the timestamp or lt to mean before the timestamp.

--changed-time= <timestamp>
Selects files that were modified relative to the specified date and time.

--metadata-changed-time= <timestamp>
Selects files whose metadata was modified relative to the specified date and time.

--accessed-time= <timestamp>
Selects files that were accessed at the specified time interval.

--custom-attribute= <value>
Selects files based on a custom attribute.

You can use the operator= option to specify a qualifier for the file-matching criterion. Specify operators in the following form:

--operator= <value>

The following operator values are valid:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>Equal. This is the default value.</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal</td>
</tr>
<tr>
<td>lt</td>
<td>Less than</td>
</tr>
<tr>
<td>le</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td>gt</td>
<td>Greater than</td>
</tr>
<tr>
<td>ge</td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td>not</td>
<td>Not</td>
</tr>
</tbody>
</table>

Link arguments can be used to specify multiple file-matching criteria. The following links are valid:
--and
Connects two file-matching criteria where files must match both criteria.

--or
Connects two file-matching criteria where files must match one or the other criteria.

--description <string>
Specifies a description of the filepool policy.

--apply-order <integer>
Specifies the order index for execution of this policy.

--data-access-pattern <string>
Data access pattern random, streaming or concurrent.

--set-requested-protection <string>
Specifies a protection level for files that match this filepool policy (for example, +3, +2:3, 8x).

--data-storage-target <string>
The name of the node pool or tier to which the policy moves files on the local cluster.

--data-ssd-strategy <string>
Specifies how to use SSDs to store local data.

  avoid
  Writes all associated file data and metadata to HDDs only.

  metadata
  Writes both file data and metadata to HDDs. This is the default setting. An extra mirror of the file metadata is written to SSDs, if SSDs are available. The SSD mirror is in addition to the number required to satisfy the requested protection. Enabling GNA makes read acceleration available to files in node pools that do not contain SSDs.

  metadata-write
  Writes file data to HDDs and metadata to SSDs, when available. This strategy accelerates metadata writes in addition to reads but requires about four to five times more SSD storage than the metadata setting. Enabling GNA does not affect read/write acceleration.

  data
  Uses SSD node pools for both data and metadata, regardless of whether global namespace acceleration is enabled. This SSD strategy does not result in the creation of additional mirrors beyond the normal requested protection but requires significantly increases storage requirements compared with the other SSD strategy options.

--snapshot-storage-target <string>
The name of the node pool or tier chosen for storage of snapshots.
--snapshot-ssd-strategy <string>
Specifies how to use SSDs to store snapshots. Valid options are metadata, metadata-write, data, avoid. The default is metadata.

--enable-coalescer {Yes | No}
Enable the coalescer.

--cloud-pool <string>
Specifies the default CloudPool and, therefore, the cloud storage account where cloud data is to be archived.

--cloud-accessibility {cached | no-cache}
Specifies whether, when a SmartLink file is accessed, cloud data is incrementally downloaded (cached) as needed, or fully downloaded (not cached).

--cloud-cache-expiration <duration>
Specifies the minimum amount of time until the cache expires. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-compression-enabled {yes | no}
Specifies whether data is to be compressed when archived to the cloud.

--cloud-data-retention <duration>
Specifies the minimum amount of time that archived data will be retained in the cloud after a SmartLink file is deleted from the cluster. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-encryption-enabled {yes | no}
Specifies whether data is to be encrypted when archived to the cloud.

--cloud-full-backup-retention <duration>
Specifies the minimum amount of time that cloud files will be retained after the creation of a full backup. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-incremental-backup-retention <duration>
Specifies the minimum amount of time that cloud files will be retained after the creation of an incremental backup. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--cloud-read-ahead {partial | full}
Specifies the cache readahead strategy when SmartLink files are accessed. A partial strategy means that only the amount of data needed by the user is cached. A full strategy means that all file data will be cached when the user accesses a SmartLink file.

--cloud-writeback-frequency <duration>
Specifies the minimum amount of time to wait before OneFS updates cloud data with local changes. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.
--cloud-archive-snapshot-files {yes | no}
Whether or not policies should archive files with snapshots.

--verbose
Display more detailed information.

Examples
The following example modifies a file pool policy to move matched files to a different local storage target named Archive_4. The next time the SmartPools job runs, matched files would be moved to the new storage target.

```
isi filepool policies modify Save_Fin_Data --begin-filter
--path=/ifs/data/chemical/arco/finance --end-filter
--data-storage-target Archive_4 --data-ssd-strategy=metadata
```

The following example matches older files that have not been accessed or modified later than specified dates, and moves the files to an archival tier of storage.

```
isi filepool policies modify archive_old
--data-storage-target ARCHIVE_1 --data-ssd-strategy avoid
--begin-filter --file-type=file --and --birth-time=2013-06-01
--operator=lt --and --accessed-time=2013-09-01 --operator=lt
--and --changed-time=2013-09-01 --operator=lt --end-filter
```

**isi filepool policies view**
Displays detailed information about a custom file pool policy.

**Syntax**

```
isi filepool policies view <name>
```

**Options**

```
<name>
```
Specifies the name of the file pool policy to view. Run the isi filepool policies list command to list the names of all custom file pool policies.

**Example**
The following example displays details about a file pool policy named my_policy:

```
isi filepool policies view my_policy
```

Output from the command would look similar to the following display:

```
Name: my_policy
Description: Archive older files to the cloud
State: OK
State Details:
  Apply Order: 1
  File Matching Pattern: Path == data/old_files (begins with) AND Name == *.*
Set Requested Protection: -
  Data Access Pattern: -
```
Enable Coalescer: -
Data Storage Target: -
Data SSD Strategy: -
Snapshot Storage Target: -
Snapshot SSD Strategy: -
Cloud Pool: my_s3_pool
Cloud Compression Enabled: False
Cloud Encryption Enabled: False
Cloud Data Retention: 604800
Cloud Incremental Backup Retention: 604800
Cloud Full Backup Retention: 157680000
Cloud Accessibility: cached
Cloud Read Ahead: partial
Cloud Cache Expiration: 86400
Cloud Writeback Frequency: 14400
Cloud Archive Snapshot Files: False

isi filepool templates list
Lists available file pool policy templates.

Syntax

```bash
isi filepool templates list
    [--limit <integer>]
    [--sort <string>]
    [--descending <string>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

--limit <integer>
    Specifies the number of templates to display.

--sort <string>
    Sorts data by the field specified.

--descending <integer>
    Sorts data in descending order.

--format
    Displays file pool templates in the specified format. The following values are valid:
    table
    json
    csv
    list

--no-header
    Displays table and CSV output without headers.

--no-footer
isi filepool templates view

View the detailed settings in a file pool policy template.

Syntax

```
isi filepool templates view <name>
```

Options

- `<name>`
  - The name of the template to view.

isi storagepool compatibilities class active create

Creates a compatibility to enable an unprovisioned node to join a node pool.

Note

This command is not applicable for IsilonSD Edge.

Syntax

```
isi storagepool compatibilities class active create <class-1> <class-2>
   [--assess {yes | no}]
   [--verbose]
   [--force]
```

Options

- `<class-1>`
  - An existing node pool class, one of S200, X200, X400, or N400.

- `<class-2>`
  - The node class that is compatible with the existing node pool, one of S210, X210, X410, or N410. Note that S210, X210, X410, and NL410 nodes are compatible only with similarly configured S200, X200, X400, and NL400 node pools, respectively. Also note that, in CLI commands, NL400 and NL410 nodes are expressed as N400 and N410.

- `--assess {yes | no}`
  - Checks whether the compatibility is valid without actually creating the compatibility.

- `--verbose`
  - Displays more detailed information.

- `--force`
Performs the action without asking for confirmation.

Examples
The following command creates a compatibility between S200 and S210 nodes without asking for confirmation:

```
isi storagepool compatibilities class active create S200 S210 --force
```

**isi storagepool compatibilities class active delete**

Deletes a node class compatibility. If fewer than three compatible nodes were added to an existing node pool, they are removed from the node pool and become unprovisioned.

---

**Note**

This command is not applicable for IsilonSD Edge.

**Syntax**

```
isi storagepool compatibilities class active delete <ID>  
[--assess {yes | no}]  
[--verbose]  
[--force]
```

**Options**

- **<ID>**
  The ID number of the compatibility. You can use the `isi storagepool compatibilities class active list` command to view the ID numbers of active compatibilities.

- **--assess {yes | no}**
  Checks the results without actually deleting the compatibility.

- **--verbose**
  Displays more detailed information.

- **--force**
  Performs the action without asking for confirmation.

**Example**

The following command provides information about the results of deleting a compatibility without actually performing the action:

```
isi storagepool compatibilities class active delete 1 --assess yes
```

Provided that a compatibility with the ID of 1 exists, OneFS displays information similar to the following example:

```
Deleting compatibility with id 1 is possible.  
This delete will cause these nodepools to split:  
1: Nodepool s200_0b_0b will be split. A tier will be created and all
```
resultant nodepools from this split will be incorporated into it. All filepool policies targeted at the splitting pool will be redirected towards this new tier. That tier's name is s200_0b_0b-tier

isi storagepool compatibilities class active list

Lists node class compatibilities that have been created.

Note

This command is not applicable for IsilonSD Edge.

Syntax

isi storagepool compatibilities class active list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]

Options

--limit <integer>
    Limits the number of compatibilities that are listed.

--format
    Lists active compatibilities in the specified format. The following values are valid:
    - table
    - json
    - csv
    - list

--no-header
    Displays table and CSV output without headers.

--no-footer
    Displays table output without footers.

--verbose
    Displays more detailed information.

Example

The following command lists active node class compatibilities:

    isi storagepool compatibilities class active list

Command output appears similar to the following example:

ID  Class 1  Class 2
------------
1    S200    S210
2    X200    X210
In CLI commands and output, NL400 and NL410 nodes are expressed as \textit{N400 and N410}, respectively.

### isi storagepool compatibilities class active view

Displays the details of an active node class compatibility.

**Note**
This command is not applicable for IsilonSD Edge.

**Syntax**

```
isi storagepool compatibilities class active view <ID>
```

**Options**

```
<ID>
```

The ID number of the compatibility to view. You can use the `isi storagepool compatibilities class active list` command to display the ID numbers of active node class compatibilities.

**Example**

The following command displays information about an active compatibility with ID number 1:

```
isi storagepool compatibilities class active view 1
```

Output from the command will be similar to the following:

```
ID: 1
Class 1: S200
Class 2: S210
```

### isi storagepool compatibilities class available list

Lists node class compatibilities that are available, but not yet created.

**Note**
This command is not applicable for IsilonSD Edge.

**Syntax**

```
isi storagepool compatibilities class available list <name>
```

[---limit <integer>]
[---format {table | json |}]

---

Note

In CLI commands and output, NL400 and NL410 nodes are expressed as \textit{N400 and N410}, respectively.
Options

--limit<integer>
Limits the number of available compatibilities that are listed.

--format
Lists available compatibilities in the specified format. The following values are valid:
- table
- json
- csv
- list

--no-header
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
The following command lists available compatibilities:

```
isi storagepool compatibilities class available list
```

If compatibilities are available, command output similar to the following example appears:

```
Class 1   Class 2
----------
S200      S210
X400      X410
----------
Total: 2
```

isi storagepool compatibilities ssd active create

Creates an SSD compatibility, which can help to provision nodes with different SSD capacities to an existing compatible node pool. Without an SSD compatibility, compatible nodes having different SSD capacities cannot join the same node pool. If you have fewer than three nodes with a different SSD capacity, the nodes would remain unprovisioned, and therefore not functional.

Note
This command is not applicable for IsilonSD Edge.
Syntax

```bash
isi storagepool compatibilities ssd active create <class-1>
  [--class-2 <string>]
  [--count {yes | no}]
  [--assess {yes | no}]
  [--verbose]
  [--force]
```

Options

`<class-1>`
The node class that the SSD compatibility will be created for. For example, you can create an SSD compatibility for S200 nodes that have larger-capacity SSDs than the nodes in an existing S200 node pool. In this way, OneFS can autoprovion the newer S200 nodes to the existing S200 node pool. You can use the `isi storagepool compatibilities ssd available list` command to display valid node class values. For example, S200.

`--class-2 <string>`
The second node class that will be made SSD-compatible with the first node class. For example, you can create an SSD compatibility for S210 nodes that have larger-capacity SSDs than the nodes in an existing S200 node pool. Because S210 nodes can be made compatible with S200 nodes, they can be autoprovioned to an S200 node pool. However, in this case, you also need to create a node class compatibility between S200 and S210 nodes.

`--count {yes | no}`
Specifies whether to create an SSD count compatibility.

`--assess {yes | no}`
Checks whether the SSD compatibility is valid without actually creating the compatibility.

`--verbose`
Displays more detailed information.

`--force`
Performs the action without asking for confirmation.

Examples

The following command creates an SSD class compatibility and SSD count compatibility between S200 and S210 nodes:

```bash
isi storagepool compatibilities ssd active create S200 --class-2 S210 --count yes
```

OneFS displays an advisory message similar to the following, and requires you to confirm the operation:

```
You are attempting to create an SSD compatibility for node class 1. You are also attempting to create an SSD compatibility for node class 2. Creating an SSD compatibility will merge all automatic node pools with nodes from the compatibility's node class with the same ssd
```
count and hdd configuration and compatible RAM into a single node pool. This will require all of these automatic node pools to have the same L3 setting, requested protection, and tier membership. Any file pool policies currently targeting any of the merging node pools will automatically be re-targeted towards the resultant merged pool. If there exists enough unprovisioned nodes belonging to this compatibility's node class to form a node pool, that node pool will be formed. This may potentially be very costly from a performance standpoint the next time the smartpools job runs. If this is a concern, please contact EMC Isilon Technical Support for more information.

Continue with creation? (yes/[no]):

Type yes, then press ENTER to continue. Type no, then press ENTER to cancel the process.

isi storagepool compatibilities ssd active delete

Deletes an SSD compatibility. If fewer than three nodes of a particular class were added to a node pool when the SSD compatibility was created, these nodes are removed from the node pool and become unprovisioned.

**Note**

This command is not applicable for IsilonSD Edge.

**Syntax**

isi storagepool compatibilities ssd active delete <ID>
[--id-2 <integer>]
[--assess {yes | no}]
[--verbose]
[--force]

**Options**

**<ID>**

The ID number of the compatibility. You can use the isi storagepool compatibilities ssd active list command to view the ID numbers of active SSD compatibilities.

**--id-2 <integer>**

The ID number of the second SSD compatibility to delete. You can use the isi storagepool compatibilities ssd active list command to view the ID numbers of active SSD compatibilities. The --id-2 setting is optional, unless the node pool with the SSD compatibility also has an associated node class compatibility. In this case, the setting is required, and deleting the second SSD compatibility will unprovision some of the nodes from the node pool.

**--assess {yes | no}**

Checks the results without actually deleting the SSD compatibility.

**--verbose**
Displays more detailed information.

```
--force
```

Performs the action without asking for confirmation.

**Example**
The following command provides information about the results of deleting an SSD compatibility without actually performing the action:

```
isistoragepool compatibilities ssd active delete 1 --id=2 2 --assess yes
```

Provided that an SSD compatibility between ID 1 and ID 2 exists, OneFS displays information similar to the following example:

```
Deleting ssd compatibility with id 1 is possible.
Deleting ssd compatibility with id 2 is possible.
This delete will cause these nodepools to split:
1: Nodepool s200_9.8kb_9.8kb-ssd_0b will be split. A tier will be created and all
resultant nodepools from this split will be incorporated into it. All filepool policies targeted at the splitting pool will be redirected towards this new tier. That tier's name is s200_9.8kb_9.8kb-ssd_0b-tier
```

**isi storagepool compatibilities ssd active list**

Lists SSD compatibilities that have been created.

**Note**

This command is not applicable for IsilonSD Edge.

**Syntax**

```
isistoragepool compatibilities ssd active list
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

```
--limit <integer>
```

Limits the number of SSD compatibilities that are listed.

```
--format
```

Lists active SSD compatibilities in the specified format. The following values are valid:

- `table`
- `json`
- `csv`
- `list`

```
--no-header
```

Sends output in the specified format without a header.
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
The following command lists active SSD compatibilities:

```
isi storagepool compatibilities ssd active list
```

Command output appears similar to the following example:

```
<table>
<thead>
<tr>
<th>ID</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S200</td>
</tr>
<tr>
<td>2</td>
<td>S210</td>
</tr>
<tr>
<td>3</td>
<td>N400</td>
</tr>
<tr>
<td>4</td>
<td>N410</td>
</tr>
</tbody>
</table>
---|------|
Total: 4
```

Note
In CLI commands and output, NL400 and NL410 nodes are expressed as N400 and N410, respectively.

isi storagepool compatibilities ssd active view
Displays the details of an active SSD compatibility.

Note
This command is not applicable for IsilonSD Edge.

Syntax

```
isi storagepool compatibilities ssd active view <ID>
```

Options

\(<ID>\)
The ID number of the SSD compatibility to view. You can use the isi storagepool compatibilities ssd active list command to display the ID numbers of active SSD compatibilities.

Example
The following command displays information about an active compatibility with ID number 1:

```
isi storagepool compatibilities ssd active view 1
```
Output from the command will be similar to the following:

<table>
<thead>
<tr>
<th>ID: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class: S200</td>
</tr>
</tbody>
</table>

**isi storagepool compatibilities ssd available list**

Lists SSD compatibilities that are available, but not yet created.

**Note**

This command is not applicable for IsilonSD Edge.

**Syntax**

```bash
isi storagepool compatibilities ssd available list

[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

**--limit <integer>**

Limits the number of SSD compatibilities that are listed.

**--format**

Lists active SSD compatibilities in the specified format. The following values are valid:

- table
- json
- csv
- list

**--no-header**

Displays table and CSV output without headers.

**--no-footer**

Displays table output without footers.

**--verbose**

Displays more detailed information.

**Example**

The following command lists available SSD compatibilities:

```bash
isi storagepool compatibilities ssd available list
```

If available SSD compatibilities exist, command output similar to the following example appears:

<table>
<thead>
<tr>
<th>Class 1</th>
</tr>
</thead>
</table>
### Storage Pools

<table>
<thead>
<tr>
<th>S200</th>
<th>S210</th>
<th>Total: 2</th>
</tr>
</thead>
</table>

#### isi storagepool health

Displays the health information of storage pools.

**Syntax**

```
isi storagepool health
```

**Options**

```
--verbose | -v
```

Displays more detailed information.

#### isi storagepool list

Displays node pools and tiers in the cluster.

**Syntax**

```
isi storagepool list
```

**Options**

```
--format {table | json | csv | list}
--no-header
--no-footer
--verbose
```

**--format**

Displays node pools and tiers in the specified format. The following values are valid:

- `table`
- `json`
- `csv`
- `list`

**--no-header | -a**

Displays table and CSV output without headers.

**--no-footer | -z**

Displays table output without footers.

**--verbose | -v**

Displays more detailed information.
isi storagepool nodepools create

Creates a manually managed node pool. This command should only be used by experienced OneFS administrators or with assistance of technical support personnel.

Syntax

```
isi storagepool nodepools create <name>
   [--lnns <lnns>]
   [--verbose]
```

Options

- `<name>`
  Specifies the name for the node pool. Names must begin with a letter or an underscore and may contain only letters, numbers, hyphens, underscores, or periods.

- `--lnns <lnns> | -n <lnns>`
  Specifies the nodes in this pool. Nodes can be a comma-separated list or range of LNNs—for example, 1,4,10,12,14,15 or 1-6.

- `--verbose | -v`
  Displays more detailed information.

isi storagepool nodepools delete

Deletes a node pool and autoprovisions the affected nodes into the appropriate node pool. This command is used only for manually managed node pools and should be executed by experienced OneFS administrators or with direction from technical support personnel.

Syntax

```
isi storagepool nodepools delete <name>
   [--force]
   [--verbose]
```

Options

- `<name>`
  Specifies the name of the node pool to be deleted.

- `--force | -f`
  Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

- `--verbose | -v`
  Displays more detailed information.
isi storagepool nodepools list

Displays a list of node pools.

Syntax

```bash
isi storagepool nodepools list
[--limit <integer>]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

Options

|--limit | -l <integer>
  Specifies the number of node pools to display.

|--format
  Displays tiers in the specified format. The following values are valid:
  table
  json
  csv
  list

|--no-header | -a
  Displays table and CSV output without headers.

|--no-footer | -z
  Displays table output without footers.

|--verbose | -v
  Displays more detailed information.

isi storagepool nodepools modify

Modifies a node pool.

Syntax

```bash
isi storagepool nodepools modify <name>
[--protection-policy <string>]
[--l1ns <integer>]
[--clear-l1ns]
[--add-l1ns <integer>]
[--remove-l1ns <integer>]
[--tier <string>]
[--clear-tier]
[--13 {yes | no}]
[--set-name <string>]
```
Options

<string>
   Name of the node pool to be modified.

--protection-policy <string>
   Requested protection for the node pool. Possible protection policy values are:
   - +1n
   - +2d:1n
   - +2n
   - +3d:1n
   - +3d:1n1d
   - +3n
   - +4d:1n
   - +4d:2n
   - +4n
   - Mirror values: 2x, 3x, 4x, 5x, 6x, 7x, 8x
   OneFS calculates the optimal protection policy (referred to as suggested protection). If the value you set is lower than the suggested protection, OneFS displays an alert.

--lnns <integer>
   Nodes for the manually managed node pool. Specify --lnns for each additional node for the manually managed node pool.

--clear-lnns
   Clear value for nodes for the manually managed node pool.

--add-lnns <integer>
   Add nodes for the manually managed node pool. Specify --add-lnns for each additional node to add.

--remove-lnns <integer>
   Remove nodes for the manually managed node pool. Specify --remove-lnns for each additional node to remove.

--tier <string>
   Set parent for the node pool. Node pools can be grouped into a tier to service particular file pools.

--clear-tier
   Remove the specified node pool from its parent tier.

--l3 {yes | no}
   Use SSDs in the specified node pool as L3 cache. Note that, on Isilon HD400 node pools, L3 cache is on by default and you cannot disable it. If you try to disable L3 cache on an HD400 node pool, OneFS generates the following error message: Disabling L3 not supported for the given node type.

--set-name <string>
   New name for the manually managed node pool.
Examples
The following command specifies that SSDs in a node pool named hq_datastore are to be used as L3 cache:

```bash
isi storagepool nodepools modify hq_datastore --l3 yes
```

The following command adds the node pool hq_datastore to an existing tier named archive-1:

```bash
isi storagepool nodepools modify hq_datastore --tier archive-1
```

**isi storagepool nodepools view**

Displays details for a node pool.

**Syntax**

```bash
isi storagepool nodepools view <name>
[--verbose]
```

**Options**

- `<name>`
  Specifies the name of the storage pool.
- `[--verbose | -v]`
  Displays more detailed information.

**isi storagepool settings modify**

Modifies global SmartPools settings.

**Syntax**

```bash
isi storagepool settings modify
[--automatically-manage-protection {all | files_at_default | none}]
[--automatically-manage-io-optimization {all | files_at_default | none}]
[--protect-directories-one-level-higher {yes | no}]
[--global-namespace-acceleration-enabled {yes | no}]
[--virtual-hot-spare-deny-writes {yes | no}]
[--virtual-hot-spare-hide-spare {yes | no}]
[--virtual-hot-spare-limit-drives <integer>]
[--virtual-hot-spare-limit-percent <integer>]
[--snapshot-disk-pool-policy-id <integer>]
[--spillover-target <string> | --no-spillover | --spillover-anywhere]
[--ssd-l3-cache-default-enabled {yes | no}]
[--verbose]
```

**Required Privileges**

`ISI_PRIV_SMARTPOOLS`
Options

--automatically-manage-protection {all | files_at_default | none}
  Specifies whether SmartPools manages files' protection settings.

--automatically-manage-io-optimization {all | files_at_default | none}
  Specifies whether SmartPools manages I/O optimization settings for files.

--protect-directories-one-level-higher {yes | no}
  Protects directories at one level higher.

--global-namespace-acceleration-enabled {yes | no}
  Enables or disables global namespace acceleration.

--virtual-hot-spare-denies-writes {yes | no}
  Denies new data writes to the virtual hot spare.

--virtual-hot-spare-hide-spare {yes | no}
  Reduces the amount of available space for the virtual hot spare.

--virtual-hot-spare-limit-drives <integer>
  Specifies the maximum number of virtual drives.

--virtual-hot-spare-limit-percent <integer>
  Limits the percentage of node resources that is allocated to virtual hot spare.

--spillover-target <string>
  Specifies the target for spillover.

--no-spillover
  Globally disables spillover.

--spillover-anywhere
  Globally sets spillover to anywhere.

--ssd-l3-cache-default-enabled {yes | no}
  Enables or disables SSDs on new node pools to serve as L3 cache.

--verbose
  Enables verbose messaging.

Examples
The following command specifies that SSDs on newly created node pools are to be used as L3 cache:

  isi storagepool settings modify --ssd-l3-cache-default-enabled yes

The following command specifies that 20 percent of node resources can be used for the virtual hot spare:

  isi storagepool settings modify --virtual-hot-spare-limit-percent 20
 isi storagepool settings view

Displays global SmartPools settings.

Syntax

    isi storagepool settings view

Options

There are no options for this command.

Example

The following command displays the global SmartPools settings on your cluster:

    isi storagepool settings view

The system displays output similar to the following example:

Automatically Manage Protection: files_at_default
Automatically Manage Io Optimization: files_at_default
Protect Directories One Level Higher: Yes
    Global Namespace Acceleration: disabled
    Virtual Hot Spare Deny Writes: Yes
    Virtual Hot Spare Hide Spare: Yes
    Virtual Hot Spare Limit Drives: 1
    Virtual Hot Spare Limit Percent: 0
    Global Spillover: anywhere
    SSD L3 Cache Default Enabled: No

 isi storagepool tiers create

Creates a tier.

Syntax

    isi storagepool tiers create <name>
        [--children <string>]
        [--verbose]

Options

 <name>
     Specifies the name for the storage pool tier. Specify as any string.

 --children <string>
     Specifies a node pool to be added to the tier. For each node pool that you intend
to add, include a separate --children argument.

 --verbose
     Displays more detailed information.

Note

Names must begin with a letter or underscore and must contain only letters, numbers,
hyphens, underscores, or periods.
Example
The following command creates a tier and adds two node pools to the tier:

```
isi storagepool tiers create ARCHIVE_1 --children hq_datastore1
    --children hq_datastore2
```

isi storagepool tiers delete

Deletes a tier.

Syntax

```
isi storagepool tiers delete {<name> | --all}
    [--verbose]
```

Options

```
{<name> | --all}
    Specifies the tier to delete. The acceptable values are the name of the tier or all.

{--verbose | -v}
    Displays more detailed information.
```

isi storagepool tiers list

Displays a list of tiers.

Syntax

```
isi storagepool tiers list
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

Options

```
--format
    Displays tiers in the specified format. The following values are valid:
        table
        json
        csv
        list

{--no-header | -a}
    Displays table and CSV output without headers.

{--no-footer | -z}
    Displays table output without footers.
```
Displays more detailed information.

isi storagepool tiers modify

Renames a tier.

Syntax

isi storagepool tiers modify <name>
   [--set-name <string>]
   [--verbose]

Options

<name>
   Specifies the tier to be renamed.

{--set-name | -s} <string>
   Sets the new name for the tier.

{--verbose | -v}
   Displays more detailed information.

Note

Names must begin with a letter or underscore and must contain only letters, numbers, hyphens, underscores, or periods.

isi storagepool tiers view

Displays details for a tier.

Syntax

isi storagepool tiers view <name>

Options

<name>
   Specifies the name of the tier.

{--verbose | -v}
   Displays more detailed information.
CHAPTER 24

CloudPools

This section contains the following topics:

- CloudPools overview.................................................................950
- Supported cloud providers.........................................................951
- CloudPools concepts.................................................................953
- CloudPools file processing.........................................................954
- Archiving files with file pool policies...........................................955
- Retrieving file data from the cloud..............................................962
- CloudPools interoperability with other OneFS functions...............963
- CloudPools best practices.........................................................967
- CloudPools troubleshooting.......................................................968
- Managing cloud accounts.........................................................972
- Managing CloudPools...............................................................974
- Archiving files with file pool policies...........................................977
- Configuring access to cloud data from a secondary cluster............980
- Managing cloud jobs...............................................................982
- Managing CloudPools settings.................................................985
- CloudPools command reference.................................................986
CloudPools overview

CloudPools extends the capabilities of OneFS by enabling you to specify data to be moved to lower-cost cloud storage. CloudPools can seamlessly connect to EMC-based cloud storage systems and to popular third-party providers, Amazon S3 and Microsoft Azure.

CloudPools is a licensed module built on the SmartPools file pool policy framework, which gives you granular control of file storage on your cluster. CloudPools extends this file storage control to one or more cloud repositories, which act as additional tiers of OneFS storage.

Prior to the introduction of CloudPools, SmartPools enabled the grouping of nodes into storage pools called node pools, and the classification of node pools as different storage tiers. SmartPools includes a policy framework that allows you to segregate files into logical groups called file pools, and to store those file pools in specific storage tiers.

CloudPools expands the SmartPools framework by treating a cloud repository as an additional storage tier. This enables you to move older or seldom-used data to cloud storage and free up space on your cluster.

As with SmartPools, you define files to be stored in the cloud by creating file pool policies. These policies use file matching criteria to determine which file pools are to be moved to the cloud.

File pool policies are applied when the SmartPools system job runs, by default on a daily basis. For each policy, all matched files on the cluster are handled according to policy specifications.

When files match a file pool policy that contains CloudPools actions, OneFS moves the file data of matched files to the cloud. Only metadata and a proxy file remain on the cluster, thus freeing up storage space.

Although file data is moved to remote storage, the files remain visible in the OneFS file system. CloudPools accomplishes this by retaining a local SmartLink file, which is a pointer to the location of data in the cloud. You can read, write, archive, and recall files from the cloud as needed.

When a user accesses a cluster and views the OneFS file system through a supported protocol (SMB, NFS, Swift, or HDFS), SmartLink files appear to be the original files. When the user opens a SmartLink file, OneFS automatically retrieves and caches as much data as needed from the cloud. This operation is called inline access. Any modifications the user makes to a file during inline access are updated in the file data stored in the cloud.

In addition to inline access, CloudPools also provides a CLI command to enable full recall of files from the cloud, in which case the SmartLink files are replaced by the actual files.
## Accessing CloudPools with IsilonSD Edge

The CloudPools software module is available only with a purchased license of IsilonSD Edge. It is not packaged with the free license of this product.

## Supported cloud providers

With CloudPools, OneFS supports these cloud providers: EMC Isilon, EMC ECS Appliance, Virtustream Storage Cloud, Amazon S3, and Microsoft Windows Azure.

### EMC Isilon

CloudPools enables an EMC Isilon cluster to function as a cloud storage provider. In this scenario, a secondary EMC Isilon cluster provides a private cloud solution. The secondary cluster archive files from your primary cluster, and is managed in your corporate data center.

To act as a cloud storage provider, an EMC Isilon cluster uses a set of APIs that include the capabilities to configure CloudPools policies, define cloud storage accounts, and retrieve cloud storage usage reports. These APIs are known collectively as the Isilon Platform API, and are described in the OneFS 8.0 API Reference.

The secondary cluster must be running the same version of OneFS as the primary cluster and must have active SmartPools and CloudPools licenses.

To configure a secondary EMC Isilon cluster as the cloud storage repository, you need to complete several tasks:

- On the secondary cluster, log on with system administrator privileges, and create a new user.
- On the secondary cluster, create a role with access to Console, Platform API, HTTP, License, Namespace Traverse, and Namespace Access privileges, and make the new user a member of this role.
- On the secondary cluster, log on as the new user, and create the directory where cloud data should be stored. For example: /ifs/data/HQ-Archive.
- On the primary cluster, set up the EMC Isilon cloud storage account, specifying the new user's credentials and the appropriate URI for the secondary cluster. Because the secondary cluster is within your corporate network, the URI would look similar to the following example:

  ```
  ```

- On the primary cluster, create a CloudPool that contains the EMC Isilon cloud storage account.

### EMC ECS Appliance

CloudPools supports EMC ECS (Elastic Cloud Service) appliance as a cloud provider. ECS is a complete software-defined cloud storage platform deployed on a turn-key appliance from EMC. It supports the storage, manipulation, and analysis of unstructured data on a massive scale.

The ECS appliance is specifically designed to support mobile, cloud, big data, and next-generation applications. As an appliance, it is simple to install and deploy with
support for multi-tenancy, self-service access, usage metering, on-demand cloud storage-as-a-service and dynamic application provisioning.

**Virtustream Storage Cloud**

CloudPools supports Virtustream Storage Cloud as a cloud provider.

Virtustream Storage Cloud (VSC) is a managed cloud computing service from EMC that offers benefits associated both with a dedicated private cloud and a public multi-tenant cloud.

VSC enables enterprises to run complex, mission-critical applications with full cloud agility, economy, and automation, and to achieve enterprise-class service-level agreements for both application performance and availability. In addition, Virtustream provides a foundation for meeting national and industry-level security, compliance and auditing requirements.

Virtustream Storage Cloud can be managed in your own data center, or provided as a solution from a third party.

**Amazon S3**

CloudPools can be configured to store data on Amazon S3 (Simple Storage System), a public cloud provider.

When you configure CloudPools to use Amazon S3 for cloud storage, in addition to URI, username, and passkey, you must specify the following additional attributes.

- S3 Account ID
- S3 Telemetry Reporting Bucket
- S3 Storage Region

When you first establish an account with Amazon S3, the cloud provider gives you an account ID and allows you to choose a storage region. Amazon S3 offers multiple storage regions in the U.S. and other regions of the world.

---

**Note**

CloudPools supports Amazon Web Services Signature V2 to authenticate queries to its cloud storage. CloudPools does not support Signature V4.

To work with CloudPools, you must also identify an S3 telemetry reporting bucket. This is where billing reports are stored on Amazon S3. This bucket must be accessible to CloudPools.

To set up an S3 telemetry reporting bucket, navigate to **Billing & Cost Management** preferences in the S3 console. There you can indicate that you want to receive billing reports, and specify the bucket to which these reports should be saved. Use this bucket name as the telemetry reporting bucket when setting up an S3 cloud storage account in CloudPools.

**Microsoft Azure**

You can configure CloudPools to store data on Microsoft Azure, a public cloud provider.

When you first establish an account with Microsoft Azure, you create a user name, and Microsoft provides you with a URI and a passkey. When you configure CloudPools to use Azure, you must specify the same URI, username and passkey.
CloudPools concepts

CloudPools is a licensed module that enables you to move file data on your Isilon cluster to the cloud, and to access or recall these files when needed. Taking advantage of CloudPools requires you to configure cloud storage accounts and file pool policies that specify cloud storage targets.

You can configure CloudPools to move files to the cloud automatically, based on file pool policies. You can also use a OneFS command to archive individual files to, or recall files from, the cloud.

CloudPools uses a similar workflow to OneFS SmartPools. To store files in the cloud, you must have at least one account with a cloud storage provider. In addition, you must configure OneFS for cloud storage, and create file pool policies that identify and move files to the cloud.

When the SmartPools job runs, typically once a day, file pool policies are executed, and matched files are sent to the cloud storage target. To access file data stored in the cloud, you can open its related SmartLink file through any supported protocol (SMB, NFS, Swift, or HDFS). This is referred to as inline access. To fully recall a file from the cloud, you can issue an `isi cloud recall` command from the OneFS command-line interface.

Following are descriptions of key CloudPools concepts:

**Archive**

The CloudPools process of moving file data to the cloud. This process involves extracting the data from the file and placing it in one or more cloud objects. CloudPools then moves these objects to cloud storage, and leaves in place on the local cluster a representative file called a SmartLink.

**Recall**

The CloudPools process of reversing the archival process. When you recall a file from the cloud, CloudPools replaces the SmartLink file by restoring the original file data on OneFS and removing the cloud objects from cloud storage.

**SmartLink file**

For every file archived to the cloud, OneFS maintains an associated SmartLink file on the cluster. A SmartLink file contains metadata and map information so the data in the cloud can be accessed or fully recalled. If allowed by a SmartLink file's archiving policy, accessing the SmartLink file on the cluster automatically retrieves and caches data from the cloud. Like other files, SmartLink files can be backed up through NDMP or synchronized to other clusters with SyncIQ. When SmartLink files are retrieved from a backup or SyncIQ operation, CloudPools maintains their links to related file data in the cloud.

**File pool policies**

File pool policies are the essential control mechanism for both SmartPools and CloudPools. OneFS runs all file pool policies on a regular basis. Each file pool policy specifies the files to be managed, actions to take on the files, protection levels, and I/O optimization settings.

If CloudPools has been enabled, each file pool policy can also contain cloud-specific parameters that specify the remote cloud account to archive files to, and how to handle files prior to archiving them. Moreover, a policy can also specify
SmartPools targets that specify where to store the locally-retained SmartLink files related to the stored cloud data.

**Cloud provider accounts**

Making use of cloud storage requires you to set up one or more accounts with a cloud provider. The types of cloud storage that are currently supported are EMC Isilon, EMC ECS Appliance, Virtustream Storage Cloud, Amazon S3, and Microsoft Azure. The account information from the cloud provider must match the information you use when configuring cloud accounts on your Isilon cluster.

**Cloud storage accounts**

A cloud storage account is a OneFS entity that defines access to a specific cloud provider account. The cloud storage account settings must match the account credentials provided by the cloud provider.

**CloudPool**

A CloudPool is a OneFS entity that contains a single cloud storage account and provides a conduit between OneFS and the cloud storage repository. Creating a CloudPool requires the availability of at least one cloud storage account. The cloud storage account must be of the same type as the CloudPool.

**Inline access**

CloudPools enables users connecting to a cluster through supported protocols to access cloud data by opening associated SmartLink files. This process is referred to as inline access. To the user connecting to OneFS through a supported protocol, a SmartLink file appears to be the original file. When the user opens a SmartLink file, CloudPools retrieves and caches cloud data locally. The user can view and edit the file as usual. CloudPools automatically retrieves and sends any updated file data back to the cloud so that the cloud contains the latest version.

**Note**

CloudPools offers inline access as a user convenience. However, CloudPools is designed mainly as an archival solution, and is not intended for storing data that is frequently updated. Such data should be left on the local cluster until it stabilizes and is ready for archival.

**CloudPools file processing**

CloudPools archives file data to the cloud, and enables you to access or fully recall this data whenever needed.

You can create file pool policies that identify the files to be archived to the cloud. When a file pool policy that contains cloud actions is run, CloudPools moves file data to the cloud and stores it in specialized cloud data objects, collectively referred to as cloud data. File data can be encrypted and compressed before it is archived to the cloud.

In place of each file that is archived, CloudPools retains a local proxy called a SmartLink file. SmartLink files include special metadata and maps to the actual file data in the cloud.

When a user browses OneFS, typically through an SMB connection or NFS export, SmartLink files appear in place as the files they link to. When a user opens a SmartLink
file, a process referred to as inline access, CloudPools retrieves file data from the cloud and caches it locally.

The user can view the file, and CloudPools continues caching as much of the data as needed by the application. If the user modifies and saves the file, the changes are also held in cache. Periodically, CloudPools scans SmartLink files for pending data changes and writes them to the appropriate objects in the cloud. In this way, the archived data is kept up to date.

You can also recall archived files from the cloud. When you do, SmartLink files are fully replaced by the recalled files.

Like any file in OneFS, SmartLink files are controlled either by the default file pool policy or by parameters included in a custom file pool policy. If you configure additional file pool policies, these policies have priority over the default file pool policy.

File pool policies contain instructions that determine how OneFS manages files across a cluster and in the cloud.

Because SmartLink files produced by CloudPools are retained on the cluster, OneFS applies file pool policies to these files, as well.

When file pool policies run, the system compares each file on the system with each file pool policy. A file can match only some aspects of a custom file pool policy (for example, SSD strategy and snapshot configuration). In this case, those aspects of file handling are governed by the custom file pool policy, and all other aspects are governed by the default file pool policy.

Refer to the *SmartPools* chapter for complete information about file pool policies.

### Archiving files with file pool policies

You can configure a file pool policy to identify the files you want to archive to the cloud and the CloudPools actions to apply to these files.

Specifying a file pool policy, you can archive files using either the OneFS web administration interface or the command-line interface. A file pool policy that archives files to the cloud must specify the following information:

- **Files to manage:** These can be files of a certain type, files in a specified path, or files that match specified criteria, such as size, creation date, or last modified date.
- **CloudPools actions:** The cloud storage pool to send file data to, and whether the data should be compressed or encrypted.

### Sample policies with CloudPools actions

Each file pool policy identifies a set of files and the CloudPools actions to apply to the file pool. You can identify files to be archived based on multiple criteria, including file type, size, directory path, time of file creation, time of last file access, and time of last file modification.

File-matching criteria in a file pool policy enable you to define a logical group of files referred to as a file pool. After defining a file pool, you specify CloudPools actions to perform on the files, including the cloud storage target, compression, and encryption.

For example, you might define file pool policies that specify files to be archived based on criteria similar to the following:

- Files of `<type>`, last accessed before `<date>`
- Files older than `<date>`, last accessed after `<date>`, and of `<type>`
Files in <directory> that are older than <date>
Files marked with <custom attribute>, that are older than <date>

You can specify file-matching criteria on a per-policy basis. Each file pool policy allows you to combine multiple criteria using AND statements and OR statements, providing significant flexibility and control for your workflow.

About file pool policy order

OneFS compares all files to file pool policies in order. The first custom policy that matches a file controls how that file is handled. All other custom file pool policies in the ordered list are ignored. For any of the attributes that the matching custom policy does not specify, the value from the default policy is applied.

This makes the order of file pool policies important. If two or more file pool policies would match the same file, you must ensure that the policy order delivers your preferred file handling instructions.

After a file match with a file pool policy occurs, the system uses the settings in the matching policy to store and protect the file. However, a matching policy might not specify all settings for the match file. In this case, the default policy is used for those settings not specified in the custom policy. For each file stored on the OneFS cluster, the system needs to determine the following:

- Requested protection level
- Data storage target for local data cache
- SSD strategy for metadata and data
- Protection level for local data cache
- Configuration for snapshots
- SmartCache setting
- L3 cache setting
- Data access pattern
- CloudPools actions (if any)

If no custom policy matches a file, the default policy specifies all storage settings for the file. The default policy, in effect, matches all files not matched by any other SmartPools policy. For this reason, the default policy is the last in the file pool policy list, and always the last policy the system applies.

Files that have been archived to the cloud are always governed by the original policy.

File pool policy cloud archive parameters

CloudPools provides a specific set of file pool parameters that support archiving files to the cloud. The following table lists and describes these parameters.

<table>
<thead>
<tr>
<th>Web admin parameter</th>
<th>CLI parameter</th>
<th>Description</th>
<th>Usage notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPool Storage Target</td>
<td>cloud-pool</td>
<td>An Isilon administrative container for a cloud storage account.</td>
<td>Each CloudPool can contain only one cloud storage account with a cloud provider. You must create a cloud storage account</td>
</tr>
<tr>
<td><strong>Web admin parameter</strong></td>
<td><strong>CLI parameter</strong></td>
<td><strong>Description</strong></td>
<td><strong>Usage notes</strong></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Encrypt data before transfer</td>
<td>cloud-encryption-enabled</td>
<td>Specifies whether CloudPools encrypts data prior to archiving it. The default value is disabled.</td>
<td>Specifies whether data is encrypted prior to archiving to the cloud. Cloud data is decrypted when accessed or recalled.</td>
</tr>
<tr>
<td>Compress data before transfer</td>
<td>cloud-compression-enabled</td>
<td>Specifies whether CloudPools compresses data prior to archiving it. The default value is disabled.</td>
<td>Specifies whether data is compressed prior to archiving to the cloud. Cloud data is decompressed when accessed or recalled.</td>
</tr>
<tr>
<td>Cloud Data Retention Period</td>
<td>cloud-data-retention</td>
<td>The length of time cloud files are retained after the files have been fully recalled. The default value is 1 week.</td>
<td>Specifies how long cloud objects are retained after a SmartLink file has been replaced by the recalled file. When this happens, CloudPools cleans up local resources allocated for the SmartLink files, and also removes the associated cloud objects. This work is performed weekly by the cloud objects garbage collector job.</td>
</tr>
<tr>
<td>Web admin parameter</td>
<td>CLI parameter</td>
<td>Description</td>
<td>Usage notes</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The system removes (garbage-collects) cloud objects when their SmartLink files and all local references to them have been removed. If a SmartLink file has been backed up and the original SmartLink file is subsequently deleted, associated cloud objects are deleted only after the retention time of the backed-up SmartLink file has expired.</td>
</tr>
<tr>
<td>Incremental Backup Retention Period for NDMP Incremental</td>
<td>cloud-incremental-</td>
<td>Specifies the length of time that OneFS retains cloud data referenced by a SmartLink file that has been replicated by SyncIQ or an incremental NDMP backup. The default value is 5 years.</td>
<td>If a SmartLink file has been backed up and the original SmartLink file is subsequently deleted, associated cloud objects are deleted only after the retention time of the backed-up SmartLink file has expired.</td>
</tr>
<tr>
<td>Backup and SyncIQ</td>
<td>backup-retention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Backup Retention Period for NDMP Only</td>
<td>cloud-full-backup-</td>
<td>Specifies the length of time that OneFS retains cloud data referenced by a SmartLink file that has been backed up by a full NDMP backup. The default value is 5 years.</td>
<td>If a SmartLink file has been backed up and the original SmartLink file is subsequently deleted, associated cloud objects are deleted only after the original retention time, or a longer incremental or full backup retention period, has expired.</td>
</tr>
<tr>
<td></td>
<td>retention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web admin parameter</td>
<td>CLI parameter</td>
<td>Description</td>
<td>Usage notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Writeback Frequency</td>
<td>cloud-writeback-frequency</td>
<td>Specified the interval at which the system writes the data stored in the cache of SmartLink files to the cloud.</td>
<td>Specifies how often SmartLink files modified on the cluster are written to their associated cloud data objects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 9 hours</td>
<td></td>
</tr>
<tr>
<td>Accessibility</td>
<td>cloud-accessibility</td>
<td>Specifies how data is cached in SmartLink files when a user or application accesses a SmartLink file on the cluster. Values are cached and no-cache. The default value is cached.</td>
<td>Determines whether cloud data is cached when a file is accessed on the local cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cached</td>
<td>When cached is selected, accessed cloud data is cached to the SmartLink file on read or write access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>no-cache</td>
<td>When no-cache is selected, the system does not cache data in the SmartLink files on read access, but passes it through to the local accessing application. If you write to data accessed when this setting applies, the system caches your changes. Choose no-cache if you want to limit the use of</td>
</tr>
<tr>
<td>Web admin parameter</td>
<td>CLI parameter</td>
<td>Description</td>
<td>Usage notes</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cache Read Ahead</td>
<td>cloud-readahead</td>
<td>Specifies the cache readahead strategy for cloud files (one of partial or full)</td>
<td>Specifies whether cloud data is fully or partially recalled when you access a SmartLink file on the cluster. If partial is specified, the system only recalls the file blocks needed when a SmartLink file is accessed. If full is specified, all cloud data is fully cached when the SmartLink file is accessed.</td>
</tr>
<tr>
<td>Cache Expiration</td>
<td>cloud-cache-expiration</td>
<td>Specifies the number of days until the system purges expired cache information in SmartLink files. The default value is 1 day.</td>
<td>Specifies how long the system retains cloud data that has been recalled in the cache of associated SmartLink files. The system purges the SmartLink file cache of data that has not been accessed for the number of days specified.</td>
</tr>
<tr>
<td>Archive Files with Snapshots</td>
<td>cloud-archive-snapshot-files</td>
<td>Specifies whether the policy should archive files with snapshots. The default is on.</td>
<td>Snapshots capture files at a moment in time. If a policy matches a file that is included in a snapshot, the file can be archived or not depending on this setting.</td>
</tr>
</tbody>
</table>

**File matching options for cloud archival policies**

Each file pool policy must provide match criteria to identify the files to archive and the cloud target where the files should be stored.

The following table describes the match criteria to use when creating file pool policies.
<table>
<thead>
<tr>
<th>Match criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web admin interface</strong></td>
<td><strong>Command line interface</strong></td>
</tr>
<tr>
<td>Filename</td>
<td>--name</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on the file name. You can specify whether to include or exclude full or partial names that contain specific text. Wildcard characters are supported.</td>
</tr>
<tr>
<td>Path</td>
<td>--path</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on the file path. You can specify whether to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters *, ?, and [ ].</td>
</tr>
<tr>
<td>File Type</td>
<td>--file-type</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on one of the following file-system object types:</td>
</tr>
<tr>
<td></td>
<td>• Regular file</td>
</tr>
<tr>
<td></td>
<td>• Directory</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>File Attribute</td>
<td>--custom-attribute</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on a custom user-defined attribute.</td>
</tr>
<tr>
<td>Modified</td>
<td>--changed-time</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on when the file was last modified. You can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot; Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Accessed</td>
<td>--accessed-time</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on when the file was last accessed. You can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot; Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Metadata Changed</td>
<td>--metadata-changed-time</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on when the file metadata was last modified. This option is available only if the global access-time-tracking option of the cluster is enabled. You can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot; Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Created</td>
<td>--birth-time</td>
</tr>
<tr>
<td></td>
<td>Includes or excludes files based on when the file was created. You can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot; Time settings are based on a 24-hour clock.</td>
</tr>
</tbody>
</table>
### Match criteria

<table>
<thead>
<tr>
<th>Match criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web admin interface</strong></td>
<td><strong>Command line interface</strong></td>
</tr>
<tr>
<td></td>
<td>&quot;before January 1, 2012.&quot; Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td><strong>--size</strong></td>
</tr>
<tr>
<td>Includes or excludes files based on their size.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

File sizes are represented in multiples of 1024, not 1000.

---

### Combining cloud and local storage policy actions

You can specify both cloud and a local storage actions in the same file pool policy. The cloud actions are applied to the data of matching files, while the local actions apply to the SmartLink files that are created in place.

SmartPools settings can determine the target storage pool or tier, file protection level, I/O optimization, and data access optimization. The SmartLink files are processed according to the specified SmartPools parameters. If some settings are not specified in the custom file pool policy, the default file pool policy settings are applied to the SmartLink files.

---

### Retrieving file data from the cloud

You can retrieve file data from the cloud either by inline access through a supported protocol (SMB, NFS, Swift, or HDFS), or by fully recalling files.

#### Inline access of cloud data

Users can retrieve file data in the cloud by accessing a SmartLink file on the local cluster through a supported protocol. This method is referred to as inline access.

When the user opens a SmartLink file, for example, through an SMB share, CloudPools retrieves and locally caches file data from the cloud. The amount of data that is cached is determined by the CloudPools **Cache Read Ahead** setting.

If the user makes changes to the file, CloudPools maintains those changes in cache and periodically updates file data to the cloud so that the latest version is always archived.

#### Recalling files from the cloud

You can fully recall a file from cloud storage. In this case, CloudPools restores the full file to the cluster and overwrites its associated SmartLink file. As part of a daily maintenance routine, CloudPools also completely removes the recalled file data from the cloud.

You can recall files from cloud storage only with the CLI command `isi cloud recall`. You can recall files individually by name or by specifying a fully recursive directory path.
CloudPools interoperability with other OneFS functions

CloudPools is designed to work seamlessly with other OneFS functions, including data encryption and compression, SMB and NFS support, SyncIQ, snapshots, and NDMP backup and recovery.

Compression and encryption of cloud data

You can specify compression and encryption of data that is moved to the cloud. With CloudPools, you can enable compression and encryption on a per-policy basis. Both encryption and compression are disabled by default.

Files encrypted or compressed when stored in the cloud are automatically decrypted and decompressed when data is cached (inline access) or the file is recalled from the cloud to local storage.

CloudPools uses a master encryption key to encrypt the data encryption keys. Encryption applies to both the SmartLink file and the file data archived to the cloud. Both the SmartLink file and the archived data include encrypted copies of the data encryption keys. After a file is encrypted, it can only be decrypted by recalling it.

CloudPools keeps track of the encryption status of SmartLink files in snapshots and referenced data in the cloud. If SmartLink files in snapshots are unencrypted and refer to unencrypted cloud objects, the SmartLink files in the snapshots remain unencrypted even if you create a new CloudPools policy that encrypts the latest version of the file.

OneFS stores the master encryption key in the local key management system. You can generate a new version of the key if you believe the key has been compromised. If regenerated, the new master key secures new data written to the cloud. Previously written data is secured by the old data encryption keys, resident in the local SmartLink files.

NFS inline access

CloudPools enables access of SmartLink files from NFS exports.

When a user connects to a cluster through an NFS export, and browses the file system, SmartLink files appear to be the original files. When the user opens a SmartLink file, CloudPools retrieves and caches the original file data from the cloud. Depending on the Cache Read Ahead setting, either a portion of the file data, or the entire file, is cached.

If the user modifies the file, CloudPools stores the changes in the cache and periodically writes the changes back to the cloud. In this way, cloud data is kept fully up to date.
**SMB inline access**

CloudPools enables access of SmartLink files from SMB shares. When a user connects to a cluster through an SMB share, and browses the file system, SmartLink files appear to be the original files. When the user opens a SmartLink file, CloudPools retrieves and caches the original file data from the cloud. Depending on the **Cache Read Ahead** setting, either a portion of the file data, or the entire file, is cached.

If the user modifies the file, CloudPools caches the changes and periodically writes the changes back to the cloud. In this way, the cloud data is kept fully up to date.

**Other protocols supporting inline access**

Cloud data can be accessed programmatically through Swift and HDFS by accessing the associated SmartLink files.

We recommend that you consult with your Isilon representative for more information on these use cases.

**SyncIQ interoperability**

SyncIQ enables you to synchronize data from your Isilon primary (source) cluster to a secondary (target) cluster. If your primary cluster becomes unavailable, you can fail over to the secondary cluster, and users can continue to access data, including data stored in the cloud.

During SyncIQ replication, all files, including SmartLink files, are copied from the source cluster to the target cluster. Users given access to the target cluster through supported protocols can retrieve cloud data or fully recall files from the cloud. In these cases, CloudPools retrieves and caches data (inline access) or recalls the full file exactly as it would from the original source cluster.

Unless you specifically grant cloud write access to the secondary cluster, CloudPools stores any changes to SmartLink files in the local cache, which is limited only by available space on the cluster.

**SyncIQ policies**

CloudPools supports SyncIQ replication of SmartLink files to one or more target clusters. SyncIQ can also be used to restore backed up SmartLink files to their original (source) cluster.

The two types of SyncIQ policies are synchronization policies and copy policies. These policies can be run manually, or configured to run automatically, based on policy settings.

CloudPools supports both types of SyncIQ policy. When SyncIQ replicates SmartLink files to a target cluster, secondary information associated with a SmartLink file, such as local cache state and unsynchronized cache data, is also replicated.

If your source (primary) cluster goes down or is unavailable for any reason, and you fail over to your secondary cluster, users can continue to access SmartLink files and, therefore, cloud data, as they would normally.

If the failover is temporary and you plan to restore your source cluster to full operation, you do not need to enable cloud write access on the secondary cluster. Any changes that users make to SmartLink files are stored in the local cache, which is limited only by the amount of free space on your cluster.
When you fail back to your source cluster, and restore updated SmartLink files, only then will CloudPools write the cached modifications back to the cloud.

⚠️ CAUTION ⚠️

If your failover is long-term or permanent, you can grant cloud write access to the secondary cluster by using the `isi cloud access add` command in the CLI. However, you should only ever allow cloud write access on one cluster at a time. Otherwise, corruption of cloud data can occur.

CloudPools cloud data retention time

In CloudPools, cloud data is governed by a concept referred to as retention. Retention time defines an absolute time for cloud data to remain in cloud storage after the related SmartLink file has been deleted.

When you use CloudPools to archive a file from your cluster to cloud storage, a SmartLink file is created on the Isilon cluster in place of the archived file. As long as data from a file remains in the cloud, the SmartLink file remains in place to represent and point to the cloud data.

Because a SmartLink file can be backed up to tape through NDMP and replicated to another Isilon cluster through SyncIQ, more than one SmartLink file can be pointing to the same cloud data at the same time.

However, importantly, cloud data can be deleted even if there is a related SmartLink file on another cluster that was restored by a SyncIQ or NDMP process. Cloud data is maintained until the minimum duration of its retention times on all clusters has expired.

Retention time is affected by the following archive policy retention periods:

- **Cloud Data Retention Period** specifies the retention time of cloud data beyond the time when an associated local Smartlink file is deleted. The default setting is one week.

- **Backup Retention Period for NDMP Incremental Backup and SyncIQ** specifies the retention time of cloud data whose SmartLink file has been backed up by an incremental NDMP backup, or replicated by a SyncIQ operation. If a local SmartLink file is deleted, the SmartLink file copy can be restored, and cloud data can still be accessed. The default setting is five years.

- **Full Backup Retention Period for NDMP Only** is the retention time of cloud data whose SmartLink file has been backed up by a full NDMP backup only. If a local SmartLink file is deleted, the SmartLink file copy can be restored from the backup, and cloud data can still be accessed. The default setting is five years.

Managing SmartLink files that have been replicated

If you modify or delete a SmartLink file that has been replicated in a SyncIQ operation, CloudPools can modify or delete its associated cloud objects.

If you modify a SmartLink file on the primary cluster, changes are cached and, depending on the **Writeback Frequency** setting, are periodically written back to the cloud. In this way, cloud data is always kept up to date.

If you modify a SmartLink file on a secondary cluster, because the primary cluster is temporarily unavailable, changes will remain in cache. When you fail back to the primary cluster, only then are changes able to be written back to the cloud according to the **Writeback Frequency** setting.

Similarly, when a SmartLink file that has been replicated in a SyncIQ operation is deleted, CloudPools appropriately manages the associated cloud data. Two retention
periods can affect the cloud objects associated with a SmartLink file that has been replicated: the **Cloud Data Retention Period** and the **Incremental Backup Retention Period for NDMP Incremental Backup and SyncIQ**.

When a SmartLink file has been replicated to a secondary cluster, and is then deleted from the primary cluster, CloudPools uses both the **Cloud Data Retention Period** and the **Incremental Backup Retention Period for NDMP Incremental Backup and SyncIQ** settings to determine when the associated cloud objects should be deleted. CloudPools uses the longer of the two durations to determine when to delete cloud data.

For example, if the longer of the two retention periods is the **Incremental Backup Retention Period for NDMP Incremental Backup and SyncIQ** setting, then CloudPools uses that setting to determine when to delete cloud data after its associated SmartLink file is deleted.

If you delete a SmartLink file on a secondary cluster, because the primary cluster is temporarily unavailable, the deleted state will remain in cache. When you fail back to the primary cluster, CloudPools deletes the SmartLink file, and uses the retention settings to determine when to delete the associated cloud data.

### SyncIQ deep copy

You can create a SyncIQ policy that restores full files rather than SmartLink files when copying data from the primary (source) cluster to a secondary (target) cluster.

When you create a SyncIQ policy, you can modify the **Deep Copy for CloudPools** setting. The default setting is **Deny**, which means that, during a SyncIQ operation, SmartLink files are replicated to the target cluster.

Alternatively, you can select either the **Allow** or **Force** option for deep copy. When you select **Allow**, SyncIQ still replicates SmartLink files to the target cluster unless there is a SmartLink version mismatch, in which case the full file data is retrieved from the cloud and replicated.

When you specify **Force** for deep copy, CloudPools retrieves and copies full file data from the cloud for all SmartLink files affected by the SyncIQ policy, and replicates the full files to the target cluster.

---

**Note**

A SyncIQ operation that forces deep copy can take significantly more time and consume more system resources. We recommend that you not specify deep copy unless you have a specific reason to do so. For example, if you are backing up data from the primary cluster to a secondary cluster that is running an older (pre-8.0) version of OneFS, then you should use deep copy. If you are unsure whether to use deep copy, contact your EMC Isilon representative for guidance.

### SnapshotIQ integration

The SnapshotIQ function enables you to create a point-in-time backup of a directory in OneFS, while continuing with normal file modifications. CloudPools can control whether files that have other snapshot versions are stored in the cloud.

As part of file matching, CloudPools finds any snapshot versions of matched files, and lets you specify whether these files should be archived to the cloud. If you specify that files with snapshots should be archived, CloudPools archives the most recent file data to the cloud and creates a local SmartLink file in its place. However, the full-data file versions in snapshots are also maintained in OneFS. The default setting is to allow files with snapshot versions to be archived, but you can change the default setting.
Note

Allowing archival of files that have snapshot versions does not result in space savings on your local cluster. It is recommended that you delete older snapshots that you no longer need to increase free space on your cluster.

CloudPools also supports SnapRevert for SmartLink files. For example, suppose that CloudPools archived a directory named /ifs/data/images to the cloud. The files in the images directory would be replaced with SmartLink files.

If you create a SnapRevert domain for the directory, and run the SnapRevert job, the CloudPools archival process is reversed, and the original files are restored to the directory. CloudPools removes any cloud data that was created as part of the original archive process.

NDMP backup and restore of cloud data

You can perform NDMP backup and restore operations on data that has been archived to the cloud.

Backup and restore capabilities with CloudPools data include:

- Archive SmartLink files when backing up from a cluster
- Restore data, including SmartLink files, to the same cluster
- Restore data, including SmartLink files, to another cluster

With NDMP backup, CloudPools supports backup of SmartLink files only. No cloud data is included in the backup. Secondary information such as account information, local cache state, and unsynchronized cache data associated with the SmartLink file is also backed up.

You can set three CloudPools retention periods that affect backed up SmartLink files and their associated cloud data:

- Full Backup Retention Period for NDMP takes effect when the SmartLink file is backed up as part of a full backup. The default is five years.
- Incremental Backup Retention Period for Incremental NDMP Backup and SyncIQ takes effect when a SmartLink file is backed up as part of an incremental backup. The default is five years.
- Cloud Data Retention Period defines the duration that data in the cloud is kept when its related SmartLink file is deleted. The default is one week.

CloudPools ensures the validity of a backed-up SmartLink file within the cloud data retention period. It is important for you to set the retention periods appropriately to ensure that when the SmartLink file is restored from tape, it remains valid. CloudPools disallows restoring invalid SmartLink files.

To check whether a backed-up SmartLink file is still valid, CloudPools checks the retention periods stored on tape for the file. If the retention time is past the restore time, CloudPools prevents NDMP from restoring the SmartLink file.

CloudPools also makes sure that the account under which the SmartLink files were originally created has not been deleted. If it has, both NDMP backup and restore of SmartLink files will fail.

CloudPools best practices

For best results using CloudPools, follow these best practices.
Use time stamps for cloud data archival and recall

Use time matching patterns (creation, modification, last access) when you archive data to and recall data from the cloud. This enables more efficient archival and recall operations, therefore better performance.

When you create a file pool policy for archiving data to the cloud, several of the file-matching criteria involve time:

- Created
- Accessed
- Modified

Therefore, you can specify file-matching criteria that specify when the files were created, when files were last accessed, or when they were last modified.

CloudPools can also more efficiently recall files based on time stamps.

CloudPools archiving and file size

You can gain the most benefit from CloudPools, in terms of freeing up storage space on your cluster, by archiving larger files. Archiving small files provides less, if any, benefit.

One of the benefits of archiving files to the cloud with CloudPools is how quickly you can recall these files when needed.

To enable fast recall, CloudPools creates a SmartLink file for every file whose data is archived to the cloud. SmartLink files each contain a map to the data in the cloud, meta data, and cache space. SmartLink files are generally small in size, but can grow if data is cached through inline access.

Therefore, if you archive small files to the cloud, SmartLink files are left in their place on the cluster, and could approach, or even exceed, the size of the original file.

Create exclusive accounts for CloudPools purposes

You should create an account with your cloud provider that is exclusively for CloudPools use. This prevents conflicts that might lead to data corruption or loss.

If your organization accesses cloud provider accounts outside of OneFS CloudPools operation, users must be careful not to in any way access or change data archived by CloudPools. Any such data access or modification would likely corrupt the data and compromise data retrieval and recall from CloudPools.

To prevent this, create an account in CloudPools that is exclusively for CloudPools use. Use entirely separate accounts for other cloud applications with your cloud provider.

CloudPools troubleshooting

If you encounter problems using CloudPools, refer to the information provided in this section before contacting Isilon Customer Support.
CloudPools expected behaviors

During normal CloudPools operation, you should be aware of the following limitations and expected behaviors.

**Rolling upgrade before CloudPools usage**
If you are performing a rolling upgrade to the new OneFS version, make sure the upgrade is fully complete before activating CloudPools.

**Cloud storage account deletion**
Warning: Do not delete a cloud storage account that is in use by archived files. This can lead to data being lost or unavailable for the archived files that use that account. Any attempt to open SmartLink files associated with a deleted account will fail with I/O error messages. In addition, NDMP backup and restore and SyncIQ failover and failback will fail when a cloud storage account has been deleted. If, through inline access, an NFS or SMB user attempts to open a SmartLink file, and receives an I/O error, this can mean that the related cloud storage account has been deleted. We recommend trying inline access of other SmartLink files in the same CloudPool. If the same error is generated for those files, the cloud storage account has been deleted and data is lost. If the other SmartLink files are accessible, the SmartLink file that generated the error might be corrupted. Either way, you should contact EMC Isilon Support for assistance.

**Accessing SmartLink files**
You can view and modify cloud data by accessing SmartLink files through supported protocols (NFS, SMB, Swift, and HDFS). If you attempt to access a SmartLink file directly on the cluster, through a command running on the cluster, or through an unsupported protocol, an I/O error is generated. Local access for SmartLink files is blocked for these commands: `tar`, `gzip`, `scp`, `AVscan`, and Job Engine jobs. Cloning of a SmartLink file is also prevented and will return an EINVAL error.

**SmartLink file timestamps can change**
Opening a SmartLink file through a supported protocol can change the timestamp data. When a file is first archived, and the SmartLink file is created in its place, the ctime timestamp stays the same as the original file's timestamp. However, the first time the SmartLink file is opened (inline access), the ctime timestamp changes as a cache component is added to the file. Also, if an archived file is fully recalled, its ctime and mtime timestamps change.

**Inline access can appear to convert a SmartLink file to a regular file**
When a user accesses a SmartLink file on the Isilon cluster from a supported protocol, the file opens in an application on the client computer. During this process, called inline access, most applications support the creation of a CloudPools cache from which users can view and, if desired, modify archived data. With inline access, the SmartLink file remains intact on the cluster, and any modifications that the user makes to file data are stored in the cache and updated to the cloud.

However, some applications do not support inline access. Instead, these applications create a new copy of the original file apart from the SmartLink file. The new file, containing all original file data, is given a new logical I-node (LIN) number and timestamps that differ from the file that was originally archived. This behavior has been observed in only a few programs, including Microsoft Office applications. In these cases, since an entirely new file is created, the original
SmartLink file and its associated data in the cloud is tagged for removal (garbage collection).

If the new file meets the criteria of the file pool policy that archived the original file to the cloud, the new file is archived to the cloud the next time the SmartPools job runs, and a new SmartLink file is created in its place on the local cluster. If the new file does not meet the policy criteria, the full file remains on the cluster.

For best results using CloudPools, we recommend that you avoid archiving files that are still being actively modified by your users.

**Copying a SmartLink file from one cluster to another can result in a corrupted SmartLink file**

If you use scp (Secure Copy) or other copy commands to copy a SmartLink file from one cluster to another, the resulting SmartLink file is corrupted.

**Running Antivirus on SmartLink files generates errors**

We recommend that you avoid creating policies that run Antivirus on directories containing SmartLink files. Running Antivirus on SmartLink files generates error messages. If you do run Antivirus on such directories, you can safely ignore these messages.

**Other issues accessing SmartLink files**

If the node does not have quorum, or the file system is read-only, or /ifs is not available, then you might encounter issues accessing SmartLink files.

**Client-based tools and SmartLink files**

If you run an SMB or NFS client-based tool such as AVScan (anti-virus scan) or a backup application, file data in the cloud is fully cached back to the SmartLink files. This can result in heavy network usage and increased service provider costs, and would also negate space saving on your cluster.

**Expired SmartLink files**

Expired SmartLink files are not restored using NDMP and do not synch back using SyncIQ. A SmartLink file on an NDMP backup or on a SyncIQ secondary (target) cluster is expired when the original SmartLink file has been deleted from the primary (source) cluster, or the original file data in the cloud has been fully recalled.

**Recall can be interrupted**

When a full cache is in process (that is, someone performed an inline access of a SmartLink file from an SMB share or NFS export), recall of the same file can fail. When this happens, the full cache is allowed to complete first, and the user should retry the recall after caching is completed.

**ADS files**

CloudPools does not archive and recall ADS (alternate data stream) files.

**SMB Oplock**

SMB Oplock (lease/notification) does not work in cases where you create a file with the SUPERCEDE flag, and the file already exists and is archived.
CloudPools logs

You can access CloudPools logs to view activity and troubleshoot problems. The following logs are available in OneFS for CloudPools operation.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client cluster-side logs</td>
<td>Cpool daemon</td>
<td>/var/log/isi_cpool_d.log</td>
</tr>
<tr>
<td></td>
<td>Job Engine</td>
<td>/var/log/isi_job_d.log</td>
</tr>
<tr>
<td></td>
<td>SMB and NFS I/O</td>
<td>/var/log/isi_cpool_io_d.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and /var/log/lwiod.log</td>
</tr>
<tr>
<td></td>
<td>Provisioning</td>
<td>/var/log/isi_papi_d.log</td>
</tr>
<tr>
<td></td>
<td>NDMP</td>
<td>/var/log/isi_ndmp_d.log</td>
</tr>
<tr>
<td></td>
<td>SyncIQ</td>
<td>/var/log/isi_migrate.log</td>
</tr>
<tr>
<td></td>
<td>Messages</td>
<td>/var/log/messages</td>
</tr>
<tr>
<td>Platform API cloud-side logs</td>
<td>Platform API (RAN)</td>
<td>/var/log/isi_object_d.log</td>
</tr>
<tr>
<td></td>
<td>HTTPd apache</td>
<td>/var/log/apache2/webui_httpd_error.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and /var/log/apache2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and webui_httpd_access.log</td>
</tr>
<tr>
<td></td>
<td>Session authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages</td>
<td>/var/log/messages</td>
</tr>
</tbody>
</table>

Note

Make sure that the client cluster-side time is accurate to within 15 minutes of the cloud provider.

Troubleshooting CloudPools

This section describes other troubleshooting items for CloudPools administration and operation.

Cloud storage account cannot connect to the cloud

In the OneFS, if a cloud storage account is shown in the web administration interface with a red Needs Attention icon, or in the CLI interface with an Unreachable state, this usually indicates that the cluster has lost Internet connectivity or the service provider's cloud storage facility is offline. Ensure that the cluster has Internet connectivity. If it does, contact your service provider for help.
Determining if a file is a SmartLink file
To determine if a file has been archived to the cloud, you can check whether the local version on the cluster is a SmartLink file. Run the `isi get -D` command as in the following example:

```
isi get -D koala.jpg | grep Stubbed:
```

The output would be as follows if the specified file was a SmartLink (stub) file:

* Stubbed: True

If the file is not a SmartLink file, the output would be False.

Managing cloud accounts
After opening an account with your cloud provider, use the credentials and access information supplied by the cloud provider to configure a cloud storage account on your Isilon cluster. When you configure a cloud storage account in OneFS, CloudPools establishes a connection to your cloud provider account.

Create a cloud storage account
You create cloud storage accounts to enable CloudPools to archive files to cloud storage. In this way, the cloud becomes another tier of storage available in OneFS.

Before you begin
Before creating a cloud storage account, you must establish an account with a cloud provider, such as EMC Elastic Cloud Storage Service. When you create a cloud storage account in OneFS, the system attempts to connect to the cloud provider using the credentials you provide.

After the cloud storage account successfully connects to the cloud provider, you must add the cloud storage account to a CloudPool in OneFS. OneFS is then able to archive files to the cloud.

OneFS enforces the following requirements for cloud storage accounts.

- Each cloud storage account can only belong to a single CloudPool storage container.
- A cloud storage account must be of the same type (EMC Isilon, EMC ECS Appliance, Virtustream Storage Cloud, Amazon S3, or Microsoft Azure) as the CloudPool.

To create a cloud storage account:

Procedure
1. Run the `isi cloud accounts create` command.

The following command creates a Microsoft Azure cloud storage account. Note that this type of account requires a key provided by the cloud provider.

```
isi cloud accounts create --name=c-acct1 --type=azure --uri=https://admin2.blob.core.windows.net --account-
List cloud storage accounts

You can list all cloud storage accounts created on your cluster.

Procedure

1. Run the `isi cloud accounts list` command.

A sample list of cloud accounts is shown below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Account Username</th>
<th>URI</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records</td>
<td>azure</td>
<td>c-acct1</td>
<td><a href="https://my.windows.net">https://my.windows.net</a></td>
<td>OK</td>
</tr>
<tr>
<td>Archive</td>
<td>s3</td>
<td>AKIJBGNXGG88Q</td>
<td><a href="https://s3.aws.com">https://s3.aws.com</a></td>
<td>OK</td>
</tr>
</tbody>
</table>

Total: 2

View a cloud storage account

You can view detailed information about a cloud storage account.

Procedure

1. Run the `isi cloud accounts view` command.

The following command displays account information for the `CloudAcct3` account.

```
isi cloud accounts view CloudAcct3
```

Output from the command would look similar to the following example:

```
ID: cloud_acct1
Name: cloud_acct1
Type: ran
Account Username: cloudadmin
State: OK
State Details:
Enabled: Yes
Bucket: e005056a31d5f93845c255bf13e95d5f9ef741bb
Account ID: 0
Telemetry Bucket: -
Storage Region: -
Skip Ssl Validation: No
```

Modify a cloud storage account

You can modify the information associated with a cloud storage account.

To modify a cloud storage account, you must specify the account name. You can run the `isi cloud accounts list` command to list cloud storage accounts.

Procedure

1. Run the `isi cloud accounts modify` command.
This sample command changes the name of the cloud storage account CloudAcct3 to CloudAcct5.

```
isi cloud accounts modify CloudAcct3 --name=CloudAcct5
```

### Delete a cloud storage account

You can delete a cloud storage account. However, proceed with extreme caution, as deleting an account can result in loss of access to cloud data. You can stop archiving data to a cloud storage account without deleting it by running the `isi cloud pools modify` command and removing the account from its parent CloudPool. Previously archived files remain in cloud storage, and SmartLink files on the local cluster still point to the cloud data.

**Procedure**

1. Run the `isi cloud accounts delete` command.

   The following command deletes the cloud storage account OldRecords.

   ```
   isi cloud accounts delete OldRecords --acknowledge yes
   ```

   In this case, OneFS responds with the following message:

   ***************************************************
   WARNING: Deleting an account is extremely dangerous.
   Continuing with this operation will result in a permanent loss of data.
   Type 'confirm delete data' to proceed. Press enter to cancel:

2. Type the confirmation string `confirm delete data`, then press ENTER.

   The cloud storage account is deleted. Although cloud data remains with your cloud provider, the data will no longer be accessible in OneFS.

### Managing CloudPools

A CloudPool is the mechanism that contains a cloud storage account and connects the account to OneFS. When creating a CloudPool, you can assign a descriptive name that identifies the type of data that you are archiving to the cloud.

### Create a CloudPool

You can create a CloudPool and add a cloud storage account.

A CloudPool is the mechanism that connects a cloud storage account to OneFS. When you create a CloudPool, OneFS enforces two requirements:

- The CloudPool may contain only one cloud storage account.
- The cloud storage account must be of the same type as the CloudPool. For example, an Azure CloudPool may only contain an Azure cloud storage account.
Procedure

1. Run the `isi cloud pools create` command.

   When you create a CloudPool, you need to provide a unique name, the
   CloudPool type (isilon, ecs, virtustream, azure, or s3), and one cloud account.
   The following command creates an Azure-based CloudPool:

   ```
   isi cloud pools create cp_az azure csa_azure1 --vendor Microsoft
   ```

Results

You can view the result of this operation by running the `isi cloud pools view`
command with the ID (name) of the CloudPool that you created, as shown in the
following example:

```
isi cloud pools view cp_az
```

The output would look similar to the following example:

```
ID: cp_az
Name: cp_az
Type: azure
State: OK
State Details:
  Accounts: csa_azure1
  Description:
  Vendor: Microsoft
```

List CloudPools

You can view a list of CloudPools that have been created on your cluster.

Procedure

1. Run the `isi cloud pools list` command.

   Following is a sample of the output from this command:

   ```
   Name      Type     State
   -------------------------
   c_pool1   isilon   OK
   c_pool2   isilon   OK
   c_pool3   azure    OK
   -------------------------
   Total: 3
   ```

View CloudPool information

You can view information about a CloudPool, including the cloud storage account,
vendor, type, and description.

Before you begin

The CloudPool must already have been created.
Procedure

1. Run the `isi cloud pools view` command.

   The following command provides information on the CloudPool named `cah_s3_cp`.

   ```
   isi cloud pools view cah_s3_cp
   ```

   The output of this command would be similar to the following example:

   ```
   ID: cah_s3_cp
   Name: cah_s3_cp
   Type: s3
   State: OK
   State Details:
   Accounts: cah_S3
   Description: Archive for older project files
   Vendor: Amazon
   ```

Modify a CloudPool

You can modify a CloudPool, changing the name, the account it contains, the cloud vendor, and the description.

Before you begin

To determine the available CloudPools on your system, run the `isi cloud pools view` command.

Procedure

1. Run the `isi cloud pools modify` command.

   The following command modifies a CloudPool named `c_pool_azure`, removing its cloud storage account

   ```
   isi cloud pool modify c_pool_azure --remove-accounts c_acct2
   --description "Secondary archive"
   ```

Delete a CloudPool

You can delete a CloudPool. However, you should proceed with caution. CloudPools provide the mechanism to connect OneFS to your cloud storage accounts. If you delete a CloudPool, the associated cloud storage account is no longer accessible.

Before you begin

Run the `isi cloud pools list` command to display the names of the CloudPools on your cluster. Run the `isi cloud pools view` command, along with the name to get information about a CloudPool.

Procedure

1. Run the `isi cloud pools delete` command.

   The following command deletes the CloudPool named `c_pool_azure`.

   ```
   isi cloud pools delete c_pool_azure
   ```
Archiving files with file pool policies

You can configure a file pool policy to identify the files you want to archive to the cloud and the CloudPools actions to apply to these files.

Specifying a file pool policy, you can archive files using either the OneFS web administration interface or the command-line interface. A file pool policy that archives files to the cloud must specify the following information:

- **Files to manage:** These can be files of a certain type, files in a specified path, or files that match specified criteria, such as size, creation date, or last modified date.
- **CloudPools actions:** The cloud storage pool to send file data to, and whether the data should be compressed or encrypted.

Create a file pool policy

You must create custom file pool policies to specify CloudPools actions.

**Procedure**

1. Run the `isi filepool policies create` command.

   The following command creates a file pool policy with the name `archive` and the CloudPool storage target, `S3_pool`. The command also specifies a file-matching pattern to archive all files in a directory path that have not been accessed after November 30, 2014.

   ```
   isi filepool policies create archive --cloud-pool=S3_pool
   --begin-filter --name="*.*" --and --path="/ifs/home/users" --and
   --accessed-time=2014-11-30 --operator=lt --end-filter
   ```

List file pool policies

You can list all file pool policies stored in OneFS.

**Procedure**

1. Run the `isi filepool policies list` command.

   Following is sample output.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpp_1</td>
<td>Move older files to cloud</td>
<td>OK</td>
</tr>
<tr>
<td>fpp_2</td>
<td>Move static JPEGs to cloud</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total: 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
View a file pool policy

You can display detailed information about a file pool policy.

To list all available file pool policies, you can run the `isi filepool policies list` command.

Procedure

1. Run the `isi filepool policies view` command.

   A sample command and its output is shown below.

   ```
   isi filepool policies view my_policy
   
   Name: my_policy
   Description: -
   State: OK
   State Details:
   Apply Order: 2
   File Matching Pattern: Path == /ifs AND Name == *
   Set Requested Protection: -
   Data Access Pattern: -
   Enable Coalescer: -
   Data Storage Target: -
   Data SSD Strategy: -
   Snapshot Storage Target: -
   Snapshot SSD Strategy: -
   Cloud Pool: my_pool
   Cloud Compression Enabled: False
   Cloud Encryption Enabled: False
   Cloud Data Retention: 604800
   Cloud Incremental Backup Retention: 604800
   Cloud Full Backup Retention: 157680000
   Cloud Accessibility: cached
   Cloud Read Ahead: partial
   Cloud Cache Expiration: 86400
   Cloud Writeback Frequency: 32400
   Cloud Archive Snapshot Files: True
   ```

Modify a file pool policy

You can modify a file pool policy. Each file pool policy for cloud archival specifies a file-matching pattern and the actions to perform on the matched files (file pool).

You can run the `isi filepool policies list` command to list available file pool policies.

Procedure

1. Run the `isi filepool policies modify` command.

   The following example modifies the file-matching pattern in a file pool policy named `my_policy`.

   ```
   isi filepool policies modify my_policy --begin-filter --name="*.jpg" --and --accessed-time=2013-08-01 --operator=lt --end-filter
   ```
Delete a file pool policy

You can delete a file pool policy.

Deleting a file pool policy has no impact on accessing data already archived to the cloud. However, SmartLink files do reference their original file pool policy for attributes such as retention times. If a file pool policy is missing, SmartLink files will revert to using default values for those attributes.

Procedure

1. Run the `isi filepool policies delete` command.
   
   The following command deletes a file pool policy named `my_policy`.
   
   ```
   isi filepool policies delete my_policy
   ```
   
   When you run the command, a confirmation message appears:
   
   ```
   Are you sure? (yes/[no]):
   ```
   
   2. Type `yes`, then press ENTER.

Apply a file pool policy to a specified file or path

You can apply a file pool policy to specified files or directories manually, rather than waiting for the SmartPools job to run.

For `isi filepool apply` to execute, the file or directory specified must match one of the defined file pool policies.

Procedure

1. Run the `isi filepool apply` command.
   
   The following command applies the appropriate file pool policy to all files and subdirectories in a given path.
   
   ```
   isi filepool apply --path=/ifs/data/images --recurse
   ```

Archive files directly to the cloud

You can archive specific files directly to the cloud. To enable this, CloudPools must match these files to an existing file pool policy.

Before you begin

A custom file pool policy that matches the specified file or files and points to cloud storage must already exist on your system.

Procedure

1. Run the `isi cloud archive` command.
The following command specifies a directory and all of its subdirectories and files to be archived:

```bash
isi cloud archive /ifs/data/shared/images/*.* --recursive yes
```

## Configuring access to cloud data from a secondary cluster

You can make cloud data available on a secondary cluster if your primary cluster becomes unavailable.

To configure such access, you need to have replicated the primary cluster’s data on a secondary cluster using SyncIQ. Alternatively, you can restore an NDMP backup of the data to a secondary cluster.

The secondary cluster must have active SyncIQ, SmartPools, and CloudPools licenses.

With SyncIQ, when failover to a secondary cluster is required, two use cases are supported: short-term failover versus long-term failover.

In the short-term failover use case, the intention is to restore and failback to the primary cluster as quickly as possible. The secondary cluster is a temporary solution, enabling users to open SmartLink files from supported protocols and access cloud data as usual. Instead of writing any changes back to the cloud, however, CloudPools caches these changes locally in the SmartLink files on the secondary cluster. After the primary cluster is restored to service, changes from the secondary cluster must be written back to the primary cluster to enable any cached data in SmartLink files to be written back to cloud storage.

In a long-term failover situation, in which the primary cluster is to be out of service for an extended period, or is to be decommissioned entirely, other considerations become important. In this scenario, because only one cluster can have write access to cloud storage, you need to transfer write access to the failover cluster. From a CloudPools perspective in this scenario, the failover cluster effectively becomes the primary cluster.

With the NDMP approach, however, the short-term failover scenario is less practical. The secondary cluster should be given cloud write access to enable any cached modifications to SmartLink files to be written back to cloud storage. The alternative would be to somehow write modified SmartLink files back to the primary cluster after it is restored to service, but this might be more time-consuming.

**CAUTION**

Never allow write access to cloud data from more than one cluster at a time because it can result in data corruption.

## List available clusters

You can list the GUIDs of clusters that are accessible for SyncIQ failover or restore operations.

Available clusters are the primary cluster and any other clusters to which data has been replicated with SyncIQ or restored with NDMP.

**Procedure**

1. Run the `isi cloud access list` command.
OneFS displays a list of the GUIDs of eligible clusters similar to the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>GUID</th>
<th>Synced From</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>isi1</td>
<td>005056bf1df93845f13e95d (current)</td>
<td>-</td>
<td>permitted</td>
</tr>
<tr>
<td>isi2</td>
<td>00df945c23bf1df9533be23</td>
<td>isi1</td>
<td>not permitted</td>
</tr>
</tbody>
</table>

Total: 2

Allow access to cloud data on a secondary cluster

You can enable write access of SmartLink files and their cloud data on a secondary (target) cluster. Data from the primary (source) cluster must have been replicated to or restored on the target cluster by a SyncIQ or NDMP process.

Before you begin

Run the `isi cloud access list` command to display available target clusters. The target cluster must also have both a SmartPools and CloudPools license.

⚠️ CAUTION

This capability is offered to work around cases where the primary cluster is going to be unavailable for an extended period. Never allow write access to cloud data from more than one cluster at a time because it can result in data corruption. Before allowing another cluster to have cloud write access, make sure that cloud write access is removed from the primary cluster, and that the primary cluster is offline.

Procedure

1. Run the `isi cloud access add` command.

   The following command enables a secondary cluster, identified by GUID, to have write access to cloud data.

   ```bash
   isi cloud access add ab9dd991261e11e382240800200c9a66
   ```

   You can also specify the secondary cluster by name:

   ```bash
   isi cloud access add isi2
   ```

   If you know when the primary cluster will be restored to service, you can set an expiration date. The following command adds an expiration date of December 1, 2015:

   ```bash
   isi cloud access add isi2 --expiration-date 12012015
   ```
Remove access to data from a source cluster

You can remove previously granted access to SmartLink files replicated from a source cluster or restored from an NDMP backup. This operation must be done on the target cluster.

Before you begin

⚠️ CAUTION

Never allow write access to cloud data from more than one cluster at a time because it can result in data corruption. Removing access to SmartLink files on a target (secondary) cluster is typically done when the source (primary) cluster has been or is about to be restored to service.

Procedure

1. Run the `isi cloud access remove` command on the target cluster.

   The following command removes SmartLink file access from a target cluster by specifying its GUID.

   ```bash
   isi cloud access remove ab9dd991261e11e382240800200c9a66
   ```

Managing cloud jobs

You can monitor and manage two types of cloud jobs: system jobs that are always running in the background, and manual jobs that are created with the `isi cloud jobs archive` and `isi cloud jobs recall` commands. OneFS enables you to monitor the status of both job types, and to monitor and manage your manual archive and recall jobs, as needed.

View a list of cloud jobs

You can list all CloudPools jobs. Both CloudPools system jobs and manual jobs are listed.

CloudPools system jobs are always running to service caching and clean-up (garbage collection) processes. CloudPools manual jobs include archive jobs specified in file pool policies, and recall jobs started from the OneFS command-line interface. Each job is listed by ID, description, state, and type.

Procedure

1. Run the `isi cloud jobs list` command.

   Sample output from the command listing CloudPools jobs is shown below.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Effective State</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Write updated data...</td>
<td>running</td>
<td>cache-writeback</td>
</tr>
<tr>
<td>2</td>
<td>Expire CloudPools ...</td>
<td>completed</td>
<td>cache-invalidation</td>
</tr>
<tr>
<td>3</td>
<td>Clean up cache and...</td>
<td>completed</td>
<td>local-garbage-collect</td>
</tr>
<tr>
<td>4</td>
<td>Clean up unreferen...</td>
<td>completed</td>
<td>cloud-garbage-collect</td>
</tr>
</tbody>
</table>
View a cloud job

You can view information about a CloudPools job.

Before you begin

You need to know the ID of the job you want to view. You can run the `isi cloud jobs list` command to see the IDs for all cloud jobs.

Procedure

1. Run the `isi cloud jobs view` command.

The following command views information about a job with the ID of 63.

```
isi cloud jobs view 63
```

Output for this command would appear similar to the following display:

```
ID: 63
Description: completed
Type: archive
Operation State: running
Job State: completed
Create Time: 2015-09-21T11:50:42
State Change Time: 2015-09-21T11:51:01
Completion Time: 2015-09-21T11:51:01
Job Engine Job: 221
Job Engine State: succeeded
Total Files: 2
Total Canceled: 0
Total Failed: 0
Total Pending: 0
Total Staged: 0
Total Processing: 0
Total Succeeded: 2
```
Pause a cloud job

You can pause a running CloudPools job. This operation is typically done only for troubleshooting purposes.

Before you begin

To pause a job, you need to know the ID of the job. Run the `isi cloud jobs list` command to see a list of all cloud job IDs.

Procedure

1. Run the `isi cloud jobs pause` command.
   
   The following command pauses a job with the ID of 63.

   ```
   isi cloud jobs pause 63
   ```

   This command pauses all running archive jobs:

   ```
   isi cloud jobs pause archive
   ```

   **Note**

   Only currently running archive jobs are paused. Any subsequent jobs that are kicked off by a file pool policy, or manually through `isi cloud archive` are not paused and will run.

Resume a paused cloud job

You can resume a cloud job that has been paused.

Before you begin

To resume a job, you need to know the ID of the job. Run the `isi cloud jobs list` command to see a list of all cloud job IDs.

Procedure

1. Run the `isi cloud jobs resume` command.
   
   The following command resumes a job with the ID of 63.

   ```
   isi cloud jobs resume 63
   ```

Cancel a cloud job

You can cancel a running CloudPools job.

Before you begin

To cancel a job, you need to know the ID of the job. Run the `isi cloud jobs list` command to see a list of all cloud job IDs.

Procedure

1. Run the `isi cloud jobs cancel` command.
The following command cancels a job with an ID of 63.

```bash
isi cloud jobs cancel 63
```

## Managing CloudPools settings

You can manage CloudPools default settings, including snapshot archival, encryption, compression, cache settings, data retention settings, and the ability to regenerate an encryption key. An encryption key should only be regenerated if you suspect the existing key has been compromised.

### View cloud settings

You can view the top-level settings for CloudPools.

#### Procedure

1. Run the `isi cloud settings view` command.

   The command displays output similar to the following:

   ```
   Default Accessibility: cached
   Default Cache Expiration: 1D
   Default Compression Enabled: No
   Default Data Retention: 1W
   Default Encryption Enabled: No
   Default Full Backup Retention: 5Y
   Default Incremental Backup Retention: 1W
   Default Read Ahead: partial
   Default Writeback Frequency: 9H
   Default Archive Snapshot Files: Yes
   ```

### Modify default cloud settings

You can modify default CloudPools settings.

You can use the `isi cloud settings view` command to display current default settings.

#### Procedure

1. Run the `isi cloud settings modify` command.

   The following command disables archival of files that have snapshot versions.

   ```bash
   isi cloud settings modify --default-archive-snapshot-files=no
   ```

   The following command enables both encryption and compression of cloud data:

   ```bash
   isi cloud settings modify --default-encryption-enabled=yes --default-compression-enabled=yes
   ```
Generate a new master encryption key

You can generate a new master encryption key. The key is used to encrypt data and is stored with cloud data objects.

Before you begin

Only generate a new master encryption key if you believe the existing key has been compromised.

Procedure

1. Run the `isi cloud settings regenerate-encryption-key` command.

   The following command generates a new encryption key in verbose mode.

   ```sh
   isi cloud settings regenerate-encryption-key --verbose
   ```

   In verbose mode, the system confirms the process:

   ```
   Encryption key has been regenerated
   ```

CloudPools command reference

Use CloudPools commands to manage general settings, and to create and manage cloud accounts and cloud storage targets. This section provides reference information for each command. For any command, you can use the `--help` option to get a full listing of command options.

**isi cloud access add**

Adds cloud write access to the cluster.

**Syntax**

```sh
isi cloud access add <guid>
   [--expiration-date <timestamp>]
   [--verbose]
```

**Options**

- `<guid>`
  - The reference number, or globally unique identifier (GUID), of the cloud account.

- `--expiration-date <timestamp>`
  - The date and time at which write access to cloud data ends on this cluster. The timestamp format is `MMDDYY:hh:mm`. For example, `022016:12:00` specifies an expiration date and time of February 20, 2016 at 12:00 PM.

- `--verbose`
  - Displays more detailed information.
Examples
The following example adds cloud write access to a cluster by specifying the cluster
GUID and an expiration date:

```
isi cloud access add 000556bf1e82059801563f1ad44a8c155acf
--expiration-date 022016:12:00
```

OneFS displays a message indicating the cloud accounts and file pool policies to which
the secondary cluster will have access, and requires confirmation. Type yes, and press
ENTER to complete the process.

**isi cloud access list**

Displays a list of clusters on your network that have, or are eligible for, write access to
cloud data. Available clusters are the primary cluster and any other clusters to which
data has been replicated with SyncIQ or restored with NDMP.

**Syntax**

```
isi cloud access list
[--limit]<integer>
[--sort {name | guid | synced_from | state | accounts | policies}]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

**--limit<integer>**

Limits the number of eligible clusters displayed in the list.

**--sort**

Sort the list of eligible clusters according to the specified category. The following
values are valid:

```
name
guid
synced_from
state
accounts
policies
```

**--format**

Outputs the list of eligible clusters in the specified format. The following values
are valid:

```
table
json
csv
list
```
--descending
   Outputs the list of eligible clusters in descending order according to the specified sort option.
--no-header
   Displays table and CSV output without headers.
--no-footer
   Displays table output without footers.
--verbose
   Displays more detailed information.

Examples
Output from the isi cloud access list command would look similar to following example:

<table>
<thead>
<tr>
<th>Name</th>
<th>GUID</th>
<th>Synced From</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>isi 1</td>
<td>005056bf1df93845f13e95d5f9 (current)</td>
<td></td>
<td>permitted</td>
</tr>
<tr>
<td>isi 2</td>
<td>00df945c23bf1df9533be23e95</td>
<td>isi1</td>
<td>not permitted</td>
</tr>
</tbody>
</table>

Total: 2

isi cloud access remove
Removes cloud write access from the specified cluster.

Syntax

isi cloud access remove <guid>
   [--force]
   [--verbose]

Options

<guid>
   The reference number, or globally unique identifier (GUID), of the cluster from which you want to remove cloud write access.
--force
   Execute the command without requiring confirmation.
--verbose
   Displays more detailed information.

Examples
The following example removes cloud write access from a cluster identified by a specified GUID:

isi cloud access remove 000556bf1e82059801563f1ad44a8c155acf

OneFS displays a message indicating the cloud accounts and file pool policies to which the cluster will no longer have access, and requires confirmation. Type yes, and press ENTER to complete the process.
isi cloud access view

View the details of a cluster with, or eligible for, write access to cloud data.

Syntax

~isi cloud access view <guid>

Options

<guid>

The reference number, or globally unique identifier (GUID), of the cluster.

Example

When you run the isi cloud access view command, a display similar to the following example appears:

<table>
<thead>
<tr>
<th>Name: my-cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID: 56bf005005981e2801563f1ad44a8c155acf (current)</td>
</tr>
<tr>
<td>Synced From: -</td>
</tr>
<tr>
<td>State: permitted</td>
</tr>
<tr>
<td>Accounts: my_ran_acct, my_s3_acct</td>
</tr>
<tr>
<td>Policies: my_cloud_policy1, my_cloud_policy2</td>
</tr>
</tbody>
</table>

isi cloud accounts create

Creates a cloud storage account that connects CloudPools to your cloud storage provider.

Syntax

isi cloud accounts create <name> <type> <uri> <account-username> <key>

[--enabled {yes | no}]
[--account-id <string>]
[--telemetry-bucket <string>]
[--storage-region <string>]
[--skip-ssl-validation {yes | no}]
[--force]
[--verbose]

Options

<name>

The name of the cloud storage account.

<type>

The type of cloud storage account: one of isilon, azure, s3, virtustream, or ecs.

<uri>

The cloud account URI. This URI must match that provided to the cloud vendor.

<account-username>

The username for the cloud account. This name must be identical to the user name provided to the cloud vendor.
The cloud account access key or password. This information is provided by the cloud vendor.

--enabled {yes | no}
By default, when you create a cloud storage account, it is enabled. To disable the account on creation, you can use this setting with the no option.

--account-id <string>
This is a required Amazon S3-only setting. The account ID number provided by Amazon when you first establish an account with the vendor.

--telemetry-bucket <string>
This is a required Amazon S3-only setting. The telemetry bucket name that you specified when you first established an account with the vendor.

--storage-region <string>
This is a required Amazon S3-only setting. The storage region that you specified when you first established an account with the vendor. For example, us-west-1.

--skip-ssl-validation {yes | no}
Specifies whether to circumvent SSL certificate validation when connecting to a cloud provider's storage repository. Unless you specify this setting with a yes instruction, OneFS will attempt to perform SSL certificate validation when connecting. For security purposes, we recommend not enabling this setting. If you are connecting to cloud provider (for example, Isilon or ECS) that is within your corporate network, and you are having trouble connecting, you can skip SSL validation.

--force
Execute the command without requiring confirmation.

--verbose
Displays more detailed information.

Examples
The following example creates a Microsoft Azure cloud account:

```
isi cloud accounts create my_azure azure https://myazure.windows.net myuser dhgXJ90AIahXvYmL
```

**isi cloud accounts delete**

Delete a cloud storage account. Caution: deleting an account can result in loss of access to cloud data.

**Syntax**

```
isi cloud accounts delete <id>
[--acknowledge <string>]
[--verbose]
```
Options

<id>
The name of the cloud account. You can use the isi cloud accounts list command to display the names of cloud accounts.

--acknowledge <string>
Enables the account deletion to proceed. This parameter is required. You must include a text string with the parameter, such as yes, proceed, or other string.

--verbose
Displays more detailed information.

Example
The following example deletes a Microsoft Azure cloud account:

```
isi cloud accounts delete my_azure --acknowledge yes
```

When you run the command, OneFS displays the following message and requires confirmation:

```
**********************************************************************
WARNING: Deleting an account is extremely dangerous. Continuing with this operation will result in a permanent loss of data.
Type 'confirm delete data' to proceed. Press enter to cancel:
```

To proceed, type confirm delete data, and press ENTER.

isi cloud accounts list
List cloud accounts.

Syntax

```
isi cloud accounts list
  [--limit <integer>]
  [--sort {id | name | type | account_username | uri | state | bucket}]
  [--descending]
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]
```

Options

--limit <integer>
Limits the number of cloud accounts displayed in the list.

--sort
Sort the list of cloud accounts according to the specified category. The following values are valid:

id
name
type
CloudPools

account_username
uri
state
bucket

--format
Outputs the list of cloud accounts in the specified format. The following values are valid:
table
json
csv
list

--descending
Outputs the list of cloud accounts in descending order according to the specified sort option.

--no-header
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
Output from the isi cloud account list command would look similar to following example:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Account Username</th>
<th>URI</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records</td>
<td>azure</td>
<td>c-acct1</td>
<td><a href="https://my.windows.net">https://my.windows.net</a></td>
<td>OK</td>
</tr>
<tr>
<td>Archive</td>
<td>s3</td>
<td>AKIJBGNXGG88Q</td>
<td><a href="https://s3.aws.com">https://s3.aws.com</a></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

isi cloud accounts modify

Modify a cloud account.

Syntax

isi cloud accounts modify <id>
|--name <string>|
|--account-username <string>|
|--key <string>|
|--uri <string>|
|--enabled {yes | no}|
|--account-id <string>|
|--telemetry-bucket <string>|
|--storage-region <string>|


Options

<i id>
The ID of the cloud account. In this case, the ID is the same as the cloud account name.

--name <string>
The name of the cloud account. In this case, the name is the same as the ID.

--account-username <string>
The username for the cloud account. This name must be identical to the user name provided to the cloud vendor.

--key <string>
The cloud account access key or password. This information is provided by the cloud vendor.

--uri <string>
The cloud account URI. This URI must match that provided to the cloud vendor.

--enabled {yes | no}
By default, when you create a cloud storage account, it is enabled. To disable the account on creation, you can use this setting with the no option.

--account-id <string>
This is a required Amazon S3-only setting. The account ID number provided by Amazon when you first establish an account with the vendor.

--telemetry-bucket <string>
This is a required Amazon S3-only setting. The telemetry bucket name that you specified when you first established an account with the vendor.

--storage-region <string>
This is a required Amazon S3-only setting. The storage region that you specified when you first established an account with the vendor. For example, us-west-1.

--skip-ssl-validation {yes | no}
Specifies whether to circumvent SSL certificate validation when connecting to a cloud provider’s storage repository. Unless you specify this setting with a yes instruction, OneFS will attempt to perform SSL certificate validation when connecting. For security purposes, we recommend not enabling this setting. If you are connecting to a cloud provider (for example, RAN or ECS) that is inside your corporate network, and you are having trouble connecting, you can skip SSL validation.

--verbose
Displays more detailed information.
Example
The following example modifies a Microsoft Azure cloud account:

```bash
isi cloud accounts modify my_azure --uri https://myazure.windows.net --account-username myuser --key dhgXJ90AIahXvYmL
```

**isi cloud accounts view**

View the details of a cloud account.

**Syntax**

```bash
isi cloud accounts view <name>
```

**Options**

- `<name>`
  
  Specifies the name of the cloud account to view. You can use the `isi cloud accounts list` command to display a list of the names of available cloud accounts.

**Example**

The following example displays the details of an Amazon S3 cloud account:

```bash
isi cloud accounts view my_s3
```

Output from the command would be similar to the following:

```
ID: my_s3
Name: my_s3
Type: s3
Account Username: KAIABUQJJGNXGKEM47Q
URI: https://s3.amazonaws.com
State: OK
State Details:
Enabled: Yes
Bucket: d005056bf1e28059801563f1ad44a8c155acfi9
Account ID: 1234566543210
Telemetry Bucket: myusagedir
Storage Region: us-west-1
Skip Ssl Validation: No
```

**isi cloud archive**

Queue one or more files to be archived to or recalled from the cloud. Specify files individually or by using a file matching pattern. For files to be archived, they must match the specified file pool policy, or any file pool policy with a cloud target.

**Syntax**

```bash
isi cloud archive <files>
[--recursive {yes | no}]
[--policy <string>]
[--verbose]
[--help]
```
Options

<files>
Specifies the files to archive or recall. Specify --files for each additional file to process. Alternatively, you can specify a file matching pattern such as /ifs/data/archive/images/*.jpg.

--recursive {yes | no}
Specifies whether the operation should apply recursively to nested directories in the file string.

--policy <string>
Specifies the file pool policy to apply to the specified files. If you specify one or more files to be archived and do not specify a policy, OneFS will compare the files with each configured file pool policy.

--verbose
Displays more detailed information.

Examples
The following example archives multiple files to the cloud according to a specific file pool policy:

```
isi cloud archive /ifs/data/images/big.jpg --file /ifs/data/huge.jpg --policy my_policy
```

The following example archives an entire directory to the cloud. The operation must match an existing file pool policy to be successful.

```
isi cloud archive /ifs/data/images/*.* --recursive yes
```

The following example recalls files from the cloud:

```
isi cloud archive /ifs/data/images/*.* --type recall
```

isi cloud jobs cancel

Cancel a CloudPools job initiated manually with isi cloud archive or isi cloud recall. CloudPools system jobs (such as cache-writeback) cannot be canceled.

Syntax

```
isi cloud jobs cancel <id>
[--verbose]
```

Options

<id>
The ID for the cloud job. Run isi cloud jobs list to see a list of all manual and system jobs and their associated IDs.

--verbose
Displays more detailed information.

**Example**
This following example cancels a CloudPools job with the ID of 21.

```bash
isi cloud cancel 21
```

### isi cloud jobs files list

Displays the list of files matched by the specified CloudPools job.

**Syntax**

```bash
isi cloud jobs files list <job-id>
|--limit <integer>
|--sort {name | state}
|--descending
|--format {table | json | csv | list}
|--no-header
|--no-footer
|--verbose
```

**Options**

- `<job-id>`
  The ID of the job. To find the list of job IDs in CloudPools, run the `isi cloud jobs list` command.

- `--limit <integer>`
  Display no more than the specified number of items.

- `--sort {name | state}`
  Order results by the specified field. The default value is `name`.

- `--descending`
  Sort and present data in descending order.

- `--format {table | json | csv | list}`
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

- `--no-header`
  Displays table and CSV output without headers.

- `--no-footer`
  Displays table output without footers.

- `--verbose`
  Displays more detailed information.
Example
The following example displays a list of files associated with a specific cloud job:

```
isi cloud jobs files list 21
```

Output from the command would be similar to the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ifs/data/Shared_Files/Images2/Desert.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Gone_fishin.png</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Jellyfish.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Koala.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Penguins.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/sedona-az.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/snow2.png</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Tulips.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Chrysanthemum.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Hydrangeas.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Lighthouse.jpg</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/snow1.png</td>
<td>pending</td>
</tr>
<tr>
<td>/ifs/data/Shared_Files/Images2/Thumbs.db</td>
<td>pending</td>
</tr>
</tbody>
</table>

---

Total: 19

isi cloud jobs list

View the status of CloudPools jobs, including system, archive, and recall jobs.

Syntax

```
isi cloud jobs list
[--limit <integer>]
[--sort {id | job_state | operation_state | effective_state | type | state_change_time | completion_time | create_time | description}]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

Options

--limit <integer>
Display no more than the specified number of items.

--sort {id | job_state | operation_state | effective_state | type | state_change_time | completion_time | create_time | description}
Order results by this field. The default value is id. Note that, to sort on other than ID, description, effective state, and type, use the --verbose parameter with the command.

--descending
Sort and present data in descending order.

--format {table | json | csv | list}
Display output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

--no-header
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
Output of the isi cloud jobs list command is similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Effective State</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Write updated data...</td>
<td>running</td>
<td>cache-writeback</td>
</tr>
<tr>
<td>2</td>
<td>Expire CloudPools ...</td>
<td>completed</td>
<td>cache-invalidation</td>
</tr>
<tr>
<td>3</td>
<td>Clean up cache and...</td>
<td>completed</td>
<td>local-garbage-collect</td>
</tr>
<tr>
<td>4</td>
<td>Clean up unreferen...</td>
<td>completed</td>
<td>cloud-garbage-collect</td>
</tr>
<tr>
<td>53</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>54</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>55</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>56</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>57</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>58</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>59</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>60</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>61</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>62</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>63</td>
<td>completed</td>
<td></td>
<td>archive</td>
</tr>
<tr>
<td>64</td>
<td>error</td>
<td></td>
<td>archive</td>
</tr>
</tbody>
</table>

Total: 16

isi cloud jobs pause

Pause a cloud job. A paused job can be resumed with the isi cloud jobs resume command.

Syntax

isi cloud jobs pause <id>
[--verbose]

Options

id
The ID of the cloud job to pause. Use the isi cloud jobs list command to view the IDs of all cloud jobs. Although possible, we recommend that you not pause any of the CloudPools system jobs that run in the background and are critical for proper operation. These include cache-writeback, cache-invalidation, local-garbage-collection, and cloud-garbage-collection.

--verbose
Displays more detailed information.

**Example**
The following example pauses a cloud job with ID 19.

```bash
isi cloud jobs pause 19
```

### isi cloud jobs resume

Resume a paused cloud job.

**Syntax**

```bash
isi cloud jobs resume <id>  
[--verbose]
```

**Options**

`<id>`

The ID for the cloud job to resume. Use the `isi cloud jobs list` command to view a list of jobs and their associated IDs.

`--verbose`

Displays more detailed information.

**Example**
The following command resumes a paused job with an ID of 26:

```bash
isi cloud jobs resume 26
```

### isi cloud jobs view

View the details of a cloud job.

**Syntax**

```bash
isi cloud jobs view <id>
```

**Options**

`<id>`

Specify the ID of the cloud job. Use the `isi cloud jobs list` command to view all jobs and their associated IDs.

**Example**
The following command views the details of a job with the ID of 27:

```bash
isi cloud jobs view 27
```
Output from the command would look similar to the following:

<table>
<thead>
<tr>
<th>ID: 27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>Effective State: running</td>
</tr>
<tr>
<td>Type: archive</td>
</tr>
<tr>
<td>Operation State: running</td>
</tr>
<tr>
<td>Job State: running</td>
</tr>
<tr>
<td>Create Time: 2015-10-06T22:00:19</td>
</tr>
<tr>
<td>Completion Time: -</td>
</tr>
<tr>
<td>Job Engine Job: 67</td>
</tr>
<tr>
<td>Job Engine State: succeeded</td>
</tr>
<tr>
<td>Total Files: 19</td>
</tr>
<tr>
<td>Total Cancelled: 0</td>
</tr>
<tr>
<td>Total Failed: 0</td>
</tr>
<tr>
<td>Total Pending: 19</td>
</tr>
<tr>
<td>Total Staged: 0</td>
</tr>
<tr>
<td>Total Processing: 0</td>
</tr>
<tr>
<td>Total Succeeded: 0</td>
</tr>
</tbody>
</table>

**isi cloud pools create**

Create a CloudPool, which provides the connection between OneFS and a cloud storage account.

**Syntax**

```bash
isi cloud pools create <name> <type> <account>
[--description <string>]
[--vendor <string>]
[--verbose]
```

**Options**

- **<name>**
  
  The name of the CloudPool.

- **<type>**
  
  The type of account, one of `isilon`, `azure`, `s3`, `ecs`, or `virtustream`.

- **<account>**
  
  The name of the cloud storage account to which the CloudPool connects. The cloud storage account is required and must match the CloudPool type. Only one cloud storage account can be specified.

- **--description <string>**
  
  A description of the CloudPool.

- **--vendor <string>**
  
  The name of the vendor hosting the cloud storage account.

- **--verbose**
  
  Displays more detailed information.
Example
This following command creates a CloudPool containing a Microsoft Azure cloud storage account:

```
isi cloud pools create my_cp azure http://myazure.microsoft.com
--description="Financial records 2013" --vendor=Microsoft
```

**isi cloud pools delete**

Delete a CloudPool. Proceed with caution, however. If you delete a CloudPool, OneFS is no longer able to access the associated cloud storage account. If the CloudPool is referenced by a file pool policy, OneFS does not allow the CloudPool to be deleted.

**Syntax**

```
isi cloud pools delete <id>
[--force]
[--verbose]
```

**Options**

- `<id>`
  The name of the CloudPool. You can use the `isi cloud pools list` command to list existing CloudPools and their associated IDs.

- `--force`
  Deletes the account without asking for confirmation.

- `--verbose`
  Displays more detailed information.

**Example 3**

The following command specifies a CloudPool to be deleted:

```
isi cloud pool delete my_azure_pool
```

When you press ENTER to run the command, OneFS asks for confirmation. Type `yes`, then press ENTER.

**isi cloud pools list**

Display a list of CloudPools.

**Syntax**

```
isi cloud pools list
[--limit <integer>] [--sort {id | name | type | state | state_details | description | vendor}] [--descending ] [--format {table | json | csv | list}]
```
Options

--limit <integer>
Displays no more than the specified number of items.

--sort {id | name | type | state | state_details | description | vendor}
Order results by this field. The default value is id, which, in this case, is the same as name. Unless you use the --verbose option, you can only sort on name, type, or state.

--descending
Sorts and presents data in descending order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

--no-header
Displays table and CSV output without headers.

--no-footer
Displays table output without footers.

--verbose
Displays more detailed information.

Example
Output from the isi cloud pools list command would look like the following example:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>my_s3_pool</td>
<td>s3</td>
<td>OK</td>
</tr>
<tr>
<td>my_isi_pool</td>
<td>isilon</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

isi cloud pools modify

Modifies a CloudPool.

Syntax

isi cloud pools modify <id>
[--name <string>]
[--accounts <string>]
[--add-accounts <string>]
[--clear-accounts]
[--remove-accounts <string>]
[--description <string>]

Options

<id>
The ID of the CloudPool. Run `isi cloud pools list` to view the IDs of all CloudPools.

--name <string>
Specify a new name for the CloudPool.

--account <string>
Specify the name of the cloud account to add to the CloudPool. Only one account per CloudPool is allowed.

--add-account <string>
Specify the name of a cloud account to add to the CloudPool. Only one account per CloudPool is allowed.

--remove-accounts <string>
Specify the name of the cloud account to remove from the CloudPool. You can only remove an account if you are adding a different account in the same command.

--description
Specify the name of the cloud account to remove from the CloudPool. You can only remove an account if you are adding a different account in the same command.

--vendor <string>
The name of the vendor hosting the cloud pool accounts.

--verbose
Displays more detailed information.

Examples
The following command adds a vendor name and description to an existing CloudPool:

```
isi cloud pools modify my_azure --vendor Microsoft
--description "preferred azure account"
```

The following command removes one cloud account from the CloudPool, and adds another cloud account:

```
isi cloud pools modify my_s3 --remove-accounts s3_acct_1
--add-accounts s3_acct_2
```
### isi cloud pools view

View detailed information about a CloudPool.

**Syntax**

```bash
isi cloud pools view <id>
```

**Options**

`<id>`

The ID of the cloud pool. Run the `isi cloud pool list` command to view all CloudPools and their associated IDs.

**Example**

The following command displays information about a CloudPool named `my_azure_pool`.

```bash
isi cloud pools view my_azure_pool
```

Output from the command would look similar to the following:

```
ID: my_azure_pool
Name: my_azure_pool
Type: azure
State: OK
State Details:
  Accounts: my_azure_acct
  Description: Archive for 2009-2011 financial records
  Vendor: Microsoft
```

### isi cloud recall

Specify one or more files to be recalled from the cloud. You can specify files individually or by using a file matching pattern. To make sure that the specified files are present in the cloud, OneFS scans the cluster for SmartLink files prior to performing the recall.

**Syntax**

```bash
isi cloud recall <files>
  [--recursive {yes | no}]
  [--verbose]
```

**Options**

`<files>`

Specifies the files to recall. Specify `--files` for each additional file name.

`--recursive {yes | no}`

Specifies whether the recall should apply recursively to nested subdirectories.

`--verbose`

Displays more detailed information about the operation.
Examples
The following example recalls all files from the cloud for a directory and its subdirectories:

```bash
isi cloud recall /ifs/data/archives/archives2014/projects/*.*
  --recursive yes
```

The command starts a cloud job. If you use the `--verbose` parameter, OneFS reports the job number, as in the following example:

```
Created job [29]
```

You can use the `isi cloud jobs view` command with the job number to see information about the job.

---

**Note**

When you use the `isi cloud recall` command to recall a file from cloud storage, the full file is restored to its original directory, and the associated SmartLink file is overwritten. If the file pool policy that originally archived the file to the cloud is still in effect, the next time the SmartPools job runs, the recalled file is archived to the cloud again. If you do not want the recalled file to be re-archived, you can move the file to a different directory that would not be affected by the file pool policy, or you can modify or delete the policy.

---

**isi cloud restore_coi**

Restores the cloud object index (COI) for a cloud storage account on the cluster. If you run the `isi cloud access add` command on a cluster, it automatically restores the COI.

**Syntax**

```bash
isi cloud restore_coi
  [--account <string>]
  [--expiration-date <timestamp>]
  [--verbose]
```

**Options**

--account <string>

Specifies the name of the cloud storage account whose COI you intend to restore. By restoring the COI, you enable OneFS to not only read data from the cloud, but also to write data to the cloud.

--expiration-date <timestamp>

Specifies the expiration date for orphaned cloud data objects.

--verbose

Displays more detailed information about the operation.
Example
The following example restores the COI for a cloud storage account:

```
isi cloud restore_coi --account my.azure_acct
```

**isi cloud settings modify**

Controls archiving of snapshot files. By default, archiving of snapshots is enabled.

**Syntax**

```
isi cloud settings modify
[--default-accessibility {cached | no-cache}]
[--default-cache-expiration <duration>]
[--default-compression-enabled {yes | no}]
[--default-data-retention <duration>]
[--default-encryption-enabled {yes | no}]
[--default-full-backup-retention <duration>]
[--default-incremental-backup-retention <duration>]
[--default-read-ahead <string>]
[--default-writeback-frequency <duration>]
[--default-archive-snapshot-files {yes | no}]
[--verbose]
```

**Options**

--**default-accessibility** {cached | no-cache}
Specifies whether, when a SmartLink file is accessed, cloud data is incrementally downloaded (cached) as needed, or fully downloaded (not cached).

--**default-cache-expiration** <duration>
Specifies the minimum amount of time until the cache expires. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--**default-compression-enabled** {yes | no}
Specifies whether data is to be compressed when archived to the cloud.

--**default-data-retention** <duration>
Specifies the minimum amount of time that cloud objects associated with a SmartLink file will be retained in the cloud after the SmartLink file is deleted from the cluster. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--**default-encryption-enabled** {yes | no}
Specifies whether data is to be encrypted when archived to the cloud.

--**default-full-backup-retention** <duration>
Specifies the length of time that OneFS retains cloud data referenced by a SmartLink file that has been backed up by a full NDMP backup and is subsequently deleted. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--**default-incremental-backup-retention** <duration>
Specifies the length of time that OneFS retains cloud data referenced by a SmartLink file that has been backed up by an incremental NDMP backup, or replicated by a SyncIQ operation, and is subsequently deleted. A number followed by a unit of time is accepted. For example, a setting of 5Y would specify a five-year duration.

--default-read-ahead {partial | full}
Specifies the cache readahead strategy when SmartLink files are accessed. A partial strategy means that only the amount of data needed by the user is cached. A full strategy means that all file data will be cached when the user accesses a SmartLink file.

--default-writeback-frequency <duration>
Specifies the minimum amount of time to wait before OneFS updates cloud data with local changes. A number followed by a unit of time is accepted. For example, a setting of 9H would specify a nine-hour duration. Similarly, a setting of 2D would specify a two-day duration.

--default-archive-snapshot-files {yes | no}
Whether or not policies should archive files with snapshots.

--verbose
Displays more information about the operation.

Example
The following examples modifies several of the default CloudPools settings:

```
isi cloud settings modify --default-writeback-frequency 12H
--default-cache-expiration 9H --default-accessability no-cache
--default-encryption-enabled yes
```

**isi cloud settings regenerate-encryption-key**

Generates a new master encryption key for data to be archived to the cloud. Encrypted data already stored in the cloud requires and stores the previous encryption key.

**Syntax**

```
isi cloud settings regenerate-encryption-key
[--verbose]
```

**Option**

--verbose
Displays more detailed information.
isi cloud settings view

Display the current default settings in CloudPools. You can use the isi cloud settings modify command to change default settings.

Syntax

isi cloud settings view

Options

There are no options for this command.

Example

When you run this command, settings similar to the following example are displayed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Accessibility</td>
<td>cached</td>
</tr>
<tr>
<td>Default Cache Expiration</td>
<td>9H</td>
</tr>
<tr>
<td>Default Compression Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Default Data Retention</td>
<td>1W</td>
</tr>
<tr>
<td>Default Encryption Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Default Full Backup Retention</td>
<td>5Y</td>
</tr>
<tr>
<td>Default Incremental Backup Retention</td>
<td>1W</td>
</tr>
<tr>
<td>Default Read Ahead</td>
<td>partial</td>
</tr>
<tr>
<td>Default Writeback Frequency</td>
<td>9H</td>
</tr>
<tr>
<td>Default Archive Snapshot Files</td>
<td>No</td>
</tr>
</tbody>
</table>
CHAPTER 25
System jobs

This section contains the following topics:

- System jobs overview ................................................................. 1010
- System jobs library ............................................................... 1010
- Job operation ........................................................................... 1013
- Job performance impact ......................................................... 1014
- Job priorities ........................................................................... 1015
- Managing system jobs .............................................................. 1015
- Managing impact policies ......................................................... 1020
- Viewing job reports and statistics ........................................... 1022
- Job management commands ................................................... 1024
System jobs overview

The most critical function of OneFS is maintaining the integrity of data on your Isilon cluster. Other important system maintenance functions include monitoring and optimizing performance, detecting and mitigating drive and node failures, and freeing up available space.

Because maintenance functions use system resources and can take hours to run, OneFS performs them as jobs that run in the background through a service called Job Engine. The time it takes for a job to run can vary significantly depending on a number of factors. These include other system jobs that are running at the same time; other processes that are taking up CPU and I/O cycles while the job is running; the configuration of your cluster; the size of your data set; and how long since the last iteration of the job was run.

Up to three jobs can run simultaneously. To ensure that maintenance jobs do not hinder your productivity or conflict with each other, Job Engine categorizes them, runs them at different priority and impact levels, and can temporarily suspend them (with no loss of progress) to enable higher priority jobs and administrator tasks to proceed.

In the case of a power failure, Job Engine uses a checkpoint system to resume jobs as close as possible to the point at which they were interrupted. The checkpoint system helps Job Engine keep track of job phases and tasks that have already been completed. When the cluster is back up and running, Job Engine restarts the job at the beginning of the phase or task that was in process when the power failure occurred.

As system administrator, through the Job Engine service, you can monitor, schedule, run, terminate, and apply other controls to system maintenance jobs. The Job Engine provides statistics and reporting tools that you can use to determine how long different system jobs take to run in your OneFS environment.

Note

To initiate any Job Engine tasks, you must have the role of SystemAdmin in the OneFS system.

System jobs library

OneFS contains a library of system jobs that run in the background to help maintain your Isilon cluster. By default, system jobs are categorized as either manual or scheduled. However, you can run any job manually or schedule any job to run periodically according to your workflow. In addition, OneFS starts some jobs automatically when particular system conditions arise—for example, FlexProtect and FlexProtectLin, which start when a drive is smartfailed.

<table>
<thead>
<tr>
<th>Job name</th>
<th>Description</th>
<th>Exclusion Set</th>
<th>Impact Policy</th>
<th>Priority</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoBalance</td>
<td>Balances free space in a cluster, and is most efficient in clusters that contain only hard disk drives (HDDs). Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Restripe</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>Job name</td>
<td>Description</td>
<td>Exclusion</td>
<td>Impact Set</td>
<td>Priority</td>
<td>Operation</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>AutoBalanceLin</td>
<td>Balances free space in a cluster, and is most efficient in clusters when file system metadata is stored on solid state drives (SSDs). Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Restripe</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>AVScan</td>
<td>Performs an antivirus scan on all files.</td>
<td>None</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>ChangelistCreate</td>
<td>Creates a list of changes between two snapshots with matching root paths. You can specify these snapshots from the CLI.</td>
<td>None</td>
<td>Low</td>
<td>5</td>
<td>Manual</td>
</tr>
<tr>
<td>Collect</td>
<td>Reclaims free space that previously could not be freed because the node or drive was unavailable. Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Mark</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>Dedupe*</td>
<td>Scans a directory for redundant data blocks and deduplicates all redundant data stored in the directory. Available only if you activate a SmartDedupe license.</td>
<td>None</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>DedupeAssessment</td>
<td>Scans a directory for redundant data blocks and reports an estimate of the amount of space that could be saved by deduplicating the directory.</td>
<td>None</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>DomainMark</td>
<td>Associates a path, and the contents of that path, with a domain.</td>
<td>None</td>
<td>Low</td>
<td>5</td>
<td>Manual</td>
</tr>
<tr>
<td>FlexProtect</td>
<td>Scans the file system after a device failure to ensure that all files remain protected. FlexProtect is most efficient on clusters that contain only HDDs. While there is a device failure on a cluster, only the FlexProtect (or FlexProtectLin) job is allowed to run. Depending on the size of your data set, this process can last for an extended period. The cluster is said to be in a degraded state until FlexProtect (or FlexProtectLin) finishes its work. If you notice that other system jobs cannot be started or have been paused, you can use the isi job status --verbose command to see if a &quot;Cluster Is Degraded&quot; message appears.</td>
<td>Restripe</td>
<td>Medium</td>
<td>1</td>
<td>Manual</td>
</tr>
</tbody>
</table>
### System jobs

<table>
<thead>
<tr>
<th>Job name</th>
<th>Description</th>
<th>Exclusion Set</th>
<th>Impact Policy</th>
<th>Priority</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Unlike HDDs and SSDs that are used for storage, when an SSD used for L3 cache fails, the drive state should immediately change to REPLACE without a FlexProtect job running. An SSD drive used for L3 cache contains only cache data that does not have to be protected by FlexProtect. After the drive state changes to REPLACE, you can pull and replace the failed SSD.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlexProtectLin</td>
<td>Scans the file system after a device failure to ensure that all files remain protected. This command is most efficient when file system metadata is stored on SSDs. In this situation, run FlexProtectLin instead of FlexProtect.</td>
<td>Restripe</td>
<td>Medium</td>
<td>1</td>
<td>Manual</td>
</tr>
<tr>
<td>FSAnalyze*</td>
<td>Gathers and reports information about all files and directories beneath the /ifs path. This job requires you to activate an InsightIQ license. Reports from this job are used by InsightIQ users for system analysis purposes. For more information, see the <em>Isilon InsightIQ User Guide</em>.</td>
<td>None</td>
<td>Low</td>
<td>1</td>
<td>Scheduled</td>
</tr>
<tr>
<td>IntegrityScan</td>
<td>Verifies file system integrity.</td>
<td>Mark</td>
<td>Medium</td>
<td>1</td>
<td>Manual</td>
</tr>
<tr>
<td>MediaScan</td>
<td>Locates and clears media-level errors from disks to ensure that all data remains protected.</td>
<td>Restripe</td>
<td>Low</td>
<td>8</td>
<td>Scheduled</td>
</tr>
<tr>
<td>MultiScan</td>
<td>Performs the work of the AutoBalance and Collect jobs simultaneously.</td>
<td>Restripe</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>PermissionRepair</td>
<td>Uses a template file or directory as the basis for permissions to set on a target file or directory. The target directory must always be subordinate to the /ifs path. This job must be manually started.</td>
<td>None</td>
<td>Low</td>
<td>5</td>
<td>Manual</td>
</tr>
<tr>
<td>QuotaScan*</td>
<td>Updates quota accounting for domains created on an existing file tree. Available only if you activate a SmartQuotas license. This job should be run manually in off-hours after setting up all quotas, and whenever setting up new quotas.</td>
<td>None</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>SetProtectPlus</td>
<td>Applies a default file policy across the cluster. Runs only if a SmartPools license is not active.</td>
<td>Restripe</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>ShadowStoreDelete</td>
<td>Frees up space that is associated with shadow stores. Shadow stores are hidden</td>
<td>None</td>
<td>Low</td>
<td>2</td>
<td>Scheduled</td>
</tr>
</tbody>
</table>

---

FSAnalyze*: This job provides information about the file system. It helps in analyzing and managing files effectively.

FlexProtectLin: This command is used to scan the file system after a device failure to ensure data integrity.

IntegrityScan: This job verifies the file system integrity, ensuring data remains safe and protected.

MediaScan: It is used to locate and clear media-level errors from disks, ensuring data remains intact.

MultiScan: This job performs the work of both AutoBalance and Collect jobs simultaneously, optimizing system maintenance.

PermissionRepair: It uses a template file or directory as the basis for setting permissions on target files or directories, ensuring access control is maintained.

QuotaScan*: This job updates quota accounting for existing file trees, managing resource allocation efficiently.

SetProtectPlus: This job applies a default file policy across the cluster, setting a standard level of protection universally.

ShadowStoreDelete: It frees up space associated with shadow stores, managing disk usage effectively.
OneFS includes system maintenance jobs that run to ensure that your Isilon cluster performs at peak health. Through the Job Engine, OneFS runs a subset of these jobs automatically, as needed, to ensure file and data integrity, check for and mitigate drive and node failures, and optimize free space. For other jobs, for example, Dedupe, you can use Job Engine to start them manually or schedule them to run automatically at regular intervals.

The Job Engine runs system maintenance jobs in the background and prevents jobs within the same classification (exclusion set) from running simultaneously. Two exclusion sets are enforced: restripe and mark.

Restripe job types are:
Mark job types are:

- Collect
- IntegrityScan
- MultiScan

Note that MultiScan is a member of both the restripe and mark exclusion sets. You cannot change the exclusion set parameter for a job type.

The Job Engine is also sensitive to job priority, and can run up to three jobs, of any priority, simultaneously. Job priority is denoted as 1–10, with 1 being the highest and 10 being the lowest. The system uses job priority when a conflict among running or queued jobs arises. For example, if you manually start a job that has a higher priority than three other jobs that are already running, Job Engine pauses the lowest-priority active job, runs the new job, then restarts the older job at the point at which it was paused. Similarly, if you start a job within the restripe exclusion set, and another restripe job is already running, the system uses priority to determine which job should run (or remain running) and which job should be paused (or remain paused).

Other job parameters determine whether jobs are enabled, their performance impact, and schedule. As system administrator, you can accept the job defaults or adjust these parameters (except for exclusion set) based on your requirements.

When a job starts, the Job Engine distributes job segments—phases and tasks—across the nodes of your cluster. One node acts as job coordinator and continually works with the other nodes to load-balance the work. In this way, no one node is overburdened, and system resources remain available for other administrator and system I/O activities not originated from the Job Engine.

After completing a task, each node reports task status to the job coordinator. The node acting as job coordinator saves this task status information to a checkpoint file. Consequently, in the case of a power outage, or when paused, a job can always be restarted from the point at which it was interrupted. This is important because some jobs can take hours to run and can use considerable system resources.

**Job performance impact**

The Job Engine service monitors system performance to ensure that maintenance jobs do not significantly interfere with regular cluster I/O activity and other system administration tasks. Job Engine uses impact policies that you can manage to control when a job can run and the system resources that it consumes.

Job Engine has four default impact policies that you can use but not modify. The default impact policies are:
### Impact policy

<table>
<thead>
<tr>
<th>Impact policy</th>
<th>Allowed to run</th>
<th>Resource consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>Any time of day.</td>
<td>Low</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Any time of day.</td>
<td>Medium</td>
</tr>
<tr>
<td>HIGH</td>
<td>Any time of day.</td>
<td>High</td>
</tr>
<tr>
<td>OFF_HOURS</td>
<td>Outside of business hours. Business hours are defined as 9AM to 5pm, Monday through Friday. OFF_HOURS is paused during business hours.</td>
<td>Low</td>
</tr>
</tbody>
</table>

If you want to specify other than a default impact policy for a job, you can create a custom policy with new settings.

Jobs with a low impact policy have the least impact on available CPU and disk I/O resources. Jobs with a high impact policy have a significantly higher impact. In all cases, however, the Job Engine uses CPU and disk throttling algorithms to ensure that tasks that you initiate manually, and other I/O tasks not related to the Job Engine, receive a higher priority.

## Job priorities

Job priorities determine which job takes precedence when more than three jobs of different exclusion sets attempt to run simultaneously. The Job Engine assigns a priority value between 1 and 10 to every job, with 1 being the most important and 10 being the least important.

The maximum number of jobs that can run simultaneously is three. If a fourth job with a higher priority is started, either manually or through a system event, the Job Engine pauses one of the lower-priority jobs that is currently running. The Job Engine places the paused job into a priority queue, and automatically resumes the paused job when one of the other jobs is completed.

If two jobs of the same priority level are scheduled to run simultaneously, and two other higher priority jobs are already running, the job that is placed into the queue first is run first.

## Managing system jobs

The Job Engine enables you to control periodic system maintenance tasks that ensure OneFS file system stability and integrity. As maintenance jobs run, the Job Engine constantly monitors and mitigates their impact on the overall performance of the cluster.

As system administrator, you can tailor these jobs to the specific workflow of your Isilon cluster. You can view active jobs and job history, modify job settings, and start, pause, resume, cancel, and update job instances.
**Start a job**

Although OneFS runs several critical system maintenance jobs automatically when necessary, you can also manually start any job at any time.

The Collect job, used here as an example, reclaims free space that previously could not be freed because the node or drive was unavailable.

**Procedure**

1. Run the `isi job jobs start` command.

   The following command runs the Collect job with a stronger impact policy and a higher priority.

   ```
   isi job jobs start Collect --policy MEDIUM --priority 2
   ```

**Results**

When the job starts, a message such as `Started job [7]` appears. In this example, 7 is the job ID number, which you can use to run other commands on the job.

**Pause a job**

To free up system resources, you can pause a job temporarily.

**Before you begin**

To pause a job, you need to know the job ID number. If you are unsure of the job ID number, you can use the `isi job jobs list` command to see a list of running jobs.

**Procedure**

1. Run the `isi job jobs pause` command.

   The following command pauses a job with an ID of 7.

   ```
   isi job jobs pause 7
   ```

   If there is only one instance of a job type currently active, you can specify the job type instead of the job ID.

   ```
   isi job jobs pause Collect
   ```

   In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

   ```
   isi job pause Collect
   ```
Modify a job

You can change the priority and impact policy of an active, waiting, or paused job.

Before you begin

To modify a job, you need to know the job ID number. If you are unsure of the job ID number, you can use the `isi job jobs list` command to see a list of running jobs.

When you modify a job, only the current instance of the job runs with the updated settings. The next instance of the job returns to the default settings for that job type.

Procedure

1. Run the `isi job jobs modify` command.

   The following command updates the priority and impact policy of an active job (job ID number 7).

   ```bash
   isi job jobs modify 7 --priority 3 --policy medium
   ```

   If there is only one instance of a job type currently active, you can specify the job type instead of the job ID.

   ```bash
   isi job jobs modify Collect --priority 3 --policy medium
   ```

Resume a job

You can resume a paused job.

Before you begin

To resume a job, you need to know the job ID number. If you are unsure of the job ID number, you can use the `isi job jobs list` command.

Procedure

1. Run the `isi job jobs resume` command.

   The following command resumes a job with the ID number 7.

   ```bash
   isi job jobs resume 7
   ```

   If there is only one instance of a job type currently active, you can specify the job type instead of the job ID.

   ```bash
   isi job jobs resume Collect
   ```
Cancel a job

If you want to free up system resources, or for any reason, you can cancel a running, paused, or waiting job.

**Before you begin**

To cancel a job, you need to know the job ID number. If you are unsure of the job ID number, you can use the `isi job jobs list` command.

**Procedure**

1. Run the `isi job jobs cancel` command.

   The following command cancels a job with the ID number 7.

   ```
   isi job jobs cancel 7
   ```

   If there is only one instance of a job type currently active, you can specify the job type instead of the job ID.

   ```
   isi job jobs cancel Collect
   ```

Modify job type settings

You can customize system maintenance jobs for your administrative workflow by modifying the default priority level, impact level, and schedule for a job type.

The job type ID is the job name, for example, MediaScan.

**Procedure**

1. Run the `isi job types modify` command.

   The following command modifies the default priority level and impact level for the MediaScan job type.

   ```
   isi job types modify mediascan --priority 2 --policy medium
   ```

   When you run this command, the system prompts you to confirm the change. Type `yes` or `no`, and then press ENTER.

2. Establish a regular schedule for a job type.

   The following command schedules the MediaScan job to run every Saturday morning at 9 AM. The `--force` option overrides the confirmation step.

   ```
   isi job types modify mediascan --schedule 'every Saturday at 09:00' --force
   ```

3. Remove a regular schedule for a job type.

   The following command removes the schedule for a job type that is scheduled.

   ```
   isi job types modify mediascan --clear-schedule --force
   ```
Results
All subsequent iterations of the MediaScan job type run with the new settings. If a MediaScan job is in progress, it continues to use the old settings.

View active jobs

You can view information about jobs that are currently running on your Isilon cluster.
You might want to check active jobs if you are noticing slower system response or to see what jobs are active before starting a new job.

Procedure
1. Run the `isi job jobs list` command.

View job history

You can view recent activity for system maintenance jobs.
You might want to check the last time a critical job ran, view all job history within a recent time period, or output job history for a certain time period into a comma-delimited format file.

Procedure
1. Run the `isi job events list` command for a specific job type.
   The following command displays the activity of the MultiScan job type.

   `isi job events list --job-type multiscan`

2. View all jobs within a specific time frame.
   The following command displays all jobs that ran since September 16, 2013.

   `isi job events list --begin 2013-09-16`

3. For reporting purposes, redirect output to a comma-delimited file.
   The following command outputs job history for a specific two-week period to a specified path name.

   `isi job events list --begin 2013-09-15 --end 2013-09-16 > /ifs/data/report1.txt`
Managing impact policies

For system maintenance jobs that run through the Job Engine service, you can create and assign policies that help control how jobs affect system performance.

As system administrator, you can create, copy, modify, and delete impact policies, and view their settings.

Create an impact policy

The Job Engine includes four default impact policies, which you cannot modify or delete. However, you can create new impact policies.

You can create custom impact policies to define the best times for system maintenance jobs to run and mitigate their impact on system resources.

Procedure

1. Run the `isi job policies create` command.

   The following command creates a custom policy defining a specific time frame and impact level. You can apply the custom policy to any job instance to enable the job to run at a higher impact over the weekend.

   ```
   isi job policies create MY_POLICY --impact medium --begin 'Saturday 00:00' --end 'Sunday 23:59'
   ```

2. View a list of available impact policies to see if your custom policy was created successfully.

   The following command displays a list of impact policies.

   ```
   isi job policies list
   ```

   The displayed list appears as follows.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Isilon template: high impact at all times</td>
</tr>
<tr>
<td>LOW</td>
<td>Isilon template: high impact at all times</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Isilon template: high impact at all times</td>
</tr>
<tr>
<td>OFF-HOURS</td>
<td>Isilon template: Paused M-F 9-5, low impact otherwise</td>
</tr>
<tr>
<td>MY_POLICY</td>
<td></td>
</tr>
</tbody>
</table>

3. Add a description to the custom policy.

   The following command adds a description to the custom policy.

   ```
   isi job policies modify MY_POLICY --description 'Custom policy: medium impact when run on weekends'
   ```
View impact policy settings

You can view the settings of any impact policy. If you intend to modify an impact policy, you can view the current policy settings. In addition, after you have modified an impact policy, you can view the policy settings to ensure that they are correct.

Procedure

1. Run the `isi job policies view` command.

   The following command displays the impact policy settings of the custom impact policy MY_POLICY.

   ```
   isi job policies view MY_POLICY
   ```

Modify an impact policy

You can change the description and policy intervals of a custom impact policy.

Before you begin

You cannot modify the default impact policies, HIGH, MEDIUM, LOW, and OFF_HOURS. You can only modify policies that you create.

Procedure

1. Run the `isi job policies modify` command to reset current settings to base defaults.

   Policy settings are cumulative, so defining a new impact level and time interval adds to any existing impact level and interval already set on the custom policy. The following command resets the policy interval settings to the base defaults: low impact and anytime operation.

   ```
   isi job policies modify MY_POLICY --reset-intervals
   ```

2. Run the `isi job policies modify` command to establish new impact level and interval settings for the custom policy.

   The following command defines the new impact level and interval of a custom policy named MY_POLICY.

   ```
   isi job policies modify MY_POLICY --impact high --begin 'Saturday 09:00' --end 'Sunday 11:59'
   ```

3. Verify that the custom policy has the settings that you intended.

   The following command displays the current settings for the custom policy.

   ```
   isi job policies view MY_POLICY
   ```
Delete an impact policy

You can delete impact policies that you have created.

Before you begin

You cannot delete default impact policies, HIGH, MEDIUM, LOW, and OFF_HOURS.

Procedure

1. Run the `isi job policies delete` command.

   The following command deletes a custom impact policy named `MY_POLICY`.

   ```bash
   isi job policies delete MY_POLICY
   ```

   OneFS displays a message asking you to confirm the deletion of your custom policy.

2. Type `yes` and press ENTER.

Viewing job reports and statistics

You can generate reports for system jobs and view statistics to better determine the amounts of system resources being used.

Most system jobs controlled by the Job Engine run at a low priority and with a low impact policy, and generally do not have a noticeable impact on cluster performance.

A few jobs, because of the critical functions they perform, run at a higher priority and with a medium impact policy. These jobs include FlexProtect and FlexProtect Lin, FSAnalyze, SnapshotDelete, and TreeDelete.

As a system administrator, if you are concerned about the impact a system job might have on cluster performance, you can view job statistics and reports. These tools enable you to view detailed information about job load, including CPU and memory usage and I/O operations.

View statistics for a job in progress

You can view statistics for a job in progress.

Before you begin

You need to specify the job ID to view statistics for a job in progress. The `isi job jobs list` command displays a list of active jobs, including job IDs.

Procedure

1. Run the `isi job statistics view` command with a specific job ID.

   The following command displays statistics for a Collect job with the ID of 857:

   ```bash
   isi job statistics view --job-id 857
   ```

   The system displays output similar to the following example:

   ```
   Job ID: 857
   Phase: 1
   ```
**Nodes**

Node: 1  
PID: 26224  
CPU: 7.96% (0.00% min, 28.96% max, 4.60% avg)

Virtual: 187.23M (187.23M min, 187.23M max, 187.23M avg)  
Physical: 19.01M (18.52M min, 19.33M max, 18.96M avg)

Read: 931043 ops, 7.099G  
Write: 1610213 ops, 12.269G  
Workers: 1 (0.00 STW avg.)

---

**View a report for a completed job**

After a job finishes, you can view a report about the job.

**Before you begin**

You need to specify the job ID to view the report for a completed job. The `isi job reports list` command displays a list of all recent jobs, including job IDs.

**Procedure**

1. Run the `isi job reports view` command with a specific job ID.

The following command displays the report of a Collect job with an ID of 857:

```
isi job reports view 857
```

The system displays output similar to the following example:

```
------------------------------------------
LIN scan
Elapsed time:                     6506 seconds
LINs traversed:                 433423
Files seen:                     396980
Directories seen:                36439
Errors:                              0
Total blocks:                 27357443452 (13678721726 KB)
CPU usage:                         max 28% (dev 1), min 0% (dev 1), avg 4%
Virtual memory size:               max 193300K (dev 1), min 191728K (dev 1), avg 1925
Resident memory size:             max 21304K (dev 1), min 18884K (dev 2), avg 20294K
Read:                              11637860 ops, 95278721726 bytes (90859.3M)
Write:                             20717079 ops, 169663891968 bytes (161804.1M)
```
Job management commands

OneFS provides a library of system maintenance jobs to ensure the integrity of your data and the health of your Isilon cluster. You can control these system maintenance jobs through the job management commands.

**isi job events list**

Lists recent job events.

**Syntax**

```
isi job events list
    [--job-type <string>]
    [--job-id <integer>]
    [{--begin} <timestamp>]
    [--end <timestamp>]
    [--state {failed | running | cancelled_user | succeeded | paused_user | unknown | paused_priority | cancelled_system | paused_policy | paused_system}]
    [--limit <integer>]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

`--job-type <string>`  
Displays all events of all instances of a specific job type (for example, SmartPools).

`--job-id <integer>`  
Displays all events of a specific job instance.

`--begin <timestamp>`  
Specifies the beginning of the time period for which job events should be listed. For example, `--begin "2013-09-17T00:00"`. This means that job events beginning at the first moment of September 17, 2013 should be listed.

`--end <timestamp>`  
Specifies the end of the time period for job events to be listed. For example, `--end "2013-09-17T23:59"` means that job events right up to the last minute of September 17, 2013 should be listed.

`--state {failed | running | cancelled_user | succeeded | paused_user | unknown | paused_priority | cancelled_system | paused_policy | paused_system}`  
Specifies that events of the given state or states should be listed.

`{--limit | -l} <integer>`
Displays no more than the specified number of job events. If no timestamp parameters are specified, the most recent job events of the specified number are listed.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information about job events.

Examples
The following command lists all FSAnalyze events that happened in the month of September.

```
isi job events list --job-type fsanalyze --begin "2013-09-01" --end "2013-09-30"
```

The system displays output similar to the following example.

<table>
<thead>
<tr>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-09-16T22:00:23</td>
<td>FSAnalyze[7] Running</td>
</tr>
<tr>
<td>2013-09-16T22:00:25</td>
<td>FSAnalyze[7] Phase 1: begin scan</td>
</tr>
<tr>
<td>2013-09-16T22:01:45</td>
<td>FSAnalyze[7] Phase 1: end scan</td>
</tr>
<tr>
<td>2013-09-16T22:02:30</td>
<td>FSAnalyze[7] Phase 2: end merge</td>
</tr>
<tr>
<td>2013-09-17T22:00:05</td>
<td>FSAnalyze[9] Waiting</td>
</tr>
<tr>
<td>2013-09-17T22:00:08</td>
<td>FSAnalyze[9] Running</td>
</tr>
<tr>
<td>2013-09-17T22:00:11</td>
<td>FSAnalyze[9] Phase 1: begin scan</td>
</tr>
<tr>
<td>2013-09-17T22:01:37</td>
<td>FSAnalyze[9] Phase 1: end scan</td>
</tr>
<tr>
<td>2013-09-17T22:01:38</td>
<td>FSAnalyze[9] Phase 2: begin merge</td>
</tr>
<tr>
<td>2013-09-17T22:02:24</td>
<td>FSAnalyze[9] Phase 2: end merge</td>
</tr>
<tr>
<td>2013-09-17T22:02:26</td>
<td>FSAnalyze[9] Succeeded</td>
</tr>
</tbody>
</table>

Total: 14

The following command lists all the job events that happened on a specific day.

```
isi job events list --begin "2013-09-17T00:00" --end "2013-09-17T23:59"
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
</table>

Total: 14
isi job jobs cancel

Cancels an active job.

Syntax

```bash
isi job jobs cancel <job>
```

Options

`<job>`

Specifies the job to cancel. You can specify the job by job ID or job type. Specify a job type only if one instance of that job type is active.

Examples

The following command cancels an active MultiScan job.

```bash
isi job jobs cancel multiscan
```

The following command cancels an active job with an instance ID of 14.

```bash
isi job jobs cancel 14
```

In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

```bash
isi job cancel 14
```

isi job jobs list

Displays information about active jobs.

Syntax

```bash
isi job jobs list
```
Options

--state {running | paused_user | paused_priority | paused_policy | paused_system}

Controls which jobs are listed according to status.

{-limit | -l} <integer>

Displays no more than the specified number of items. If no other parameters are specified, displays the most recently activated jobs up to the specified number.

--sort {id | type | state | impact | policy | priority | start_time | running_time}

Sorts the output by the specified attribute.

--descending

Sorts the output in descending order of activation time.

--format {table | json | csv | list}

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{-no-header}

Displays table and CSV output without headers.

{-no-footer}

Displays table output without footers.

{-verbose}

Displays more detailed information about active jobs.

Examples

The following example lists jobs that have been manually paused.

isi job jobs list --state paused_user

The system displays output similar to the following example.

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>State</th>
<th>Impact</th>
<th>Pri</th>
<th>Phase</th>
<th>Running Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Collect</td>
<td>Paused by user Low</td>
<td>4</td>
<td>1/2</td>
<td>11s</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>SmartPools</td>
<td>Paused by user Low</td>
<td>6</td>
<td>1/8</td>
<td>40s</td>
<td></td>
</tr>
</tbody>
</table>
Total: 2

The following example outputs a CSV-formatted list of jobs to a file in the /ifs/data path.

```
isil job jobs list --format csv > /ifs/data/joblist.csv
```

In all instructions that include the isi job jobs command, you can omit the jobs entry.

```
isil job list --format csv > /ifs/data/joblist.csv
```

**isi job jobs modify**

Changes the priority level or impact policy of a queued, running, or paused job.

**Syntax**

```
isil job jobs modify <job>
    [--priority <integer>]
    [--policy <string>]
```

**Options**

- `<job>`
  - Specifies the job ID or job type to modify. If you specify job type (for example, FlexProtect), only one instance of that type can be active.

- `{--priority | -p} <integer>`
  - Sets the priority level for the specified job.

- `{--policy | -o} <string>`
  - Sets the impact policy for the specified job.

**Examples**

The following command changes the impact policy of an active MultiScan job. This command example, which specifies the job type, works only when a single instance of MultiScan is active.

```
isil job jobs modify multiscan --policy high
```

If more than one instance of a job type is active, you can specify the job ID number instead of job type. The following command changes the priority of an active job with an ID of 7.

```
isil job jobs modify 7 --priority 2
```
In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

```
isi job modify 7 --priority 2
```

## isi job jobs pause

Pauses an active job.

### Syntax

```
isi job jobs pause <job>
```

### Options

- `<job>`
  - Specifies the job to pause. You can specify the job by job type or job ID. If you use job type, only one instance of the job type can be active.

### Examples

The following command pauses an active AutoBalance job.

```
isi job jobs pause autobalance
```

The following command pauses an active job with an ID of 18.

```
isi job jobs pause 18
```

In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

```
isi job pause 18
```

To resume a paused job, use the `isi job resume` command.

## isi job jobs resume

Resumes a paused job.

You can confirm that a job has resumed by using the `isi job jobs list` command. Actual resumption of the job can take a while, depending on other activity in the Job Engine queue.

### Syntax

```
isi job jobs resume <job>
```

### Options

- `<job>`
Specifies the job to resume. You can specify the job by job type or job ID. If you use the job type parameter, only one instance of this job type can be in the Job Engine queue.

Examples
The following command resumes a paused AutoBalance job.

```
isi job jobs resume autobalance
```

The following command resumes a paused job with an ID of 16.

```
isi job jobs resume 16
```

In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

```
isi job resume 16
```

### isi job jobs start

Starts a new job.

The `isi job jobs start` command does not control jobs that are already in progress. If an active job is paused, you can use the `isi job jobs resume` command to start it from the point it was paused.

**Syntax**

```
isi job jobs start <type>
   [--policy <string>]
   [--priority <integer>]
   [--no-dup]
   [--paths <path>]
   [--delete]
   [--root <path>]
   [--dm-type {snaprevert | synciq}]
   [--mapping-type {clone | sid | unix | native}]
   [--mode {clone | inherit | convert}]
   [--template <path>]
   [--zone <string>]
   [--snapid <integer>]
   [--verbose]
```

**Options**

- `<type>`
  Specifies the type of job to add to the job queue (for example, MediaScan).

- `[--priority] <integer>`
  Sets the priority level for the specified job, with 1 being the highest priority and 10 being the lowest.

- `[--policy] <string>`
Sets the impact policy for the specified job.

{-no-dup}
Disallows duplicate jobs. If an instance of the specified job is already in the queue, the new job does not start.

--paths <path>
Specifies the path of the job, which must be within /ifs. This option is valid only for the TreeDelete and PermissionRepair jobs.

--delete
Valid for the DomainMark job only. Deletes the domain mark.

--root <path>
Valid for the DomainMark job only. Specifies the root path location for the DomainMark job.

--dm-type {snaprevert | synciq}
Valid for the DomainMark job only. Specifies the domain type for the DomainMark job.

--mapping-type {global | sid | unix | native}
Valid for the PermissionRepair job only, and is only used with the --mode convert option. Specifies the type for PermissionRepair.

--mode {clone | inherit | convert}
Valid for the PermissionRepair job only. Specifies the mode for PermissionRepair.

--template <path>
Valid for the PermissionRepair job only. Specifies the pathname of a template file to use as a model for the PermissionRepair job. Must be within the /ifs path.

--zone <string>
Valid for the PermissionRepair job only. Specifies the access zone for PermissionRepair.

--snapid <integer>
Valid for the SnapRevert job only. Specifies a snapshot ID for the SnapRevert job.

{-verbose | -v}
Displays more detailed information.

Examples
The following command starts an AutoBalance job.

isi job jobs start autobalance
The following command starts a MultiScan job with a priority of 8 and a high impact policy.


```bash
isi job jobs start multiscan --priority 8 --policy high
```

The following command starts a TreeDelete job with a priority of 10 and a low impact policy that deletes the `/ifs/data/old` directory.


```bash
isi job jobs start treedelete --path /ifs/data/old --priority 10 --policy low
```

In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

```bash
isi job start autobalance
```

### `isi job jobs view`

Displays information about a running or queued job, including the state, impact policy, priority, and schedule.

**Syntax**

```bash
isi job jobs view <job>
```

**Options**

- `<job>`
  - Specifies the job to view. You can specify the job by job type or job ID. If you specify a job type, only one instance of this job can be active.

**Examples**

The following command displays information about an AutoBalance job with a job ID of 15.

```bash
isi job jobs view 15
```

The system displays information similar to the following example.

```
ID: 15
Type: AutoBalance
State: Paused by user
Impact: Low
Policy: LOW
Pri: 4
Phase: 1/5
Start Time: 2013-09-19T09:08:28
Running Time: 24s
Participants: 1, 2, 3
Progress: Drives: 6 done, 0 in progress; last updated 3:0;
Processed 4624 LINs and 918669 KB; 0 ECCs and 0 errors
```
In all instructions that include the `isi job jobs` command, you can omit the `jobs` entry.

`isi job view 15`

**isi job policies create**

Creates a custom job impact policy.

By default, the new impact policy is assigned a low impact level. You can specify multiple time periods (intervals) during which the job can run at higher impact levels or be paused.

**Syntax**

```
isi job policies create <name>
[--description <string>]
[--impact {Low | Medium | High | Paused}]
[--begin <interval_time>]
[--end <interval_time>]
```

**Options**

- `<name>`
  Specifies a name for the new impact policy. The following names are reserved and cannot be used: LOW, MEDIUM, HIGH, and OFF_HOURS.

- `--description <string>`
  Describes the job policy.

- `--impact {Low | Medium | High | Paused}`
  Specifies an impact level for the policy: Low, Medium, High, or Paused. You can specify an `--impact` parameter for each impact interval that you define.

- `--begin <interval_time>`
  Specifies the beginning time, on a 24-hour clock, of the period during which a job can run. For example: `--begin "Friday 20:00"`.

- `--end <interval_time>`
  Specifies the ending time, on a 24-hour clock, of the period during which a job can run. For example: `--end "Sunday 11:59"`.

**Examples**

The following command creates a new impact policy named HIGH-WKEND.

```
isi job policies create HIGH-WKEND --impact high --begin "Saturday 00:01" --end "Sunday 23:59"
```

The following command creates a more complex impact policy named HI-MED-WKEND. This policy includes multiple impact levels and time intervals. At the end of
the specified intervals, a job running with this policy would automatically return to LOW impact.

```
isi job policies create HI-MED-WKEND --description "High to medium impact when run on the weekend" --impact high --begin "Friday 20:00" --end "Monday 03:00" --impact medium --begin "Monday 03:01" --end "Monday 08:00"
```

**isi job policies delete**

Deletes a job impact policy.

The following policies are reserved and cannot be deleted: LOW, MEDIUM, HIGH, and OFF_HOURS.

**Syntax**

```
isi job policies delete <id> [--force]
```

**Options**

- `<id>`
  
  Specifies the name of the impact policy to delete. If you are unsure of the name, you can use the `isi job policies list` command.
  
- `--force`
  
  Forces deletion of the impact policy without the system asking for confirmation.

**Examples**

The following command deletes a custom impact policy named HIGH-MED.

```
isi job policies delete HIGH-MED
```

When you press ENTER, OneFS displays a confirmation message: Are you sure you want to delete the policy HIGH-MED? (yes/[no]):

Type `yes`, and then press ENTER.

The following command deletes a custom impact policy named HIGH-WKEND without the confirmation message being displayed.

```
isi job policies delete HIGH-WKEND --force
```

**isi job policies list**

Displays the names and descriptions of job impact policies.

**Syntax**

```
isi job policies list [--limit <integer>]
```
Options

```bash
--limit | -l <integer>
  Displays no more than the specified number of items.

--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

--no-header | -a
  Displays table and CSV output without headers.

--no-footer | -z
  Displays table output without footers.

--verbose | -v
  Displays more detailed information.
```

Examples

The following command displays a list of available impact policies.

```bash
isi job policies list
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Isilon template: high impact at all times</td>
</tr>
<tr>
<td>LOW</td>
<td>Isilon template: low impact at all times</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Isilon template: medium impact at all times</td>
</tr>
<tr>
<td>OFF_HOURS</td>
<td>Isilon template: paused M-F 9-5, low-impact at other times</td>
</tr>
<tr>
<td>HI-MED</td>
<td>High to medium to low</td>
</tr>
<tr>
<td>HI-WKEND</td>
<td>High impact when run on weekends</td>
</tr>
<tr>
<td>MED-WKEND</td>
<td>Medium impact when run on weekends</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>7</td>
</tr>
</tbody>
</table>

The following command displays more information about available policies.

```bash
isi job policies list --verbose
```

The system displays verbose output in a list format as shown in the following partial example:

```
ID: HIGH
Description: Isilon template: high impact at all times
```
isi job policies modify

Change the description, impact levels and time intervals of a custom impact policy.

To confirm that the custom policy reflects your changes, you can use the isi job policy view command.

Syntax

    isi job policy modify  <ID>
        [--description<string>]
        [--impact {Low | Medium | High | Paused}]
        [--begin <interval_time>]
        [--end <interval_time>]
        [--reset-intervals]

Options

<ID>
    Specifies the name of the policy to modify.

    --description <string>
        Specifies a description for the policy. Replaces an older description if one was in place.

    --impact {Low | Medium | High | Paused}
        Specifies an impact level for the policy: Low, Medium, High, or Paused. Specify an --impact parameter for each additional impact interval that you define.

    --begin <interval_time>
        Specifies the beginning time, on a 24-hour clock, of the period during which a job can run. For example: --begin "Friday 20:00".

    --end <interval_time>
        Specifies the ending time, on a 24-hour clock, of the period during which a job can run. For example: --end "Sunday 11:59".

    --reset-intervals
        Clears all job policy intervals and restores the defaults.
Examples
The following command clears the custom intervals from a custom policy named MY_POLICY as the first step to adding new intervals.

```
isi job policies modify MY_POLICY --reset-intervals
```

The following command adds new intervals to a custom policy.

```
isi job policies modify MY_POLICY --impact high --begin "Friday 20:00" --end "Sunday 11:59"
```

**isi job policies view**

Displays the details for a specific Job Engine job policy.

**Syntax**

```
isi job policies view
  [<id> <string>]
```

**Options**

`<id> <string>`

Specifies the job policy to display by policy ID.

**Examples**

The following command displays the details for the default job policy, HIGH.

```
isi job policies view HIGH
```

The system displays the following policy details:

```
ID: HIGH
Description: Isilon template: high impact at all times
  System: True
Impact Intervals
  Impact : High
  Begin : Sunday 00:00
  End : Sunday 00:00
```

**isi job reports list**

Displays information about successful job operations, including date and time, job ID, job type, and job phases that fully completed.

**Syntax**

```
isi job reports list
    [--job-type <string>]
    [--job-id <integer>]
    [--begin <timestamp>]
```
System jobs

```
[{--end} <timestamp>
[--limit <integer>]
[---format {table | json | csv | list}]
[--no-header]
[--no-footer]
```

Options

--job-type <string>
Displays reports for all instances of the specified job type.

--job-id <integer>
Displays the report for a job with the specified job ID. If a job has multiple phases, Job Engines displays a report for each phase of the specified job ID.

{--begin | -b} <interval_time>
Specifies the beginning of the time period for the job reports list. For example: --begin "2013-09-19".

{--end | -e} <interval_time>
Specifies the end of the time period for the job reports list. For example: --end "2013-09-20".

{--limit | -l} <integer>
Displays no more than the specified number of reports.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

Examples

The following command displays reports for all MultiScan jobs within a specified time period.

```
isi job reports list --job-type multiscan --begin "2013-9-19" --end "2013-9-20"
```

The system displays output similar to the following example.

<table>
<thead>
<tr>
<th>Time</th>
<th>Job ID</th>
<th>Job Type</th>
<th>Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-09-19T10:00:08 1</td>
<td>MultiScan 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-09-19T10:00:20 1</td>
<td>MultiScan 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-09-19T10:00:21 1</td>
<td>MultiScan 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-09-19T10:00:34 1</td>
<td>MultiScan 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
isi job reports view

Displays a detailed report for a specific job. Reports can be displayed only for successful jobs or for successful phases of a job.

Syntax

```
isi job reports view <id>
```

Options

- `<id>`
  Specifies the job ID for the reports you want to view.

Examples

The following command requests reports for an FSAnalyze job with an ID of 7.

```
isi job reports view 7
```

The system displays output similar to the following example. Note that when a job has more than one phase, a report for each phase is provided.

```
------------------------------------------
FSA JOB QUERY PHASE
Elapsed time:              83 seconds
LINS traversed:             433
Errors:                     0
CPU usage:                  max 30% (dev 2), min 0% (dev 1), avg 10%
Virtual memory size:        max 111772K (dev 1), min 104444K (dev 2),
                             avg 109423K
Resident memory size:       max 14348K (dev 1), min 9804K (dev 3),
                             avg 12706K
Read:                       9 ops, 73728 bytes (0.1M)
Write:                      3035 ops, 24517120 bytes (23.4M)
------------------------------------------
------------------------------------------
FSA JOB MERGE PHASE
Elapsed time:              47 seconds
Errors:                     0
CPU usage:                  max 33% (dev 1), min 0% (dev 1), avg 8%
Virtual memory size:        max 113052K (dev 1), min 104444K (dev 2),
                             avg 109423K
Resident memory size:       max 16412K (dev 1), min 13424K (dev 3),
                             avg 14268K
Read:                       2 ops, 16384 bytes (0.0M)
Write:                      2157 ops, 16871424 bytes (16.1M)
```
isi job statistics list

Displays a statistical summary of active jobs in the Job Engine queue.

Syntax

```
isi job statistics list
  [--format {table | json | csv | list}]
  [--no-header]
  [--no-footer]
  [--verbose]
```

Options

```
--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
  Displays table and CSV output without headers.

{--no-footer | -z}
  Displays table output without footers.

{--verbose | -v}
  Displays more detailed information about active jobs, including node activity, CPU and memory usage, and number of workers (processes) involved.
```

Examples

The following command requests a statistical summary for active jobs.

```
isii job statistics list
```

The system displays output similar to the following example.

```
------------------------------------------------------------------
16    1     5.91%    102.25M       9.72M         9133    67.22M
------------------------------------------------------------------
Total: 1
```

The following command requests more detailed statistics about active jobs.

```
isii job statistics list --verbose
```

The system displays output similar to the following example. In the example, PID is the process ID and CPU indicates CPU utilization by the job. Also indicated are how many worker threads exist for the job on each node and what the sleep-to-work (STW) ratio
is for each thread. The statistics represent how the system throttles the job based on impact policies.

<table>
<thead>
<tr>
<th>Job ID: 16</th>
<th>Phase: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
<td></td>
</tr>
<tr>
<td>Node: 1</td>
<td>PID: 30977</td>
</tr>
<tr>
<td>CPU: 0.00% (0.00% min, 5.91% max, 2.84% avg)</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Virtual: 102.25M (102.12M min, 102.25M max, 102.23M avg)</td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td></td>
</tr>
<tr>
<td>Read: 5637 ops, 62.23M</td>
<td></td>
</tr>
<tr>
<td>Write: 3601 ops, 23.11M</td>
<td></td>
</tr>
<tr>
<td>Workers: 2 (0.60 STW avg.)</td>
<td></td>
</tr>
<tr>
<td>Node: 2</td>
<td>PID: 27704</td>
</tr>
<tr>
<td>CPU: 0.00% (0.00% min, 5.91% max, 2.18% avg)</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Virtual: 102.25M (102.00M min, 102.25M max, 102.22M avg)</td>
<td></td>
</tr>
<tr>
<td>Physical: 9.57M (9.46M min, 9.57M max, 9.56M avg)</td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td></td>
</tr>
<tr>
<td>Read: 4814 ops, 53.30M</td>
<td></td>
</tr>
<tr>
<td>Write: 1658 ops, 7.94M</td>
<td></td>
</tr>
<tr>
<td>Workers: 2 (0.60 STW avg.)</td>
<td></td>
</tr>
<tr>
<td>Node: 3</td>
<td>PID: 27533</td>
</tr>
<tr>
<td>CPU: 7.96% (1.95% min, 7.96% max, 5.62% avg)</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Virtual: 102.25M (102.25M min, 102.25M max, 102.25M avg)</td>
<td></td>
</tr>
<tr>
<td>Physical: 9.57M (9.57M min, 9.61M max, 9.59M avg)</td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td></td>
</tr>
<tr>
<td>Read: 5967 ops, 65.31M</td>
<td></td>
</tr>
<tr>
<td>Write: 5721 ops, 39.69M</td>
<td></td>
</tr>
<tr>
<td>Workers: 2 (0.60 STW avg.)</td>
<td></td>
</tr>
</tbody>
</table>

**isi job statistics view**

Displays statistics for an active job or jobs on an entire cluster or a specific node.

**Syntax**

`isi job statistics view
|--job-id <integer>
|--devid <integer>
|--verbose
|--format {table | json | csv | list}

**Options**

`--job-id <integer>
Displays statistics for a specific job ID.

`--devid <integer>
Displays statistics for a specific node (device) in the cluster.

`|--verbose | -v
Displays more detailed statistics for an active job or jobs.

`--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

Examples
The following command requests statistics for an AutoBalance job with an ID of 6.

```
isi job statistics view --job-id 6
```

The system displays output similar to the following example. In the example, PID is the process ID, and CPU indicates CPU utilization by the job. Also indicated are how many worker threads exist for the job on each node and what the sleep-to-work (STW) ratio is for each thread. The statistics represent how the system throttles the job based on impact policies.

<table>
<thead>
<tr>
<th>Node</th>
<th>PID</th>
<th>CPU</th>
<th>Memory</th>
<th>I/O</th>
<th>Workers</th>
<th>STW avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17006</td>
<td>0.00%</td>
<td>Virtual: 104.62M (104.37M min, 104.62M max, 104.59M avg)</td>
<td>Physical: 10.08M (10.01M min, 10.11M max, 10.09M avg)</td>
<td>2</td>
<td>0.60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Read: 4141 ops, 45.33M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Write: 5035 ops, 35.28M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>16352</td>
<td>13.96%</td>
<td>Virtual: 104.62M (104.37M min, 104.62M max, 104.59M avg)</td>
<td>Physical: 10.01M (9.90M min, 10.01M max, 10.00M avg)</td>
<td>2</td>
<td>0.60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Read: 3925 ops, 43.39M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Write: 4890 ops, 34.13M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15929</td>
<td>0.98%</td>
<td>Virtual: 104.62M (104.37M min, 104.62M max, 104.57M avg)</td>
<td>Physical: 9.86M (9.84M min, 9.94M max, 9.92M avg)</td>
<td>2</td>
<td>0.60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Read: 3354 ops, 36.77M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Write: 772 ops, 2.12M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**isi job types list**

Displays a list of job types and default settings.

**Syntax**

```
isi job types list
[--all]
[--sort {id | policy | exclusion_set | priority}]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
```
Options
--all
Displays all job types available in the Job Engine.

--sort {id | policy | exclusion_set | priority}
Sorts the output by the specified parameter.

--descending
In conjunction with --sort option, specifies that output be sorted descending
order. By default, output is sorted in ascending order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-
separated values (CSV), or list format.

{--no-header | -a}
Displays table and CSV output without headers.

{--no-footer | -z}
Displays table output without footers.

{--verbose | -v}
Displays more detailed information about a specific job type or all job types.

Examples
The following command provides detailed information about job types.

isi job types list --sort id --verbose

The system displays output similar to the following example.

| ID: AVScan |
| Description: Perform an antivirus scan on all files. |
| Enabled: Yes |
| Policy: LOW |
| Schedule: |
| Exclusion Set: None |
| Priority: 6 |

-------------------------------------------------------------------

| ID: AutoBalance |
| Description: Balance free space in a cluster. AutoBalance is most efficient in clusters that contain only HDDs. |
| Enabled: Yes |
| Policy: LOW |
| Schedule: |
| Exclusion Set: Restripe |
| Priority: 4 |

-------------------------------------------------------------------

| ID: AutoBalanceLin |
| Description: Balance free space in a cluster. AutoBalanceLin is |
isi job status

Displays a summary of active, completed, and failed jobs.

Syntax

    isi job status
        [--verbose]

Options

    {--verbose | -v}

        Displays more detailed job status information, including information about the
        cluster and nodes.

Examples

The following command provides basic job status.

    isi job status

The system displays output that is similar to the following example.

The job engine is running.
No running or queued jobs.

Recent finished jobs:
  ID  Type                    State                  Time
  ----------------------  ----------------------  ---------------------
  1  MultiScan              System Cancelled  2013-09-24T08:23:44
  3  MultiScan              Succeeded             2013-09-24T08:26:37
  2  SetProtectPlus        Succeeded             2013-09-24T08:27:16
  4  FlexProtect           Succeeded             2013-09-24T09:14:27

Total: 4

The following command provides more detailed job status information.

    isi job status --verbose

The system displays additional output that includes cluster and node information.

The job engine is running.
    Coordinator: 1
    Connected: True
    Disconnected Nodes: -
Down or Read-Only Nodes: False
Statistics Ready: True
Cluster Is Degraded: False
Run Jobs When Degraded: False

No running or queued jobs.

Recent finished jobs:

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>State</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MultiScan</td>
<td>System Cancelled</td>
<td>2013-09-24T08:23:44</td>
</tr>
<tr>
<td>3</td>
<td>MultiScan</td>
<td>Succeeded</td>
<td>2013-09-24T08:26:37</td>
</tr>
<tr>
<td>2</td>
<td>SetProtectPlus</td>
<td>Succeeded</td>
<td>2013-09-24T08:27:16</td>
</tr>
<tr>
<td>4</td>
<td>FlexProtect</td>
<td>Succeeded</td>
<td>2013-09-24T09:14:27</td>
</tr>
</tbody>
</table>

Total: 4

**isi job types modify**

Modifies the parameters of a specified job type.

You can view the current parameters of any job type by using the `isi job types view` command.

**Syntax**

```shell
isi job types modify <id>
[--enabled <boolean>]
[--policy <string>]
[--schedule <string>]
[--priority <integer>]
[--clear-schedule]
```

**Options**

- `<id>`
  Specifies the job type to modify.

- `--enabled <boolean>`
  Specifies whether the job type is enabled or disabled.

- `--policy <string>`
  Sets the policy for the specified job type.

- `--schedule <string>`
  Sets a recurring date pattern to run the specified job type.

- `--priority <integer>`
  Sets the priority level for the specified job type. Job types have a priority value between 1 and 10, with 1 being the highest priority and 10 being the lowest.

- `--clear-schedule`
  Clears any schedule associated with the specified job type.

- `--force`
  Forces the modification without a confirmation message.
Examples
The following command adds a recurring schedule to the MultiScan command.

```bash
isi job types modify multiscan --schedule "Every Friday at 22:00"
```

When you run this command, the system prompts you to confirm the change. Type `yes` or `no`, and then press ENTER.

### isi job types view

Displays the parameters of a specific job type, including the description, schedule, policy, priority, and whether the job type is a member of an exclusion set.

**Syntax**

```bash
isi job types view <id>
```

**Options**

- `<id>`
  - Specifies the job type to view.

**Examples**

The following command displays the parameters of the job type MultiScan.

```bash
isi job types view multiscan
```

The system displays output similar to the following example.

```
ID: MultiScan
Description: Perform the work of the AutoBalance and Collect jobs simultaneously.
   Enabled: Yes
   Policy: LOW
   Schedule: 
   Exclusion Set: Restripe, Mark
   Priority: 4
```
CHAPTER 26

Networking

This section contains the following topics:

- Networking overview ................................................................. 1048
- About the internal network .......................................................... 1048
- About the external network .......................................................... 1049
- Managing internal network settings .............................................. 1057
- Managing groupnets ................................................................. 1059
- Managing external network subnets .............................................. 1062
- Managing IP address pools ......................................................... 1066
- Managing SmartConnect Settings ............................................... 1070
- Managing connection rebalancing .............................................. 1074
- Managing network interface members ....................................... 1076
- Managing node provisioning rules .............................................. 1078
- Managing routing options ........................................................ 1081
- Managing DNS cache settings .................................................. 1082
- Managing TCP ports ................................................................. 1084
- Networking commands ............................................................. 1084
Networking overview

After you determine the topology of your network, you can set up and manage your internal and external networks.

There are two types of networks on the EMC Isilon cluster:

**Internal**

Nodes communicate with each other using a high speed low latency InfiniBand network. You can optionally configure a second InfiniBand network to enable failover for redundancy.

**External**

Clients connect to the cluster through the external network with Ethernet. The Isilon cluster supports standard network communication protocols, including NFS, SMB, HDFS, HTTP, and FTP. The cluster includes various external Ethernet connections, providing flexibility for a wide variety of network configurations.

About the internal network

The EMC Isilon cluster must connect to at least one high-speed, low-latency InfiniBand switch for internal communications and data transfer. The connection to the InfiniBand switch is also referred to as an internal network. The internal network is separate from the external network (Ethernet) by which users access the cluster.

Upon initial configuration of your cluster, OneFS creates an initial internal network for the InfiniBand switch. The interface to the default internal network is int-a. An internal network for a second InfiniBand switch can be added for redundancy and failover. Failover allows continuous connectivity during path failures. The interface to the secondary internal network is int-b, which is referred to as int-b/failover in the web administration interface.

**CAUTION**

Only Isilon nodes should be connected to your InfiniBand switch. Information exchanged on the back-end network is not encrypted. Connecting anything other than Isilon nodes to the InfiniBand switch creates a security risk.

Internal IP address ranges

The number of IP addresses assigned to the internal network determines how many nodes can be joined to the EMC Isilon cluster.

When you initially configure the cluster, you specify one or more IP address ranges for the primary InfiniBand switch. This range of addresses is used by the nodes to communicate with each other. It is recommended that you create a range of addresses large enough to accommodate adding additional nodes to your cluster.

While all clusters will have, at minimum, one internal InfiniBand network (int-a), you can enable a second internal network to support another Infiniband switch with network failover (int-b/failover). You must assign at least one IP address range for the secondary network and one range for failover.

If any IP address ranges defined during the initial configuration are too restrictive for the size of the internal network, you can add ranges to the int-a network or int-b/failover networks, which might require a cluster restart. Other configuration changes,
such as deleting an IP address assigned to a node, might also required the cluster to be restarted.

**Internal network failover**

You can configure an internal switch as a failover network to provide redundancy for intra-cluster communications.

In order to support an internal failover network, the int-a port on each node in the cluster must be physically connected to one of the Infiniband switches, and the int-b port on each node must be connected to the other Infiniband switch.

After the ports are connected, you must configure two IP address ranges; an address range to support the int-b internal interfaces, and an address range to support failover. The failover addresses enable seamless failover in the event that either the int-a or int-b switches fail.

**Configuring the internal network for IsilonSD Edge**

In the case of IsilonSD Edge, internal communications and data transfer between the IsilonSD nodes take place through the Ethernet switch.

You must isolate the internal network and ideally route it through a dedicated virtual LAN or physical switch. You can configure LACP or a port channel group to improve the network reliability and to increase the inter-cluster traffic throughput.

For the internal IP address range, you must specify one IP address per IsilonSD node. The IP addresses that you configure for the nodes must be contiguous.

For the internal network failover, IsilonSD Edge depends on the network failover and load balancing policies that are supported by VMware vSphere. You do not need to configure the int-b/failover network.

For more information on the networking requirements, see the *IsilonSD Edge Installation and Administration Guide*.

**About the external network**

You connect a client computer to the EMC Isilon cluster through the external network. External network configuration is composed of groupnets, subnets, IP address pools, and features node provisioning rules.

Groupnets are the configuration level for managing multiple tenants on your external network. DNS client settings, such as nameservers and a DNS search list, are properties of the groupnet. Groupnets reside at the top tier of the networking hierarchy. You can create one or more subnets within a groupnet.

Subnets simplify external (front-end) network management and provide flexibility in implementing and maintaining the cluster network. You can create IP address pools within subnets to partition your network interfaces according to workflow or node type.

The IP address pool of a subnet consists of one or more IP address ranges. IP address pools can be associated with network interfaces on cluster nodes. Client connection settings are configured at the IP address pool level.

An initial external network subnet is created during the set up of your EMC Isilon with the following configuration:

- An initial groupnet called groupnet0 with the specified global, outbound DNS settings to the domain name server list and DNS search list, if provided.
An initial subnet called subnet0 with the specified netmask, gateway, and SmartConnect service address.

An initial IP address pool called pool0 with the specified IP address range, the SmartConnect zone name, and the network interface of the first node in the cluster as the only pool member.

An initial node provisioning rule called rule0 that automatically assigns the first network interface for all newly added nodes to pool0.

Adds subnet0 to groupnet0.

Adds pool0 to subnet0 and configures pool0 to use the virtual IP of subnet0 as its SmartConnect service address.

**Groupnets**

Groupnets reside at the top tier of the networking hierarchy and are the configuration level for managing multiple tenants on your external network. DNS client settings, such as nameservers and a DNS search list, are properties of the groupnet. You can create a separate groupnet for each DNS namespace that you want to use to enable portions of the Isilon cluster to have different networking properties for name resolution. Each groupnet maintains its own DNS cache, which is enabled by default.

A groupnet is a container that includes subnets, IP address pools, and provisioning rules. Groupnets can contain one or more subnets, and every subnet is assigned to a single groupnet. Each EMC Isilon cluster contains a default groupnet named groupnet0 that contains an initial subnet named subnet0, an initial IP address pool named pool0, and an initial provisioning rule named rule0.

Each groupnet is referenced by one or more access zones. When you create an access zone, you can specify a groupnet. If a groupnet is not specified, the access zone will reference the default groupnet. The default System access zone is automatically associated with the default groupnet. Authentication providers that communicate with an external server, such as Active Directory and LDAP, must also reference a groupnet. You can specify the authentication provider with a specific groupnet; otherwise, the provider will reference the default groupnet. You can only add an authentication provider to an access zone if they are associated with the same groupnet. Client protocols such as SMB, NFS, HDFS, and Swift, are supported by groupnets through their associated access zones.

**DNS name resolution**

You can designate up to three DNS servers per groupnet to handle DNS name resolution.

DNS servers must be configured as an IPv4 or IPv6 address. You can specify up to six DNS search suffixes per groupnet; the suffixes settings are appended to domain names that are not fully qualified.

Additional DNS server settings at the groupnet level include enabling a DNS cache, enabling server-side search, and enabling DNS resolution on a rotating basis.

**Subnets**

Subnets are networking containers that enable you to sub-divide your network into smaller, logical IP networks.

On an EMC Isilon cluster, subnets are created under a groupnet and each subnet contains one or more IP address pools. Both IPv4 and IPv6 addresses are supported on OneFS; however, a subnet cannot contain a combination of both. When you create a subnet, you specify whether it supports IPv4 or IPv6 addresses.
You can configure the following options when you create a subnet:

- Gateway servers that route outgoing packets and gateway priority.
- Maximum transmission unit (MTU) that network interfaces in the subnet will use for network communications.
- SmartConnect service address, which is the IP address on which the SmartConnect module listens for DNS requests on this subnet.
- VLAN tagging to allow the cluster to participate in multiple virtual networks.
- Direct Server Return (DSR) address, if your cluster contains an external hardware load balancing switch that uses DSR.

How you set up your external network subnets depends on your network topology. For example, in a basic network topology where all client-node communication occurs through direct connections, only a single external subnet is required. In another example, if you want clients to connect through both IPv4 and IPv6 addresses, you must configure multiple subnets.

IPv6 support

OneFS supports both IPv4 and IPv6 address formats on an EMC Isilon cluster. IPv6 is the next generation of internet protocol addresses and was designed with the growing demand for IP addresses in mind. The following table describes distinctions between IPv4 and IPv6.

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit addresses</td>
<td>128-bit addresses</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>Neighbor Discovery Protocol (NDP)</td>
</tr>
</tbody>
</table>

You can configure the Isilon cluster for IPv4, IPv6, or both (dual-stack) in OneFS. You set the IP family when creating a subnet, and all IP address pools assigned to the subnet must use the selected format.

VLANs

Virtual LAN (VLAN) tagging is an optional setting that enables an EMC Isilon cluster to participate in multiple virtual networks.

You can partition a physical network into multiple broadcast domains, or virtual local area networks (VLANs). You can enable a cluster to participate in a VLAN which allows multiple cluster subnet support without multiple network switches; one physical switch enables multiple virtual subnets.

VLAN tagging inserts an ID into packet headers. The switch refers to the ID to identify from which VLAN the packet originated and to which network interface a packet should be sent.

IP address pools

IP address pools are assigned to a subnet and consist of one or more IP address ranges. You can partition nodes and network interfaces into logical IP address pools. IP address pools are also utilized when configuring SmartConnect DNS zones and client connection management.

Each IP address pool belongs to a single subnet. Multiple pools for a single subnet are available only if you activate a SmartConnect Advanced license.

The IP address ranges assigned to a pool must be unique and belong to the IP address family (IPv4 or IPv6) specified by the subnet that contains the pool.
You can add network interfaces to IP address pools to associate address ranges with a node or a group of nodes. For example, based on the network traffic that you expect, you might decide to establish one IP address pool for storage nodes and another for accelerator nodes.

SmartConnect settings that manage DNS query responses and client connections are configured at the IP address pool level.

**Note**

IsilonSD Edge does not support IPv6 addresses for connecting to IsilonSD clusters.

**Link aggregation**

Link aggregation, also known as network interface card (NIC) aggregation, combines the network interfaces on a physical node into a single, logical connection to provide improved network throughput.

You can add network interfaces to an IP address pool singly or as an aggregate. A link aggregation mode is selected on a per-pool basis and applies to all aggregated network interfaces in the IP address pool. The link aggregation mode determines how traffic is balanced and routed among aggregated network interfaces.

**SmartConnect module**

SmartConnect is a module that specifies how the DNS server on the EMC Isilon cluster handles connection requests from clients and the policies used to assign IP addresses to network interfaces, including failover and rebalancing.

Settings and policies configured for SmartConnect are applied per IP address pool. You can configure basic and advanced SmartConnect settings.

**SmartConnect Basic**

SmartConnect Basic is included with OneFS as a standard feature and does not require a license. SmartConnect Basic supports the following settings:

- Specification of the DNS zone
- Round-robin connection balancing method only
- Service subnet to answer DNS requests

SmartConnect Basic has the following limitations to IP address pool configuration:

- You may only specify a static IP address allocation policy.
- You cannot specify an IP address failover policy.
- You cannot specify an IP address rebalance policy.
- You may only assign one IP address pool per external network subnet.

**SmartConnect Advanced**

SmartConnect Advanced extends the settings available from SmartConnect Basic. It requires an active license. SmartConnect Advanced supports the following settings:

- Round-robin, CPU utilization, connection counting, and throughput balancing methods.
- Static and dynamic IP address allocation.

SmartConnect Advanced allows you to specify the following IP address pool configuration options:

- You can define an IP address failover policy for the IP address pool.
You can define an IP address rebalance policy for the IP address pool.

SmartConnect Advanced supports multiple IP address pools per external subnet to allow multiple DNS zones within a single subnet.

**SmartConnect zones and aliases**

Clients can connect to the EMC Isilon cluster through a specific IP address or through a domain that represents an IP address pool.

You can configure a SmartConnect DNS zone name for each IP address pool. The zone name must be a fully qualified domain name. SmartConnect requires that you add a new name server (NS) record that references the SmartConnect service IP address in the existing authoritative DNS zone that contains the cluster. You must also provide a zone delegation to the fully qualified domain name (FQDN) of the SmartConnect zone in your DNS infrastructure.

If you have a SmartConnect Advanced license, you can also specify a list of alternate SmartConnect DNS zone names for the IP address pool.

When a client connects to the cluster through a SmartConnect DNS zone, SmartConnect handles the incoming DNS requests on behalf of the IP address pool, and the service subnet distributes incoming DNS requests according to the pool's connection balancing policy.

**DNS request handling**

SmartConnect handles all incoming DNS requests on behalf of an IP address pool if a SmartConnect service subnet has been associated with the pool.

The SmartConnect service subnet is an IP address pool setting. You can specify any subnet that has been configured with a SmartConnect service IP address and references the same groupnet as the pool. You must have at least one subnet configured with a SmartConnect service IP address in order to handle client DNS requests. You can configure only one service IP address per subnet.

A SmartConnect service IP address should be used exclusively for answering DNS requests and cannot be an IP address that is in any pool's IP address range. Client connections through the SmartConnect service IP address result in unexpected behavior or disconnection.

Once a SmartConnect service subnet has been associated with an IP address pool, the service subnet distributes incoming DNS requests according to the pool's connection balancing policy. If a pool does not have a designated service subnet, incoming DNS requests are answered by the subnet that contains the pool, provided that the subnet is configured with a SmartConnect service IP address. Otherwise, the DNS requests are excluded.

---

**Note**

SmartConnect requires that you add a new name server (NS) record that references the SmartConnect service IP address in the existing authoritative DNS zone that contains the cluster. You must also provide a zone delegation to the fully qualified domain name (FQDN) of the SmartConnect zone.

---

**IP address allocation**

The IP address allocation policy specifies how IP addresses in the pool are assigned to an available network interface.

You can specify whether to use static or dynamic allocation.
Static

Assigns one IP address to each network interface added to the IP address pool, but does not guarantee that all IP addresses are assigned.

Once assigned, the network interface keeps the IP address indefinitely, even if the network interface becomes unavailable. To release the IP address, remove the network interface from the pool or remove it from the node.

Without a license for SmartConnect Advanced, static is the only method available for IP address allocation.

Dynamic

Assigns IP addresses to each network interface added to the IP address pool until all IP addresses are assigned. This guarantees a response when clients connect to any IP address in the pool.

If a network interface becomes unavailable, its IP addresses are automatically moved to other available network interfaces in the pool as determined by the IP address failover policy.

This method is only available with a license for SmartConnect Advanced.

IP address failover

When a network interface becomes unavailable, the IP address failover policy specifies how to handle the IP addresses that were assigned to the network interface.

To define an IP address failover policy, you must have a license for SmartConnect Advanced, and the IP address allocation policy must be set to dynamic. Dynamic IP allocation ensures that all of the IP addresses in the pool are assigned to available network interfaces.

When a network interface becomes unavailable, the IP addresses that were assigned to it are redistributed to available network interfaces according to the IP address failover policy. Subsequent client connections are directed to the new network interfaces.

You can select one of the following connection balancing methods to determine how the IP address failover policy selects which network interface receives a redistributed IP address:

- Round-robin
- Connection count
- Network throughput
- CPU usage

Connection balancing

The connection balancing policy determines how the DNS server handles client connections to the EMC Isilon cluster.

You can specify one of the following balancing methods:

Round-robin

Selects the next available network interface on a rotating basis. This is the default method. Without a SmartConnect license for advanced settings, this is the only method available for load balancing.
Connection count
Determines the number of open TCP connections on each available network interface and selects the network interface with the fewest client connections.

Network throughput
Determines the average throughput on each available network interface and selects the network interface with the lowest network interface load.

CPU usage
Determines the average CPU utilization on each available network interface and selects the network interface with lightest processor usage.

IP address rebalancing
The IP address rebalance policy specifies when to redistribute IP addresses if one or more previously unavailable network interfaces becomes available again.

To define an IP address rebalance policy, you must have a license for SmartConnect Advanced, and the IP address allocation policy must be set to dynamic. Dynamic IP addresses allocation ensures that all of the IP addresses in the pool are assigned to available network interfaces.

You can set rebalancing to occur manually or automatically:

Manual
Does not redistribute IP addresses until you manually start the rebalancing process.

Upon rebalancing, IP addresses will be redistributed according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic
Automatically redistributes IP addresses according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic rebalancing may also be triggered by changes to cluster nodes, network interfaces, or the configuration of the external network.

Note
Rebalancing can disrupt client connections. Ensure the client workflow on the IP address pool is appropriate for automatic rebalancing.

Node provisioning rules
Node provisioning rules specify how new nodes are configured when they are added to an EMC Isilon cluster.

If the new node type matches the type defined in a rule, the network interfaces on the node are added to the subnet and the IP address pool specified in the rule.

For example, you can create a node provisioning rule that configures new Isilon storage nodes, and another rule that configures new accelerator nodes.

OneFS automatically checks for multiple provisioning rules when new rules are added to ensure there are no conflicts.
Routing options

OneFS supports source-based routing and static routes which allow for more granular control of the direction of outgoing client traffic on the EMC Isilon cluster.

If no routing options are defined, by default, outgoing client traffic on the cluster is routed through the default gateway, which is the gateway with the lowest priority setting on the node. If traffic is being routed to a local subnet and does not need to route through a gateway, the traffic will go directly out through an interface on that subnet.

Source-based routing

Source-based routing selects which gateway to direct outgoing client traffic through based on the source IP address in each packet header.

When enabled, source-based routing automatically scans your network configuration to create client traffic rules. If you make modifications to your network configuration, such as changing the IP address of a gateway server, source-based routing adjusts the rules. Source-based routing is applied across the entire EMC Isilon cluster and does not support the IPv6 protocol.

In the following example, you enable source-based routing on an Isilon cluster that is connected to SubnetA and SubnetB. Each subnet is configured with a SmartConnect zone and a gateway, also labeled A and B. When a client on SubnetA makes a request to SmartConnect ZoneB, the response originates from ZoneB. This results in a ZoneB address as the source IP in the packet header, and the response is routed through GatewayB. Without source-based routing, the default route is destination-based, so the response is routed through GatewayA.

In another example, a client on SubnetC, which is not connected to the Isilon cluster, makes a request to SmartConnect ZoneA and ZoneB. The response from ZoneA is routed through GatewayA, and the response from ZoneB is routed through GatewayB. In other words, the traffic is split between gateways. Without source-based routing, both responses are routed through the same gateway.

Source-based routing is disabled by default. Enabling or disabling source-based routing goes into effect immediately. Packets in transit continue on their original courses, and subsequent traffic is routed based on the status change. Transactions composed of multiple packets might be disrupted or delayed if the status of source-based routing changes during transmission.

Source-based routing can conflict with static routes. If a routing conflict occurs, source-based routing rules are prioritized over the static route.

You might enable source-based routing if you have a large network with a complex topology. For example, if your network is a multi-tenant environment with several gateways, traffic is more efficiently distributed with source-based routing.

Static routing

A static route directs outgoing client traffic to a specified gateway based on the IP address of the client connection.

You configure static routes by IP address pool, and each route applies to all nodes that have network interfaces as IP address pool members.

You might configure static routing in order to connect to networks that are unavailable through the default routes or if you have a small network that only requires one or two routes.
Managing internal network settings

You can modify internal IP address ranges and configure an Infiniband switch for failover.

Add or remove an internal IP address range

You can configure IP address ranges for the int-a, int-b, and failover networks.

Each internal Infiniband switch requires an IP address range. The ranges should have a sufficient number of IP addresses for present operating conditions as well as future expansion and addition of nodes.

Procedure

1. Run the `isi config` command.
   
   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Modify the internal IP address ranges by running the `iprange` command.
   
   The following command adds an IP range to the int-a internal network:
   
   ```
   iprange int-a 192.168.206.10-192.168.206.20
   ```

   The following command deletes an existing IP address range from the int-a internal network:
   
   ```
   deliprange int-a 192.168.206.15-192.168.206.20
   ```

3. Run the `commit` command to complete the configuration changes and exit `isi config`.

Modify an internal network netmask

You can modify the subnet mask, or netmask, value for the int-a and int-b internal network interfaces.

If the netmask is too restrictive for the size of the internal network, you must modify the netmask settings. It is recommended that you specify a class C netmask, such as 255.255.255.0, for the internal netmask, that is large enough to accommodate future growth of your Isilon clusters.

It is recommended that the netmask values you specify for int-a and int-b/failover are the same. If you modify the netmask value of one, modify the other.

Note

- You must reboot the cluster to apply modifications to the netmask.

- Ignore the previous recommendation if you are running IsilonSD Edge because you cannot specify a netmask value for int-b/failover for an IsilonSD cluster.
Procedure

1. Run the `isi config` command.
   
   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Modify the internal network netmask by running the `netmask` command.
   
   The following command changes the int-a internal network netmask:

   ```
   netmask int-a 255.255.255.0
   ```

   The system displays output similar to the following example:

   ```
   !! WARNING: The new netmask will not take effect until the nodes are rebooted.
   ```

3. Run the `commit` command to complete the configuration changes and exit `isi config`.

Configure and enable internal network failover

You can configure the int-b internal interfaces to provide backup in the event of an int-a network failure.

Failover configuration involves enabling the int-b interface, specifying a valid netmask, and adding IP address ranges for the int-b interface and the failover network. By default, the int-b interface and failover network are disabled.

**Note**

- You must reboot the EMC Isilon cluster to apply modifications to internal network failover.
- In the case of IsilonSD Edge, internal failover on an IsilonSD cluster is enabled through the failover policy supported by VMware vSphere. Therefore, ignore this procedure if you are running IsilonSD Edge.

Procedure

1. Run the `isi config` command.
   
   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Set a netmask for the second interface by running the `netmask` command.
   
   The following command changes the int-b internal network netmask:

   ```
   netmask int-b 255.255.255.0
   ```

   The system displays output similar to the following example:

   ```
   !! WARNING: The new netmask will not take effect until the nodes are rebooted.
   ```

3. Set an IP address range for the second interface by running the `iprange` command.
The following command adds an IP range to the int-b internal network:

```
iprange int-b 192.168.206.21-192.168.206.30
```

4. Set an IP address range for the failover interface by running the `iprange` command.

The following command adds an IP range to the internal failover network:

```
iprange failover 192.168.206.31-192.168.206.40
```

5. Enable a second interface by running the `interface` command.

The following command specifies the interface name as int-b and enables it:

```
interface int-b enable
```

6. Run the `commit` command to complete the configuration changes and exit `isi config`.

7. Restart the cluster to apply netmask modifications.

### Disable internal network failover

You can disable internal network failover by disabling the int-b interface.

You must reboot the cluster to apply modifications to internal network failover.

**Note**

Ignore this procedure if you are running IsilonSD Edge.

**Procedure**

1. Run the `isi config` command.

   The command-line prompt changes to indicate that you are in the `isi config` subsystem.

2. Disable the int-b interface by running the interface command.

   The following command specifies the int-b interface and disables it:

   ```
   interface int-b disable
   ```

3. Run the `commit` command to complete the configuration changes and exit `isi config`.

4. Restart the cluster to apply failover modifications.

### Managing groupnets

You can create and manage groupnets on the EMC Isilon cluster.
Create a groupnet

You can create a groupnet and configure DNS client settings.

Procedure

1. Run the `isi network groupnet create` command.

   The following command creates a groupnet named `groupnet1` that supports two DNS servers, which are specified by IPv6 addresses:

   ```bash
   isi network groupnet create groupnet1 \
   --dns-servers=2001:DB8:170:9904::be06,2001:DB8:170:9904::be07
   ```

   The following command creates a groupnet named `groupnet1` that supports one DNS server, which is specified by an IPv4 address, and enables DNS caching:

   ```bash
   isi network groupnet create groupnet1 \
   --dns-servers=192.0.2.0 --dns-cache-enabled=true
   ```

Modify a groupnet

You can modify groupnet attributes including the name, supported DNS servers, and DNS configuration settings.

Procedure

1. Run the `isi network groupnet modify` command.

   The following command modifies `groupnet1` to enable DNS search on three suffixes:

   ```bash
   isi network groupnet modify groupnet1 \
   --dns-search=data.company.com,storage.company.com
   ```

   The following command modifies `groupnet1` to support a second DNS server and to enable rotation through the configured DNS resolvers:

   ```bash
   isi network groupnet modify groupnet1 \
   --add-dns-servers=192.0.2.1 --dns-options=rotate
   ```

Delete a groupnet

You can delete a groupnet from the system, unless it is the default groupnet. If the groupnet is associated with an access zone, an authentication provider, removal from the system might affect several other areas of OneFS and should be performed with caution.

Before you begin

In several cases, the association between a groupnet and another OneFS component, such as access zones or authentication providers, is absolute. You cannot modify these components to associate them with another groupnet.

In the event that you need to delete a groupnet, EMC recommends that you complete the these tasks in the following order:
1. Delete IP address pools in subnets associated with the groupnet.
2. Delete subnets associated with the groupnet.
3. Delete authentication providers associated with the groupnet.
4. Delete access zones associated with the groupnet.

Procedure

1. Run the `isi network groupnet delete` command.
2. At the prompt to confirm deletion, type `yes`.

The following command deletes a groupnet named `groupnet1`:

```
isi network groupnet delete groupnet1
```

The following command attempts to delete `groupnet1`, which is still associated with an access zone:

```
isi network modify groupnet groupnet1
```

The system displays output similar to the following example:

```
Groupnet groupnet1 is not deleted; groupnet can't be deleted while pointed at by zone(s) zoneB
```

View groupnets

You can retrieve and sort a list of all groupnets on the system and view the details of a specific groupnet.

Procedure

1. To retrieve a list of groupnets in the system, run the `isi network groupnets list` command.

   The following command sorts the list of groupnets by ID in descending order:

   ```
   isi network groupnets list --sort=id --descending
   ```

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>DNS Cache</th>
<th>DNS Search</th>
<th>DNS Servers</th>
<th>Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupnet2</td>
<td>True</td>
<td>data.company.com</td>
<td>192.0.2.75</td>
<td>subnet2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.0.2.67</td>
<td>subnet4</td>
</tr>
<tr>
<td>groupnet1</td>
<td>True</td>
<td></td>
<td>192.0.2.92</td>
<td>subnet1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.0.2.83</td>
<td>subnet3</td>
</tr>
<tr>
<td>groupnet0</td>
<td>False</td>
<td></td>
<td>192.0.2.11</td>
<td>subnet0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.0.2.20</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Total: 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. To view the details of a specific groupnet, run the `isi network groupnets view` command.

   The following command displays the details of a groupnet named `groupnet1`:

   ```
   isi network groupnets view groupnet1
   ```
The system displays output similar to the following example:

```
ID: groupnet1
Name: groupnet1
Description: Data storage groupnet
DNS Cache Enabled: True
DNS Options: -
DNS Search: data.company.com
DNS Servers: 192.0.1.75, 10.7.2.67
Server Side DNS Search: True
Subnets: subnet1, subnet3
```

### Managing external network subnets

You can create and manage subnets on the EMC Isilon cluster.

#### Create a subnet

You can add a subnet to the external network of an EMC Isilon cluster.

**Before you begin**

Subnets must be associated with a groupnet. Ensure that the groupnet you want to associate with this subnet exists in the system.

An IP address family designation and prefix length are required when creating a subnet.

**Procedure**

1. Run the `isi network subnets create` command and specify a subnet ID, IP address family, and prefix length.

   Specify the subnet ID you want to create in the following format:

   ```
   <groupnet_name>.<subnet_name>
   ```

   The subnet name must be unique in the system.

   The following command creates a subnet associated with groupnet1, designates the IP address family as IPv4 and specifies an IPv4 prefix length:

   ```
   isi network subnets create \
   groupnet1.subnet3 ipv4 255.255.255.0
   ```

   The following command creates a subnet with an associated IPv6 prefix length:

   ```
   isi network subnets create \
   groupnet1.subnet3 ipv6 64
   ```

#### Modify a subnet

You can modify a subnet on the external network.

**Note**

Modifying an external network subnet that is in use can disable access to the cluster.
Procedure

1. (Optional) To identify the ID of the external subnet you want to modify, run the following command:

   ```
   isi network subnets list
   ```

2. Run the `isi networks modify subnet` command

   Specify the subnet ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>
   ```

   The following command changes the name of subnet3 under groupnet1 to subnet5:

   ```
   isi network subnets modify groupnet1.subnet3 --name=subnet5
   ```

   The following command sets the MTU to 1500, specifies the gateway address as 198.162.205.10, and sets the gateway priority to 1:

   ```
   isi network subnets modify groupnet1.subnet3 --mtu=1500 --gateway=198.162.205.10 --gateway-priority=1
   ```

Delete a subnet

You can delete an external network subnet that you no longer need.

Note

Deleting an external network subnet also deletes any associated IP address pools. Deleting a subnet that is in use can prevent access to the cluster.

Procedure

1. (Optional) To identify the name of the subnet you want to delete, run the following command:

   ```
   isi network subnets list
   ```

2. Run the `isi networks delete subnet` command.

   Specify the subnet ID you want to delete in the following format:

   ```
   <groupnet_name>.<subnet_name>
   ```

   The following command deletes subnet3 under groupnet1:

   ```
   isi network subnets delete groupnet1.subnet3
   ```

3. At the prompt, type `yes`. 
View subnets

You can view all subnets on the external network, sort subnets by specified criteria, or view details for a specific subnet.

Procedure

1. To view all subnets, run the **isi network subnets list** command.

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Subnet</th>
<th>Gateway</th>
<th>Priority</th>
<th>Pools</th>
<th>SC Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupnet1.subnet0</td>
<td>203.0.113.10/24</td>
<td>203.0.113.12</td>
<td>1</td>
<td>pool0</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td>groupnet1.subnet3</td>
<td>192.0.2.20/24</td>
<td>192.0.2.22</td>
<td>2</td>
<td>pool3</td>
<td>198.51.100.15</td>
</tr>
</tbody>
</table>

2. To view the details of a specific subnet, run the **isi network subnets view** command and specify the subnet ID.

   Specify the subnet ID you want to view in the following format:

   `<groupnet_name>.<subnet_name>`

   The following command displays details for subnet3 under groupnet1:

   ```
   isi network subnets view groupnet1.subnet3
   ```

   The system displays output similar to the following example:

   ```
   ID: groupnet1.subnet3
   Name: subnet3
   Groupnet: groupnet1
   Pools: pool3
   Addr Family: ipv4
   Base Addr: 192.0.2.20
   CIDR: 192.0.2.20/24
   Description: Sales subnet
   Dsr Addr: -
   Gateway: 192.0.2.22
   Gateway Priority: 2
   MTU: 1500
   Prefixlen: 24
   Netmask: 255.255.255.0
   Sc Service Addr: 198.51.100.15
   VLAN Enabled: False
   VLAN ID: -
   ```
**Configure a SmartConnect service IP address**

You can specify a SmartConnect service IP address on a subnet.

**Procedure**

1. (Optional) To identify the name of the external subnet you want to modify, run the following command:

   ```
   isi network subnets list
   ```

2. Run the `isi networks modify subnet` command

   Specify the subnet ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>
   ```

   The following command specifies the SmartConnect service IP address on subnet3 under groupnet1:

   ```
   isi network subnets modify groupnet1.subnet3 --sc-service-addr=198.51.100.15
   ```

**After you finish**

Assign this subnet to one or more IP address pools in order to handle DNS requests for those pools.

**Enable or disable VLAN tagging**

You can partition the external network into Virtual Local Area Networks or VLANs.

VLAN tagging requires a VLAN ID that corresponds to the ID number for the VLAN set on the switch. Valid VLAN IDs are 2 to 4094.

**Procedure**

1. (Optional) To identify the name of the external subnet you want to modify for VLAN tagging, run the following command:

   ```
   isi network subnets list
   ```

2. Enable or disable VLAN tagging on the external subnet by running the `isi networks modify subnet` command.

   Specify the subnet ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>
   ```
The following command enables VLAN tagging on subnet3 under groupnet1 and sets the required VLAN ID to 256:

```
isi network subnets modify groupnet1.subnet3 \
   --vlan-enabled=true --vlan-id=256
```

The following command disables VLAN tagging on subnet3 under groupnet1:

```
isi network subnets modify groupnet1.subnet3 \
   --vlan-enabled=false
```

3. At the prompt, type yes.

### Add or remove a DSR address

You can specify a Direct Server Return (DSR) address for a subnet if your EMC Isilon cluster contains an external hardware load balancing switch that uses DSR.

**Procedure**

1. (Optional) To identify the name of the external subnet you want to modify for DRS addresses, run the following command:

   ```
   isi network subnets list
   ```

2. Run the `isi network subnets modify` command.

   Specify the subnet ID you want to modify in the following format:

   `<groupnet_name>.<subnet_name>`

   The following command adds a DSR address to subnet3 under groupnet1:

   ```
   isi network subnets modify groupnet1.subnet3 \
      --add-dsr-addrs=198.51.100.20
   ```

   The following command removes a DSR address from subnet3 under groupnet1:

   ```
   isi network subnets modify groupnet1.subnet3 \
      --remove-dsr-addrs=198.51.100.20
   ```

### Managing IP address pools

You can create and manage IP address pools on the EMC Isilon cluster.
Create an IP address pool

You can partition the external network interface into groups, or pools, of unique IP address ranges.

Note

If you have not activated a SmartConnect Advanced license, the EMC Isilon cluster is allowed one IP address pool per subnet. If you activate a SmartConnect Advanced license, the cluster is allowed unlimited IP address pools per subnet.

When you create an address pool, you must assign it to a subnet. If the subnet is not under the default groupnet, groupnet0, then you must also assign an access zone to the pool.

Procedure

1. Run the `isi network pools create` command.
   
   Specify the ID of the pool you want to create in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>`

   The following command creates a pool named pool5 and assigns it to subnet3 under groupnet1:

   ```
   isi network pools create groupnet1.subnet3.pool5
   ```

   The following command creates a pool named pool5, assigns it to groupnet1.subnet3, and specifies zoneB as the access zone:

   ```
   isi network pools create groupnet1.subnet3.pool5 \
   --access-zone=zoneB
   ```

Modify an IP address pool

You can modify IP address pools to update pool settings.

Procedure

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```
   isi network pools list
   ```

2. Run the `isi networks modify pool` command.
   
   Specify the pool ID you want to modify in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>`
The following command changes the name of the pool from pool3 to pool5:

```bash
isi network pools modify groupnet1.subnet3.pool3 --name=pool5
```

**Delete an IP address pool**

You can delete an IP address pool that you no longer need.

When a pool is deleted, the pool and pool settings are removed from the assigned subnet.

**Procedure**

1. (Optional) To identify the name of the IP address pool you want to delete, run the following command:

   ```bash
   isi network pools list
   ```

2. Run the `isi networks delete pool` command.

   Specify the pool ID you want to delete in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command deletes the pool name pool5 from groupnet1.subnet3:

   ```bash
   isi network pools delete groupnet1.subnet3.pool5
   ```

3. At the prompt, type `yes`.

**View IP address pools**

You can view all IP address pools within a groupnet or subnet, sort pools by specified criteria, or view details for a specific pool.

**Procedure**

1. To view all IP address pools within a groupnet or subnet, run the `isi network pools list` command.

   The following command displays all IP address pools under groupnet1.subnet3:

   ```bash
   isi network pools list groupnet1.subnet3
   ```

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>SC Zone</th>
<th>Allocation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupnet1.subnet3.pool5</td>
<td>data.company.com</td>
<td>static</td>
</tr>
<tr>
<td>groupnet1.subnet3.pool7</td>
<td>data.company.com</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

2. To view the details of a specific IP address pool, run the `isi network pools view` command and specify the pool ID.
Specify the pool ID you want to view in the following format:

```
<groupnet_name>.<subnet_name>.<pool_name>
```

The following command displays the setting details of pool5 under groupnet1.subnet3:

```
isi network pools view groupnet1.subnet3.pool5
```

The system displays output similar to the following example:

```
ID: groupnet0.subnet3.pool5
  Groupnet: groupnet1
  Subnet: subnet3
  Name: pool5
  Rules: -
  Access Zone: zone3
  Allocation Method: static
  Aggregation Mode: lacp
  SC Suspended Nodes: -
  Description: -
  Ifaces: 1:ext-2, 2:ext-2, 3:ext-2
  IP Ranges: 203.0.223.12-203.0.223.22
  Rebalance Policy: auto
  SC Auto Unsuspend Delay: 0
  SC Connect Policy: round_robin
  SC Zone: data.company.com
  SC DNS Zone Aliases: -
  SC Failover Policy: round_robin
  SC Subnet: groupnet0.subnet3
  SC Ttl: 0
  Static Routes: -
```

### Add or remove an IP address range

You can configure a range of IP addresses for a pool.

All IP address ranges in a pool must be unique.

**Procedure**

1. (Optional) To identify the name of the IP address pool you want to modify for IP address ranges, run the following command:

   ```
   isi network pools list
   ```

2. **Run the** `isi network pools modify` **command.**

   Specify the pool ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>.<pool_name>
   ```
The following command adds an address range to pool5 under groupnet1.subnet3:

```bash
isi network pools modify groupnet1.subnet3.pool5 \
--add-ranges=203.0.223.12-203.0.223.22
```

The following command deletes an address range from pool5:

```bash
isi network pools modify groupnet1.subnet3.pool5 \
--remove-ranges=203.0.223.12-203.0.223.14
```

Configure IP address allocation

You can specify whether the IP addresses in an IP address pool are allocated to network interfaces statically or dynamically.

**Before you begin**

To configure dynamic IP address allocation, you must activate a SmartConnect Advanced license.

**Procedure**

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```bash
   isi network pools list
   ```

2. Run the `isi network pools modify` command.
   
   Specify the pool ID you want to modify in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command specifies dynamic distribution of IP addresses in pool5 under groupnet1.subnet 3:

   ```bash
   isi network pools modify groupnet1.subnet3.pool5 \
   --alloc-method=dynamic
   ```

Managing SmartConnect Settings

You can configure SmartConnect settings within each IP address pool on the EMC Isilon cluster.
Configure a SmartConnect DNS zone

You can specify a SmartConnect DNS zone and alternate DNS zone aliases for an IP address pool.

Procedure

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   isi network pools list

2. To configure a SmartConnect DNS zone, run the `isi networks modify pool` command:

   Specify the pool ID you want to modify in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>`

   The following command specifies a SmartConnect DNS zone in pool5 under subnet3 and groupnet1:

   ```
   isi network pools modify groupnet1.subnet3.pool5
     --sc-dns-zone=www.company.com
   ```

   It is recommended that the SmartConnect DNS zone be a fully-qualified domain name (FQDN).

3. To configure a SmartConnect DNS zone alias, run the `isi networks modify pool` command:

   The following command specifies SmartConnect DNS aliases in pool5 under subnet3 and groupnet1:

   ```
   isi network pools modify groupnet1.subnet3.pool5
     --add-sc-dns-zone-aliases=data.company.com,storage.company.com
   ```

   You cannot specify more than three SmartConnect DNS zone aliases.

4. To remove a SmartConnect DNS zone alias, run the `isi networks modify pool` command:

   The following command removes a SmartConnect DNS aliases from pool5 under subnet3 and groupnet1:

   ```
   isi network pools modify groupnet1.subnet3.pool5
     --remove-dns-zone-aliases=data.company.com
   ```

After you finish

SmartConnect requires that you add a new name server (NS) record to the existing authoritative DNS zone that contains the cluster and that you delegate the FQDN of the SmartConnect DNS zone.
Specify a SmartConnect service subnet

You can designate a subnet as the SmartConnect service subnet for an IP address pool.

**Before you begin**

The subnet that you designate as the SmartConnect service subnet must have a SmartConnect service IP address configured, and the subnet must be in the same groupnet as the IP address pool. For example, although a pool might belong to subnet3, you can designate subnet5 as the SmartConnect service subnet as long as both subnets are under the same groupnet.

**Procedure**

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```
   isi network pools list
   ```

2. **Run the** `isi networks modify pool` **command:**

   Specify the pool ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command specifies subnet0 as the a SmartConnect service subnet of pool5 under subnet3 and groupnet1:

   ```
   isi network pools modify groupnet1.subnet3.pool5 --sc-subnet=subnet0
   ```

Suspend or resume a node

You can suspend and resume SmartConnect DNS query responses on a node.

**Procedure**

1. To suspend DNS query responses for a node:
   a. (Optional) To identify a list of nodes and IP address pools, run the following command:

   ```
   isi network interfaces list
   ```

   b. **Run the** `isi network pools sc-suspend-nodes` **command and specify the pool ID and logical node number (LNN).**

   Specify the pool ID you want in the following format:

   ```
   <groupnet_name>.<subnet_name>.<pool_name>
   ```
The following command suspends DNS query responses on node 3 when queries come through IP addresses in pool5 under groupnet1.subnet 3:

\[
\text{isi network pools sc-suspend-nodes groupnet1.subnet3.pool5 3}
\]

2. To resume DNS query responses for an IP address pool, run the \text{isi network pools sc-resume-nodes} command and specify the pool ID and logical node number (LNN).

The following command resumes DNS query responses on node 3 when queries come through IP addresses in pool5 under groupnet1.subnet 3:

\[
\text{isi network pools sc-resume-nodes groupnet1.subnet3.pool5 3}
\]

Configure a connection balancing policy

You can set a connection balancing policy for an IP address pool. SmartConnect supports the following balancing methods:

- Round robin
- Connection count
- Network throughput
- CPU usage

Procedure

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

\[
\text{isi network pools list}
\]

2. Run the \text{isi network pools modify} command.

Specify the pool ID you want to modify in the following format:

\[
<\text{groupnet\textunderscore name}.<\text{subnet\textunderscore name}.<\text{pool\textunderscore name}>
\]

The following command specifies a connection balancing policy based on connection count in pool5 under subnet 3 and groupnet1:

\[
\text{isi network pools modify groupnet1.subnet3.pool5 \ --sc-connect-policy=conn\_count}
\]
Configure an IP failover policy

You can set an IP failover policy for an IP address pool.

**Before you begin**
To configure an IP failover policy, you must activate a SmartConnect Advanced license.

SmartConnect supports the following distribution methods:
- Round robin
- Connection count
- Network throughput
- CPU usage

**Procedure**
1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```bash
   isi network pools list
   ```

2. Run the `isi network pools modify` command.
   Specify the pool ID you want to modify in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command specifies a IP failover policy based on CPU usage in pool5 under subnet 3 and groupnet0:

   ```bash
   isi network pools modify groupnet0.subnet3.pool5 --sc-failover-policy=cpu_usage
   ```

Managing connection rebalancing

You can configure and manage a connection rebalancing policy that specifies when to rebalance IP addresses after a previously unavailable node becomes available again.

Configure an IP rebalance policy

You can configure a manual or automatic rebalance policy for an IP address pool.

**Before you begin**
To configure a rebalance policy for an IP address pool, you must activate a SmartConnect Advanced license and set the allocation method to `dynamic`.

**Procedure**
1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```bash
   isi network pools list
   ```
2. Run the `isi network pools modify` command.

   Specify the pool ID you want to modify in the following format:

   `<groupnet_id>.<subnet_name>.<pool_name>`

   The following command specifies manual rebalancing of IP addresses in pool5 under groupnet1.subnet 3:

   ```
   isi network pools modify groupnet1.subnet3.pool5 --rebalance-policy=manual
   ```

**After you finish**

If you configure an automatic rebalance policy, you can specify a rebalance delay which is a period of time (in seconds) that should pass after a qualifying event before an automatic rebalance is performed. The default value is 0 seconds. You can specify the delay by running the `isi network external modify` command with the `--sc-balance-delay` option.

---

**Manually rebalance IP addresses**

You can manually rebalance a specific IP address pool or all of the pools on the external network.

**Before you begin**

You must activate a SmartConnect Advanced license.

**Procedure**

1. To manually rebalance IP addresses in a pool:
   a. (Optional) To identify the name of the IP address pool you want to rebalance, run the following command:

      ```
      isi network pools list
      ```

   b. Run the `isi network pools rebalance-ips` command.

      Specify the pool ID you want to modify in the following format:

      `<groupnet_id>.<subnet_name>.<pool_name>`

      The following command rebalances the IP addresses in pool5 under groupnet1.subnet 3:

      ```
      isi network pools rebalance-ips groupnet1.subnet3.pool5
      ```

      c. Type `yes` at the confirmation prompt.

2. To manually rebalance all IP address pools:
   a. Run the `isi network sc-rebalance-all` command.
   b. Type `yes` at the confirmation prompt.
Managing network interface members

You can add and remove network interfaces to IP address pools.

Add or remove a network interface

You can configure which network interfaces are assigned to an IP address pool.

Before you begin

Network interfaces must be specified in the following format <lnn>:<interface_name>. Run the `isi network interfaces list` command to identify the node numbers and interface names that you need.

If you add an aggregated interface to the pool, you cannot individually add any interfaces that are part of the aggregated interface.

Procedure

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```bash
   isi network pools list
   ```

2. Run the `isi networks modify pool` command.

   Specify the pool ID you want to modify in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command modifies pool5 under groupnet1.subnet3 to add the first external network interfaces on nodes 1 through 3:

   ```bash
   isi network pools modify groupnet1.subnet3.pool5 --add-ifaces=1-3:ext-1
   ```

   The following command removes the first network interface on node 3 from pool5:

   ```bash
   isi network pools modify groupnet1.subnet3.pool5 --remove-ifaces=3:ext-1
   ```

Specify a link aggregation mode

You can combine multiple, physical external network interfaces on a node into a single logical interface through link aggregation.

You can add an aggregated interface to a pool and specify one of the following aggregation modes:

- LACP
- Round robin
Failover

FEC

Procedure

1. (Optional) To identify the name of the IP address pool you want to modify, run the following command:

   ```bash
   isi network pools list
   ```

2. Run the `isi networks modify pool` command. Specify the pool ID you want to modify in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command modifies pool5 under groupnet1.subnet3 to specify FEC as the aggregation mode for all aggregated interfaces in the pool:

   ```bash
   isi network pools modify groupnet1.subnet3.pool5 --aggregation-mode=fec
   ```

   The following command modifies pool5 under groupnet1.subnet3 to add ext-agg on node 1 and specify LACP as the aggregation mode:

   ```bash
   isi network pools modify groupnet1.subnet3.pool5 --add-ifaces=1:ext-agg --aggregation-mode=lacp
   ```

Link aggregation modes

The link aggregation mode determines how traffic is balanced and routed among aggregated network interfaces. The aggregation mode is selected on a per-pool basis and applies to all aggregated network interfaces in the IP address pool.

OneFS supports dynamic and static aggregation modes. A dynamic aggregation mode enables nodes with aggregated interfaces to communicate with the switch so that the switch can use an analogous aggregation mode. Static modes do not facilitate communication between nodes and the switch.

OneFS provides support for the following link aggregation modes:

**Link Aggregation Control Protocol (LACP)**

Dynamic aggregation mode that supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP). You can configure LACP at the switch level, which allows the node to negotiate interface aggregation with the switch. LACP balances outgoing traffic across the interfaces based on hashed protocol header information that includes the source and destination address and the VLAN tag, if available. This option is the default aggregation mode.

**Loadbalance (FEC)**

Static aggregation method that accepts all incoming traffic and balances outgoing traffic over aggregated interfaces based on hashed protocol header information that includes source and destination addresses.

**Active/Passive Failover**

Static aggregation mode that switches to the next active interface when the primary interface becomes unavailable. The primary interface handles traffic until
there is an interruption in communication. At that point, one of the secondary interfaces will take over the work of the primary.

**Round-robin**

Static aggregation mode that rotates connections through the nodes in a first-in, first-out sequence, handling all processes without priority. Balances outbound traffic across all active ports in the aggregated link and accepts inbound traffic on any port.

**Note**

This method is not recommended if your EMC Isilon cluster is using TCP/IP workloads.

---

**View network interfaces**

You can retrieve and sort a list of all external network interfaces on the EMC Isilon cluster.

**Procedure**

1. Run the `isi network interfaces list` command.
   
The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>LNN</th>
<th>Name</th>
<th>Status</th>
<th>Owners</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ext-1</td>
<td>Up</td>
<td>groupnet0.subnet0.pool10</td>
<td>10.7.144.0</td>
</tr>
<tr>
<td>1</td>
<td>ext-2</td>
<td>Not Available</td>
<td>groupnet1.subnet3.pool15</td>
<td>203.0.223.12</td>
</tr>
<tr>
<td>2</td>
<td>ext-1</td>
<td>Up</td>
<td>groupnet0.subnet0.pool10</td>
<td>10.7.144.0</td>
</tr>
<tr>
<td>2</td>
<td>ext-2</td>
<td>Not Available</td>
<td>groupnet1.subnet3.pool15</td>
<td>203.0.223.12</td>
</tr>
<tr>
<td>3</td>
<td>ext-1</td>
<td>Up</td>
<td>groupnet0.subnet0.pool10</td>
<td>10.7.144.0</td>
</tr>
<tr>
<td>3</td>
<td>ext-2</td>
<td>Not Available</td>
<td>groupnet1.subnet3.pool15</td>
<td>203.0.223.12</td>
</tr>
</tbody>
</table>

   The following command displays interfaces only on nodes 1 and 3:

   `isi network interfaces list --nodes=1,3`

   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>LNN</th>
<th>Name</th>
<th>Status</th>
<th>Owners</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ext-1</td>
<td>Up</td>
<td>groupnet0.subnet0.pool10</td>
<td>10.7.144.0</td>
</tr>
<tr>
<td>1</td>
<td>ext-2</td>
<td>Not Available</td>
<td>groupnet1.subnet3.pool15</td>
<td>203.0.223.12</td>
</tr>
<tr>
<td>3</td>
<td>ext-1</td>
<td>Up</td>
<td>groupnet0.subnet0.pool10</td>
<td>10.7.144.0</td>
</tr>
<tr>
<td>3</td>
<td>ext-2</td>
<td>Not Available</td>
<td>groupnet1.subnet3.pool15</td>
<td>203.0.223.12</td>
</tr>
</tbody>
</table>

---

**Managing node provisioning rules**

You can create and manage node provisioning rules that automate the configuration of new network interfaces.
Create a node provisioning rule

You can create a node provisioning rule to specify how network interfaces on new nodes are configured when the nodes are added to the EMC Isilon cluster.

Procedure

1. Run the `isi network rules create` command.
   
   Specify the ID of the rule you want to create in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

   The following command creates a rule named rule7 that assigns the first external network interface on each new accelerator node to groupnet1.subnet3.pool5:

   ```bash
   isi network rules create groupnet1.subnet3.pool5.rule7 --iface=ext-1 --node-type=accelerator
   ```

Modify a node provisioning rule

You can modify node provisioning rules settings.

Procedure

1. (Optional) To identify the name of the provisioning rule you want to modify, run the following command:

   ```bash
   isi network rules list
   ```

2. Run the `isi network rules modify` command.
   
   Specify the ID of the rule you want to modify in the following format:

   `<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

   The following command changes the name of rule7 to rule7accelerator:

   ```bash
   isi network rules modify groupnet1.subnet3.pool5.rule7 --name=rule7accelerator
   ```

   The following command changes rule7 so that it applies only to backup accelerator nodes:

   ```bash
   isi network rules modify groupnet1.subnet3.pool5.rule7 --node-type=backup-accelerator
   ```
Delete a node provisioning rule

You can delete a node provisioning rule that you no longer need.

Procedure

1. (Optional) To identify the name of the provisioning rule you want to delete, run the following command:

   ```bash
   isi network rules list
   ```

2. Run the `isi networks delete rule` command.
   
   Specify the ID of the rule you want to delete in the following format:

   ```bash
   <groupnet_name>.<subnet_name>.<pool_name>.<rule_name>
   ```

   The following command deletes rule7 from pool5:

   ```bash
   isi network rules delete groupnet1.subnet3.pool5.rule7
   ```

3. At the prompt, type `yes`.

View node provisioning rules

You can retrieve and sort a list of all node provisioning rules on the external network or view details of a specific rule.

Procedure

1. To list all of the provisioning rules in the system, run the `isi network rules list` command:

   The system displays output similar to the following example:

   ```
   ID                             Node Type   Interface
   ----------------------------------------
   groupnet0.subnet0.pool10.rule0      any        ext-1
   groupnet0.subnet1.pool1.rule1      accelerator ext-3
   groupnet1.subnet3.pool3.rule2     storage     ext-3
   groupnet1.subnet3.pool5.rule7     storage           ext-2
   ----------------------------------------
   ```

   The following command only lists rules in groupnet1:

   ```bash
   isi network rules list --groupnet=groupnet1
   ```

   The system displays output similar to the following example:

   ```
   ID                             Node Type   Interface
   ----------------------------------------
   groupnet1.subnet1.pool1.rule1  accelerator ext-3
   groupnet1.subnet3.pool3.rule2  storage     ext-3
   ----------------------------------------
   ```

2. To view the details of a specific provisioning rule, run the `isi network rules view` command and specify the rule ID.
Specify the rule ID you want to view in the following format:

<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

The following command displays the setting details of rule7 under groupnet1.subnet3.pool5:

isi network rules view groupnet1.subnet3.pool5.rule7

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID:</th>
<th>groupnet1.subnet3.pool5.rule7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type:</td>
<td>storage</td>
</tr>
<tr>
<td>Interface:</td>
<td>ext-2</td>
</tr>
<tr>
<td>Description:</td>
<td>-</td>
</tr>
<tr>
<td>Name:</td>
<td>rule7</td>
</tr>
<tr>
<td>Groupnet:</td>
<td>groupnet1</td>
</tr>
<tr>
<td>Subnet:</td>
<td>subnet3</td>
</tr>
<tr>
<td>Pool:</td>
<td>pool5</td>
</tr>
</tbody>
</table>

Managing routing options

You can provide additional control of the direction of outgoing client traffic through source-based routing or static route configuration.

If both source-based routing and static routes are configured, the static routes will take priority for traffic that matches the static routes.

Enable or disable source-based routing

You can enable source-based routing to ensure that outgoing client traffic is routed to the gateway of the source IP address in the packet header. If you disable source-based routing, outgoing traffic is destination-based or it follows static routes. Source-based routing is enabled or disabled globally on the EMC Isilon cluster.

Before you begin

Source-based routing rules are prioritized over static routes. You can check if there are static routes configured in any IP address pools by running the following command:

isi networks list pools -v

Procedure

1. Enable source-based routing on the cluster by running the following command:

   isi network external modify --sbr=true
2. Disable source-based routing on the cluster by running the following command:

   ```
   isi network external modify --sbr=false
   ```

## Add or remove a static route

You can configure static routes to direct outgoing traffic to specific destinations through a specific gateway.

### Procedure

1. (Optional) Identify the name of the IP address pool that you want to modify for static routes by running the following command:

   ```
   isi network pools list
   ```

2. Run the `isi networks modify pool` command.

   Specify the route in classless inter-domain routing (CIDR) notation format. Specify the pool ID you want to modify in the following format:

   ```
   <groupnet_name>.<subnet_name>.<pool_name>
   ```

   The following command adds an IPv4 static route to pool5 and assigns the route to all network interfaces that are members of the pool:

   ```
   isi network pools modify groupnet1.subnet3.pool5 --add-static-routes=192.168.100.0/24-192.168.205.2
   ```

   The following command removes an IPv6 static route from pool4:

   ```
   isi network pools modify groupnet2.subnet2.pool4 --remove-static-routes=2001:DB8:170:7c00::/64-2001:DB8:170:7cff::c008
   ```

## Managing DNS cache settings

You can set DNS cache settings for the external network.

### Before you begin

### Procedure

1.  
2.  

### Results
Before you begin

Procedure

1.
2.

Results

DNS cache settings

You can configure settings for the DNS cache.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL No Error Minimum</td>
<td>Specifies the lower boundary on time-to-live for cache hits. The default value is 30 seconds.</td>
</tr>
<tr>
<td>TTL No Error Maximum</td>
<td>Specifies the upper boundary on time-to-live for cache hits. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>TTL Non-existent Domain Minimum</td>
<td>Specifies the lower boundary on time-to-live for nxdomain. The default value is 15 seconds.</td>
</tr>
<tr>
<td>TTL Non-existent Domain Maximum</td>
<td>Specifies the upper boundary on time-to-live for nxdomain. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>TTL Other Failures Minimum</td>
<td>Specifies the lower boundary on time-to-live for non-nxdomain failures. The default value is 0 seconds.</td>
</tr>
<tr>
<td>TTL Other Failures Maximum</td>
<td>Specifies the upper boundary on time-to-live for non-nxdomain failures. The default value is 60 seconds.</td>
</tr>
<tr>
<td>TTL Lower Limit For Server Failures</td>
<td>Specifies the lower boundary on time-to-live for DNS server failures. The default value is 300 seconds.</td>
</tr>
<tr>
<td>TTL Upper Limit For Server Failures</td>
<td>Specifies the upper boundary on time-to-live for DNS server failures. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>Eager Refresh</td>
<td>Specifies the lead time to refresh cache entries that are nearing expiration. The default value is 0 seconds.</td>
</tr>
<tr>
<td>Cache Entry Limit</td>
<td>Specifies the maximum number of entries that the DNS cache can contain.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The default value is 65536 entries.</td>
</tr>
<tr>
<td>Test Ping Delta</td>
<td>Specifies the delta for checking the cbind cluster health.</td>
</tr>
<tr>
<td></td>
<td>The default value is 30 seconds.</td>
</tr>
</tbody>
</table>

### Managing TCP ports

You can modify the list of client TCP ports available to the external network.

### Add or remove TCP ports

You can add and remove TCP ports from the list of ports available for the external network.

#### Before you begin

#### Procedure

1.
2.

#### Results

### Networking commands

You can view and configure settings for the external networks on an EMC Isilon cluster through the networking commands.

**isi network dnscache flush**

Simultaneously flushes the DNS cache of each groupnet that has enabled DNS caching.

**Syntax**

```
isi network dnscache flush
[--verbose]
```

**Options**

```
{ --verbose | -v }
```

Displays more detailed information.
isi network dnscache modify

Modifies global DNS cache settings for each DNS cache that is enabled per groupnet.

Syntax

isi network dnscache modify
   [--cache-entry-limit <integer>]
   [--revert-cache-entry-limit]
   [--cluster-timeout <integer>]
   [--revert-cluster-timeout]
   [--dns-timeout <integer>]
   [--revert-dns-timeout]
   [--eager-refresh <integer>]
   [--revert-eager-refresh]
   [--testing-delta <integer>]
   [--revert-testing-delta]
   [--ttl-max-noerror <integer>]
   [--revert-ttl-max-noerror]
   [--ttl-min-noerror <integer>]
   [--revert-ttl-min-noerror]
   [--ttl-max-nxdomain <integer>]
   [--revert-ttl-max-nxdomain]
   [--ttl-min-nxdomain <integer>]
   [--revert-ttl-min-nxdomain]
   [--ttl-max-other <integer>]
   [--revert-ttl-max-other]
   [--ttl-min-other <integer>]
   [--revert-ttl-min-other]
   [--ttl-max-servfail <integer>]
   [--revert-ttl-max-servfail]
   [--ttl-min-servfail <integer>]
   [--revert-ttl-min-servfail]
   [--verbose]

Options

--cache-entry-limit <integer>
   Specifies the maximum number of entries that the DNS cache can contain. The limit must be a value between 1024 and 1048576. The default value is 65536 entries.

--revert-cache-entry-limit
   Sets the value of --cache-entry-limit to the default system value.

--cluster-timeout <integer>
   Specifies the timeout limit, in seconds, for calls made to other nodes in the EMC Isilon cluster. The limit must be a value between 0 and 60. The default value is 5.

--revert-cluster-timeout
   Sets the value of --cluster-timeout to the default system value.

--dns-timeout <integer>
   Specifies the timeout limit, in seconds, for calls made to the DNS resolver. The limit must be a value between 0 and 60. The default value is 5.

--revert-dns-timeout
   Sets the value of --dns-timeout to the default system value.
--eager-refresh <integer>
  Specifies the lead time, in seconds, to refresh cache entries that are nearing
  expiration. The lead time must be a value between 0 and 30. The default value is
  0.

--revert-eager-refresh
  Sets the value of --eager-refresh to the default system value.

--testping-delta <integer>
  Specifies the delta, in seconds, for checking the cbind cluster health. The delta
  must be a value between 0 and 60. The default value is 30.

--revert-testping-delta
  Sets the value of --testping-delta to the default system value.

--ttl-max-noerror <integer>
  Specifies the upper time-to-live boundary, in seconds, on cache hits. The
  boundary must be a value between 0 and 3600. The default value is 3600.

--revert-ttl-max-noerror
  Sets the value of --ttl-max-noerror to the default system value.

--ttl-min-noerror <integer>
  Specifies the lower time-to-live boundary, in seconds, on cache hits. The
  boundary must be a value between 0 and 3600. The default value is 30.

--revert-ttl-min-noerror
  Sets the value of --ttl-min-noerror to the default system value.

--ttl-max-nxdomain <integer>
  Specifies the upper time-to-live boundary, in seconds, for nxdomain failures. The
  boundary must be a value between 0 and 3600. The default value is 3600.

--revert-ttl-max-nxdomain
  Sets the value of --ttl-max-nxdomain to the default system value.

--ttl-min-nxdomain <integer>
  Specifies the lower time-to-live boundary, in seconds, for nxdomain failures. The
  boundary must be a value between 0 and 3600. The default value is 15.

--revert-ttl-min-nxdomain
  Sets the value of --ttl-min-nxdomain to the default system value.

--ttl-max-other <integer>
  Specifies the upper time-to-live boundary, in seconds, for non-nxdomain failures.
  The boundary must be a value between 0 and 3600. The default value is 60.

--revert-ttl-max-other
  Sets the value of --ttl-max-other to the default system value.

--ttl-min-other <integer>
  Specifies the lower time-to-live boundary, in seconds, for non-nxdomain failures.
  The boundary must be a value between 0 and 3600. The default value is 0.

--revert-ttl-min-other
Sets the value of --ttl-min-other to the default system value.

--ttl-max-servfail <integer>
Specifies the upper time-to-live boundary, in seconds, for DNS server failures. The boundary must be a value between 0 and 3600. The default value is 3600.

--revert-ttl-max-servfail
Sets the value of --ttl-max-servfail to the default system value.

--ttl-min-servfail <integer>
Specifies the lower time-to-live boundary, in seconds, for DNS server failures. The boundary must be a value between 0 and 3600. The default value is 300.

--revert-ttl-min-servfail
Sets the value of --ttl-min-servfail to the default system value.

|--verbose | -v|
Displays more detailed information.

isi network dnscache view
Displays DNS cache settings.

Syntax

isi network dnscache view

Options
There are no options for this command.

isi network external modify
Modifies global external network settings on the EMC Isilon cluster.

Syntax

isi network external modify
|--sbr {true | false}]
|--revert-sbr]
|--sc-rebalance-delay <integer>]
|--revert-sc-rebalance-delay]
|--tcp-ports <integer>]
|--clear-tcp-ports]
|--add-tcp-ports <integer>]
|--remove-tcp-ports <integer>]
|--revert-tcp-ports]
|--verbose]

Options

|--sbr {true | false}
Enables or disables source-based routing on the EMC Isilon cluster. Source-based routing is disabled by default.

|--revert-sbr
Sets the value of \(--sbr\) to the default system value.

\(--sc\text{-}rebalance\text{-}delay\ <integer>\)

Specifies a period of time (in seconds) that should pass after a qualifying event before an automatic rebalance is performed. The default value is 0 seconds.

\(--revert\text{-}sc\text{-}rebalance\text{-}delay\)

Sets the value of \(--sc\text{-}rebalance\text{-}delay\) to the default system value.

\(--tcp\text{-}ports\ <integer>\)

Sets a list of recognized client TCP ports. 65535 is the maximum supported port number. You can specify multiple TCP ports separated by commas, or specify this option for each additional TCP port.

\(--clear\text{-}tcp\text{-}ports\)

Removes all client TCP ports.

\(--add\text{-}tcp\text{-}ports\ <integer>\)

Adds one or more recognized client TCP ports, separated by commas, to the existing list. 65535 is the maximum supported port number.

\(--remove\text{-}tcp\text{-}ports\ <integer>\)

Removes one or more recognized client TCP ports, separated by commas.

\(--revert\text{-}tcp\text{-}ports\)

Sets the value of \(--tcp\text{-}ports\) to the default system value.

\{ --verbose | -v \}

Displays more detailed information.

isi network external view

Displays configuration settings for the external network.

Syntax

\(\text{isi network external view}\)

Options

There are no options for this command.

isi network groupnets create

Creates a groupnet which defines the client DNS settings applied to services that connect through the groupnet.

Syntax

\(\text{isi network groupnets create } <id>\)

\[\text{[--description } <\text{string}>\]\n
\[\text{[--dns\text{-}cache\text{-}enabled } \{\text{true | false}\}\]\n
\[\text{[--dns\text{-}search } <\text{domain name}>\]\n
\[\text{[--dns\text{-}servers } <\text{ip address}>\]
Options

=id>
Specifies a unique ID for the groupnet. The ID can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation. The ID cannot exceed 32 characters.

--description <string>
Specifies an optional description of the groupnet. The description cannot exceed 128 bytes.

--dns-cache-enabled {true | false}
Specifies whether DNS caching for the groupnet is enabled. DNS caching is enabled by default.

--dns-search <domain name>
Sets the list of DNS search suffixes. Suffixes are appended to domain names that are not fully qualified. The list cannot contain more than six suffixes.

Note
Do not begin suffixes with a leading dot; leading dots are automatically added.

--dns-servers <ip address>
Sets a list of DNS IP addresses. Nodes issue DNS requests to these IP addresses. The list cannot contain more than three IP addresses.

--dns-options <string>
Sets the DNS resolver option. The only valid value for this option is `rotate`.

--server-side-dns-search {true | false}
Specifies whether server-side DNS searching is enabled, which appends DNS search lists to client DNS inquiries handled by a SmartConnect service IP address. Server-side search is enabled by default.

{---verbose | -v}
Displays more detailed information.

isi network groupnets delete

Deletes a groupnet from the EMC Isilon cluster. You cannot delete the default groupnet from the system.

If the groupnet is associated with an access zone, an authentication provider, removal of the groupnet from the system might affect several other areas of OneFS and should be performed with caution. When you delete a groupnet, client connections to each subnet-pool association in the groupnet are lost. Deleting a groupnet that is in use can prevent access to the EMC Isilon cluster. Client connections to the cluster through any subnet-pool in the deleted groupnet will be terminated.
Syntax

```bash
isi network groupnets delete <id>
    [--force]
    [--verbose]
```

Options

`< id>`

- Specifies the ID of the groupnet to be deleted.

`{--force | -f}`

- Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

`{--verbose | -v}`

- Displays more detailed information.

**isi network groupnets list**

Retrieves a list of groupnets that exist on the EMC Isilon cluster.

Syntax

```bash
isi network groupnets list
    [{--limit | -l} <integer>]
    [{--sort {description | dns_cache_enabled | id | name | server_side_dns_search}}]
    [{--descending | -d}]
    [{--format {true | table | json | csv | list}}]
    [{--no-header | -a}]
    [{--no-footer | -z}]
    [{--verbose | -v}]
```

Options

`{ --limit | -l} <integer>`

- Displays no more than the specified number.

`{ --sort {description | dns_cache_enabled | id | name | server_side_dns_search}}`

- Sorts output displayed by the specified attribute.

`{ --descending | -d}`

- Displays output in reverse order.

`{ --format {table | json | csv | list}}`

- Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{ --no-header | -a}`

- Displays table and CSV output without headers.

`{ --no-footer | -z}`

- Displays table output without footers.
Displays more detailed information.

**isi network groupnets modify**

Modifies a groupnet which defines the DNS settings applied to services that connect through the groupnet.

**Syntax**

```bash
isi network groupnets modify <id>

[--description <string>]
[--clear description]
[--dns-cache-enabled {true | false}]
[--revert-dns-cache-enabled]
[--dns-search <domain name>]
[--clear-dns-search]
[--add-dns-search <domain name>]
[--remove-dns-search <domain name>]
[--dns-servers <IP address>]
[--clear-dns-servers]
[--add-dns-servers <IP address>]
[--remove-dns-servers <IP address>]
[--dns-options <string>]
[--clear-dns-options]
[--add-dns-options <string>]
[--remove-dns-options <string>]
[--name <string>]
[--server-side-dns-search {true | false}]
[--revert server-side-dns-search]
[--verbose]
```

**Options**

 `<id>`

Specifies the ID of the groupnet to be modified.

`--description <string>`

Specifies an optional description of the groupnet. This option overwrites the existing description. The description cannot exceed 128 bytes.

`--clear-description`

Clears the current description.

`--dns-cache-enabled {true | false}`

Specifies whether DNS caching for the groupnet is enabled. DNS caching is enabled by default.

`--revert-dns-cache-enabled`

Sets the value of `--dns-cache-enabled` to the system default value.

`--dns-search <domain name>`

Sets the list of DNS search suffixes. Suffixes are appended to domain names that are not fully qualified. The list cannot contain more than six suffixes. This option overwrites the current list of DNS search suffixes.
Note
Do not begin suffixes with a leading dot; leading dots are automatically added.

```
--clear-dns-search
  Removes the current list of DNS search suffixes.

--add-dns-search <domain name>
  Adds one or more DNS search suffixes to the current list.

--remove-dns-search <domain name>
  Removes one or more DNS search suffixes from the current list.

--dns-servers <IP address>
  Sets a list of DNS IP addresses. Nodes issue DNS requests to these IP addresses. The list cannot contain more than three IP addresses. This option overwrites the current list of DNS IP addresses.

--clear-dns-servers
  Removes the current list of DNS servers.

--add-dns-servers <IP address>
  Adds one or more DNS servers to the current list.

--remove-dns-servers <IP address>
  Removes one or more DNS servers from the current list.

--dns-options <string>
  Sets the DNS resolver option. The only valid value for this option is rotate.

--clear-dns-options
  Removes the current list of DNS resolver options.

--add-dns-options <string>
  Adds one or more DNS resolver options to the current list.

--remove-dns-options <string>
  Removes one or more DNS resolver options from the current list.

--name <string>
  Specifies a new name for the groupnet. The ID can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation. The name cannot exceed 32 characters.

--server-side-dns-search {true | false}
  Specifies whether server-side DNS searching is enabled, which appends DNS search lists to client DNS inquiries handled by a SmartConnect service IP address. Server-side search is enabled by default.

--revert-server-side-dns-search
  Sets the value of --server-side-dns-search to the system default value.

{--verbose | -v}
  Displays more detailed information.
```
**isi network groupnets view**

Displays the configuration details of a specific groupnet on the EMC Isilon cluster.

**Syntax**

```
isi network groupnets view <id>
```

**Options**

`<id>`

Specifies the ID of the groupnet to be viewed.

---

**isi network interfaces list**

Displays a list of network interfaces on the EMC Isilon cluster.

**Syntax**

```
isi network interfaces list
[--nodes <integer>]
[--show-inactive]
[--limit <integer>]
[--sort {lnn | name | status}]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

If no options are specified, the command displays a list of all network interfaces on the cluster.

`--nodes <lnn>`

Lists interfaces only from the specified nodes. Specify nodes by Logical Node Number. Separate multiple nodes by commas.

`--show-inactive`

Includes inactive interfaces in the output.

`{ --limit | -l } <integer>`

Displays no more than the specified number of interfaces.

`--sort {lnn | name | status}`

Sorts output displayed by the specified attribute.

`{ --descending | -d }`

Displays output in reverse order.

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
Displays table and CSV output without headers.

Displays table output without footers.

Displays more detailed information.

Examples
The following command lists network interfaces on node 1:

```
isi network interfaces list --nodes=1
```

The system displays output similar to the following example:

```
LNN Name         Status        Owners                  IP Addresses
-------------------------------------------------------------------
1   10gige-1     Up            -                       -
1   10gige-2     No Carrier    -                       -
1   10gige-agg-1 Not Available -                       -
1   ext-1        Up            groupnet0.subnet0.pool0 198.51.100.0
1   ext-2        Up            -                       -
1   ext-agg      Not Available -                       -
-------------------------------------------------------------------
Total: 6
```

**isi network pools create**

Creates a pool of IP addresses within a subnet. A SmartConnect Advanced license is required to create more than one pool within a subnet.

**Syntax**

```
isi network pools create <id>
    [--access-zone <zone-name>]
    [--aggregation-mode {roundrobin | failover | lacp | fec}]
    [--alloc-method {dynamic | static}]
    [--description <string>]
    [--ifaces <node-interface-range>]|...
    [--ranges <ip-address-range>]|...
    [--rebalance-policy{manual | auto}]
    [--sc-auto-unsuspend-delay <integer>]
    [--sc-connect-policy {roundrobin | conn_count | throughput | cpu_usage}]
    [--sc-dns-zone <domain-name>]
    [--sc-dns-zone-aliases <domain-name>]|...
    [--sc-failover-policy {roundrobin | conn_count | throughput | cpu_usage}]
    [--sc-subnet <string>]
    [--sc-ttl <integer>]
    [--static-routes <route>]|...
    [--force]
    [--verbose]
```

**Options**

`<id>`

Specifies the ID of the new pool that you want to create. The pool must be added to an existing groupnet and subnet. The ID can be up to 32 alphanumeric characters.
characters long and can include underscores or hyphens, but cannot include spaces or other punctuation. Specify the pool ID in the following format:

```
<groupnet_name>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colonets are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0. The pool name must be unique in the subnet.

```
--access-zone <zone-name>
```

Associates an access zone with the pool. Clients will be allowed to connect to the specified access zone only through IP addresses in the pool. The access zone must belong to the same groupnet as the IP address pool.

```
--aggregation-mode {roundrobin | failover | lacp | fec}
```

Specifies how outgoing traffic is distributed across aggregated network interfaces. The aggregation mode is applied only if at least one aggregated network interface is a member of the IP address pool.

The following values are valid:

**roundrobin**

Rotates connections through the nodes in a first-in, first-out sequence, handling all processes without priority. Balances outbound traffic across all active ports in the aggregated link and accepts inbound traffic on any port.

**failover**

Switches to the next active interface when the primary interface becomes unavailable. Manages traffic only through a primary interface. The second interface takes over the work of the first as soon as it detects an interruption in communication.

**lacp**

Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP). Balances outgoing traffic across the interfaces based on hashed protocol header information that includes the source and destination address and the VLAN tag, if available. Also assembles interfaces of the same speed into groups called Link Aggregated Groups (LAGs) and balances traffic across the fastest LAGs. This option is the default mode for new pools.

**fec**

Provides static balancing on aggregated interfaces through the Cisco Fast EtherChannel (FEC) driver, which is found on older Cisco switches. Capable of load-balancing traffic across Fast Ethernet links. Enables multiple physical Fast Ethernet links to combine into one logical channel.

```
--alloc-method {dynamic | static}
```

Specifies the method by which IP addresses are allocated to the network interfaces that are members of the pool.

The following values are valid:

**static**

Assigns each network interface in the IP address pool a single, permanent IP address from the pool. Depending on the number of IP addresses available, some IP addresses might go unused. The static option is the default setting.
**dynamic**

Specifies that all pool IP addresses must be assigned to a network interface at all times. Enables multiple IP addresses to be assigned to an interface. If a network interface becomes unavailable, this option helps to ensure that the assigned IP address are redistributed to another interface.

---

**Note**

This option is only available if a SmartConnect Advanced license is active on the cluster.

---

**--description <string>**

Specifies an optional description of the IP address pool. The description cannot exceed 128 bytes.

**--ifaces <node-interface-range>...**

Specifies which network interfaces should be members of the IP address pool. Specify network interfaces in the following format:

```
<node>:<interface>
```

To specify a range of nodes, separate the lower and upper node IDs with a dash (-). To specify multiple network interfaces, separate each interface with a comma. The following example adds the interfaces from nodes 1, 2 and 3:

```
--ifaces 1-2:ext-1,3:ext-2,1:10gige-agg-1,3:10gige-1
```

---

**Note**

If you attempt to add an interface that has already been added as part of an aggregated interface, you will receive an error message.

---

**--ranges <ip-address-range>...**

Specifies one or more IP address ranges for the pool. IP addresses within these ranges are assigned to the network interfaces that are members of the pool. Specify the IP address range in the following format:

```
<low-ip-address>-<high-ip-address>
```

---

**--rebalance-policy {manual | auto}**

Specifies when to redistribute pool IP addresses if a network interface that was previously unavailable becomes available.

**manual**

Requires that connection rebalancing be performed manually after network interface failback.
To manually rebalance all IP addresses in a specific pool, run the following command:

`isi network pools rebalance-ips`

To manually rebalance all IP addresses across the EMC Isilon cluster, run the following command:

`isi network sc-rebalance-all`

**auto**

Causes connections to be rebalanced automatically after network interface failback. This is the default value.

`--sc-auto-unsuspend-delay <integer>`

Specifies the time delay (in seconds) before a node that is automatically unsuspended resumes SmartConnect DNS query responses for the node. During certain cluster operations such as rolling upgrades, general node splits, or node reboots, a node is automatically suspended and then unsuspended by the system.

`--sc-connect-policy {roundrobin | conn_count | throughput | cpu_usage}`

Specifies how incoming DNS queries for client connections are balanced across IP addresses.

The following values are valid:

- **round-robin**
  
  Rotates connections through nodes equally. This value is the default policy.

- **conn-count**
  
  Assigns connections to the node that has the fewest number of connections.

- **throughput**
  
  Assigns connections to the node with the least throughput.

- **cpu-usage**
  
  Assigns connections to the node with the lowest CPU usage.

`--sc-dns-zone <domain-name>`

Specifies the SmartConnect DNS zone name for this pool. IP addresses are returned in response to DNS queries to this SmartConnect zone.

`--sc-dns-zone-aliases <domain-name>`

Specifies a list of alternate SmartConnect DNS zone names for the pool. Multiple aliases can be specified in a comma-separated list.

`--sc-failover-policy {roundrobin | conn_count | throughput | cpu_usage}`

Specifies how IP addresses that belong to an unavailable interface are rebalanced across the remaining network interfaces.

The following values are valid:
round-robin
Assigns IP addresses across nodes equally. This is the default policy.

conn-count
Assigns IP addresses to the node that has fewest number of connections.

throughput
Assigns IP addresses to the node with least throughput.

cpu-usage
Assigns IP addresses to the node with lowest CPU usage.

--sc-subnet <string>
Specifies the name of the service subnet that is responsible for handling DNS requests for the SmartConnect zone.

--sc-ttl <integer>
Specifies the time-to-live value for SmartConnect DNS query responses (in seconds). DNS responses are only valid for the time specified. The default value is 0 seconds.

--static-routes <route>
Designates an IP addresses as a static route and specifies the destination gateway. If a client connects through a static route IP address, outgoing client traffic is routed through the specified gateway. Multiple routes can be specified in a comma-separated list.
Specify the static route in the following classless inter-domain routing (CIDR) notation format:

<network-address>/<subnet-mask>-<gateway-ip-address>

{--verbose | -v}
Displays more detailed information.

{--force | -f}
Forces commands without warnings.

Examples
The following command creates a new IP address pool called pool1 under groupnet0.subnet0 and assigns IP addresses 198.51.100.10-198.51.100.20 to ext-1 network on nodes 1, 2, and 3. The SmartConnect zone name of this pool is storage.company.com, but it accepts the alias of storage.company:

```
isi network pools create groupnet0.subnet0.pool1 \
--ranges=192.168.8.10-192.168.8.15 --ifaces=1-3:ext-1 \
--sc-dns-zone=storage.company.com --sc-dns-zone-aliases=storage.company
```

The following command creates a new IP address pool called pool1 under groupnet0.subnet0 and assigns IP addresses 198.51.100.10-198.51.100.20 to the pool.
The command also includes aggregated interfaces from nodes 1-3 and specifies FEC as the aggregation mode:

```
isi network pools create groupnet0.subnet0.pool1 \  --ranges=192.168.8.10-192.168.8.15 --ifaces=1-3:10gige-agg-1 \  --aggregation-mode=fec
```

The following command creates a new IP address pool called pool1 under groupnet0.subnet0, assigns IP addresses 198.51.100.10-198.51.100.20 to the pool, and specifies that connection rebalancing must be performed manually:

```
isi network pools create groupnet0.subnet0.pool1 \  --ranges=192.168.8.10-192.168.8.15 --alloc-method=dynamic \  --rebalance-policy=manual
```

### isi network pools delete

Deletes IP address pools.

Deleting an IP address pool that is in use can prevent access to the EMC Isilon cluster. Client connections to the cluster through any IP address in the deleted pool will be terminated.

**Syntax**

```
isi network pools delete <id>  
  [--force]  
  [--verbose]
```

**Options**

<id>...

Specifies the ID of the IP address pool to be deleted. Specify the pool ID in the following format:

```
<groupnet_name>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0.

{--force | -f}

Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

{--verbose | -v}

Displays more detailed information.

### isi network pools list

Retrieves a list of IP address pools that exist on the EMC Isilon cluster.
Syntax

```
isi network pools list
  [--subnet-id <string>...]
  [--groupnet <string>...]
  [--subnet <string>...]
  [{--limit | -l} <integer>]
  [--sort {aggregation_mode | alloc_method | description | id | name | rebalance_policy | sc_auto_suspend_dealy | sc_connect_policy | sc_dns_zone | sc_failover_policy | sc_subnet | sc_ttl}]
  [{--descending | -d}]
  [--format {table | json | csv | list}]
  [{--no-header | -a}]
  [{--no-footer | -z}]
  [{--verbose | -v}]
```

Options

If no options are specified, the command displays a list of all IP address pool on the cluster.

```
--subnet-id <string>...
  Displays IP address pools only from the specified subnet ID. Specify the subnet ID in the following format:

  <groupnet_name>.<subnet_name>

  The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0.
```

```
--groupnet <string>...
  Displays IP address pools only from the specified groupnet name.
```

```
--subnet <string>...
  Displays IP address pools only subnets with the specified name.

{--limit | -l} <integer>
  Displays no more than the specified number.
```

```
--sort {aggregation_mode | alloc_method | description | id | name | rebalance_policy | sc_auto_suspend_dealy | sc_connect_policy | sc_dns_zone | sc_failover_policy | sc_subnet | sc_ttl}]
  Sorts output displayed by the specified attribute.

{--descending | -d}
  Displays output in reverse order.
```

```
--format {true | table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{--no-header | -a}
  Displays table and CSV output without headers.
```

```
{--no-footer | -z}
  Displays table output without footers.
```
Displays more detailed information.

Examples
The following command displays a list all available IP address pools:

```
isi network pools list
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>SC Zone</th>
<th>Alloc Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupnet0.subnet0.pool0</td>
<td>storage.company.com</td>
<td>dynamic</td>
</tr>
<tr>
<td>groupnet3.subnet0.pool3</td>
<td></td>
<td>static</td>
</tr>
<tr>
<td>Total: 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following command displays a list of all pools that use the dynamic allocation method:

```
isi network pools list --alloc-method=dynamic
```

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>SC Zone</th>
<th>Alloc Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupnet0.subnet0.pool0</td>
<td>storage.company.com</td>
<td>dynamic</td>
</tr>
<tr>
<td>Total: 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**isi network pools modify**

Modifies IP address pool settings.

Syntax

```
isi network pools modify <id>
[--access-zone <zone-name>]
[--revert-access-zone]
[--aggregation-mode {roundrobin | failover | lACP | fec}]
[--revert-aggregation-mode]
[--alloc-method {dynamic | static}]
[--revert-alloc-method]
[--description <string>]
[--clear-description]
[--ifaces <node-interface-range>]...
[--clear-ifaces]
[--add-ifaces <node-interface-range>]...
[--remove-ifaces <node-interface-range>]...
[--name <string>]
[--ranges <ip-address-range>]...
[--clear-ranges]
[--add-ranges <ip-address-range>]...
[--remove-ranges <ip-address-range>]...
[--rebalance-policy {manual | auto}]
[--revert-rebalance-policy]
[--sc-auto-unsuspend-delay <integer>]
[--revert-sc-auto-unsuspend-delay]
[--sc-connect-policy {roundrobin | conn_count | throughput | cpu_usage}]
```
Options

<id>

Specifies the ID of the IP address pool that you want to modify. Specify the ID in the following format:

<groupnet_name>.<subnet_name>.<pool_name>

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0. The pool name must be unique in the subnet.

--access-zone <zone-name>

Associates an access zone with the pool. Clients will be allowed to connect to the specified access zone only through IP addresses in the pool. The access zone must belong to the same groupnet as the IP address pool.

--revert-access-zone

Sets the value of --access-zone to the system default value.

--aggregation-mode {roundrobin | failover | lacp | fec}

Specifies how outgoing traffic is distributed across aggregated network interfaces. The aggregation mode is applied only if at least one aggregated network interface is a member of the IP address pool.

The following values are valid:

roundrobin

Rotates connections through the nodes in a first-in, first-out sequence, handling all processes without priority. Balances outbound traffic across all active ports in the aggregated link and accepts inbound traffic on any port.

failover

Switches to the next active interface when the primary interface becomes unavailable. Manages traffic only through a primary interface. The second interface takes over the work of the first as soon as it detects an interruption in communication.
lacp
Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP). Balances outgoing traffic across the interfaces based on hashed protocol header information that includes the source and destination address and the VLAN tag, if available. Also assembles interfaces of the same speed into groups called Link Aggregated Groups (LAGs) and balances traffic across the fastest LAGs. This option is the default mode for new pools.

fec
Provides static balancing on aggregated interfaces through the Cisco Fast EtherChannel (FEC) driver, which is found on older Cisco switches. Capable of load-balancing traffic across Fast Ethernet links. Enables multiple physical Fast Ethernet links to combine into one logical channel.

--revert-aggregation-mode
Sets the value of --aggregation-mode to the system default value.

--alloc-method {dynamic | static}
Specifies the method by which IP addresses are allocated to the network interfaces that are members of the pool.
The following values are valid:

static
Assigns each network interface in the IP address pool a single, permanent IP address from the pool. Depending on the number of IP addresses available, some IP addresses might go unused. The static option is the default setting.

dynamic
Specifies that all pool IP addresses must be assigned to a network interface at all times. Enables multiple IP addresses to be assigned to an interface. If a network interface becomes unavailable, this option helps to ensure that the assigned IP address are redistributed to another interface.

Note
This option is only available if a SmartConnect Advanced license is active on the cluster.

--revert-alloc-method
Sets the value of --alloc-method to the system default value.

--description <string>
Specifies an optional description of the IP address pool. This option overwrites the existing description. The description cannot exceed 128 bytes.

--clear-description
Clears the description of the IP address pool.

--ifaces <node-interface-range>...
Adds network interfaces to the IP address pool. Specify network interfaces in the following format:

```
<node>:<interface>
```

To specify a range of nodes, separate the lower and upper node IDs with a dash (-). To specify multiple network interfaces, separate each interface with a comma. The following example adds the interfaces from nodes 1, 2 and 3:

```
--ifaces 1-2:ext-1,3:ext-2,1:10gige-agg-1,3:10gige-1
```

```
--clear-ifaces
Removes all network interfaces from the IP address pool.
```

```
--add-ifaces <node-interface-range>...
Adds one or more network interfaces to the IP address pool.
```

```
--remove-ifaces <node-interface-range>...
Removes one or more network interfaces from the IP address pool.
```

```
--name <string>
Specifies a new name for the IP address pool. The name can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation. The new pool name must be unique in the subnet.
```

```
--ranges <ip-address-range>...
Specifies one or more IP address ranges for the pool. IP addresses within these ranges are assigned to the network interfaces that are members of the pool. Specify the IP address range in the following format:

```
<low-ip-address>-<high-ip-address>
```

This option overwrites the existing list of IP address ranges. Use the --add-ranges and --remove-ranges options to modify the existing list.

```
--clear-ranges
Removes all IP address ranges from the pool.
```

```
--add-ranges
Adds one or more IP address ranges to the pool.
```

```
--remove-ranges
Removes one or more IP address ranges from the pool.
```

```
--rebalance-policy{manual | auto}
Specifies when to redistribute pool IP addresses if a network interface that was previously unavailable becomes available.

```
manual
Requires that connection rebalancing be performed manually after network interface failback.
```

To manually rebalance all IP addresses in a specific pool, run the following command:

```
isi network pools rebalance-ips
```

To manually rebalance all IP addresses across the EMC Isilon cluster, run the following command:

```
isi network sc-rebalance-all
```

```
auto
Causes connections to be rebalanced automatically after network interface failback. This is the default value.
```

```
--revert-rebalance-policy
Sets the value of --rebalance-policy to the system default value.
```

```
--sc-auto-unsuspend-delay <integer>
Specifies the time delay (in seconds) before a node that is automatically unsuspended resumes SmartConnect DNS query responses for the node. During certain cluster operations such as rolling upgrades, general node splits, or node reboots, a node is automatically suspended and then unsuspended by the system.
```

```
--revert-sc-auto-unsuspend-delay
Sets the value of --sc-auto-unsuspend-delay to the system default value.
```

```
--sc-connect-policy {roundrobin | conn_count | throughput | cpu_usage}
Specifies how incoming DNS requests for client connections are balanced across IP addresses.
The following values are valid:

  roundrobin
  Rotates connections through nodes equally. This value is the default policy.

  conn_count
  Assigns connections to the node that has the fewest number of connections.

  throughput
  Assigns connections to the node with the least throughput.

  cpu_usage
 Assigns connections to the node with the lowest CPU usage.
```

```
--revert-sc-connect-policy
Sets the value of --sc-connect-policy to the system default value.
```

```
--sc-dns-zone <domain-name>
 Specifies the SmartConnect DNS zone name for this pool. IP addresses are returned in response to DNS queries to this SmartConnect zone.
```

```
--sc-dns-zone-aliases <domain-name>...
```
Specifies a list of alternate SmartConnect DNS zone names for the pool. Multiple aliases can be specified in a comma-separated list. This option overwrites the existing list of SmartConnect DNS zone aliases. Use the `--add-sc-dns-zone-aliases` and `--remove-sc-dns-zone-aliases` options to modify the existing list.

`--clear-sc-dns-zone-aliases`
Removes all SmartConnect DNS zone aliases from the pool.

`--add-sc-dns-zone-aliases <domain-name>...`
Adds one or more SmartConnect DNS zone aliases to the pool.

`--remove-sc-dns-zone-aliases <domain-name>...`
Removes one or more SmartConnect DNS zone aliases from the pool.

`--sc-failover-policy {roundrobin | conn_count | throughput | cpu_usage}`
Specifies how IP addresses that belong to an unavailable interface are rebalanced across the remaining network interfaces. The following values are valid:

- **roundrobin**
  Assigns IP addresses across nodes equally. This is the default policy.

- **conn_count**
  Assigns IP addresses to the node that has fewest number of connections.

- **throughput**
  Assigns IP addresses to the node with least throughput.

- **cpu_usage**
  Assigns IP addresses to the node with lowest CPU usage.

`--revert-failover-policy`
Sets the value of `--sc-failover-policy` to the system default value.

`--sc-subnet <string>`
Specifies the name of the service subnet that is responsible for handling DNS requests for the SmartConnect zone.

`--sc-ttl <integer>`
Specifies the time-to-live value for SmartConnect DNS query responses (in seconds). DNS responses are only valid for the time specified. The default value is 0 seconds.

`--static-routes <route>...`
Designates an IP addresses as a static route and specifies the destination gateway. If a client connects through a static route IP address, outgoing client traffic is routed through the specified gateway. Multiple routes can be specified in a comma-separated list. Specify the static route in the following classless inter-domain routing (CIDR) notation format:

```
<network-address>/<subnet-mask><gateway-ip-address>
```
This option overwrites the existing list of static routes. Use the `--add-static-routes` and `--remove-static-routes` options to modify the existing list.

`--clear-static-routes`
Removes all static routes from the pool.

`--add-static-routes <route>...`
Adds one or more static routes to the pool.

`--remove-static-routes <route>...`
Removes one or more static routes from the pool.

`{--verbose | -v}`
Displays more detailed information.

`{--force | -f}`
Forces commands without warnings.

**isi network pools rebalance-ips**

Redistributes the IP addresses in a specified pool across network interface members. Run this command for pools that specify a manual rebalance policy.

**Syntax**

```
isi network pools rebalance-ips <id>...
    [--force]
    [--verbose]
```

**Options**

`<id>...`
Specifies the name of the IP address pool to be rebalanced. Specify the pool name in the following format:

```
<groupnet_name>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, `groupnet0:subnet1:pool0`.

`{--force | -f}`
Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

`{--verbose | -v}`
Displays more detailed information.
isi network pools sc-resume-nodes

Resumes SmartConnect DNS query responses on a node.

Syntax

```
isi network pools sc-resume-nodes <id> <lnn>...
      [--force]
      [--verbose]
```

Options

```
<id>...
  Specifies the name of the IP address pool for which SmartConnect DNS query
  responses should be resumed. Specify the pool name in the following format:

  <groupnet_id>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are
also acceptable as delimiters between component names—for example,
groupnet0:subnet1:pool0.

```
<lnn>...
  Specifies the Logical Node Number of the node for which SmartConnect DNS
  query responses should be resumed.
```

```
{--force | -f}
  Suppresses any prompts, warnings, or confirmation messages that would
  otherwise appear.
```

```
{--verbose | -v}
  Displays more detailed information.
```

isi network pools sc-suspend-nodes

Suspends SmartConnect DNS query responses on a node.

Syntax

```
isi network pools sc-suspend-nodes <id> <lnn>...
      [--force]
      [--verbose]
```

Options

```
<id>...
  Specifies the name of the IP address pool for which SmartConnect DNS query
  responses should be suspended. Specify the pool name in the following format:

  <groupnet_name>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are
also acceptable as delimiters—for example, groupnet0:subnet1:pool0.
Specifies the Logical Node Number of the node for which SmartConnect DNS query responses should be suspended.

{--force | -f}
Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

{--verbose | -v}
Displays more detailed information.

**isi network pools view**
Displays the configuration details of a specific IP address pool on the EMC Isilon cluster.

**Syntax**

```bash
isi network pools view <id>
```

**Options**

- `<id>`
  Specifies the ID of the IP address pool to be viewed. Specify the pool ID in the following format:

  `<groupnet_name>.<subnet_name>.<pool_name>`

  The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, `groupnet0:subnet1:pool0`.

**isi network rules create**
Creates a provisioning rule to automatically configure new network interfaces that are added to the EMC Isilon cluster.

**Syntax**

```bash
isi network rules create <id> <iface>  
  [--desc <string>]  
  [--node-type {any | storage | accelerator | backup-accelerator}]  
  [--verbose]
```

**Options**

- `<id>`
  Specifies the ID and location of the new provisioning rule. New network interfaces that meet the rule criteria will be assigned to the IP address pool that contains the rule. Valid IDs include the groupnet, subnet, pool, and rule name. The rule name
must be unique throughout the given IP address pool. Specify the rule ID in the following format:

<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0:rule3. The rule name must be unique in the pool.

<iface>
Specifies the network interface name the rule applies to. To view a list of interfaces on your system, run the isi network interfaces list command.

--description <string>
Specifies an optional description of the provisioning rule. The description cannot exceed 128 bytes.

--node-type {any | storage | accelerator | backup-accelerator}
Sets the provisioning rule to apply to one or more of the specified type of node. The default setting is any.

{--verbose | -v}
Displays more detailed information.

isi network rules delete

Deletes provisioning rules.

Syntax

isi network rules delete <id>

Options

<id>...
Specifies the ID of the provisioning rule to be deleted. Specify the rule ID in the following format:

<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0:rule3.

{--force | -f}
Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

{--verbose | -v}
Displays more detailed information.
isi network rules list

Retrieves a list of provisioning rules on the EMC Isilon cluster.

Syntax

```plaintext
isi network rules list
[--pool-id <string>]
[--groupnet <string>]
[--subnet <string>]
[--pool <string>]
[|--limit | -l] <integer>
[|--sort {id | description | iface | node_type | name}]
[|--descending | -d]}
[|--format {true | table | json | csv | list}]
[|--no-header | -a]
[|--no-footer | -z]}
[|--verbose]
```

Options

If no options are specified, the command displays a list of all provisioning rules on the cluster.

|--pool-id <string>

Displays provisioning rules only from the specified pool ID. Specify the pool ID in the following format:

```plaintext
<groupnet_name>.<subnet_name>.<pool_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0:rule3.

|--groupnet <string>

Displays provisioning rules only from the specified groupnet name.

|--subnet <string>

Displays provisioning rules only from subnets with the specified name.

|--pool <string>

Displays provisioning rules only from IP address pools with the specified name.

{ --limit | -l } <integer>

Displays no more than the specified number.

|--sort {id | description | iface | node_type | name}

Sorts output displayed by the specified attribute.

{ --descending | -d}

Displays output in reverse order.

|--format {table | json | csv | list}

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

{ --no-header | -a}

Displays table and CSV output without headers.

`{ --no-footer | -z }
Displays table output without footers.

`{ --verbose | -v }
Displays more detailed information.

**Examples**
The following example displays a list of provisioning rules on a node:

```
isi networks list rules
```

The system displays the list of rules in output similar to the following example:

```
ID                        Node Type  Interface
------------------------- ------------  --------
groupnet0.subnet0.pool0.rule0 any        ext-1
groupnet3.subnet3.pool3.rule3 any        ext-4
------------------------- ------------  --------
Total: 2
```

**isi network rules modify**

Modifies network provisioning rule settings.

**Syntax**

```
isi network rules modify <id>
   [ --description <string> ]
   [ --clear-description ]
   [ --iface <node_interface> ]
   [ --name <string> ]
   [ --node-type { any | storage | accelerator | backup-accelerator } ]
   [ --revert-node-type ]
   [ --verbose ]
```

**Options**

`<id>`

Specifies the ID of the provisioning rule to be modified. Specify the rule ID in the following format:

```
<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0:rule3.

`--description <string>`

Specifies an optional description of the provisioning rule. This option overwrites the existing description. The description cannot exceed 128 bytes.

`--clear-description`

Clears the description of the provisioning rule.

`--iface <node_interface>`
Specifies the network interface name the rule applies to. This option overwrites the existing interface name.

--name <string>

Specifies a new name for the rule. The new rule name must be unique in the pool.

--node-type {any | storage | accelerator | backup-accelerator}

Sets the provisioning rule to apply to one or more of the specified type of node. The default node type is any.

--revert-node-type

Sets the value of --node-type to the system default value.

{--verbose | -v}

Displays more detailed information.

isi network rules view

Displays the configuration details of a specific provisioning rule on the EMC Isilon cluster.

Syntax

isi network rules view <id>

Options

<iid>

Specifies the ID of the provisioning rule to be viewed. Specify the rule ID in the following format:

<groupnet_name>.<subnet_name>.<pool_name>.<rule_name>

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1:pool0:rule3.

isi network sc-rebalance-all

Redistributes IP addresses in all pools on the EMC Isilon cluster.

To redistribute IP addresses in a specific pool, run the isi network pools rebalance-ips command.

Syntax

isi network sc-rebalance-all

[--force]

[--verbose]

Options

{--force | -f}
Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

```
{--verbose | -v}
```

Displays more detailed information.

### isi network subnets create

Creates network subnets.

**Syntax**

```
isi networks create subnet <id> <addr-family> {ipv4 | ipv6} <prefixlen>
```

---

**Options**

**<id>**

Specifies the ID of the new subnet that you want to create. The subnet must be added to an existing groupnet. The ID can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation. Specify the subnet ID in the following format:

```
<groupnet_name>.<subnet_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1. The subnet name must be unique in the groupnet.

**<addr-family>** {ipv4 | ipv6}

Specifies IP address format to be applied to the subnet. All subnet settings and IP address pools added to the subnet must use the specified address format. You cannot modify the address family once the subnet has been created.

**<prefixlen>**

Sets the prefix length of the subnet. Specify a prefix length appropriate for the selected address family.

---

**--description <string>**

Specifies an optional description of the subnet. The description cannot exceed 128 bytes.

---

**--dsr-addrs <ip_address>...**

Sets one or more Direct Server Return addresses for the subnet. If an external hardware load balancer that uses DSR addresses is used, this parameter is required.
--gateway <ip_address>
    Specifies the gateway IP address used by the subnet.

**Note**

The IP address must belong to the appropriate gateway. If no gateway is assigned or an incorrect IP address is specified, communication with the cluster might be disabled.

--gateway-priority <integer>
    Specifies the gateway priority for the subnet. Valid values start at 1. A lower value has a higher priority—for example, a gateway with priority 3 is given priority over a gateway with priority 7. When a new gateway is configured on the system, it is given a default priority of the current lowest priority plus 10 to ensure it does not take priority over existing gateways until you modify the priority level.

--mtu <integer>
    Sets the maximum transmission unit (MTU) of the subnet. Common values are 1500 and 9000.

**Note**

Using a larger frame size for network traffic permits more efficient communication on the external network between clients and cluster nodes. For example, if a subnet is connected through a 10 GbE interface, we recommend that you set the MTU to 9000. To benefit from using jumbo frames, all devices in the network path must be configured to use jumbo frames.

--sc-service-addr <ip_address>
    Specifies the IP address on which the SmartConnect module listens for domain name server (DNS) requests on this subnet.

--vlan-enabled {true | false}
    Enables or disables VLAN tagging on the subnet.

--vlan-id <integer>
    Specifies the VLAN ID for all interfaces in the subnet.

{--verbose | -v}
    Displays more detailed information.

### isi network subnets delete

Deletes a subnet. Clients connected to the EMC Isilon cluster through a pool in the subnet might lose their connection when the subnet is deleted.

Deleting a subnet that is in use can prevent access to the EMC Isilon cluster. Client connections to the cluster through any IP address pool in the deleted subnet will be terminated.

**Syntax**

`isi network subnets delete <id>`

**Note**

Deleting a subnet might cause clients to lose connection to the Isilon cluster.
Options

<iid>...</i>

Specifies the ID of the subnet to be deleted. Specify the subnet ID in the following format:

```
<groupnet_name>.<subnet_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1.

{--force | -f}

Suppresses any prompts, warnings, or confirmation messages that would otherwise appear.

{--verbose | -v}

Displays more detailed information.

isi network subnets list

Displays available subnets.

Syntax

```
isi network subnets list
   [--groupnet-id <string>]
   [--groupnet <string>]
   [{--limit | -l} <integer>]
   [--sort {id | name | addr_family | base_addr | description | gateway | gateway_priority | mtu | prefixlen | sc_service_addr | vlan_enabled | vlan_id}]
   [{--descending | -d}]
   [--format {true | table | json | csv | list}]
   [{--no-header | -a}]
   [{--no-footer | -z}]
   [--verbose]
```

Options

If no options are specified, the command displays a list of all subnets on the cluster.

--groupnet-id <string>

Displays subnets only from the specified groupnet ID.

--groupnet <string>

Displays subnets only from the specified groupnet ID.

{ --limit | -l} <integer>

Displays no more than the specified number.

--sort {id | description | iface | node_type | name}

Sorts output displayed by the specified attribute.

{--descending | -d}

Displays output in reverse order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`{ --no-header | -a }
Displays table and CSV output without headers.

`{ --no-footer | -z }
Displays table output without footers.

`{--verbose | -v}
Displays more detailed information.

**Examples**
The following command displays a list of all subnets:

`isi networks list subnets`

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Subnet</th>
<th>Gateway</th>
<th>Prio</th>
<th>Pools SC Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>--------</td>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>groupnet0.subnet0 10.7.135.0/24</td>
<td>10.7.135.1</td>
<td>10</td>
<td>pool0 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>groupnet3.subnet3 10.7.136.0/24</td>
<td>0.0.0.0</td>
<td>20</td>
<td>pool3 0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

Total: 2

**isi network subnets modify**

Modifies network subnet settings.

**Syntax**

`isi network subnets modify <id>
[--description <string>]
[--clear-description]
[--dsr-address <ip-address>]...
[--clear-dsr-address]
[--add-dsr-address <ip-address>]...
[--remove-dsr-address <ip-address>]...
[--revert-dsr-address]
[--gateway <ip-address>]
[--gateway-priority <integer>]
[--mtu <integer>]
[--revert-mtu]
[--prefixlen <integer>]
[--name <subnet>]
[--sc-service-addr <ip-address>]
[--vlan-enabled {true | false}]
[--revert-vlan-enabled]
[--vlan-id <integer>]
[--force]
[--verbose]

**Options**

`<id>`

Specifies the ID of the subnet that you want to modify. The ID can be up to 32 alphanumeric characters long and can include underscores or hyphens, but
cannot include spaces or other punctuation. Specify the subnet ID in the following format:

```
<groupnet_name>.<subnet_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1.

`--description <string>`
Specifies an optional description of the subnet. This option overwrites the existing description. The description cannot exceed 128 bytes.

`--clear-description`
Clears the description of the subnet.

`--dsr-addrs <ip_address>...`
Sets one or more Direct Server Return addresses for the subnet. If an external hardware load balancer that uses DSR addresses is used, this parameter is required.

`--clear-dsr-addrs`
Removes all DSR addresses from the subnet.

`--add-dsr-addrs <ip_address>...`
Adds one or more Direct Server Return addresses to the subnet.

`--remove-dsr-addrs <ip_address>...`
Removes one or more Direct Server Return addresses from the subnet.

`--revert-dsr-addrs`
Sets the value of `--dsr-addrs` to the system default value.

`--gateway <ip_address>`
Specifies the gateway IP address used by the subnet.

**Note**
The IP address must belong to the appropriate gateway. If no gateway is assigned or an incorrect IP address is specified, communication with the cluster might be disabled.

`--gateway-priority <integer>`
Specifies the gateway priority for the subnet. Valid values start at 1. A lower value has a higher priority—for example, a gateway with priority 3 is given priority over a gateway with priority 7. When a new gateway is configured on the system, it is given a default priority of the current lowest priority plus 10 to ensure it does not take priority over existing gateways until you modify the priority level.

`--mtu <integer>`
Sets the maximum transmission unit (MTU) of the subnet. Common values are 1500 and 9000.
Note

Using a larger frame size for network traffic permits more efficient communication on the external network between clients and cluster nodes. For example, if a subnet is connected through a 10 GbE interface, we recommend that you set the MTU to 9000. To benefit from using jumbo frames, all devices in the network path must be configured to use jumbo frames.

```
--revert-mtu
Sets the value of --mtu to the system default value.

--prefixlen <integer>
Sets the prefix length of the subnet. Specify a prefix length appropriate for the selected address family. This option overwrites the existing prefix length.

--name <string>
Specifies a new name for the subnet. The new subnet name must be unique in the groupnet.

--sc-service-addr <ip_address>
Specifies the address on which SmartConnect listens for DNS requests on this subnet. This option overwrites the existing SmartConnect service address.

--vlan-enabled {true | false}
Enables or disables VLAN tagging on the subnet.

--revert-vlan-enabled
Sets the value of --vlan-enabled to the system default value.

--vlan-id <integer>
Specifies the VLAN ID or tag for all interfaces on this subnet. This option overwrites the existing VLAN ID.
```

```
{--verbose | -v}
Displays more detailed information.

{--force | -f }
Suppresses any prompts or warnings messages that would otherwise appear before or during the subnet modification operation.
```

isi network subnets view

Displays the configuration details of a specific subnet on the EMC Isilon cluster.

**Syntax**

```
isi network subnets view <id>
```

**Options**

```
<id>
```
Specifies the ID of the subnet to be viewed. Specify the subnet ID in the following format:

```
<groupnet_name>.<subnet_name>
```

The groupnet name is optional if referring to the default groupnet0. Colons are also acceptable as delimiters between component names—for example, groupnet0:subnet1.
CHAPTER 27

Hadoop

This section contains the following topics:

- Hadoop overview..................................................................................................1122
- Hadoop architecture..........................................................................................1122
- How Hadoop is implemented on OneFS...........................................................1123
- Hadoop distributions supported by OneFS......................................................1123
- HDFS files and directories...............................................................................1123
- Hadoop user and group accounts.....................................................................1124
- HDFS authentication methods.........................................................................1124
- HDFS and SmartConnect................................................................................1124
- WebHDFS...........................................................................................................1125
- Secure impersonation.......................................................................................1125
- Ambari agent.....................................................................................................1125
- Virtual HDFS racks..........................................................................................1126
- Deploying Hadoop with OneFS.........................................................................1126
- Managing the HDFS service.............................................................................1127
- Set the HDFS root directory...........................................................................1129
- Configuring HDFS authentication methods......................................................1129
- Create a local Hadoop user..............................................................................1131
- Enable or disable WebHDFS within an access zone........................................1132
- Configuring secure impersonation.....................................................................1132
- Configure Ambari agent settings......................................................................1134
- Managing virtual HDFS racks..........................................................................1135
- HDFS commands..............................................................................................1137
Hadoop overview

Hadoop is an open-source platform that runs analytics on large sets of data across a distributed file system.

In a Hadoop implementation on an EMC Isilon cluster, OneFS acts as the distributed file system and HDFS is supported as a native protocol. Clients from a Hadoop cluster connect to the Isilon cluster through the HDFS protocol to manage and process data.

Hadoop support on the cluster requires you to activate an HDFS license. To obtain a license, contact your EMC Isilon sales representative.

Hadoop architecture

Hadoop consists of a compute layer and a storage layer.

In a typical Hadoop implementation, both layers exist on the same cluster.

Compute layer

YARN is the task processing engine of the Hadoop compute layer.

YARN runs a variety of jobs (also known as applications), or queries, on large sets of data and pulls information out. YARN relies on the following key components:

ResourceManager
- Global authority that allocates resources (such as CPU, memory, disk, network) to NodeManagers, and schedules jobs based on their resource requirements.

NodeManager
- Per-node component that launches jobs and monitors job resource consumption.

Storage layer

The storage layer is known as the Hadoop distributed file system (HDFS).

The storage layer contains the data accessed and processed by the compute layer. HDFS relies on two key components:

NameNode
- Node that stores in-memory maps of every file, including information about which DataNode the file resides on and the location of the file on the DataNode.

DataNode
- Node that stores data and serves read and write requests as directed by the NameNode component.

A typical Hadoop implementation contains one NameNode that acts as a master and routes requests for data access to the proper DataNode.
How Hadoop is implemented on OneFS

In a Hadoop implementation on the EMC Isilon cluster, data is stored on OneFS. HDFS is supported as a protocol, which is used by Hadoop compute clients to access data.

A Hadoop implementation with OneFS differs from a typical Hadoop implementation in the following ways:

- The compute and storage layers are on separate clusters instead of the same cluster.
- Instead of storing data within a Hadoop distributed file system, the storage layer functionality is fulfilled by OneFS on an EMC Isilon cluster. Nodes on the Isilon cluster function as both a NameNode and a DataNode.
- The compute layer is established on a Hadoop compute cluster that is separate from the Isilon cluster. MapReduce and its components are installed on the Hadoop compute cluster only.
- Rather than a storage layer, HDFS is implemented on OneFS as a native, lightweight protocol layer between the Isilon cluster and the Hadoop compute cluster. Clients from the Hadoop compute cluster connect over HDFS to access data on the Isilon cluster.
- In addition to HDFS, clients from the Hadoop compute cluster can connect to the Isilon cluster over any protocol that OneFS supports such as NFS, SMB, FTP, and HTTP.
- Hadoop compute clients can connect to any node on the Isilon cluster that functions as a NameNode instead of being routed by a single NameNode.

Hadoop distributions supported by OneFS

You can run most common Hadoop distributions with the EMC Isilon cluster.

OneFS supports many distributions of the Hadoop Distributed File System (HDFS). These distributions are updated independently of OneFS and on their own schedules.

For the latest information about Hadoop distributions that OneFS supports, see the Supported Hadoop Distributions and Products page on the EMC Community Network (ECN).

HDFS files and directories

Before implementing Hadoop, ensure that the directories that you will need are configured on the EMC Isilon cluster.

You configure one HDFS root directory in each access zone that will contain data accessible to Hadoop compute clients. When a Hadoop compute client connects to the cluster, the user can access all files and sub-directories in the specified root directory. The default HDFS directory is /ifs.

Each IP address pool on the cluster must be associated with an access zone. When Hadoop compute clients connect to the cluster through a given IP address pool, the clients can access only the HDFS data in the associated access zone. This configuration isolates data within access zones and allows you to restrict client access to the data.

Unlike NFS mounts or SMB shares, clients connecting to the cluster through HDFS cannot be given access to individual folders within the root directory. If you have
multiple Hadoop workflows that require separate sets of data, you can create multiple access zones and configure a unique HDFS root directory for each zone.

When you set up directories and files under the root directory, ensure that they have the correct permissions so that Hadoop clients and applications can access them. Directories and permissions will vary by Hadoop distribution, environment, requirements, and security policies.

**Hadoop user and group accounts**

Before implementing Hadoop, ensure that the user and groups accounts that you will need to connect over HDFS are configured on the EMC Isilon cluster.

You must also ensure that the user accounts that your Hadoop distribution requires are configured on the Isilon cluster on a per-zone basis. The user accounts that you need and the associated owner and group settings vary by distribution, requirements, and security policies. The profiles of the accounts, including UIDs and GIDS, on the Isilon cluster should match those of the accounts on your Hadoop compute clients.

OneFS must be able to look up a local Hadoop user or group by name. If there are no directory services, such as Active Directory or LDAP, that can perform a user lookup, you must create a local Hadoop user or group. If directory services are available, a local user account or user group is not required.

**HDFS authentication methods**

You can configure an HDFS authentication method on a per-access zone basis.

When a Hadoop compute client connects to the EMC Isilon cluster through an access zone, the client must authenticate with the method specified for that access zone. HDFS supports simple authentication, Kerberos authentication, or both. By default, HDFS accepts both simple and Kerberos authentication.

**HDFS and SmartConnect**

You can configure a SmartConnect DNS zone to manage connections from Hadoop compute clients.

SmartConnect is a module that specifies how the DNS server on the EMC Isilon cluster handles connection requests from clients. For each IP address pool on your Isilon cluster, you can configure a SmartConnect DNS zone which is a fully qualified domain name (FQDN). Hadoop compute clients can connect to the cluster through the SmartConnect DNS zone name, and SmartConnect evenly distributes NameNode requests across IP addresses and nodes in the pool.

When a Hadoop compute client makes an initial DNS request to connect to the SmartConnect zone, the Hadoop client is routed to the IP address of an Isilon node that serves as a NameNode. Subsequent requests from the Hadoop compute client go the same node. When a second Hadoop client makes a DNS request for the SmartConnect zone, SmartConnect balances traffic and routes the client connection to a different node than that used by the previous Hadoop compute client.

If you specify a SmartConnect DNS zone that you want Hadoop compute clients to connect through, you must add a new name server (NS) record as a delegated domain to the authoritative DNS zone that contains the Isilon cluster. On the Hadoop compute cluster, you must set the value of the `fs.defaultFS` property to the SmartConnect DNS zone name in the `core-site.xml` file.
SmartConnect is discussed in further detail in the Networking section of this guide.

### WebHDFS

OneFS supports access to HDFS data through WebHDFS client applications. WebHDFS is a RESTful programming interface based on HTTP operations such as GET, PUT, POST, and DELETE that is available for creating client applications. WebHDFS client applications allow you to access HDFS data and perform HDFS operations through HTTP and HTTPS.

WebHDFS is supported by OneFS on a per-access zone basis and is enabled by default.

WebHDFS supports simple authentication or Kerberos authentication. If the HDFS authentication method for an access zone is set to All, OneFS uses simple authentication for WebHDFS.

**Note**

To prevent unauthorized client access through simple authentication, disable WebHDFS in each access zone that should not support it.

### Secure impersonation

Secure impersonation enables you to create proxy users that can impersonate other users to run Hadoop jobs.

You might configure secure impersonation if you use applications, such as Apache Oozie, to automatically schedule, manage, and run Hadoop jobs. For example, you can create an Oozie proxy user that securely impersonates a user called HadoopAdmin, which allows the Oozie user to request that Hadoop jobs be performed by the HadoopAdmin user.

You configure proxy users for secure impersonation on a per–zone basis, and users or groups of users that you assign as members to the proxy user must be from the same access zone. A member can be one or more of the following identity types:

- User specified by user name or UID
- Group of users specified by group name or GID
- User, group, machine, or account specified by SID
- Well-known user specified by name

If the proxy user does not present valid credentials or if a proxy user member does not exist on the cluster, access is denied. The proxy user can only access files and subdirectories located in the HDFS root directory of the access zone. It is recommended that you limit the members that the proxy user can impersonate to users that have access only to the data the proxy user needs.

### Ambari agent

The Ambari client/server framework is a third-party tool that enables you to configure, manage, and monitor a Hadoop cluster through a browser-based interface.

The Ambari agent is configured per access zone; you can configure the OneFS Ambari agent in any access zone that contains HDFS data. To start an Ambari agent in an access zone, you must specify the IPv4 address of the external Ambari server and the address of a NameNode that acts as the point of contact for the access zone.
The external Ambari server receives communications from the OneFS Ambari agent. Once the Ambari agent assigned to the access zone registers with the Ambari server, the agent provides a heartbeat status at regular intervals. The OneFS Ambari agent does not provide metrics or alerts to the Ambari server. The external Ambari server must be specified by a resolvable hostname, FQDN, or IPv4 address and must be assigned to an access zone.

The NameNode is the designated point of contact in an access zone that Hadoop services managed through the Ambari interface should connect through. For example, if you manage services such as YARN or Oozie through the Ambari interface, the services will connect to the access zone through the specified NameNode. The Ambari agent communicates the location of the designated NameNode to the Ambari server, and to the Ambari interface, the NameNode represents the access zone. If you change the designated NameNode address, the Ambari agent will inform the Ambari server. The NameNode must be a resolvable SmartConnect zone name or an IP address from the IP address pool associated with the access zone.

---

**Note**

The specified NameNode value maps to the NameNode, secondary NameNode, and DataNode components on the Ambari interface.

---

The OneFS Ambari agent is based on the Apache Ambari framework and is compatible with multiple Ambari server versions. For a complete list, see the Supported Hadoop Distributions and Products page on the EMC Community Network (ECN).

---

**Virtual HDFS racks**

You can create a virtual HDFS rack of nodes on the EMC Isilon cluster to optimize performance and reduce latency when accessing HDFS data.

OneFS enables you to specify a group of preferred HDFS nodes on the EMC Isilon cluster and an associated group of Hadoop compute clients as a virtual HDFS rack. Virtual HDFS racks allow you to fine-tune client connectivity by directing Hadoop compute clients to go through quicker, less-busy switches or to faster nodes, depending on your network topology.

When a Hadoop compute client from the specified group connects to the cluster, OneFS returns at least two IP addresses from the group of preferred HDFS nodes. You specify the preferred HDFS nodes by IP address pool. IP address pools in the IPv6 family are not supported by virtual HDFS racks.

---

**Deploying Hadoop with OneFS**

To support Hadoop on the EMC Isilon cluster, you must configure HDFS on the Isilon cluster to communicate with a Hadoop cluster.

The process for configuring HDFS on the Isilon cluster is summarized in the following list:

- Activate a license for HDFS. When a license is activated, the HDFS service is enabled by default.
- Create directories on the cluster that will be set as HDFS root directories.
- Create a SmartConnect zone for balancing connections from Hadoop compute clients.
Create local Hadoop users in access zones that do not have directory services such as Active Directory or LDAP.

- Set the HDFS root directory in each access zone that supports HDFS connections.
- Enable or disable WebHDFS in each access zone.
- Set an authentication method in each access zone that supports HDFS connections.
- Configure HDFS service settings on the cluster.
- Configure proxy users for secure impersonation.
- Configure virtual HDFS racks.

**Managing the HDFS service**

You can configure HDFS service settings on the EMC Isilon cluster to improve performance for HDFS workflows.

**Enable or disable the HDFS service**

The HDFS service, which is enabled by default after you activate an HDFS license, can be enabled or disabled per access zone.

**Procedure**

1. Run the `isi hdfs settings modify` command.

   The following command enables the HDFS service in zone3:

   ```bash
   isi hdfs settings modify --service=yes --zone=zone3
   ```

   The following command disables the HDFS service in zone3:

   ```bash
   isi hdfs settings modify --service=no --zone=zone3
   ```

**Configure HDFS service settings**

You can configure HDFS service settings in each zone to improve performance for HDFS workflows.

**Procedure**

1. Run the `isi hdfs settings modify` command.

   The following command sets the block size to 256 KB in the zone3 access zone:

   ```bash
   isi hdfs settings modify --default-block-size=256K --zone=zone3
   ```

   You must specify the block size in bytes. Suffixes K, M, and G are allowed.

   The following command sets the checksum type to crc32 in the zone3 access zone:

   ```bash
   isi hdfs settings modify --default-checksum-type=crc32 --zone=zone3
   ```
HDFS service settings

HDFS service settings affect the performance of HDFS workflows.

You can configure the following HDFS service settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block size</td>
<td>The HDFS block size setting on the EMC cluster determines how the HDFS service returns data upon read requests from Hadoop compute client. You can modify the HDFS block size on the cluster to increase the block size from 4 KB up to 1 G. The default block size is 128 MB. Increasing the block size enables the Isilon cluster nodes to read and write HDFS data in larger blocks and optimize performance for most use cases. The Hadoop cluster maintains a different block size that determines how a Hadoop compute client writes a block of file data to the Isilon cluster. The optimal block size depends on your data, how you process your data, and other factors. You can configure the block size on the Hadoop cluster in the hdfs-site.xml configuration file in the dfs.block.size property.</td>
</tr>
<tr>
<td>Checksum type</td>
<td>The HDFS service sends the checksum type to Hadoop compute clients, but it does not send any checksum data, regardless of the checksum type. The default checksum type is set to None. If your Hadoop distribution requires sending a checksum type other than None to the client, you can set the checksum type to CRC32 or CRC32C.</td>
</tr>
</tbody>
</table>

View HDFS settings

You can view HDFS settings in an access zone.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and then log in.
2. Run the isi hdfs settings view command.
   
   The following command displays the HDFS settings in the zone1 access zone:

   ```
   isi hdfs settings view --zone=zone1
   ```

   The system displays output similar to the following example:

   ```
   Service: Yes
   Default Block Size: 128M
   Default Checksum Type: none
   HDFS Authentication: all
   HDFS Root Directory: /ifs/zone1/hdfsdata/home
   WebHDFS Enabled: Yes
   HDFS Ambari Server: -
   HDFS Ambari Namenode: -
   ```

Modify HDFS log levels

You can set the default logging level of HDFS services events for any node on the EMC Isilon cluster.

This procedure is available only through the command-line interface
Procedure

1. Open a secure shell (SSH) connection to a node in the cluster and log in.
2. Run the `isi hdfs log-level modify` command.

The following command sets the HDFS log level to trace on the node:

```
isi hdfs log-level modify --set=trace
```

View HDFS log levels

You can view the default logging level of HDFS services events for any node on the EMC Isilon cluster.

This procedure is available only through the command-line interface

Procedure

1. Open a secure shell (SSH) connection to a node in the cluster and log in.
2. Run the `isi hdfs log-level view` command.

The system displays output similar to the following example:

```
Current HDFS service log-level at the node is: trace
```

Set the HDFS root directory

You can configure one HDFS root directory in each access zone. Hadoop compute clients that connect to the access zone can only access subdirectories and files within the root directory hierarchy.

Before you begin

The directory structure you want to set as the root path should already exist on the OneFS file system.

Procedure

1. Run the `isi hdfs settings modify` command.

The following command specifies that Hadoop compute clients connecting to the zone3 access zone are given access to the `/ifs/data/hadoop` directory:

```
isi hdfs settings modify --root-directory=/ifs/zone3/hadoop --zone3
```

Configuring HDFS authentication methods

You can configure an HDFS authentication method on a per-access zone basis.

If you want Hadoop compute clients running Hadoop 2.2 and later to connect to an access zone through Kerberos, you must Configure HDFS authentication properties on the Hadoop client.
Set the HDFS authentication method

You can configure the HDFS authentication method in each access zone. Hadoop compute clients that connect to an access zone are authenticated using the specified authentication method.

Before you begin

If you want to Hadoop clients to connect to an access zone through Kerberos, a Kerberos authentication provider must be configured and added to the access zone.

Procedure

1. Run the `isi hdfs settings modify` command.

The following command specifies that Hadoop compute clients connecting to the zone3 must be identified through the simple authentication method:

   ```
   isi hdfs settings modify --authentication-mode=simple_only --zone3
   ```

   The following command specifies that Hadoop compute clients connecting to zone3 must be identified through the Kerberos authentication method:

   ```
   isi zone zones modify zone3 --authentication-mode=kerberos_only
   ```

After you finish

To ensure that users can authenticate through Kerberos, you must modify the `core-site.xml` file on clients running Hadoop 2.2 and later.

Supported HDFS authentication methods

The authentication method determines what credentials are required by OneFS to establish a Hadoop compute client connection.

An HDFS authentication method is specified for each access zone. OneFS supports the following authentication methods for HDFS:

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple only</td>
<td>Requires only a user name to establish client connections.</td>
</tr>
<tr>
<td>Kerberos only</td>
<td>Requires Kerberos credentials to establish client connections.</td>
</tr>
</tbody>
</table>

**Note**

You must configure Kerberos as an authentication provider on the EMC Isilon cluster, and you must modify the `core-site.xml` file on clients running Hadoop 2.2 and later.

| All (default value) | Accepts both simple authentication and Kerberos credentials. If Kerberos settings and file modifications are not completed, client connections default to simple authentication. |
Configure HDFS authentication properties on the Hadoop client

If you want Hadoop compute clients running Hadoop 2.2 and later to connect to an access zone through Kerberos, you must make some modifications to the core-site.xml and hdfs-site.xml files on the Hadoop clients.

Before you begin

Kerberos must be set as the HDFS authentication method in the access zone and a Kerberos authentication provider must be configured and assigned to the access zone.

Procedure

1. Go to the $HADOOP_CONF directory on your Hadoop client.
2. Open the core-site.xml file in a text editor.
3. Set the value of the hadoop.security.token.service.use_ip property to false as shown in the following example:

   
   <property>
   <name>hadoop.security.token.service.use_ip</name>
   <value>false</value>
   </property>

4. Save and close the core-site.xml file.
5. Open the hdfs-site.xml file in a text editor.
6. Set the value of the dfs.namenode.kerberos.principal.pattern property to the Kerberos realm configured in the Kerberos authentication provider as shown in the following example:

   
   <property>
   <name>dfs.namenode.kerberos.principal.pattern</name>
   <value>hdfs/*@storage.company.com</value>
   </property>

7. Save and close the hdfs-site.xml file.

Create a local Hadoop user

OneFS must be able to look up a local Hadoop user by name. If there are no directory services in an access zone that can perform a user lookup, you must create a local Hadoop user that maps to a user on a Hadoop compute client for that access zone. If directory services are available, a local user account is not required.

Procedure

1. Run the isi auth users create command.
The following command creates a user named hadoop-user1 and assigns the user to the local authentication provider in the zone3 access zone:

```
isi auth users create --name=hadoop-user1 --provider=local --zone=zone3
```

Enable or disable WebHDFS within an access zone

You can specify whether access to HDFS data through WebHDFS client applications is supported in each access zone.

**Procedure**

1. Run the `isi hdfs settings modify` command.

   The following command enables WebHDFS in zone3:

   ```
   isi hdfs settings modify --webhdfs-enabled=yes --zone=zone3
   ```

   The following command disables WebHDFS in zone3:

   ```
   isi hdfs settings modify --webhdfs-enabled=no --zone=zone3
   ```

Configuring secure impersonation

Configure and manage proxy users that can securely impersonate other users and groups.

**Note**

Names cannot contain the following invalid characters:

```
" /\[::|+=*?<>}
```

Create a proxy user

You can create a proxy user by designating an existing user to securely impersonate another user or a group of users.

**Procedure**

1. Run the `isi hdfs proxyusers create` command.

   The following command designates hadoop-user23 in zone1 as a new proxy user:

   ```
   isi hdfs proxyusers create hadoop-user23 --zone=zone1
   ```

   The following command designates hadoop-user23 in zone1 as a new proxy user and adds the group hadoop-users to the list of members that the proxy user can impersonate:

   ```
   isi hdfs proxyusers create hadoop-user23 --zone=zone1 --add-group=hadoop-users
   ```
The following command designates hadoop-user23 in zone1 as a new proxy user and adds UID 2155 to the list of members that the proxy user can impersonate:

\[
\text{isi hdfs proxyusers create hadoop-user23 --zone=zonel --add-UID=2155}
\]

Modify a proxy user

You can modify the list of members that a proxy user securely impersonates.

Procedure

1. Run the `isi hdfs proxyusers modify` command.

The following command removes a user with the user ID 2155 and adds a well-known user named LOCAL to the list of members for proxy user hadoop-user23 in zone1:

\[
\text{isi hdfs proxyusers modify hadoop-user23 --zone=zonel --add-wellknown=LOCAL --remove-uid=2155}
\]

Delete a proxy user

You can delete a proxy user from an access zone.

Procedure

1. Run the `isi hdfs proxyusers delete` command.

The following command deletes the proxy user hadoop-user23 from the zone1 access zone:

\[
\text{isi hdfs proxyusers delete hadoop-user23 --zone=zonel}
\]

List the members of a proxy user

You can display the list of users and groups, known as members, assigned to a proxy user. The proxy user can securely impersonate any user in the member list.

Procedure

1. Run the `isi hdfs proxyusers members list` command.

The following command displays a detailed list of the users and groups of users that are members of proxy user hadoop-user23 in zone1:

\[
\text{isi hdfs proxyusers members list hadoop-user23 --zone=zonel -v}
\]

The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Type: user</th>
<th>Name: krb_user_005</th>
<th>ID: UID:1004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: group</td>
<td>Name: krb_users</td>
<td>ID: SID:S-1-22-2-1003</td>
</tr>
<tr>
<td>Type: wellknown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
View proxy users

You can view a list of all proxy users in an access zone and view individual proxy user details.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. To view a list of all proxy users configured in a specific access zone, run the `isi hdfs proxyusers list` command.

   The following command displays a list of all proxy users configured in zone1:

   ```
   isi hdfs proxyusers list --zone=zone1
   ```

   The system displays output similar to the following example:

   ```
   Name
   -----------------
   hadoop-user23
   hadoop-user25
   hadoop-user28
   -----------------
   Total: 3
   ```

3. To view the configuration details for a specific proxy user, run the `isi hdfs proxyusers view` command.

   The following command displays the configuration details for the hadoop-user23 proxy user in zone1:

   ```
   isi hdfs proxyusers view hadoop-user23 --zone=zone1
   ```

   The system displays output similar to the following example:

   ```
   Name: hadoop-user23
   Members: krb_users
   LOCAL
   krb_user_004
   ```

Configure Ambari agent settings

You can configure Ambari agent support in each access zone that contains HDFS data.

Procedure

1. Run the `isi hdfs settings modify` command.

   The following command specifies company.ambari.server.com as the external Ambari server that receives communication from the Ambari agent running in the zone3 access zone:

   ```
   isi hdfs settings modify \
   --ambari-server=company.ambari.server.com \
   --zone=zone3
   ```
The following command designates 192.168.205.5 as the point of contact in the zone3 access zone for Hadoop services managed through the Ambari interface:

```
isi hdfs settings modify  
   --ambari-namenode=192.168.205.5 
   --zone=zone3
```

**Managing virtual HDFS racks**

You can manage virtual HDFS racks of nodes on the EMC Isilon cluster. A virtual HDFS rack is a pool of nodes on the Isilon cluster associated with a pool of Hadoop compute clients. You can create, modify, delete, and view virtual racks.

**Create a virtual HDFS rack**

You can create a virtual HDFS rack of nodes on the EMC Isilon cluster to optimize performance and reduce latency when accessing HDFS data.

**Procedure**

1. Run the `isi hdfs racks create` command.

   A rack name begins with a forward slash—for example, `/hdfs-rack2`.

   The following command creates a rack named `/hdfs-rack2` in the zone5 access zone:

   ```
   isi hdfs racks create /hdfs-rack2 --zone=zone5
   ```

   The following command creates a rack named `hdfs-rack2` in the zone5 access zone, specifies 120.135.26.10-120.135.26.20 as the IP address range of Hadoop compute clients associated with the rack, and specifies `subnet0:pool0` as the IP address pool of Isilon nodes assigned to the rack:

   ```
   isi hdfs racks create /hdfs-rack2 --zone=zone5 --client-ip-ranges=120.135.26.10-120.135.26.20 --ip-pools=subnet0:pool0
   ```

**Modify a virtual HDFS rack**

You can modify the settings of a virtual HDFS rack.

**Procedure**

1. Run the `isi hdfs racks modify` command.

   A rack name begins with a forward slash—for example, `/hdfs-rack2`.

   The following command renames a rack named `/hdfs-rack2` in the zone3 access zone to `/hdfs-rack5`:

   ```
   isi hdfs racks modify /hdfs-rack2 --new-name=/hdfs-rack5 --zone=zone3
   ```
The following command adds 120.135.26.30-120.135.26.40 to the list of existing Hadoop compute client IP addresses assigned to /hdfs-rack2 in the zone3 access zone:

```
isi hdfs racks modify /hdfs-rack2 --add-client-ip-ranges=120.135.26.30-120.135.26.40 --zone=zone3
```

In addition to adding a new range to the list of existing ranges, you can modify the client IP address ranges by replacing the current ranges, deleting a specific range or deleting all ranges.

The following command replaces the existing IP pools with subnet1:pool1 and subnet2:pool2 assigned to /hdfs-rack2 in the zone3 access zone:

```
isi hdfs racks modify /hdfs-rack2 --ip-pools=subnet1:pool1,subnet2:pool2 --zone=zone3
```

In addition to replacing the list of existing pools with new pools, you can modify the IP pools by adding pools to the list of current pools, deleting a specific pool or deleting all pools.

### Delete a virtual HDFS rack

You can delete a virtual HDFS rack from an access zone.

**Procedure**

1. Run the `isi hdfs racks delete` command.
   
   A rack name begins with a forward slash—for example, /hdfs-rack2.
   
   The following command deletes the virtual HDFS rack named /hdfs-rack2 from the zone1 access zone:

   ```
   isi hdfs racks delete /hdfs-rack2 --zone=zone1
   ```

2. At the prompt, type `yes`.

### View virtual HDFS racks

You can view a list of all virtual HDFS racks in an access zone and view individual virtual rack details.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.

2. To view a list of all virtual HDFS racks configured in an access zone, run the `isi hdfs racks list` command.
   
   The following command lists all HDFS racks configured in the zone1 access zone:

   ```
   isi hdfs racks list --zone=zone1
   ```

   The system displays output similar to the following example:

   ```
   Name        Client IP Ranges        IP Pools
   -----------------------------------------------
   ```
The following command displays setting details for all virtual HDFS racks configured in the zone1 access zone:

```
isi hdfs racks list --zone=zone1 -v
```

The system displays output similar to the following example:

```
Name: /hdfs-rack1
Client IP Ranges: 10.20.30.40-10.20.30.50
IP Pools: subnet0:pool0

Name: /hdfs-rack2
Client IP Ranges: 20.10.30.10-20.10.30.20
IP Pools: subnet1:pool1
```

3. To view the setting details for a specific virtual HDFS rack, run the `isi hdfs racks view` command:

```
isi hdfs racks view /hdfs-rack2 --zone=zone1
```

The system displays output similar to the following example:

```
Name: /hdfs-rack2
Client IP Ranges: 20.10.30.10-20.10.30.20
IP Pools: subnet1:pool1
```

**HDFS commands**

You can access and configure the HDFS service through the HDFS commands.

**isi hdfs log-level modify**

Modifies the log level of the HDFS service on the node.

**Syntax**

```
isi hdfs log-level modify
   [--set {always|error|warning|info|verbose|debug|trace|default} ]
   [--verbose| -v]
```

**Options**

```
--set {always | error | warning | info | verbose | debug | trace | default}
```
Sets the default logging level for the HDFS service on the cluster. The default value is default.

--verbose | -v
Displays more detailed information.

isi hdfs log-level view
Displays the current log level of the HDFS service on the node.

Syntax
isi hdfs log-level view

Options
There are no options for this command.

isi hdfs proxyusers create
Creates a proxy user that can securely impersonate another user or group.

Syntax
isi hdfs proxyusers create <proxyuser-name>  
[--zone <zone-name>]  
[--add-group <group-name>...]  
[--add-gid <group-identifier>...]  
[--add-user <user-name>...]  
[--add-sid <security-identifier>...]  
[--add-wellknown <well-known-name>...]  
[--verbose]

Options

<proxyuser-name>
Specifies the user name of a user currently configured on the cluster to be designated as a proxy user.

--zone <zone-name>
Specifies the access zone the user authenticates through.

--add-group <group-name>...
Adds the group specified by name to the list of proxy user members. The proxy user can impersonate any user in the group. The users in the group must authenticate to the same access zone as the proxy user. You can specify multiple group names in a comma-separated list.

--add-gid <group-identifier>...
Adds the group by specified by UNIX GID to the list of proxy user members. The proxy user can impersonate any user in the group. The users in the group must authenticate to the same access zone as the proxy user. You can specify multiple UNIX GIDs in a comma-separated list.

--add-user <user-name>...
Adds the user specified by name to the list of members the proxy user can impersonate. The user must authenticate to the same access zone as the proxy user. You can specify multiple user names in a comma-separated list.

--add-uid <user-identifier>...

Adds the user specified by UNIX UID to the list of members the proxy user can impersonate. The user must authenticate to the same access zone as the proxy user. You can specify multiple UNIX UIDs in a comma-separated list.

--add-sid <security-identifier>...

Adds the user, group of users, machine or account specified by Windows SID to the list of proxy user members. The object must authenticate to the same access zone as the proxy user. You can specify multiple Windows SIDs in a comma-separated list.

--add-wellknown <well-known-name>...

Adds the well-known user specified by name to the list of members the proxy user can impersonate. The well-known user must authenticate to the same access zone as the proxy user. You can specify multiple well-known user names in a comma-separated list.

{ --verbose | -v }

Displays more detailed information.

Examples

The following command designates hadoop-user23 in zone1 as a new proxy user:

```
isi hdfs proxyusers create hadoop-user23 --zone=zone1
```

The following command designates hadoop-user23 in zone1 as a new proxy user and adds the group of users named hadoop-users to the list of members that the proxy user can impersonate:

```
isi hdfs proxyusers create hadoop-user23 --zone=zone1 --add-group=hadoop-users
```

The following command designates hadoop-user23 in zone1 as a new proxy user and adds UID 2155 to the list of members that the proxy user can impersonate:

```
isi hdfs proxyusers create hadoop-user23 --zone=zone1 --add-UID=2155
```

**isi hdfs proxyusers modify**

Modifies a proxy user that can securely impersonate another user or group.

**Syntax**

```
isi hdfs proxyusers modify <proxyuser-name>
    [--zone <zone-name>]
    [--add-group <group-name>...]
    [--add-gid <group-identifier>...]
    [--add-user <user-name>...]
    [--add-uid <user-identifier>...]
    [--add-sid <security-identifier>...]
```
Options

<proxyuser-name>
   Specifies the user name of the proxy user to be modified.

--zone <zone-name>
   Specifies the access zone that the proxy user authenticates through.

--add-group <group-name>...
   Adds the group specified by name to the list of proxy user members. The proxy user can impersonate any user in the group. The users in the group must authenticate to the same access zone as the proxy user. You can specify multiple group names in a comma-separated list.

--add-gid <group-identifier>...
   Adds the group specified by UNIX GID to the list of proxy user members. The proxy user can impersonate any user in the group. The users in the group must authenticate to the same access zone as the proxy user. You can specify multiple UNIX GIDs in a comma-separated list.

--add-user <user-name>...
   Adds the user specified by name to the list of members the proxy user can impersonate. The user must authenticate to the same access zone as the proxy user. You can specify multiple user names in a comma-separated list.

--add-uid <user-identifier>...
   Adds the user specified by UNIX UID to the list of members the proxy user can impersonate. The user must authenticate to the same access zone as the proxy user. You can specify multiple UNIX UIDs in a comma-separated list.

--add-sid <security-identifier>...
   Adds the user, group of users, machine or account specified by Windows SID to the list of proxy user members. The object must authenticate to the same access zone as the proxy user. You can specify multiple Windows SIDs in a comma-separated list.

--add-wellknown <well-known-name>...
   Adds the well-known user specified by name to the list of members the proxy user can impersonate. The well-known user must authenticate to the same access zone as the proxy user. You can specify multiple well-known user names in a comma-separated list.

--remove-group <group-name>...
   Removes the group specified by name from the list of proxy user members so that the proxy user can no longer impersonate any user in the group. You can specify multiple group names in a comma-separated list.
--remove-gid <group-identifier>...
Removes the group specified by UNIX GID from the list of proxy user members so that the proxy user can no longer impersonate any user in the group. You can specify multiple UNIX GIDs in a comma-separated list.

--remove-user <user-name>...
Removes the user specified by name from the list of members the proxy user can impersonate. You can specify multiple user names in a comma-separated list.

--remove-uid <user-identifier>...
Removes the user specified by UNIX UID from the list of members the proxy user can impersonate. You can specify multiple UNIX UIDs in a comma-separated list.

--remove-sid <security-identifier>...
Removes the user, group of users, machine or account specified by Windows SID from the list of proxy user members. You can specify multiple Windows SIDs in a comma-separated list.

--remove-wellknown <well-known-name>...
Removes the well-known user specified by name from the list of members the proxy user can impersonate. You can specify multiple well-known user names in a comma-separated list.

{---verbose | -v}
Displays more detailed information.

Examples
The following command adds the well-known local user to, and removes the user whose UID is 2155 from, the list of members for proxy user hadoop-user23 in zone1:

```
isi hdfs proxyusers modify hadoop-user23 --zone=zone1 \
--add-wellknown=local --remove-uid=2155
```

**isi hdfs proxyusers delete**

Deletes a proxy user.

**Syntax**

```
isi hdfs proxyusers delete <proxyuser-name> 
[--zone <zone-name>]
[--force]
[--verbose]
```

**Options**

**<proxyuser-name>**
Specifies the user name of the proxy user to be deleted.

**--zone <zone-name>**
Specifies the access zone that the proxy user authenticates through.

{---force | -f}
Deletes the specified proxy user without requesting confirmation.
{ --verbose | -v}
   Displays more detailed information.

Examples
The following command deletes hadoop-user23 in zone1 from the list of proxy users:

    isi hdfs proxyusers delete hadoop-user23 --zone=zone1

**isi hdfs proxyusers members list**

Displays the users and groups of users, known as members, that can be impersonated by a proxy user.

Syntax

    isi hdfs proxyusers members list <proxyuser-name>
        [--zone <zone-name>]
        [--format {table | json | csv | list}]
        [--no-header ]
        [--no-footer ]
        [--verbose]  

Options

**<proxyuser-name>**
   Specifies the name of the proxy user.

**--zone <zone-name>**
   Specifies the access zone the proxy user authenticates through.

**--format {table | json | csv | list}**
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

**--no-header**
   Displays table and CSV output without headers.

**--no-footer**
   Displays table output without footers.

{ --verbose | -v}
   Displays more detailed information.

Examples
The following command displays a detailed list of the users and groups that are members of proxy user hadoop-user23 in zone1:

    isi hdfs proxyusers members list hadoop-user23 --zone=zone1 -v

The system displays output similar to the following example:

    Type: user
    Name: krb_user_005
    ID: UID:1004
isi hdfs proxyusers list

Displays all proxy users that are configured in an access zone.

Syntax

```bash
isi hdfs proxyusers list
    [--zone <zone-name>]
    [--format {table | json | csv | list}]
    [--no-header ]
    [--no-footer ]
    [--verbose]
```

Options

--zone <zone-name>
  Specifies the name of the access zone.

--format {table | json | csv | list}
  Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

--no-header
  Displays table and CSV output without headers.

--no-footer
  Displays table output without footers.

{ --verbose | -v}
  Displays more detailed information.

Examples

The following command displays a list of all proxy users that are configured in zone1:

```bash
isi hdfs proxyusers list --zone=zone1
```

The system displays output similar to the following example:

```
Name
------
hadoop-user23
hadoop-user25
hadoop-user28
------
Total: 3
```
isi hdfs proxyusers view

Displays the configuration details of a specific proxy user.

Syntax

isi hdfs proxyusers view <proxyuser-name>
   [--zone <zone-name>]

Options

<proxyuser-name>
   Specifies the user name of the proxy user.

--zone <zone-name>
   Specifies the access zone the proxy user authenticates through.

Examples

The following command displays the configuration details for the hadoop-user23 proxy user in zone1:

```
isi hdfs proxyusers view hadoop-user23 --zone=zone1
```

The system displays output similar to the following example:

```
Name: hadoop-user23
Members: krb_users
       LOCAL
       krb_user_004
```

isi hdfs racks create

Creates a new virtual HDFS rack.

Syntax

isi hdfs racks create <rack-name>
   [--client-ip-ranges <low-ip-address>-<high-ip-address>]...
   [--ip-pools <subnet>:<pool>]...
   [--zone <string>]
   [--verbose]

Options

<rack-name>
   Specifies the name of the virtual HDFS rack. The rack name must begin with a forward slash—for example, /example-name.

--client-ip-ranges <low-ip-address>-<high-ip-address>...
   Specifies IP address ranges of external Hadoop compute clients assigned to the virtual rack.

--ip-pools <subnet>:<pool>...
   Assigns a pool of Isilon cluster IP addresses to the virtual rack.
--zone <string>
  Specifies the access zone that will contain the virtual rack.

{--verbose | -v}
  Displays more detailed information.

**isi hdfs racks modify**

Modifies a virtual HDFS rack.

**Syntax**

```plaintext
isi hdfs racks modify <rack-name>
  [--name <rack-name>]
  [--client-ip-ranges <low-ip-address>-<high-ip-address>]
  [--add-client-ip-ranges <low-ip-address>-<high-ip-address>]
  [--remove-client-ip-ranges <low-ip-address>-<high-ip-address>]
  [--clear-client-ip-ranges]
  [--ip-pools <subnet>:<pool>]
  [--add-ip-pools <subnet>:<pool>]
  [--remove-ip-pools <subnet>:<pool>]
  [--clear-ip-pools]
  [--zone <string>]
  [--verbose]
```

**Options**

**<rack-name>*
  Specifies the virtual HDFS rack to be modified. Each rack name begins with a forward slash—for example /example-name.

**--name <rack-name>*
  Assigns a new name to the specified virtual rack. The rack name must begin with a forward slash—for example /example-name.

**--client-ip-ranges <low-ip-address>-<high-ip-address>*
  Specifies IP address ranges of external Hadoop compute clients assigned to the virtual rack. The value assigned through this option overwrites any existing IP address ranges. You can add a new range through the --add-client-ip-ranges option.

**--add-client-ip-ranges <low-ip-address>-<high-ip-address>*
  Adds a specified IP address range of external Hadoop compute clients to the virtual rack.

**--remove-client-ip-ranges <low-ip-address>-<high-ip-address>*
  Removes a specified IP address range of external Hadoop compute clients from the virtual rack. You can only remove an entire range; you cannot delete a subset of a range.

**--clear-client-ip-ranges*
  Removes all IP address ranges of external Hadoop compute clients from the virtual rack.

**--ip-pools <subnet>:<pool>*
  Hadoop
Assigns pools of Isilon node IP addresses to the virtual rack. The value assigned through this option overwrites any existing IP address pools. You can add a new pool through the --add-ip-pools option.

--add-ip-pools <subnet>:<pool>...
   Adds a specified pool of Isilon cluster IP addresses to the virtual rack.

--remove-ip-pools <subnet>:<pool>...
   Removes a specified pool of Isilon cluster IP addresses from the virtual rack.

--clear-ip-pools
   Removes all pools of Isilon cluster IP addresses from the virtual rack.

--zone <string>
   Specifies the access zone that contains the virtual rack you want to modify.

{---verbose | -v}
   Displays more detailed information.

isi hdfs racks delete

Deletes a virtual HDFS rack.

Syntax

isi hdfs racks delete <rack-name>
   [--zone <string>]
   [--force]
   [--verbose]

Options

<rack-name>
   Deletes the specified virtual HDFS rack. Each rack name begins with a forward slash—for example, /example-name.

--zone <string>
   Specifies the access zone that contains the virtual rack you want to delete.

{---force | -f}
   Suppresses command-line prompts and messages.

{---verbose | -v}
   Displays more detailed information.

isi hdfs racks list

Lists the HDFS racks in an access zone.

Syntax

isi hdfs racks list
Options

--zone <string>
   Specifies the access zone. The system displays all virtual racks in the specified zone.

{--verbose | -v}
   Displays more detailed information.

isi hdfs racks view

Displays information for a specific virtual HDFS rack.

Syntax

isi hdfs racks view <rack-name>
   [--zone <string>]

Options

<rack-name>
   Specifies the name of the virtual HDFS rack to view. Each rack name begins with a forward slash—for example, /example-name.

--zone <string>
   Specifies the access zone that contains the virtual rack you want to view.

isi hdfs settings modify

Modifies the HDFS settings for an access zone.

Syntax

isi hdfs settings modify
   [--service {yes | no}]
   [--default-block-size <size>]
   [--default-checksum-type {none | crc32 | crc32c}]
   [--authentication-mode {all | simple_only | kerberos_only}]
   [--root-directory <path>]
   [--webhdfs-enabled {yes | no}]
   [--ambari-server <string>]
   [--ambari-namenode <string>]
   [--odp-version <string>]
   [--zone <string>]
   [--verbose]

Options

--service {yes | no}
   Enables or disables the HDFS service in the specified access zone. The HDFS service is enabled by default.
--default-block-size <size>
Specifies the block size (in bytes) reported by the HDFS service. K, M, and G; for example, 64M, 512K, 1G, are valid suffixes. The default value is 128 MB.

--default-checksum-type {none | crc32 | crc32c}
Specifies the checksum type reported by the HDFS service. The default value is none.

--authentication-mode {all | simple_only | kerberos_only}
Specifies the authentication method used for HDFS connections through the specified access zone. The default value is all.

--root-directory <path>
Root path that contains HDFS data in the access zone that can be accessed by Hadoop compute client connections. The root directory must be within the access zone base directory.

--webhdfs-enabled {yes | no}
Enables or disables the WebHDFS in the specified access zone. WebHDFS is enabled by default.

--ambari-server <string>
Specifies the Ambari server that receives communication from an Ambari agent. The value must be a resolvable hostname, FQDN, or IPv4 address.

--ambari-namenode <string>
Specifies a point of contact in the access zone that Hadoop services managed through the Ambari interface should connect through. The value must be a resolvable IPv4 address or a SmartConnect zone name.

--odp-version <string>
Specifies the version of the Open Data Platform (ODP) stack repository, including build number if one exists, installed by the Ambari server. This is required to support ODP upgrades on other systems that are part of the Hadoop cluster.

--zone <string>
Specifies the access zone to which the HDFS settings apply.

{--verbose | -v}
Displays more detailed information.

isi hdfs settings view
Displays the HDFS settings in an access zone.

Syntax

isi hdfs settings view
[---zone <string>]
[---verbose]

Options

---zone <string>
Specifies the access zone. The system will display the HDFS settings for the specified zone.
Hadoop
CHAPTER 28

Antivirus

This section contains the following topics:

- Antivirus overview ................................................................. 1152
- On-access scanning .............................................................. 1152
- Antivirus policy scanning ......................................................... 1153
- Individual file scanning .......................................................... 1153
- Antivirus scan reports ............................................................ 1153
- ICAP servers ........................................................................ 1153
- Supported ICAP servers .......................................................... 1154
- Antivirus threat responses ......................................................... 1154
- Configuring global antivirus settings ........................................ 1155
- Managing ICAP servers ........................................................... 1156
- Create an antivirus policy ......................................................... 1158
- Managing antivirus policies ...................................................... 1158
- Managing antivirus scans ......................................................... 1159
- Managing antivirus threats ...................................................... 1160
- Managing antivirus reports ...................................................... 1161
- Antivirus commands ............................................................... 1162
Antivirus overview

You can scan the files you store on an Isilon cluster for computer viruses and other security threats by integrating with third-party scanning services through the Internet Content Adaptation Protocol (ICAP).

OneFS sends files through ICAP to a server running third-party antivirus scanning software. These servers are referred to as ICAP servers. ICAP servers scan files for viruses.

After an ICAP server scans a file, it informs OneFS of whether the file is a threat. If a threat is detected, OneFS informs system administrators by creating an event, displaying near real-time summary information, and documenting the threat in an antivirus scan report. You can configure OneFS to request that ICAP servers attempt to repair infected files. You can also configure OneFS to protect users against potentially dangerous files by truncating or quarantining infected files.

Before OneFS sends a file to be scanned, it ensures that the scan is not redundant. If a file has already been scanned and has not been modified, OneFS will not send the file to be scanned unless the virus database on the ICAP server has been updated since the last scan.

Note

Antivirus scanning is available only if all nodes in the cluster are connected to the external network.

On-access scanning

You can configure OneFS to send files to be scanned before they are opened, after they are closed, or both. Sending files to be scanned after they are closed is faster but less secure. Sending files to be scanned before they are opened is slower but more secure.

If OneFS is configured to ensure that files are scanned after they are closed, when a user creates or modifies a file on the cluster, OneFS queues the file to be scanned. OneFS then sends the file to an ICAP server to be scanned when convenient. In this configuration, users can always access files without any delay. However, it is possible that after a user modifies or creates a file, a second user might access the file before the file is scanned. If a virus was introduced to the file from the first user, the second user will be able to access the infected file. Also, if an ICAP server is unable to scan a file, the file will still be accessible to users.

If OneFS ensures that files are scanned before they are opened, when a user attempts to download a file from the cluster, OneFS first sends the file to an ICAP server to be scanned. The file is not sent to the user until the scan is complete. Scanning files before they are opened is more secure than scanning files after they are closed, because users can access only scanned files. However, scanning files before they are opened requires users to wait for files to be scanned. You can also configure OneFS to deny access to files that cannot be scanned by an ICAP server, which can increase the delay. For example, if no ICAP servers are available, users will not be able to access any files until the ICAP servers become available again.

If you configure OneFS to ensure that files are scanned before they are opened, it is recommended that you also configure OneFS to ensure that files are scanned after they are closed. Scanning files as they are both opened and closed will not necessarily improve security, but it will usually improve data availability when compared to...
scanning files only when they are opened. If a user wants to access a file, the file may have already been scanned after the file was last modified, and will not need to be scanned again if the ICAP server database has not been updated since the last scan.

**Antivirus policy scanning**

You can create antivirus scanning policies that send files from a specified directory to be scanned. Antivirus policies can be run manually at any time, or configured to run according to a schedule.

Antivirus policies target a specific directory on the cluster. You can prevent an antivirus policy from sending certain files within the specified root directory based on the size, name, or extension of the file. Antivirus policies do not target snapshots. Only on-access scans include snapshots. Antivirus scans are handled by the OneFS Job Engine, and function the same as any system job.

**Individual file scanning**

You can send a specific file to an ICAP server to be scanned at any time.

If a virus is detected in a file but the ICAP server is unable to repair it, you can send the file to the ICAP server after the virus database had been updated, and the ICAP server might be able to repair the file. You can also scan individual files to test the connection between the cluster and ICAP servers.

**Antivirus scan reports**

OneFS generates reports about antivirus scans. Each time that an antivirus policy is run, OneFS generates a report for that policy. OneFS also generates a report every 24 hours that includes all on-access scans that occurred during the day.

Antivirus scan reports contain the following information:

- The time that the scan started.
- The time that the scan ended.
- The total number of files scanned.
- The total size of the files scanned.
- The total network traffic sent.
- The network throughput that was consumed by virus scanning.
- Whether the scan succeeded.
- The total number of infected files detected.
- The names of infected files.
- The threats associated with infected files.
- How OneFS responded to detected threats.

**ICAP servers**

The number of ICAP servers that are required to support an Isilon cluster depends on how virus scanning is configured, the amount of data a cluster processes, and the processing power of the ICAP servers.

If you intend to scan files exclusively through antivirus scan policies, it is recommended that you have a minimum of two ICAP servers per cluster.
to scan files on access, it is recommended that you have at least one ICAP server for each node in the cluster.

If you configure more than one ICAP server for a cluster, it is important to ensure that the processing power of each ICAP server is relatively equal. OneFS distributes files to the ICAP servers on a rotating basis, regardless of the processing power of the ICAP servers. If one server is significantly more powerful than another, OneFS does not send more files to the more powerful server.

**Supported ICAP servers**

For a list of supported ICAP servers, see the *Isilon Third-Party Software & Hardware Compatibility Guide*.

**Antivirus threat responses**

You can configure the system to repair, quarantine, or truncate any files that the ICAP server detects viruses in.

OneFS and ICAP servers react in one or more of the following ways when threats are detected:

**Alert**

All threats that are detected cause an event to be generated in OneFS at the warning level, regardless of the threat response configuration.

**Repair**

The ICAP server attempts to repair the infected file before returning the file to OneFS.

**Quarantine**

OneFS quarantines the infected file. A quarantined file cannot be accessed by any user. However, a quarantined file can be removed from quarantine by the root user if the root user is connected to the cluster through secure shell (SSH). If you backup your cluster through NDMP backup, quarantined files will remain quarantined when the files are restored. If you replicate quarantined files to another Isilon cluster, the quarantined files will continue to be quarantined on the target cluster. Quarantines operate independently of access control lists (ACLs).

**Truncate**

OneFS truncates the infected file. When a file is truncated, OneFS reduces the size of the file to zero bytes to render the file harmless.

You can configure OneFS and ICAP servers to react in one of the following ways when threats are detected:

**Repair or quarantine**

Attempts to repair infected files. If an ICAP server fails to repair a file, OneFS quarantines the file. If the ICAP server repairs the file successfully, OneFS sends the file to the user. Repair or quarantine can be useful if you want to protect users from accessing infected files while retaining all data on a cluster.

**Repair or truncate**

Attempts to repair infected files. If an ICAP server fails to repair a file, OneFS truncates the file. If the ICAP server repairs the file successfully, OneFS sends the file to the user. Repair or truncate can be useful if you do not care about
retaining all data on your cluster, and you want to free storage space. However, data in infected files will be lost.

**Alert only**
Only generates an event for each infected file. It is recommended that you do not apply this setting.

**Repair only**
Attempts to repair infected files. Afterwards, OneFS sends the files to the user, whether or not the ICAP server repaired the files successfully. It is recommended that you do not apply this setting. If you only attempt to repair files, users will still be able to access infected files that cannot be repaired.

**Quarantine**
Quarantines all infected files. It is recommended that you do not apply this setting. If you quarantine files without attempting to repair them, you might deny access to infected files that could have been repaired.

**Truncate**
Truncates all infected files. It is recommended that you do not apply this setting. If you truncate files without attempting to repair them, you might delete data unnecessarily.

### Configuring global antivirus settings
You can configure global antivirus settings that are applied to all antivirus scans by default.

### Include specific files in antivirus scans
You can target specific files for scans by antivirus policies.

**Procedure**
1. Run the `isi antivirus settings modify` command.

   The following command configures OneFS to scan only files with the `.txt` extension:

   ```bash
   isi antivirus settings modify --glob-filters-enabled true \--glob-filters .txt
   ```

### Configure on-access scanning settings
You can configure OneFS to automatically scan files as they are accessed by users. On-access scans operate independently of antivirus policies.

**Procedure**
1. Run the `isi antivirus settings modify` command.

   The following command configures OneFS to scan files and directories under `/ifs/data/media` when they are closed:

   ```bash
   isi antivirus settings modify --scan-on-close true \--path-prefixes /ifs/data/media
   ```
Configure antivirus threat response settings

You can configure how OneFS responds to detected threats.

Procedure

1. Run the `isi antivirus settings modify` command.

   The following command configures OneFS and ICAP servers to attempt to repair infected files and quarantine files that cannot be repaired:

   ```
   isi antivirus settings modify --repair true --quarantine true
   ```

Configure antivirus report retention settings

You can configure how long OneFS retains antivirus reports before automatically deleting them.

Procedure

1. Run the `isi antivirus settings modify` command.

   The following command configures OneFS to delete antivirus reports older than 12 weeks.

   ```
   isi antivirus settings modify --report-expiry 12w
   ```

Enable or disable antivirus scanning

You can enable or disable all antivirus scanning. This procedure is available only through the web administration interface.

Procedure

1. Run the `isi antivirus settings modify` command.

   The following command enables antivirus scanning

   ```
   isi antivirus settings modify --service enable
   ```

   The following command disables antivirus scanning

   ```
   isi antivirus settings modify --service disable
   ```

Managing ICAP servers

Before you can send files to be scanned on an ICAP server, you must configure OneFS to connect to the server. You can test, modify, and remove an ICAP server connection. You can also temporarily disconnect and reconnect to an ICAP server.
Add and connect to an ICAP server

You can add and connect to an ICAP server. After a server is added, OneFS can send files to the server to be scanned for viruses.

Procedure

1. Run the `isi antivirus servers create` command.

   The following command adds and connects to an ICAP server at 10.7.180.108:

   ```
   isi antivirus servers create icap://10.7.180.108 --enabled yes
   ```

Temporarily disconnect from an ICAP server

If you want to prevent OneFS from sending files to an ICAP server, but want to retain the ICAP server connection settings, you can temporarily disconnect from the ICAP server.

Procedure

1. Run the `isi antivirus servers modify` command.

   The following command temporarily disconnects from an ICAP server with a URL of `icap://10.7.180.108`:

   ```
   isi antivirus servers modify icap://10.7.180.108 --enabled yes
   ```

Reconnect to an ICAP server

You can reconnect to an ICAP server that you have temporarily disconnected from.

Procedure

1. Run the `isi antivirus servers modify` command.

   The following command reconnects to an ICAP server with a URL of `icap://10.7.180.108`:

   ```
   isi antivirus servers modify icap://10.7.180.108 --enabled no
   ```

Remove an ICAP server

You can permanently disconnect from the ICAP server.

Procedure

1. Run the `isi antivirus servers delete` command.

   The following command removes an ICAP server with an ID of `icap://10.7.180.108`:

   ```
   isi antivirus servers delete icap://10.7.180.108
   ```

2. Type `yes` and then press ENTER.
Create an antivirus policy

You can create an antivirus policy that causes specific files to be scanned for viruses each time the policy is run.

Procedure

1. Run the `isi antivirus policies create` command.

   The following command creates an antivirus policy that scans `/ifs/data` every Friday at 12:00 PM:

   ```
   isi antivirus policies create WeekendVirusScan --paths /ifs/data --schedule "Every Friday at 12:00 PM"
   ```

Managing antivirus policies

You can modify and delete antivirus policies. You can also temporarily disable antivirus policies if you want to retain the policy but do not want to scan files.

Modify an antivirus policy

You can modify an antivirus policy.

Procedure

1. Run the `isi antivirus policies modify` command.

   The following command modifies a policy called `WeekendVirusScan` to be run on Saturday at 12:00 PM:

   ```
   isi antivirus policies modify WeekendVirusScan --schedule "Every Friday at 12:00 PM"
   ```

Delete an antivirus policy

You can delete an antivirus policy.

Procedure

1. Run the `isi antivirus policies delete` command.

   The following command deletes a policy called `WeekendVirusScan`:

   ```
   isi antivirus policies delete WeekendVirusScan
   ```

Enable or disable an antivirus policy

You can temporarily disable antivirus policies if you want to retain the policy but do not want to scan files.

Procedure

1. Run the `isi antivirus policies modify` command.
The following command enables a policy called WeekendVirusScan:

```bash
isi antivirus policies modify WeekendVirusScan --enabled yes
```

The following command disables a policy called WeekendVirusScan:

```bash
isi antivirus policies modify WeekendVirusScan --enabled no
```

### View antivirus policies

You can view antivirus policies.

**Procedure**

1. Run the following command:

```bash
isi antivirus policies list
```

### Managing antivirus scans

You can scan multiple files for viruses by manually running an antivirus policy, or scan an individual file without an antivirus policy. You can also stop antivirus scans.

#### Scan a file

You can manually scan an individual file for viruses.

**Procedure**

1. Run the `isi antivirus scan` command.

   The following command scans the `/ifs/data/virus_file` file for viruses:

   ```bash
   isi antivirus scan /ifs/data/virus_file
   ```

#### Manually run an antivirus policy

You can manually run an antivirus policy at any time.

This procedure is available only through the web administration interface.

**Procedure**

1. Click **Data Protection > Antivirus > Policies**.
2. In the **Antivirus Policies** table, in the row for a policy, click **More > Run Policy**.

#### Stop a running antivirus scan

You can stop a running antivirus scan. This procedure is available only through the web administration interface.

**Procedure**

1. Click **Cluster Management > Job Operations > Job Summary**.
2. In the **Active Jobs** table, in the row with type **AVScan**, click **More > Cancel Running Job**.

**Managing antivirus threats**

You can repair, quarantine, or truncate files in which threats are detected. If you think that a quarantined file is no longer a threat, you can rescan the file or remove the file from quarantine.

**Manually quarantine a file**

You can quarantine a file to prevent the file from being accessed by users.

**Procedure**

1. Run the `isi antivirus quarantine` command.

   The following command quarantines `/ifs/data/badFile.txt`:

   ```
   isi antivirus quarantine /ifs/data/badFile.txt
   ```

**Rescan a file**

You can rescan a file for viruses if, for example, you believe that a file is no longer a threat.

**Procedure**

1. Run the `isi antivirus scan` command.

   For example, the following command scans `/ifs/data/virus_file`:

   ```
   isi antivirus scan /ifs/data/virus_file
   ```

**Remove a file from quarantine**

You can remove a file from quarantine if, for example, you believe that the file is no longer a threat.

**Procedure**

1. Run the `isi antivirus release` command.

   The following command removes `/ifs/data/badFile.txt` from quarantine:

   ```
   isi antivirus release /ifs/data/newFile
   ```

**Manually truncate a file**

If a threat is detected in a file, and the file is irreparable and no longer needed, you can manually truncate the file.

**Procedure**

1. Run the `rm` command on a file.
The following command truncates the `/ifs/data/virus_file` file:

```
rm /ifs/data/virus_file
```

**View threats**

You can view files that have been identified as threats by an ICAP server.

**Procedure**

1. Run the following command:

   ```
   isi antivirus reports threats list
   ```

**Antivirus threat information**

You can view information about the antivirus threats that are reported by an ICAP server.

The following information is displayed in the output of the `isi antivirus reports threats list` command.

- **Scan**
  - The ID of the antivirus report.

- **ID:**
  - The ID of the antivirus policy that detected the threat. If the threat was detected as a result of a manual antivirus scan of an individual file, `MANUAL` is displayed.

- **Remediation**
  - How OneFS responded to the file when the threat was detected. If OneFS did not quarantine or truncate the file, `Infected` is displayed.

- **Threat**
  - The name of the detected threat as it is recognized by the ICAP server.

- **Time**
  - The time that the threat was detected.

**Managing antivirus reports**

You can view antivirus reports through the web administration interface. You can also view events that are related to antivirus activity.
View antivirus reports

You can view antivirus reports.

Procedure

1. Run the following command:

```
isi antivirus reports scans list
```

View antivirus events

You can view events that relate to antivirus activity.

Procedure

1. Run the following command:

```
isi event events list
```

All events related to antivirus scans are classified as warnings. The following events are related to antivirus activities:

**AVScan Infected File Found**

A threat was detected by an antivirus scan. These events refer to specific reports on the Antivirus Reports page but do not provide threat details.

**No ICAP Servers available**

OneFS is unable to communicate with any ICAP servers.

**ICAP Server Misconfigured, Unreachable or Unresponsive**

OneFS is unable to communicate with an ICAP server.

Antivirus commands

You can control antivirus scanning activity on an Isilon cluster through the antivirus commands.

**isi antivirus policies create**

Creates an antivirus scan policy.

Syntax

```
isi antivirus policies create <name>
[-description <string>]
[-enabled {true | false}]
[-schedule <schedule>]
[-impact <impact-policy>]
[-force-run {yes | no}]
[-paths <path>...] 
[-recursion-depth <integer>]
[-verbose]
```
Options

<name>
  Specifies a name for the policy.

--description <string>
  Specifies a description for the policy.

{--enabled | -e} {true | false}
  Determines whether the policy is enabled or disabled. If set to true, the policy is enabled. The default value is false.

{--schedule | -s} <schedule>
  Specifies when the policy is run.
  Specify in the following format:

  "<interval> [<frequency>]

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>[, ...] [of every [{other | <integer>}] week]]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>[:<mm>] [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>[:<mm>] [{AM | PM}] and <hh>[:<mm>] [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>[:<mm>] [{AM | PM}] to <hh>[:<mm>] [{AM | PM}]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "Saturday" and "sat" are valid.

{--impact | -i} <impact_policy>
Specifies an impact policy for the antivirus scan jobs. You can specify LOW, MEDIUM, HIGH, OFF_HOURS, or a custom impact policy that you created.

```bash
--force-run | -r} {yes | no}
```

Determines whether to force policy scans. If a scan is forced, all files are scanned regardless of whether OneFS has marked files as having been scanned, or if global settings specify that certain files should not be scanned.

```bash
--paths <path>
```

Specifies directories to scan when the policy is run. To specify multiple paths, repeat the --path option. For example:

```bash
--paths /ifs/data/directory1 --paths /ifs/data/directory2
```

```bash
--recursion-depth <integer>
```

**Note**

This option has been deprecated and will not impact antivirus scans if specified.

Specifies the depth of subdirectories to include in the scan.

```bash
{--verbose | -v}
```

Displays a message confirming that the antivirus policy was created.

### isi antivirus policies delete

Deletes an antivirus scan policy.

**Syntax**

```bash
isi antivirus policies delete {<name> | --all} [--force] [--verbose]
```

**Options**

```bash
{<name> | --all}
```

Deletes the specified policy or all policies.

```bash
--force | -f
```

Does not prompt you to confirm that you want to delete the policy.

```bash
{--verbose | -v}
```

Displays a message confirming that the antivirus policy was deleted.
**isi antivirus policies list**

Displays a list of antivirus policies.

**Syntax**

```plaintext
isi antivirus policies list
    [--limit <integer>]
    [--sort {name | description | enabled}]
    [--descending]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]
```

**Options**

If no options are specified, displays a table of all antivirus policies.

`[--limit | -l] <integer>`

Displays no more than the specified number of items.

`--sort <attribute>`

Sorts output displayed by the specified attribute.

The following values are valid:

- **name**
  
  Sorts output by the name of the antivirus policy.

- **description**
  
  Sorts output by the description of the antivirus policy.

- **enabled**
  
  Sorts output by whether the policy is enabled or disabled.

`[--descending | -d]`

Displays output in reverse order.

`--format {table | json | csv | list}`

Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

`[--no-header | -a]`

Displays table and CSV output without headers.

`[--no-footer | -z]`

Displays table output without footers.

`[--verbose | -v]`

Displays more detailed information.
isi antivirus policies start

Runs an antivirus policy.

Syntax

```bash
isi antivirus policies start <policy>  
  [--report-id <id>]  
  [--force-run {true | false}]  
  [--update {yes | no}]
```

Options

- `<policy>`
  Runs the specified policy.

- `--report-id <id>`
  Assigns the specified ID to the report generated for this run of the avscan policy. If you do not specify an ID, OneFS will automatically assign one.

- `{ --force-run | -r } {true | false}`
  Determines whether to force the scan. If the scan is forced, all files are scanned regardless of whether OneFS has marked files as having been scanned, or if global settings specify that certain files should not be scanned.

- `--update {yes | no}`
  Specifies whether to update the last run time in the policy file. The default value is `yes`.

isi antivirus policies modify

Modifies an antivirus scan policy.

Syntax

```bash
isi antivirus policies modify <id>  
  [--name <new-name>]  
  [--enabled {true | false}]  
  [--description <string>]  
  [--schedule <schedule>]  
  [--impact <impact-policy>]  
  [--force-run {true | false}]  
  [{--paths <path>... | --clear-paths | --add-paths <path> | --remove-paths <path>}])  
  [--recursion-depth <integer>]
```

Options

- `<id>`
  Modifies the policy with the specified policy identification number.

- `{--name | -n} <new-name>`
  Specifies a new name for this policy.

- `--description <string>`
Specifies a description for the policy.

\{---enabled | -e\} \{true | false\}

Determines whether this policy is enabled or disabled. If set to true, the policy is enabled. The default value is false.

\{---schedule | -s\} <schedule>

Specifies when the policy is run.
Specify in the following format:

"<interval> [<frequency>]"

Specify <interval> in one of the following formats:

- Every [{other | <integer>}] {weekday | day}
- Every [{other | <integer>}] week [on <day>]
- Every [{other | <integer>}] month [on the <integer>]
- Every [<day>[, ...] [of every [{other | <integer>}] week]]
- The last {day | weekday | <day>} of every [{other | <integer>}] month
- The <integer> {weekday | <day>} of every [{other | <integer>}] month
- Yearly on <month> <integer>
- Yearly on the {last | <integer>} [weekday | <day>] of <month>

Specify <frequency> in one of the following formats:

- at <hh>[:<mm>] [{AM | PM}]
- every [<integer>] {hours | minutes} [between <hh>[:<mm>] [{AM | PM}] and <hh>[:<mm>] [{AM | PM}]]
- every [<integer>] {hours | minutes} [from <hh>[:<mm>] [{AM | PM}] to <hh>[:<mm>] [{AM | PM}]]

You can optionally append "st", "th", or "rd" to <integer>. For example, you can specify "Every 1st month"

Specify <day> as any day of the week or a three-letter abbreviation for the day. For example, both "Saturday" and "sat" are valid.

\--clear-schedule

Deletes the current schedule for the policy.

\{---impact | -i\} <impact_policy>

Specifies an impact policy for the antivirus scan jobs. You can specify LOW, MEDIUM, HIGH, OFF_HOURS, or a custom impact policy that you created.

\--clear-impact

Antivirus
Clears the current impact policy for antivirus scan jobs.

|--force-run | -r {yes | no}

Determines whether to force policy scans. If a scan is forced, all files are scanned regardless of whether OneFS has marked files as having been scanned, or if global settings specify that certain files should not be scanned.

--paths <path>

Specify directories to scan when the policy is run. To specify multiple paths, repeat the --path option. For example:

```bash
--paths /ifs/data/directory1 --paths /ifs/data/directory2
```

**Note**

If you specify this option, the specified paths will replace all previously specified paths in the list.

--clear-paths

Clears the list of paths to scan.

--add-paths <path>

Adds the specified path to the list of paths to scan.

--remove-paths <path>

Removes the specified path from the list of paths to scan.

--recursion-depth <integer>

**Note**

This option has been deprecated and will not impact antivirus scans if specified.

Specifies the depth of subdirectories to include in the scan.

|--verbose | -v

Displays a message confirming that the antivirus policy was modified.

**isi antivirus policies view**

Displays information about antivirus scan policies.

**Syntax**

```bash
isi antivirus policies view <policy>
```

**Options**

```
<policy>
```

Displays information on only the policy of the specified ID.
isi antivirus release

Removes a file from quarantine. Quarantined files cannot be read or written to.

Syntax

```bash
isi antivirus release <name>
[--verbose]
```

Options

- `<name>`
  - Removes the specified file from quarantine. Specify as a file path.
- `{--verbose | -v}`
  - Displays a message confirming that the file was removed from quarantine.

isi antivirus scan

Manually scans a file for viruses.

Syntax

```bash
isi antivirus scan <path>
[--policy <id>]
[--report-id <id>]
[--force-run {yes | no}]
```

Options

- `<path>`
  - Scans the specified file.
- `{--policy | -p} <id>`
  - Assigns a policy ID for this scan. The default ID is `MANUAL`.
- `--report-id <id>`
  - Assigns the specified ID to the report generated for this antivirus scan. If you do not specify an ID, OneFS will automatically assign one.
- `{--force-run | -r} {true | false}`
  - Determines whether to force the scan. If the scan is forced, all files are scanned regardless of whether OneFS has marked files as having been scanned, or if global settings specify that certain files should not be scanned.

isi antivirus settings modify

Sets and displays global configuration settings for anti-virus scanning.

Syntax

```bash
isi antivirus settings modify
[--fail-open {true | false}]
[|--glob-filters <string>... | --clear-glob-filters
```
Options

--fail-open {true | false}

If --scan-on-open is set to true, determines whether users can access files that cannot be scanned. If this option is set to false, users cannot access a file until the file is scanned by an ICAP server.

If --scan-on-open is set to true, this option has no effect.

--glob-filter <string>

Specifies a file name or extension. To specify multiple filters, you must include multiple --glob-filter options within the same command. Specifying this option will remove any existing glob filters.

You can include the following wildcards:

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, specifying &quot;m*&quot; would match &quot;movies&quot; and &quot;m123&quot;</td>
</tr>
<tr>
<td>[]</td>
<td>Matches any characters contained in the brackets, or a range of characters separated by a dash. For example, specifying &quot;b[aei]t&quot; would match &quot;bat&quot;, &quot;bet&quot;, and &quot;bit&quot;</td>
</tr>
<tr>
<td></td>
<td>You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, specifying &quot;b[!ie]t&quot; would match &quot;bat&quot; but not &quot;bit&quot; or &quot;bet&quot;</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, specifying &quot;t?p&quot; would match &quot;tap&quot;, &quot;tip&quot;, and &quot;top&quot;</td>
</tr>
</tbody>
</table>
Note

If you specify this option, the specified filters will replace all previously specified filters in the list.

--clear-glob-filters
Clears the list of filters.

--add-glob-filters <string>
Adds the specified filters to the list of filters.

--remove-glob-filters <string>
Removes the specified filters to the list of filters.

--glob-filters-enabled {true | false}
Determines whether glob filters are enabled. If no glob filters are specified, glob filters will remain disabled even if this option is set to true.

--glob-filters-include {true | false}
Determines how glob filters are interpreted by OneFS. If set to true, OneFS will scan only files that match a glob filter. If set to false, OneFS will scan only files that do not match any glob filters.

--path-prefix <path>
If specified, only files contained in the specified directory path will be scanned. This option affects only on-access scans. To specify multiple directories, you must include multiple --path-prefix options within the same command. Specifying this option will remove any existing path prefixes.

Note

If you specify this option, the specified filters will replace all previously specified filters in the list.

--clear-path-prefixes
Clears the list of paths.

--add-path-prefixes <path>
Adds the specified paths to the list of paths.

--remove-path-prefixes <path>
Removes the specified paths to the list of paths.

--repair {true | false}
Determines whether OneFS attempts to repair files that threats are detected in.

--report-expiry <integer> <time>
Determines how long OneFS will retain antivirus scan reports before deleting them.
The following <time> values are valid:

Y
  Specifies years
M
  Specifies months

W
  Specifies weeks

D
  Specifies days

H
  Specifies hours

m
  Specifies minutes

s
  Specifies seconds

--scan-on-close {true | false}
  Determines whether files are scanned after the files are closed.

--scan-on-open {true | false}
  Determines whether files are scanned before the files are sent to users.

--scan-size-maximum <integer>{k | M | G | T | P}
  If specified, OneFS will not send files larger than the specified size to an ICAP server to be scanned.

Note
  Although the parameter accepts values larger than 2GB, OneFS does not scan files larger than 2GB.

--service {true | false}
  Determines whether the antivirus service is running.

--quarantine {true | false}
  Determines whether OneFS quarantines files that threats are detected in. If --repair is set to true, OneFS will attempt to repair the files before quarantining them. If both --truncate and --quarantine are set to true, the --truncate option is ignored.

--truncate {true | false}
  Determines whether OneFS truncates files that threats are detected in. If --repair is set to true, OneFS will attempt to repair the files before truncating them. If both --truncate and --quarantine are set to true, the --truncate option is ignored.

{--verbose | -v}
  Displays a message confirming that the settings have been modified.
**isi antivirus settings view**

Displays antivirus settings.

**Syntax**

```bash
isi antivirus settings view
```

**Options**

There are no options for this command.

**isi antivirus quarantine**

Quarantines a file manually. Quarantined files cannot be read or written to.

**Syntax**

```bash
isi antivirus quarantine <path>
[--verbose]
```

**Options**

- `<path>`
  Quarantines the specified file. Specify as a file path.
- `{--verbose | -v}`
  Displays a message confirming that the file has been quarantined.

**isi antivirus reports scans list**

Displays information about recent antivirus scans.

**Syntax**

```bash
isi antivirus reports scans list
[--policy-id <string>]
[--status <status>]
[--limit <integer>]
[--sort <attribute>]
[--descending]
[--format {table | json | csv | list}]
[--no-header]
[--no-footer]
[--verbose]
```

**Options**

- `--policy-id <string>`
  Filters output based on the ID of the policy.
- `--status <status>`
  Filters output based on the current status of the scan job.
  The following values are valid:
Antivirus

Finish
Displays only completed jobs.

Succeeded
Displays only successfully completed jobs.

Failed
Displays only failed jobs.

Cancelled
Displays only cancelled jobs.

Started
Displays only running jobs.

Paused
Displays only paused jobs.

Resumed
Displays only jobs that were paused, then resumed.

Pending
Displays only pending jobs.

{--limit | -l} <integer>
Displays no more than the specified number of items.

--sort <attribute>
Sorts output displayed by the specified attribute.
The following values are valid:

  id
  Sorts output by the ID of the antivirus report.

  policy_id
  Sorts output by the ID of the policy that created the report.

  status
  Sorts output by the status of the antivirus scan.

  start
  Sorts output by the time that the antivirus scan started.

  files
  Sorts output by the number of files that were scanned by the antivirus scan.

  infections
  Sorts output by the number of threats detected by the antivirus scan.

{--descending | -d}
Displays output in reverse order.

--format {table | json | csv | list}
Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.
Displays table and CSV output without headers.

Displays table output without footers.

Displays more detailed information.

isi antivirus reports scans view
Displays an antivirus report.

Syntax

isi antivirus reports scans view <id>

Options

<i id>
Displays the antivirus report of the specified ID.

isi antivirus reports threats list
Displays a list of detected threats.

Syntax

isi antivirus reports threats list
    [--scan-id <id>]
    [--file <path>]
    [--remediation <action>]
    [--limit <integer>]
    [--sort <attribute>]
    [--descending]
    [--format {table | json | csv | list}]
    [--no-header]
    [--no-footer]
    [--verbose]

Options

If no options are specified, displays a list of recently detected threats.

--scan-id <id>
Displays only threats included in the antivirus report with the specified ID.

--file <path>
Displays only threats detected in the specified file.

--remediation <action>
Displays only threats that OneFS performed the specified action on.

{--limit | -l} <integer>
Displays no more than the specified number of items.

--sort <attribute>
Antivirus

Sorts output displayed by the specified attribute.
The following values are valid:

scan_id
   Sorts output by the ID of the antivirus report that the threat was detected in.

file
   Sorts output by the path of the file that the threat was detected in.

remediation
   Sorts output by the action that OneFS performed on the infected file.

threat
   Sorts output by the name of the detected threat.

time
   Sorts output by the time that the threat was detected.

|--descending | -d
   Displays output in reverse order.

--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-
   separated value (CSV), or list format.

|--no-header | -a
   Displays table and CSV output without headers.

|--no-footer | -z
   Displays table output without footers.

|--verbose | -v
   Displays more detailed information.

**isi antivirus reports threats view**

Displays information about a detected threat.

**Syntax**

```bash
isi antivirus reports threats view <id>
```

**Options**

`<id>`
   Displays information about the threat with the specified ID.
isi antivirus reports delete

Deletes antivirus reports.

Syntax

```
isiv antivirus reports delete {<scan-id> | --all}
    [--age <integer><time>]
    [--verbose]
    [--force]
```

Options

`<scan-id>`
Deletes the antivirus report with the specified ID.

`--all`
Deletes all antivirus reports.

`--age <integer><time>`
Deletes all reports older than the specified age.
The following `<time>` values are valid:

- `Y` specifies years
- `M` specifies months
- `W` specifies weeks
- `D` specifies days
- `H` specifies hours
- `m` specifies minutes
- `s` specifies seconds

`{--verbose | -v}`
Displays a message confirming that the reports have been deleted.

`{--force | -f}`
Does not display a confirmation prompt.
isi antivirus servers create

Adds and connects to an ICAP server.

Syntax

```
isi antivirus servers create <url>
   [--description <string>]
   [--enabled {yes | no}]
   [--verbose]
```

Options

- `<url>`
  Specifies the URL of the ICAP server.

- `--description <string>`
  Specifies an optional description for the policy.

- `--enabled {yes | no}`
  Determines whether the ICAP server is enabled.

- `--verbose | -v`
  Displays a message confirming that the server has been added.

isi antivirus servers delete

Permanently disconnects from an ICAP server.

Syntax

```
isi antivirus servers delete {<url> | --all}
   [--verbose]
   [--force]
```

Options

- `<url> | --all`
  Deletes the specified ICAP server.

- `--verbose | -v`
  Displays a message confirming that OneFS has disconnected from the ICAP server.

- `--force | -f`
  Does not display a confirmation prompt.
isi antivirus servers list

Displays a list of ICAP servers that OneFS is currently connected to.

Syntax

```
isi antivirus servers list
   [--limit <integer>]
   [--sort <attribute>]
   [--descending]
   [--format {table | json | csv | list}]
   [--no-header]
   [--no-footer]
   [--verbose]
```

Options

```
|--limit | -l| <integer>
   Displays no more than the specified number of items.

|--sort <attribute>
   Sorts output displayed by the specified attribute.
   The following values are valid:
   url
      Sorts output by the URL of the server.
   description
      Sorts output by the description of the server.
   enabled
      Sorts output by the state of the server.

|--descending | -d
   Displays output in reverse order.

|--format {table | json | csv | list}
   Displays output in table (default), JavaScript Object Notation (JSON), comma-separated value (CSV), or list format.

|--no-header | -a
   Displays table and CSV output without headers.

|--no-footer | -z
   Displays table output without footers.

|--verbose | -v
   Displays more detailed information.
```
isi antivirus servers modify

Modifies the settings of an ICAP server.

Syntax

```bash
isi antivirus servers modify <url>
   [--enabled {yes | no}]
   [--description <string>]
   [--verbose]
```

Options

- `<url>`
  Specifies the URL of the ICAP server.

- `--description <string>`
  Specifies an optional description for the policy.

- `{--enabled | -n} {yes | no}`
  Determines whether the ICAP server is enabled.

- `{--verbose | -v}`
  Displays a message confirming that the server has been added.

isi antivirus servers view

Displays information about an ICAP server.

Syntax

```bash
isi antivirus servers view <url>
```

Options

- `<url>`
  Displays information about the specified ICAP server.

isi antivirus status

Displays information about the scan status of files.

Syntax

```bash
isi antivirus status <path>
```

Options

- `<path>`
  Displays information about the file of the specified path.

- `{--verbose | -v}`
  Displays more detailed information.
CHAPTER 29

IsilonSD Edge

This section contains the following topics:

- IsilonSD Edge storage and architecture ................................................................. 1182
- IsilonSD cluster overview ..................................................................................... 1183
- IsilonSD Edge licensing overview ......................................................................... 1183
- IsilonSD Management Server overview .............................................................. 1186
- Deploying and configuring IsilonSD clusters ....................................................... 1186
IsilonSD Edge creates OneFS virtual clusters through the resources available on VMware ESXi hosts. The OneFS clusters are deployed as virtual machines (VMs) and drives are hosted on data disks.

IsilonSD Edge components include the IsilonSD Management Server, IsilonSD Management Plug-in, and the OneFS virtual machine files. The management plug-in is bundled with the management server and automatically installs when the management server is deployed on an ESXi host and a VMware vCenter server is registered.

The management plug-in enables you to create an IsilonSD cluster by choosing ESXi hosts and drives on those hosts. A maximum of six nodes, which are actually OneFS virtual machines, can be added to a cluster. In order to maintain the same protection model that is followed for physical EMC Isilon clusters, a one-to-one correspondence is maintained between an ESXi host and a node. Similarly, a one-to-one correspondence is maintained between a drive that is accessible to a node and a physical drive. All these checks are performed by the management server.

When the management server deploys nodes, it prevents two or more nodes of the same cluster from sharing the same ESXi host. When selecting physical drives for a node, the management server prevents hosting of more than one virtual disk on any single drive.

---

**Note**

IsilonSD Edge supports homogenous node configurations. You can have only one node type in a cluster.

---

**IsilonSD Edge networking considerations**

The OneFS data-path requires a minimum of two NICs to provide connectivity for back-end and front-end networks respectively. In an IsilonSD Edge deployment, a node has virtual NICs allocated to it that are plumbed into virtual switches. We recommend that you connect the back-end and front-end Ethernet networks to two different subnets. The front-end Ethernet subnet is for client and management access and must be always accessible. A management or service IP address must be allocated to the cluster in the same subnet as the front-end IP range. The management server interacts with the cluster through this IP address. We recommend that you create a cluster with the maximum possible range of IP addresses considering future requirements. A supportability consideration for nodes is that their serial port device must be accessible over the network. This is accomplished through a virtual serial port concentrator (vSPC) that runs on the management server. The ESXi host of a node must be able to establish a TCP connection to port number 8080 on the management server. Make sure that there is a proper route and there is no firewall set up between the hosts and vCenter.

---

**IsilonSD Edge storage considerations**

In IsilonSD Edge, the boot disk and journal disk of a node are backed by storage devices. These devices determine the reliability of a node. The throughput and latency of the journal disk determines the write throughput and latency of the node. Hence we recommend that you host a journal disk over a flash-backed storage device. In summary, each node requires as many unique storage devices as the number of data disks required for a node. The storage device on a given host cannot be shared between the data disks of same node.

The architecture of a three-node cluster is shown in the following figure:
**IsilonSD cluster overview**

An IsilonSD cluster consists of three to six virtual nodes hosted on VMware ESXi. Each virtual node runs the Isilon OneFS operating system, the distributed file-system software that unites the nodes into a cluster.

The cluster's storage capacity varies depending on the following factors:

- IsilonSD license type
- Minimum data disk size
- Minimum number of data disks per node
- Number of nodes in the cluster

For more information on cluster capacity, see the *IsilonSD Edge Installation and Administration Guide*.

**IsilonSD Edge licensing overview**

With IsilonSD Edge, you can configure one license per cluster to manage your storage requirements. This license contains a cluster license and a OneFS features license. These two licenses determine the maximum number of nodes, capacity, memory, vCPU, disks, and IsilonSD cluster features that are available to you.

You can install IsilonSD Edge by configuring the free license that is bundled with the installation package. However, this license does not support all of the cluster features. To access advanced cluster features, you must purchase a license that supports these features. After obtaining the license keys, you can activate the licenses through the IsilonSD Management Server.

For questions related to the licensing support, contact the EMC eLicensing team. For information regarding the purchase of licenses, contact your EMC Isilon sales representative.
If you have deployed an IsilonSD cluster by configuring the free license, you are not entitled to any support from EMC Isilon for product-related questions. You can post your questions at https://community.emc.com/community/products/isilon for assistance.

The following table summarizes the availability of the cluster features depending on the type of licenses you have configured for your installation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Function</th>
<th>Free license</th>
<th>Paid license</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPools</td>
<td>Creates file pool policies that archive files to the cloud</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NFS, SMB, HTTP, FTP, HDFS</td>
<td>File-sharing and transfer protocols</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>InsightIQ</td>
<td>Monitors and analyzes the performance of a cluster to help you optimize storage resources and forecast capacity</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>Asynchronously replicates data on another cluster and supports failover and failback between clusters</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SmartLock</td>
<td>Protects critical data from malicious, accidental, or premature alteration or deletion.</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SmartConnect Advanced</td>
<td>Manages round-robin connections, CPU utilization, connection counting, and</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Note

IsilonSD Edge supports the SmartLock software module both in the enterprise and compliance modes. However, if the cluster is running in compliance mode, you cannot add new nodes to the cluster. Also, the IsilonSD cluster may not comply with SEC regulations.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Function</th>
<th>Free license</th>
<th>Paid license</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>throughput balancing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartPools</td>
<td>Groups nodes and files into pools</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SmartDedupe</td>
<td>Saves storage space on a cluster by reducing redundant data</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SmartQuota</td>
<td>Monitors and enforces administrator-defined storage limits</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SnapShotIQ</td>
<td>Creates snapshots to protect data against accidental data deletion and modification and restores modified or deleted data</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Isilon Swift</td>
<td>Provides object-based storage capabilities</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Two-way NDMP backup</td>
<td>A Network Data Management Protocol (NDMP) in which a data management application (DMA) on a backup server instructs a Backup Accelerator node on the cluster to back up data to a tape media server that is attached to the Backup Accelerator node</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Three-way NDMP backup</td>
<td>A Network Data Management Protocol (NDMP) in which a data management application (DMA) on a backup server instructs the cluster to back up data to a tape media server that is attached</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
IsilonSD Management Server overview

IsilonSD Management Server serves as a gateway for deploying OneFS clusters on VMware ESXi. You must successfully deploy and configure the management server in order to deploy the OneFS clusters.

The management server manages IsilonSD licenses and these licenses in turn determine the software modules that are available to you for accessing the advanced cluster capabilities. For information on deploying and configuring the IsilonSD Management Server, see the IsilonSD Edge Installation and Administration Guide.

After you deploy and configure the management server, the IsilonSD Management Plug-in gets registered within VMware vCenter. You can access this plug-in to perform the following tasks:

- Deploy a cluster
- Delete a cluster
- Configure IsilonSD licenses
- Upgrade IsilonSD licenses
- Add nodes to a cluster
- Remove nodes from a cluster
- Add drives
- Remove drives
- Smartfail nodes
- Smartfail drives

**Note**

You cannot perform the aforementioned tasks through the web administration interface.

For information about the above tasks, refer to the IsilonSD Edge Installation and Administration Guide.

Deploying and configuring IsilonSD clusters

You can use the IsilonSD Management Plug-in to deploy and configure IsilonSD clusters. After successfully registering a VMware vCenter server through the IsilonSD Management Server interface, the management plug-in gets installed within that vCenter server.

The management plug-in also enables you to scale the clusters by adding nodes. The number of nodes that you can add to your cluster depends on the number of licenses you own and on the underlying virtualization infrastructure.

You can also use the management plug-in to configure storage for the clusters, provided you configure direct attached storage through RAID, LUNs, or Raw Disks,
and then expose them to the ESXi host. The management plug-in thereafter creates virtual disks, formats the disks, and makes them available to the clusters.
CHAPTER 30

VMware integration

This section contains the following topics:

- VMware integration overview.................................................................1190
- VAAI........................................................................................................1190
- VASA.......................................................................................................1190
- Configuring VASA support....................................................................1191
- Disable or re-enable VASA.................................................................1193
- Troubleshooting VASA storage display failures...............................1193
VMware integration overview

OneFS integrates with VMware infrastructures, including vSphere, vCenter, and ESXi. VMware integration enables you to view information about and interact with Isilon clusters through VMware applications.

OneFS interacts with VMware infrastructures through VMware vSphere API for Storage Awareness (VASA) and VMware vSphere API for Array Integration (VAAI). For more information about VAAI, see the Isilon VAAI NAS Plug-In for Isilon Release Notes.

OneFS integrates with VMware vCenter Site Recovery Manager (SRM) through the Isilon Storage Replication Adapter (SRA). VMware SRM facilitates the migration and disaster recovery of virtual machines stored on Isilon clusters. Isilon SRA enables VMware vCenter SRM to automatically manage the setup, testing, and failover components of the disaster recovery processes for Isilon clusters. For information about Isilon SRA for VMware SRM, see the Isilon SRA for VMware SRM Release Notes.

VAAI

OneFS uses VMware vSphere API for Array Integration (VAAI) to support offloading specific virtual machine storage and management operations from VMware ESXi hypervisors to an Isilon cluster.

VAAI support enables you to accelerate the process of creating virtual machines and virtual disks. For OneFS to interact with your vSphere environment through VAAI, your VMware environment must include ESXi 5.0 or later hypervisors.

If you enable VAAI capabilities for an Isilon cluster, when you clone a virtual machine residing on the cluster through VMware, OneFS clones the files related to that virtual machine.

To enable OneFS to use VMware vSphere API for Array Integration (VAAI), you must install the VAAI NAS plug-in for Isilon on the ESXi server. For more information on the VAAI NAS plug-in for Isilon, see the VAAI NAS plug-in for Isilon Release Notes.

VASA

OneFS communicates with VMware vSphere through VMware vSphere API for Storage Awareness (VASA).

VASA support enables you to view information about Isilon clusters through vSphere, including Isilon-specific alarms in vCenter. VASA support also enables you to integrate with VMware profile driven storage by providing storage capabilities for Isilon clusters in vCenter. For OneFS to communicate with vSphere through VASA, your VMware environment must include ESXi 5.0 or later hypervisors.

Isilon VASA alarms

If the VASA service is enabled on an Isilon cluster and the cluster is added as a VMware vSphere API for Storage Awareness (VASA) vendor provider in vCenter, OneFS generates alarms in vSphere.

The following table describes the alarm that OneFS generates:
### Table

<table>
<thead>
<tr>
<th>Alarm name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thin-provisioned LUN capacity exceeded</td>
<td>There is not enough available space on the cluster to allocate space for writing data to thinly provisioned LUNs. If this condition persists, you will not be able to write to the virtual machine on this cluster. To resolve this issue, you must free storage space on the cluster.</td>
</tr>
</tbody>
</table>

### VASA storage capabilities

OneFS integrates with VMware vCenter through VMware vSphere API for Storage Awareness (VASA) to display storage capabilities of Isilon clusters in vCenter.

The following storage capabilities are displayed through vCenter:

**Archive**

The Isilon cluster is composed of Isilon NL-Series nodes. The cluster is configured for maximum capacity.

**Performance**

The Isilon cluster is composed of Isilon i-Series, Isilon X-Series, or Isilon S-Series nodes. The cluster is configured for maximum performance.

**Capacity**

The Isilon cluster is composed of Isilon X-Series nodes that do not contain SSDs. The cluster is configured for a balance between performance and capacity.

**Hybrid**

The Isilon cluster is composed of nodes associated with two or more storage capabilities. For example, if the cluster contained both Isilon S-Series and NL-Series nodes, the storage capability of the cluster is displayed as Hybrid.

### Configuring VASA support

To enable VMware vSphere API for Storage Awareness (VASA) support for a cluster, you must enable the VASA daemon on the cluster, download the Isilon vendor provider certificate and add the Isilon vendor provider in vCenter.

### Enable VASA

You must enable an Isilon cluster to communicate with VMware vSphere API for Storage Awareness (VASA) by enabling the VASA daemon.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Enable VASA by running the following command:
Download the Isilon vendor provider certificate

To add an Isilon cluster VASA vendor provider in VMware vCenter, you must use a vendor provider certificate.

Procedure

1. In a supported web browser, connect to an Isilon cluster at https://<IPAddress>, where <IPAddress> is the IP address of the Isilon cluster.
2. Add a security exception and view the security certificate to make sure that it is current.
3. Download the security certificate and save it to a location on your machine.
   For more information about exporting a security certificate, see the documentation of your browser.

Note

Record the location of where you saved the certificate. You will need this file path when adding the vendor provider in vCenter.

Add the Isilon vendor provider

You must add an Isilon cluster as a vendor provider in VMware vCenter before you can view information about the storage capabilities of the cluster through vCenter.

Before you begin

Download a vendor provider certificate.

Procedure

1. In vCenter, navigate to the Add Vendor Provider window.
2. Fill out the following fields in the Add Vendor Provider window:

   Name
   Type a name for this VASA provider. Specify as any string. For example, type EMC Isilon Systems.

   URL
   Type https://<IPAddress>:8081/vasaprovider, where <IPAddress> is the IP address of a node in the Isilon cluster.

   Login
   Type root.

   Password
   Type the password of the root user.

   Certificate location
   Type the file path of the vendor provider certificate for this cluster.
3. Select the **Use Vendor Provider Certificate** box.
4. Click **OK**.

## Disable or re-enable VASA

You can disable or re-enable an Isilon cluster to communicate with VMware vSphere through VMware vSphere API for Storage Awareness (VASA).

To disable support for VASA, you must disable both the VASA daemon and the Isilon web administration interface. You will not be able to administer the cluster through an internet browser while the web interface is disabled. To re-enable support for VASA, you must enable both the VASA daemon and the web interface.

### Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Disable or enable the web interface by running one of the following commands:
   - `isi services apache2 disable`
   - `isi services apache2 enable`
3. Disable or enable the VASA daemon by running one of the following commands:
   - `isi services isi_vasa_d disable`
   - `isi services isi_vasa_d enable`

## Troubleshooting VASA storage display failures

If you are unable to view information about Isilon clusters through vSphere, follow the troubleshooting tips given below to fix the issue.

- Verify that the vendor provider certificate is current and has not expired.
- Verify that the Isilon cluster is able to communicate with VASA through the VASA daemon. If the VASA daemon is disabled, run the following command to enable it:

```
isi services isi_vasa_d enable
```

- Verify that the date and time on the cluster is set correctly.
- Verify that data has been synchronized properly from vCenter.
VMware integration