## CONTENTS

**Figures**  
11

**Tables**  
13

**Preface**  
15

**Chapter 1**  
**Introduction**  
19

- EMC Avamar system overview ................................................................. 20
- Avamar server ................................................................................. 20
- Avamar clients .............................................................................. 23
- User interfaces ............................................................................... 24
- Data Domain system support ............................................................ 27
- Data deduplication .......................................................................... 27
- Security and networking ................................................................. 28
- Encryption ...................................................................................... 28
- IPv4 and IPv6 support .................................................................... 28

**Chapter 2**  
**Avamar Administrator**  
31

- Overview of Avamar Administrator .................................................. 32
- Installing Avamar Administrator ....................................................... 32
  - Installing Avamar Administrator on Microsoft Windows ............... 32
  - Installing Avamar Administrator on Linux ................................... 33
- Upgrading Avamar Administrator ..................................................... 34
- Uninstalling Avamar Administrator ............................................... 34
- Editing Avamar Administrator client preferences ............................. 34
- Setting a session time-out for Avamar Administrator ....................... 35
- Starting Avamar Administrator ........................................................ 36
- Starting Avamar Administrator from Avamar Enterprise Manager ....... 36
- Avamar Administrator dashboard .................................................... 38
  - Launcher buttons ......................................................................... 38
  - System Information panel .............................................................. 39
  - Activities panel .......................................................................... 41
  - Capacity panel .......................................................................... 42
  - Critical Events panel .................................................................. 43
- Avamar Administrator user interface elements ............................... 43
  - Status bar .................................................................................. 43
  - Navigation tree features ............................................................... 46
  - Mouse shortcuts ........................................................................... 47

**Chapter 3**  
**Client Management**  
49

- Overview of Avamar clients .............................................................. 50
- Client domains ............................................................................... 50
  - Creating a domain ....................................................................... 51
  - Editing domain information ......................................................... 51
  - Deleting a domain ....................................................................... 52
- Client registration ......................................................................... 52

EMC Avamar 7.1 Administration Guide  
3
Client-side registration................................................................. 52
Registering a client in Avamar Administrator................................. 53
Batch client registration............................................................... 53
Activating a client..........................................................................56
Client paging.................................................................................. 56
Pageable clients............................................................................. 56
Non-pageable clients..................................................................... 57
Editing client paging settings.......................................................... 58
Editing client information............................................................... 58
Viewing client properties............................................................... 59
Enabling and disabling a client........................................................ 60
Moving a client to a new domain...................................................... 60
Retiring a client...............................................................................61
Deleting a client.............................................................................. 61

Chapter 4  User Management and Authentication  63
Overview of Avamar user accounts.................................................. 64
User authentication..........................................................................64
Avamar internal authentication...................................................... 65
Directory service authentication..................................................... 65
Enterprise authentication...............................................................74
How Avamar authenticates users and assigns roles......................... 75
Roles.............................................................................................. 75
Administrator roles........................................................................ 76
Operator roles................................................................................ 76
User roles...................................................................................... 78
Adding a user to a client or domain................................................... 79
Editing user information.................................................................. 80
Deleting a user................................................................................ 81

Chapter 5  Backup  83
Performing on-demand backups....................................................... 84
Performing an on-demand backup of a client.................................... 84
Performing an on-demand group backup.......................................... 85
Scheduling backups......................................................................... 85
Datasets.......................................................................................... 86
Schedules....................................................................................... 91
Retention policies........................................................................... 96
Groups.......................................................................................... 101
Enabling scheduled backups.......................................................... 109
Monitoring backups........................................................................ 110
Canceling backups.......................................................................... 110
Managing completed backups......................................................... 111
Finding a completed backup to manage.......................................... 111
Validating a backup........................................................................ 112
Changing the expiration date for a backup...................................... 112
Changing the retention type for a backup........................................ 113
Viewing backup statistics............................................................... 114
Deleting a backup.......................................................................... 115

Chapter 6  Restore and Recovery  117
Restoring data from a backup.......................................................... 118
Finding a backup............................................................................ 118
Chapter 7  Server Administration  141

Server shutdown and restart ......................................................... 142
  Shutting down the server .......................................................... 142
  Restarting the server ................................................................ 142
  Stopping the MCS ................................................................... 143
  Starting the MCS ..................................................................... 143
  Getting MCS status .................................................................. 143
  Stopping the EMS .................................................................... 144
  Starting the EMS ..................................................................... 144
  Stopping the Avamar Desktop/Laptop server............................... 144
  Starting the Avamar Desktop/Laptop server............................... 144
  Getting Avamar Desktop/Laptop server status........................... 144

Suspending and resuming server activities ..................................... 145
  Suspending and resuming backups and restores......................... 145
  Suspending and resuming scheduled operations........................ 145
  Suspending and resuming maintenance activities........................ 145

Managing client sessions ............................................................... 145
  Monitoring client sessions ....................................................... 145
  Viewing a detailed client session log ........................................... 146
  Creating a Zip file for EMC Customer Support........................... 147
  Canceling a client session .......................................................... 148
  Resetting a client .................................................................... 148

Managing client agents and plug-ins .............................................. 148
  Adding a build record ............................................................... 149
  Editing version or build records ................................................. 149
  Deleting a build record ............................................................. 150
  Disabling all client initiated activations ...................................... 150
  Disabling all client initiated backups ........................................ 150

Backup and maintenance windows .............................................. 150
  Editing the backup and maintenance windows........................... 152

Checkpoints .............................................................................. 152
  Creating a checkpoint ............................................................... 153
  Deleting a checkpoint ............................................................... 153
  Rolling back to a checkpoint ..................................................... 153
Clearing a data integrity alert................................................................. 155
Generating and installing a server license........................................... 155
  Obtaining assigned license keys..................................................... 155
  Generating a license key information file......................................... 156
  Generating a permanent license key file......................................... 156
  Installing and activating a license.................................................. 157
Managing services.................................................................................. 158
Changing server passwords and OpenSSH keys................................. 159
MCS configuration settings................................................................... 160
  Backing up MCS data................................................................. 160
  Restoring MCS data................................................................. 161
  Reverting to the default MCS configuration settings....................... 162
Using network address translation (NAT)................................................... 164
Editing network settings for a single-node server...................................... 165
Adding a custom security notification for web browser logins...................... 165
Viewing and editing server contact information...................................... 166

Chapter 8 Server Monitoring 167
Recommended daily server monitoring.................................................. 168
Monitoring activities............................................................................. 168
  Activity Monitor details................................................................ 168
Monitoring server status and statistics............................................... 170
  Server Monitor tab.................................................................... 171
  Server Management tab............................................................. 173
Event monitoring.................................................................................... 181
  Event notifications.................................................................... 182
  Event profiles.......................................................................... 184
  Viewing events in the Event Monitor........................................... 189
  Viewing the event catalog........................................................ 190
  Acknowledging system events..................................................... 191
  Customizing error events.......................................................... 191
Server monitoring with syslog.............................................................. 191
  Configuring local syslog............................................................. 192
  Configuring remote syslog.......................................................... 193
Server monitoring with SNMP.............................................................. 196
  Configuring server monitoring with SNMP.................................. 197
Viewing Avamar server log files........................................................... 199
Audit logging......................................................................................... 200
  Viewing the Audit Log............................................................... 201
Automatic notifications to EMC Customer Support.................................. 202
  Email Home.......................................................................... 202
  ConnectEMC........................................................................ 203
Verifying system integrity...................................................................... 207

Chapter 9 Capacity Management 209
Viewing capacity utilization................................................................. 210
Capacity limits and thresholds............................................................. 210
Capacity forecasting............................................................................ 211
Viewing a graph of capacity utilization and forecasting.......................... 211
Average daily change rates.................................................................. 212
  Viewing the average daily change rate for an Avamar server........... 212
  Viewing the average daily change rate for clients......................... 212
Customizing capacity limits and behavior............................................ 213
  Editing capacity settings for Avamar Administrator....................... 213
Chapter 10 Replication

Overview of Avamar replication .............................................. 218
Types of replication .................................................................. 218
Replication scheduling ............................................................. 219
Replication authentication ......................................................... 220
Location of replicated backups on the destination server .......... 220
Retention of replicated backups ............................................... 221
Replication with Data Domain systems .................................... 221
Restore of replicated backups .................................................. 222
Configuring policy-based replication .................................. 222
Replication destinations ......................................................... 222
Replication groups .................................................................. 224
Configuring cron-based replication .................................. 229
Configuring cron-based replication with Avamar Administrator... 229
Configuring cron-based replication with Avamar Enterprise Manager ... 230
Performing on-demand replication ...................................... 232
Performing on-demand replication from the Replication window... 232
Performing on-demand replication from the Policy window ......... 232
Performing command line replication .................................. 233
Command reference ............................................................... 233
CLI examples ........................................................................ 243
Monitoring replication .......................................................... 244
Monitoring replication in Avamar Administrator .................. 244
Monitoring cron-based replication in Avamar Enterprise Manager . 245
Canceling a replication activity ............................................. 245
Restoring replicated backup data ........................................... 246

Chapter 11 Server Updates and Hotfixes

Overview of the Avamar server software update process ........... 250
Avamar Downloader Service .................................................. 250
AvlInstaller and Avamar Installation Manager ....................... 251
System Maintenance in Avamar Enterprise Manager ............. 251
Installing and configuring the Avamar Downloader Service ... 252
Avamar Downloader Service installation requirements ............... 252
Downloading the Avamar Downloader Service software .......... 252
Installing the Avamar Downloader Service software .............. 253
Defining an outbound rule for Microsoft Windows 7 hosts ....... 253
Configuring the Avamar Downloader Service ....................... 254
Updating the Avamar Downloader Service ......................... 256
Uninstalling the Avamar Downloader Service ....................... 256
Downloading new packages from the EMC repository .......... 256
Managing the Avamar Downloader Service ......................... 257
Viewing a list of packages available fordownload .................. 257
Verifying connectivity with the EMC repository ...................... 257
Monitoring Avamar Downloader Service status .......................... 257
Stopping and restarting the Avamar Downloader Service monitor ... 259
Troubleshooting Avamar Downloader Service issues .............. 259
Downloading and installing packages on the Avamar server ... 260
Viewing a list of installation packages on the Avamar server .................. 261
Deleting packages from the Avamar server ......................... 262
Viewing the history of installations ..................................... 263
## Chapter 12  Avamar Enterprise Manager 265

Overview of Avamar Enterprise Manager ...................................................... 266
  Comparison of Avamar Enterprise Manager with other Avamar user interfaces...................................................... 266
  Web browser security ........................................................................ 266
  Session time-outs ............................................................................. 266

Logging in to Avamar Enterprise Manager.................................................... 267

Avamar Enterprise Manager dashboard ....................................................... 267
  General system information........................................................... 268
  Capacity information...................................................................... 269
  Data protected information............................................................ 270
  Backup information........................................................................ 270

Adding an Avamar system in Avamar Enterprise Manager............................ 271

Viewing system status................................................................................. 272
  Last Contacted............................................................................... 272
  General server status information.................................................. 273
  Data Domain system information................................................... 276
  Garbage collection information...................................................... 277
  Last Checkpoint............................................................................. 278
  Last Validated Checkpoint............................................................. 278
  Replication..................................................................................... 279
  System Activity............................................................................... 279

Viewing capacity information...................................................................... 280

Viewing policy information.......................................................................... 280

Running reports.......................................................................................... 281

Managing cron-based replication............................................................... 281

Managing server updates and hotfixes........................................................ 282

Starting Avamar Client Manager.................................................................. 282

## Chapter 13  Avamar Client Manager 285

Overview of Avamar Client Manager............................................................ 286

Connection security.................................................................................... 286

Apache web server authentication......................................................... 286

Editing the session time-out period......................................................... 286

Increasing the JavaScript time-out period............................................... 287

Avamar Client Manager configuration properties....................................... 288

Starting Avamar Client Manager.................................................................. 289

Global tools................................................................................................ 289
  Selecting a server........................................................................... 290
  Filters............................................................................................. 290
  Viewing details.............................................................................. 296
  Exporting data.............................................................................. 296
  Setting the entries per page limit.................................................... 296
  Viewing tool tips............................................................................ 297

Overview..................................................................................................... 297
  Server Summary............................................................................. 297
  Dashboard..................................................................................... 298

Clients........................................................................................................ 301
  Client and server tools................................................................. 301
  Add Clients .................................................................................. 301
  Registered Clients......................................................................... 312
  Activated Clients.......................................................................... 312
  Failed Clients.............................................................................. 315
  Idle Clients.................................................................................. 315
## Avamar Desktop/Laptop

Overview of Avamar Desktop/Laptop .......................................................... 324

Requirements for Avamar Desktop/Laptop .............................................. 325
  - Client computer requirements ......................................................... 325
  - Web browser requirements .............................................................. 326
  - Network requirements .................................................................. 327

Avamar client software installation ....................................................... 327
  - Supported systems management tools ............................................ 328
  - Push installation on Windows computers ....................................... 328
  - Push installation on Macintosh computers ..................................... 329
  - Local client installation ................................................................. 330
  - Avamar client software uninstall .................................................... 330

Avamar Desktop/Laptop user authentication ........................................... 331
  - Pass-through authentication .......................................................... 331
  - LDAP authentication .................................................................... 332
  - NIS authentication ....................................................................... 334
  - Avamar authentication ................................................................. 334
  - Mixed authentication ................................................................. 335

Avamar Desktop/Laptop user interfaces .................................................. 335
  - Client UI ................................................................................. 335
  - Web UI ................................................................................... 337

Backup with Avamar Desktop/Laptop .................................................... 341
  - On-demand backups ................................................................... 341
  - Scheduled backups ..................................................................... 344
  - Allowing users to add data to backups ......................................... 345

Restore with Avamar Desktop/Laptop .................................................... 345
  - Finding data to restore ................................................................ 345
  - Restore types ............................................................................. 346
  - Restore requirements ................................................................. 346
  - Restore limits ............................................................................ 348
  - Restore of replicated backups .................................................... 349

Client backup and restore activity history ............................................. 349

Editing the Avamar Desktop/Laptop properties file ............................... 349
  - Avamar Desktop/Laptop properties ................................................. 349

Client log locations ................................................................................ 351

## Data Domain System Integration

Overview of Data Domain system integration ........................................ 354
  - Architecture of Avamar with Data Domain .................................... 354
  - File system backups on a Data Domain system ............................... 355
  - Application backups on a Data Domain system ............................... 356
<table>
<thead>
<tr>
<th>FIGURES</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avamar server nodes, stripes, and objects</td>
</tr>
<tr>
<td>2</td>
<td>Avamar server functional block diagram</td>
</tr>
<tr>
<td>3</td>
<td>Avamar client agent and plug-ins</td>
</tr>
<tr>
<td>4</td>
<td>Data deduplication</td>
</tr>
<tr>
<td>5</td>
<td>Avamar Administrator dashboard</td>
</tr>
<tr>
<td>6</td>
<td>Avamar Administrator status bar</td>
</tr>
<tr>
<td>7</td>
<td>Navigation tree features</td>
</tr>
<tr>
<td>8</td>
<td>Avamar domain example</td>
</tr>
<tr>
<td>9</td>
<td>Users in Avamar domains</td>
</tr>
<tr>
<td>10</td>
<td>Schedule start time, end time, and duration</td>
</tr>
<tr>
<td>11</td>
<td>Default backup and maintenance windows</td>
</tr>
<tr>
<td>12</td>
<td>Multi-node server configuration with NAT</td>
</tr>
<tr>
<td>13</td>
<td>Example replication domain structure</td>
</tr>
<tr>
<td>14</td>
<td>Avamar Enterprise Manager dashboard</td>
</tr>
<tr>
<td>15</td>
<td>View after uploading the example CSV file</td>
</tr>
<tr>
<td>16</td>
<td>Avamar architecture with a Data Domain system</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Revision history</td>
</tr>
<tr>
<td>2</td>
<td>MCS functions</td>
</tr>
<tr>
<td>3</td>
<td>Supported plug-ins</td>
</tr>
<tr>
<td>4</td>
<td>Comparison of supported enterprise management user interfaces</td>
</tr>
<tr>
<td>5</td>
<td>Dashboard launcher buttons</td>
</tr>
<tr>
<td>6</td>
<td>System State fields on the Avamar Administrator dashboard</td>
</tr>
<tr>
<td>7</td>
<td>Backup job fields in the Avamar Administrator dashboard</td>
</tr>
<tr>
<td>8</td>
<td>System alerts in the Critical Events panel</td>
</tr>
<tr>
<td>9</td>
<td>Launcher shortcut icons on the status bar</td>
</tr>
<tr>
<td>10</td>
<td>Scheduler and backup dispatching status messages</td>
</tr>
<tr>
<td>11</td>
<td>Status messages for unacknowledged events</td>
</tr>
<tr>
<td>12</td>
<td>Operational status messages for Avamar or Data Domain</td>
</tr>
<tr>
<td>13</td>
<td>Attributes for each entry in a clients definition file</td>
</tr>
<tr>
<td>14</td>
<td>Avamar user account information</td>
</tr>
<tr>
<td>15</td>
<td>Error messages during directory service configuration</td>
</tr>
<tr>
<td>16</td>
<td>Key/value pair rules for ldap.properties</td>
</tr>
<tr>
<td>17</td>
<td>Key/value pairs in ldap.properties</td>
</tr>
<tr>
<td>18</td>
<td>Administrator roles</td>
</tr>
<tr>
<td>19</td>
<td>Operator roles</td>
</tr>
<tr>
<td>20</td>
<td>User roles</td>
</tr>
<tr>
<td>21</td>
<td>Directories excluded from Default Dataset backups</td>
</tr>
<tr>
<td>22</td>
<td>Directories excluded from Unix Dataset backups</td>
</tr>
<tr>
<td>23</td>
<td>Directories excluded from Windows Dataset backups</td>
</tr>
<tr>
<td>24</td>
<td>Schedule types</td>
</tr>
<tr>
<td>25</td>
<td>Schedule catalog</td>
</tr>
<tr>
<td>26</td>
<td>Basic retention settings</td>
</tr>
<tr>
<td>27</td>
<td>Retention policy catalog</td>
</tr>
<tr>
<td>28</td>
<td>VMware groups</td>
</tr>
<tr>
<td>29</td>
<td>Target locations for system recovery backups of an Oracle Solaris client</td>
</tr>
<tr>
<td>30</td>
<td>Session Monitor tab properties</td>
</tr>
<tr>
<td>31</td>
<td>Avamar server maintenance activities</td>
</tr>
<tr>
<td>32</td>
<td>Checkpoint states</td>
</tr>
<tr>
<td>33</td>
<td>Default live file directory for MCS configuration files</td>
</tr>
<tr>
<td>34</td>
<td>MCS backup timestamp files</td>
</tr>
<tr>
<td>35</td>
<td>System monitoring tools and tasks</td>
</tr>
<tr>
<td>36</td>
<td>Activity Monitor details</td>
</tr>
<tr>
<td>37</td>
<td>Avamar tab details in the Server Monitor</td>
</tr>
<tr>
<td>38</td>
<td>Data Domain tab details in the Server Monitor</td>
</tr>
<tr>
<td>39</td>
<td>Data display based on selections on the Server Management tab</td>
</tr>
<tr>
<td>40</td>
<td>Bytes Protected Summary properties on the Server Management tab</td>
</tr>
<tr>
<td>41</td>
<td>Server properties on the Server Management tab</td>
</tr>
<tr>
<td>42</td>
<td>Module properties on the Server Management tab</td>
</tr>
<tr>
<td>43</td>
<td>Node properties on the Server Management tab</td>
</tr>
<tr>
<td>44</td>
<td>Partition properties on the Server Management tab</td>
</tr>
<tr>
<td>45</td>
<td>Data Domain system properties on the Server Management tab</td>
</tr>
<tr>
<td>46</td>
<td>Event information</td>
</tr>
<tr>
<td>47</td>
<td>Mappings of syslog fields to Avamar event data</td>
</tr>
<tr>
<td>48</td>
<td>Capacity limits and thresholds</td>
</tr>
<tr>
<td>49</td>
<td>Capacity forecast icons</td>
</tr>
<tr>
<td>50</td>
<td>Account options for the avrepl command</td>
</tr>
<tr>
<td>51</td>
<td>Logging options for the avrepl command</td>
</tr>
</tbody>
</table>
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

**Note**
This document was accurate at publication time. Go to EMC Online Support (https://support.EMC.com) to ensure that you are using the latest version of this document.

**Purpose**
This guide describes how to configure, administer, monitor, and maintain the Avamar system.

**Audience**
The information in this guide is primarily intended for system administrators who are responsible for maintaining servers and clients on a network, as well as operators who monitor daily backups and storage devices.

**Revision history**
The following table presents the revision history of this document.

**Table 1 Revision history**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 04       | January 15, 2015 | • Updated licensing procedure in Obtaining assigned license keys on page 155.  
• Updated licensing procedure in Generating a permanent license key file on page 156.  
• Updated Installing and activating a license on page 157 to correct typographical errors. |
| 03       | December 15, 2014 | • Moved Managing client agents and plug-ins on page 148 from the "Client Management" chapter to the "Server Management" chapter.  
• Added Restoring replicated backup data on page 246. |
|          |               | **Note**  
Revision 03 was erroneously published with "REV 02" on the cover page. Revision 03 can be identified by the copyright page which lists December, 2014 as the date of publication. |
| 02       | August 15, 2014 | • Added Boolean values to options in Command reference on page 233. |

**Note**
Revision 03 was erroneously published with "REV 02" on the cover page. Revision 03 can be identified by the copyright page which lists December, 2014 as the date of publication.
Table 1 Revision history (continued)

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>June 11, 2014</td>
<td>• Updated the explanation of replication configuration scenarios with a Data Domain system in <em>Replication with Data Domain systems on page 221.</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provided details on plug-in options and clarified scenarios with multiple backup types when changing the expiration setting for a replicated backup in <em>Creating a replication group on page 224.</em></td>
</tr>
<tr>
<td>01</td>
<td></td>
<td>Initial release of Avamar 7.1.</td>
</tr>
</tbody>
</table>

Related documentation

The following EMC publications provide additional information:

- *EMC Avamar Compatibility and Interoperability Matrix*
- *EMC Avamar Release Notes*
- *EMC Avamar Operational Best Practices*
- *EMC Avamar and EMC Data Domain System Integration Guide*
- *EMC Avamar Reports Guide*
- All EMC Avamar client and plug-in user guides

Special notice conventions used in this document

EMC uses the following conventions for special notices:

**NOTICE**

Addresses practices not related to personal injury.

**Note**

Presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

**Bold**

Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)

**Italic**

Use for full titles of publications referenced in text

**Monospace**

Use for:

- System code
- System output, such as an error message or script
- Pathnames, file names, prompts, and syntax
- Commands and options

**Monospace italic**

Use for variables

**Monospace bold**

Use for user input

[]

Square brackets enclose optional values
Where to get help

The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact EMC Customer Support.

To access the Avamar support page:
1. Go to https://support.EMC.com/products.
2. Type a product name in the Find a Product box.
3. Select the product from the list that appears.
4. Click the arrow next to the Find a Product box.
5. (Optional) Add the product to the My Products list by clicking Add to my products in the top right corner of the Support by Product page.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. Review the following documents in addition to product administration and user guides:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

The EMC Knowledgebase contains applicable solutions that you can search for either by solution number (for example, esgxxxxxx) or by keyword.

To search the EMC Knowledgebase:
1. Click the Search link at the top of the page.
2. Type either the solution number or keywords in the search box.
3. (Optional) Limit the search to specific products by typing a product name in the Scope by product box and then selecting the product from the list that appears.
4. Select Knowledgebase from the Scope by resource list.
5. (Optional) Specify advanced options by clicking Advanced options and specifying values in the available fields.
6. Click the search button.

Online communities

Visit EMC Community Network at http://community.EMC.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners and certified professionals for all EMC products.

Live chat

To engage EMC Customer Support by using live interactive chat, click Join Live Chat on the Service Center panel of the Avamar support page.
**Service Requests**
For in-depth help from EMC Customer Support, submit a service request by clicking **Create Service Requests** on the **Service Center** panel of the Avamar support page.

**Note**
To open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

To review an open service request, click the **Service Center** link on the **Service Center** panel, and then click **View and manage service requests**.

**Facilitating support**
EMC recommends that you enable ConnectEMC and Email Home on all Avamar systems:
- ConnectEMC automatically generates service requests for high priority events.
- Email Home emails configuration, capacity, and general system information to EMC Customer Support.

**Your comments**
Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to **DPAD.Doc.Feedback@emc.com**.

Please include the following information:
- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details that will help us address the documentation issue
CHAPTER 1

Introduction

This chapter includes the following topics:

- **EMC Avamar system overview** ................................................................. 20
- **Data deduplication** .............................................................................. 27
- **Security and networking** ................................................................. 28
EMC Avamar system overview

An EMC® Avamar® system is a client/server network backup and restore solution that consists of one or more Avamar servers and the network servers or desktop clients that back up data to those servers. The Avamar system also provides centralized management through the Avamar Administrator graphical management console software application.

Avamar server

Avamar is a hard-disk based IP network backup and restore solution. Avamar servers manufactured by EMC use internal hard disk storage. An Avamar server is a logical grouping of one or more nodes that is used to store and manage client backups.

Hardware manufacturers typically call their equipment servers (for instance, the Dell PowerEdge 2950 server). In the context of an Avamar system, this equipment is called a node. An Avamar node is a self-contained, rack-mountable, network-addressable computer that runs Avamar server software on the Linux operating system.

A stripe is a unit of disk drive space managed by Avamar to ensure fault tolerance.

In the Avamar system, an object is a single instance of deduplicated data. Each Avamar object inherently has a unique ID. Objects are stored and managed within stripes on the Avamar server.

Figure 1  Avamar server nodes, stripes, and objects

All Avamar servers store client backups and also provide essential processes and services required for client access and remote system administration.

Avamar servers are available in either single-node or scalable multi-node configurations. For the most part, when using Avamar Administrator management console software, all Avamar servers look and behave the same. The main differences among Avamar server configurations are the number of nodes and disk drives reported in the server monitor.

Documenting specific differences in Avamar server hardware configurations is beyond the scope of this guide. Whenever specific limitations and best practices for certain configurations are known, they are noted. However, these occasional notes should not be considered definitive or exhaustive. Consult your EMC sales representative or an EMC reseller for additional information about specific hardware.
Nodes

The primary building block in any Avamar server is a node. Each node is a self-contained, rack-mountable, network-addressable computer that runs Avamar server software on the Linux operating system.

Nodes can also contain internal storage in the form of hard disk drives. If the node is configured with internal storage (that is, a single-node server), it is internally mirrored to provide robust fault tolerance.

There are three types of nodes.

**Utility node**
A utility node is dedicated to scheduling and managing background Avamar server jobs. In scalable multi-node Avamar servers, a single utility node provides essential internal services for the server:

- Management Console Server (MCS)
- cronjob
- External authentication
- Network Time Protocol (NTP)
- Web access

Because utility nodes are dedicated to running these essential services on multi-node Avamar servers, they cannot be used to store backups. Single-node Avamar servers combine all of the features and functions of utility and storage nodes on a single node.

**Storage nodes**
Storage nodes are nodes that store backup data. Multiple storage nodes are configured with multi-node Avamar servers based upon performance and capacity requirements. You can add storage nodes to an Avamar server over time to expand performance with no downtime.

Avamar clients connect directly with Avamar storage nodes. Client connections and data are load balanced across storage nodes.

**NDMP Accelerator**
An NDMP Accelerator node is a specialized node that uses NDMP to provide data protection for certain NAS devices, including the EMC Celerra® IP storage systems and Network Appliance filers.

**Avamar server functional blocks**
The major Avamar server functional blocks include the data server, Management Console Server (MCS), and the Enterprise Manager Server (EMS). The following figure illustrates the interaction of these components.
When performing a backup, restore, or validation, Avamar backup clients communicate directly with the data server. All scheduled backups are initiated by the MCS scheduler.

Management Console Server (MCS)

The Management Console Server (MCS) provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by the Avamar Administrator graphical management console.

The following table provides details on the functions that the MCS provides.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client registry</td>
<td>Controls client registration and activation.</td>
</tr>
<tr>
<td>Account management</td>
<td>Used to create and manage domains, clients, users, and groups.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Used to create and export system reports. The <em>EMC Avamar Reports Guide</em> provides more information.</td>
</tr>
<tr>
<td>Events</td>
<td>Displays system events and activities.</td>
</tr>
<tr>
<td>Scheduler/ dispatcher</td>
<td>Controls when backup and restore operations occur, or if the operations can be queued for processing.</td>
</tr>
<tr>
<td>PostgreSQL database</td>
<td>Stores Avamar server data. PostgreSQL is an open architecture. Information in the MCS database is accessible through any PostgreSQL-compliant ODBC interface.</td>
</tr>
</tbody>
</table>
Table 2 MCS functions (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The MCS database filename is <code>mcdb</code>, and it is located on the utility node in the <code>/usr/local/avamar/var/mc/server_data/postgres</code> directory. MCS database contents are fully backed up on the Avamar server and can be restored if the MCS fails.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTICE</strong> The MCS database is intended for read-only access for reporting or query purposes. Do not manually modify any data in <code>mcdb</code> tables unless instructed to do so by EMC Customer Support. Directly modifying MCS operational data can cause loss of referential integrity, which could result in irretrievable loss of data.</td>
</tr>
</tbody>
</table>

**Enterprise Manager Server (EMS)**

The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar server information and provides a mechanism for managing Avamar servers by using a standard web browser. The EMS also communicates directly with MCSs, which are an integral part of all Avamar systems in an enterprise.

**Avamar clients**

Avamar provides client software for various computing platforms. Each client comprises a client agent and one or more plug-ins.

**Figure 3** Avamar client agent and plug-ins

**Agents**

Avamar agents are platform-specific software processes that run on the client and communicate with the Management Console Server (MCS) and any plug-ins installed on that client.

**Plug-ins**

There are two types of Avamar plug-ins:

- File system plug-ins are used to browse, back up, and restore files or directories on a specific client file system.
- Application plug-ins support backup and restore of databases or other special applications.

The following table lists the file system and application plug-ins that Avamar supports.
Table 3 Supported plug-ins

<table>
<thead>
<tr>
<th>Type of plug-in</th>
<th>Supported file systems and applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>File system</td>
<td>• Free BSD</td>
</tr>
<tr>
<td></td>
<td>• HP-UX</td>
</tr>
<tr>
<td></td>
<td>• IBM AIX</td>
</tr>
<tr>
<td></td>
<td>• Linux</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Volume Shadow Copy Service (VSS)</td>
</tr>
<tr>
<td></td>
<td>• SCO Open Server</td>
</tr>
<tr>
<td></td>
<td>• SCO UnixWare</td>
</tr>
<tr>
<td></td>
<td>• Oracle Solaris</td>
</tr>
<tr>
<td></td>
<td>• VMware</td>
</tr>
<tr>
<td>Application</td>
<td>• IBM DB2</td>
</tr>
<tr>
<td></td>
<td>• Lotus Domino</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Hyper-V</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Office SharePoint Server (MOSS)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server</td>
</tr>
<tr>
<td></td>
<td>• NDMP for NAS devices, including EMC Celerra IP storage systems and Network Appliance filers</td>
</tr>
<tr>
<td></td>
<td>• Oracle</td>
</tr>
<tr>
<td></td>
<td>• SAP with Oracle</td>
</tr>
<tr>
<td></td>
<td>• Sybase ASE</td>
</tr>
</tbody>
</table>

Client compatibility requirements are available in the *EMC Avamar Compatibility and Interoperability Matrix* on EMC Online Support at [https://support.EMC.com](https://support.EMC.com). The requirements in the matrix include supported operating systems and application versions.

The Avamar file system client and the plug-ins that you install on the host must have the same version number.

**User interfaces**

Several user interfaces are available in the Avamar system to facilitate management and monitoring.

**Avamar Administrator**

Avamar Administrator is a graphical management console software application that is used to remotely administer an Avamar system from a supported Windows client computer.
Avamar Enterprise Manager
Avamar Enterprise Manager is a web-based multi-system management console application that provides centralized Avamar system administration capabilities for larger businesses and enterprises. With Avamar Enterprise Manager, you can monitor all Avamar systems in the enterprise from a single web browser session.

An integrated dashboard provides an “at-a-glance” view that enables you to assess the operational status of each Avamar system and determine if backups are completing successfully.

EMC Backup & Recovery Manager
Like Avamar Enterprise Manager, Backup & Recovery Manager manages all Avamar systems in the enterprise. However, Backup & Recovery Manager additionally has an integrated user interface to manage the enterprise’s NetWorker servers and Data Domain backup targets.

The following table provides an overview comparison of the enterprise management capabilities of both products. The comparison focuses on Avamar-specific features and does not include the features in Backup & Recovery Manager that are specific to NetWorker servers and to Data Domain backup targets.

Table 4 Comparison of supported enterprise management user interfaces

<table>
<thead>
<tr>
<th>Comparison criteria</th>
<th>Avamar Enterprise Manager</th>
<th>Backup &amp; Recovery Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software host</td>
<td>Avamar utility node</td>
<td>VMware vSphere client</td>
</tr>
<tr>
<td>At-a-glance dashboard</td>
<td>Status view of Avamar systems</td>
<td>Select between consolidated and individual status views of Avamar systems, NetWorker servers, and Data Domain systems</td>
</tr>
<tr>
<td>Detailed backup and capacity information for Avamar systems</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitor backups</td>
<td>No</td>
<td>Yes, through an Activity Monitor screen. Use the Activity Monitor screen to view backup and replication details, and to start, stop, and restart tasks.</td>
</tr>
<tr>
<td>Replication management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Launch other management applications</td>
<td>• Avamar Administrator</td>
<td>• Avamar Administrator</td>
</tr>
<tr>
<td></td>
<td>• Avamar Client Manager</td>
<td>• Avamar Enterprise Manager</td>
</tr>
<tr>
<td></td>
<td>• Avamar Installation Manager</td>
<td>• Avamar Client Manager</td>
</tr>
<tr>
<td></td>
<td>• Avamar Installation Manager embedded in System Maintenance</td>
<td>• Avamar Installation Manager</td>
</tr>
<tr>
<td></td>
<td>• AvInstaller service</td>
<td></td>
</tr>
<tr>
<td>Display warnings, errors, and system alerts</td>
<td>No</td>
<td>Yes, in a quick-look graphical display and in detailed text. Filter the view by product, system, and category.</td>
</tr>
<tr>
<td>Management reports: select, view, and export</td>
<td>• Backup</td>
<td>• Backup</td>
</tr>
<tr>
<td></td>
<td>• System</td>
<td>• System</td>
</tr>
</tbody>
</table>
Table 4 Comparison of supported enterprise management user interfaces (continued)

<table>
<thead>
<tr>
<th>Comparison criteria</th>
<th>Avamar Enterprise Manager</th>
<th>Backup &amp; Recovery Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Configuration</td>
</tr>
</tbody>
</table>

The Backup & Recovery Manager product documentation provides complete details on the user interface.

**Avamar Client Manager**
Avamar Client Manager is a web-based management application that provides centralized Avamar client administration capabilities for larger businesses and enterprises. Avamar Client Manager facilitates the management of large numbers of Avamar clients.

Avamar Client Manager works with Avamar clients on a supported native operating system and Avamar clients on a supported operating system running in a VMware virtual machine. Avamar Client Manager cannot work with Avamar clients through virtual center, virtual machine, or virtual proxy configurations. The Avamar Client Manager UI displays supported Avamar clients and hides all unsupported clients.

**Avamar Desktop/Laptop**
Avamar Desktop/Laptop is a version of the Avamar client software that adds enhanced features for enterprise desktop and laptop computers.

The Avamar Desktop/Laptop features are designed to improve the functionality of Avamar client for Windows and Macintosh desktops and laptops. Many of the features are also supported on qualifying Linux computers.

Avamar Desktop/Laptop functionality is available through two user interfaces:

- The client local user interface (client UI) is installed on the client computer when you install either the Avamar Client for Windows or the Avamar Client for Mac OS X. With the client UI, an Avamar icon appears in the notification area ("system tray") on Windows computers or on the menu bar on Mac computers. Right-click the icon on Windows or click the icon on Mac to open the client menu, which provides access to backup, restore, program settings, and logs.

- Use the web browser user interface (web UI) to start an on-demand backup or restore, view backup and restore activity for a client computer, or configure other backup settings for a client computer.

**Avamar Installation Manager**
The Avamar Installation Manager user interface is part of the AvInstaller software that EMC Customer Support installs on the utility node during an Avamar server software installation or upgrade. Avamar Installation Manager facilitates the process of installing and upgrading the Avamar server.

**Avamar Downloader Service**
The Avamar Downloader Service manages the process of checking for and downloading Avamar server software updates. The Avamar Downloader Service software runs on a stand-alone Microsoft Windows server that allows network access to EMC sites on the Internet and to all Avamar servers at a site.

**Avamar Web Restore**
Avamar Web Restore provides access to the following functionality:

- Search for or browse backed up directories and files to restore.
• Download Avamar client software.
• View Avamar product documentation that is stored on the Avamar server.

**NOTICE**

The most up-to-date Avamar product documentation is available on EMC Online Support.

---

**Data Domain system support**

You can store backups on either the Avamar server or an EMC Data Domain® system. Backup metadata is stored on the Avamar server.

Before you can store backups on a Data Domain system, you must add the Data Domain system to the Avamar configuration by using Avamar Administrator. Then you select the Data Domain system in the plug-in options when you perform an on-demand backup or when you create a dataset for a scheduled backup. You can also use the command line interface (CLI) to perform backups to a Data Domain system.

The steps to restore backups are the same whether you restore from the Avamar server or a Data Domain system. The restore process determines the location of the backup and restores the backup.

---

**Data deduplication**

Data deduplication is a key feature of the Avamar system. Data deduplication ensures that each unique sub-file, variable length object is stored only once across sites and servers.

During backups, Avamar client software examines the client file system and applies a data deduplication algorithm that identifies redundant data sequences and breaks the client file system into sub-file, variable length data segments. Each data segment is assigned a unique ID.

The client software then determines whether this unique ID has already been stored on the Avamar server. If this object resides on the Avamar server, a link to the stored object is referenced in the backup.

Once an object has been stored on the server, it never has to be re-sent over the network, no matter how many times it is encountered on any number of clients. This feature significantly reduces network traffic and provides for greatly enhanced storage efficiency on the server.

**Figure 4** Data deduplication

1. Break data into atom (sub-file, variable-length segments of data)
2. Send and store each atom only once
3. Avamar backup repository

...up to 500 times daily data reduction
Security and networking

The following sections provide an overview of key Avamar security and networking features. The *EMC Avamar Product Security Guide* provides full details on product security and network configuration.

Encryption

Avamar can encrypt all data sent between clients and the server “in flight.”

To provide enhanced security during client/server data transfers, Avamar supports two levels of “in-flight” encryption: medium and high.

You can set the encryption level on a client-by-client basis in client properties, or for an entire group of clients in group properties. You also can disable “in-flight” encryption entirely.

Each individual Avamar server can also be configured to encrypt data stored on the server “at rest.” The decision to encrypt all data stored in an Avamar server is typically a one-time decision that is made when the server is initially deployed at a customer site.

IPv4 and IPv6 support

Internet Protocol (IP) is a set of communication rules for routing traffic across networks to addressable devices like Avamar system components. The Avamar system supports both Internet Protocol Version 4 (IPv4) and IPv6 address notation.

**IPv4 notation**

IPv4 notation is displayed as four octets, that is 1- to 3-digit base 10 numbers in a range of 0 to 255. Each octet is separated by periods and represents 8 bits of data for a total address space of 32 bits.

A subnet mask identifies a range (a subnet) of IP addresses on the same network. For Avamar purposes, the subnet mask is /24, representative of a 255.255.255.0 netmask.

An example IPv4 address and subnet mask is `10.99.99.99/24`.

IPv4 notation cannot be abbreviated. If an octet has zero (0) value, it is indicated by a 0.

**IPv6 notation**

IPv6 notation is displayed as 16 octets, that is 2-digit hexadecimal (base 16) numbers in a range of 00 to FF. Octets are combined by pairs into eight groups separated by colons, each group representing 16 bits of data for a total address space of 128 bits.

For Avamar purposes, the subnet mask (called prefix in IPv6) is /64.

An example IPv6 address and prefix is `2001:0db8:85a3:0042:1000:8a2e:0370:7334/64`.

As for a group with zero (0) value, IPv6 notation is different from IPv4 in that it can be abbreviated. For example, the following is a valid IPv6 address and prefix: `2001:db8:abcd:0012::0/64`.

**Avamar IP configurations**

In the Avamar user interface, an IP address may be displayed in either IPv4 or IPv6 notation. The type notation you see is dependent on how that particular component was initially configured when the hardware and software were installed.

IPv4 and IPv6 are not interoperable. They operate in separate stacks (that is, parallel, independent networks).
Avamar can be set up in a dual stack configuration. In that case, each Avamar component may have an IPv4 address, an IPv6 address, or both (one primary and the other secondary). The Avamar user interface may display a component's primary address or both dual stack addresses. So if you see the following IP address for a particular device, it is configured as dual stack: 10.99.99.99/24, 2001:db8:abcd:0012::0/64.
Introduction
CHAPTER 2
Avamar Administrator

This chapter includes the following topics:

- Overview of Avamar Administrator ................................................................. 32
- Installing Avamar Administrator ..................................................................... 32
- Upgrading Avamar Administrator ................................................................... 34
- Uninstalling Avamar Administrator ............................................................... 34
- Editing Avamar Administrator client preferences ........................................... 34
- Setting a session time-out for Avamar Administrator ....................................... 35
- Starting Avamar Administrator ....................................................................... 36
- Starting Avamar Administrator from Avamar Enterprise Manager ............... 36
- Avamar Administrator dashboard .................................................................. 38
- Avamar Administrator user interface elements .............................................. 43
Overview of Avamar Administrator

Avamar Administrator is a graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.

You can install Avamar Administrator on a computer and launch the software from the desktop icon or a command shell, or you can launch Avamar Administrator from Avamar Enterprise Manager.

Avamar Administrator is the primary user interface for monitoring and configuring the Avamar system. You can monitor backup, restore, and system maintenance activities, as well as configure backup policies, manage clients and user accounts, and configure other system settings.

You can administer one Avamar system at a time from Avamar Administrator.

The Avamar Administrator dashboard appears when you log in to Avamar Administrator. The dashboard provides an at-a-glance view of Avamar system status, as well as access to all functionality through menus and launcher buttons.

Installing Avamar Administrator

You can install Avamar Administrator on supported Microsoft Windows and 64-bit Linux platforms.

Details on support for specific operating system versions is available in the EMC Avamar Compatibility and Interoperability Matrix on EMC Online Support at https://support.EMC.com.

Installing Avamar Administrator on Microsoft Windows

Procedure

1. Log in to the computer on which you are installing Avamar Administrator.
2. Open a web browser and type the following URL:
   
   http://Avamar_server

   where Avamar_server is the DNS name or IP address of the Avamar server.

   The EMC Avamar Web Restore page appears.
3. Click Downloads.
4. Click + next to the Windows (32 bit) folder.
5. Click + next to the Microsoft Windows Vista, 7, 8, 8.1, Microsoft Windows Server 2008 folder.
6. Locate the Java Runtime Environment (JRE) install package, which is typically the last entry in the folder.
7. If the JRE on the client computer is older than the JRE hosted on the Avamar server, download and install the newer JRE from the Avamar server:
   a. Click the jre-version-windows-i586-p install package, where version is the JRE version.
   b. Open the installation file, or download the file and then open it from the saved location.
c. Follow the onscreen instructions to complete the JRE installation.

8. Click the `AvamarConsoleMultiple-windows-x86-version.exe` install package, where `version` is the Avamar Administrator software version.

   Avamar Administrator is only available as a 32-bit application. However, it will also run on 64-bit Windows computers.

9. Open the installation file, or download the file and then open it from the saved location.

10. Follow the onscreen instructions to complete the Avamar Administrator software installation.

### Installing Avamar Administrator on Linux

**Procedure**

1. Log in to the computer on which you are installing Avamar Administrator.

2. Open a web browser and type the following URL:
   
   http://Avamar_server
   
   where Avamar_server is the DNS name or IP address of the Avamar server.

   The EMC Avamar Web Restore page appears.

3. Click **Downloads**.

4. Click + next to the **Linux for x86 (64 bit)** folder.

5. Click + next to the **Red Hat Enterprise Linux 4** folder.

6. Locate the JRE RPM install package, which is typically the last entry in the folder.

7. If the JRE on the client computer is older than the JRE hosted on the Avamar server, then download the install package to a temporary folder such as `/tmp`.

   The install package filename is `jre-version-platform.rpm`, where `version` is the JRE version and `platform` is the computing platform.

8. **Download the** `AvamarConsole-linux-rhel4-x86_64-version.rpm` **install package to a temporary install folder such as /tmp.**

   Use the Red Hat Enterprise Linux 4 install packages for all supported Linux versions.

9. Open a command shell and log in as root on the computer where the software will be installed.

10. Change directory to the temporary folder to which you downloaded the install packages by typing a command such as `cd /tmp`.

11. If you downloaded a JRE, install it by typing `rpm -ivh jre-version-platform.rpm`.

12. Follow the onscreen instructions to complete the JRE installation.

13. Install Avamar Administrator by typing `rpm -ih AvamarConsole-linux-rhel4-x86_64-version.rpm`

   The install process prompts you to run `avsetup_mcc` to configure Avamar Administrator.


   The configuration process prompts you to specify the location of the JRE installation.

15. Press **Enter** to accept the default install location.
The configuration process prompts you to specify the root directory of the Avamar software.

16. Press Enter to accept the default install location.

A confirmation message appears.

Upgrading Avamar Administrator

You can upgrade Avamar Administrator on either Microsoft Windows or Linux computers.

Procedure

- You can install multiple versions of Avamar Administrator on the same Microsoft Windows computer. If you install Avamar Administrator on a computer where it is already installed, select a destination folder carefully during the installation procedure:
  - To keep an older version, select a different installation folder.
  - To directly upgrade the Avamar Administrator installation, select the same installation folder. The two versions are identified by their full version numbers.
- To upgrade the Avamar Administrator software on the Linux platform, uninstall the previous version and install the new software. Use of the Linux software upgrade command (rpm -Uh) is not supported.

Uninstalling Avamar Administrator

You can uninstall Avamar Administrator from either a Microsoft Windows or a Linux computer.

Before you begin

Close any open Avamar Administrator sessions. Otherwise, the uninstall process may not complete successfully, which can complicate future installation of Avamar Administrator.

Procedure

- On a Microsoft Windows computer, open the Windows Start menu and select Programs > EMC Avamar > Administrator > version > Uninstall, and then click OK on the confirmation message.
- On a Linux computer:
  a. Open a command shell and log in as root.
  b. Determine the package name by typing rpm -qa | grep Av.
  c. Type rpm -e AvamarConsole-version, where AvamarConsole-version is the Avamar Administrator install package.

Editing Avamar Administrator client preferences

You can edit some Avamar Administrator client preferences directly in Avamar Administrator. However, a number of preferences are only available for editing in the mcclient.xml client preferences file.

Procedure

1. Close Avamar Administrator.
2. Open `install_dir/var/mc/gui_data/prefs/mcclient.xml` in a text editor, where `install_dir` is the Avamar Administrator installation directory.

3. Edit the preference elements.

4. Save and close the file.

   The changes take effect the next time that you start Avamar Administrator.

## Setting a session time-out for Avamar Administrator

An Avamar Administrator session remains active until a user closes the application by choosing Exit from the menu. To protect the assets available through Avamar Administrator, set a session time-out value. The value applies to all Avamar Administrator sessions connected to the Avamar server.

After you set a session time-out value, Avamar Administrator monitors the UI for activity. When Avamar Administrator detects no mouse or keyboard activity within the UI for the number of minutes set in the time-out value, it shuts down all processes, closes all windows, and displays the Inactive dialog box.

### Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press Enter.

2. Stop the Management Console Server (mcs) service by typing `dpnctl stop mcs`.


4. Open `mcserver.xml` in a plain text editor.

5. Find the `<node name="mon">` entry.

6. Edit the value of the `<entry key="consoleInactiveMinutesToReport" value="n" />` entry within the `<node name="mon">` entry, where `n` is the session time-out value in minutes.

7. Save the change and close the text editor.

8. Start the MCS and the scheduler by typing:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

9. Close the command shell.

   Avamar Administrator uses the new session time-out value the next time that you open Avamar Administrator and connect with the Avamar server.
Starting Avamar Administrator

These steps explain how to start Avamar Administrator when it is installed on a local computer. You can also launch Avamar Administrator from an Avamar Enterprise Manager session.

Before you begin

Ensure that a minimum of 512 MB of system RAM is available on the local computer. Otherwise, Java heap errors may occur when you start Avamar Administrator.

Procedure

1. Launch Avamar Administrator:
   - On Microsoft Windows platforms, double-click the Avamar Administrator icon on the Windows desktop.
   - On Linux platforms, open a command shell and type mcgui.
   The login window appears.

2. In the User Name box, type a username.
   To access all Avamar Administrator functionality, the account associated with this username must be assigned the role of Administrator. Other roles provide reduced functionality.
   To authenticate by using the internal authentication system, type only a username. To authenticate by using the enterprise authentication system (deprecated) or directory service authentication, type username@server, where username is the username and server is the fully qualified domain name of the authentication server.
   If you use the format username@server for the username, then the system attempts to authenticate the user by using enterprise authentication. If authentication with enterprise authentication fails, then the system attempts to authenticate the user by using directory service authentication.

3. In the Password box, type the password for the user account.

4. In the Domain Name box, type the Avamar domain to log in to:
   - To log in to the root domain, use the default entry of a single slash (/) character.
   - To log in to a specific domain or subdomain, type the domain path by using the syntax /domain/subdomain1/subdomain2.

5. In the Administrator Server box, type the IP address or DNS name of the Avamar server to log in to.

   Note
   To prepopulate the Administrator Server and Domain Name boxes with a specific Avamar server and domain every time that you start Avamar Administrator, click Options and type that server name and domain in the Default Administrator Server and Default Domain boxes, respectively.

6. Click Log On.
   The Avamar Administrator dashboard appears.

Starting Avamar Administrator from Avamar Enterprise Manager

You can launch Avamar Administrator directly from an Avamar Enterprise Manager session. Avamar Enterprise Manager uses the Java Webstart technology from Sun
Microsystems to start Avamar Administrator. Webstart is an environment for automatic
download of the latest version of an application from the Web. By incorporating this
technology into Avamar Enterprise Manager, you no longer have to manually install
individual versions of Avamar Administrator software to maintain an Avamar system in
the enterprise.

Before you begin

- Install Java Runtime Environment (JRE):
  1. Open a web browser and type the following URL:
     \[ \text{http://Avamar_server} \]
     where \text{Avamar_server} is the DNS name or IP address of the Avamar server.
     The \text{EMC Avamar Web Restore} page appears.
   2. Click Downloads.
   3. Click + next to the Windows (32 bit) folder.
   4. Click + next to the Microsoft Windows Vista, 7, 8, 8.1, Microsoft Windows Server
      2008 folder.
   5. Click the link for the JRE install package, which is typically the last entry in the
      folder, and download or open the installation file.
   6. Follow the onscreen instructions to complete the JRE installation.

- Ensure that you are using the correct version of the Java Web Start Launcher:
  1. In Windows Explorer, select Tools > Folder Options.
  2. In the Folder Options dialog box, select the File Types tab.
  3. In the Registered file types list, select the JNLP file type and click Change.
  4. In the Open With dialog box, click Browse, and then navigate to the directory
     where JRE 1.5.x is installed.
  5. In the bin folder, select javaws.exe and click Open.
  6. Click Apply on the Folder Options dialog box.

\section*{NOTICE}

Under certain circumstances, stale Java temporary Internet files can cause errors when
attempting to launch Avamar Administrator from an Avamar Enterprise Manager session.
If this occurs on Windows computers, open the Windows Start menu and select Control
Panel > Java. In the Temporary Internet Files area of the Java Control Panel, click Delete
Files. A confirmation message appears. Ensure that all temporary Internet file types are
selected and click OK.

Procedure

1. Open a web browser and type the following URL:
   \[ \text{http://Avamar_server/em} \]
   where \text{Avamar_server} is the DNS name or IP address of the Avamar server that hosts
   the EMS.
   The login page appears.
2. Select Administrator.
3. In the User Name box, type the username for the Avamar administrative user account.
4. In the Domain Name box, type the Avamar domain to log in to:
To log in to the root domain, use the default entry of a single slash (/) character.

To log in to a specific domain or subdomain, type the domain path by using the syntax /domain/subdomain1/subdomain2.

5. From the Administrator Server list, select the Avamar server to manage.
6. Click Launch.
7. If a security warning appears, click Yes to proceed with the login.
   The Avamar Administrator login window appears.
8. In the Password box, type the password for the Avamar administrative user account.
9. Click Log On.
   The Avamar Administrator dashboard appears.

Avamar Administrator dashboard

The Avamar Administrator dashboard provides an at-a-glance view of Avamar system status, as well as access to all functionality through menus and launcher buttons.

The dashboard appears when you log in to Avamar Administrator.

Figure 5 Avamar Administrator dashboard

Launcher buttons

The dashboard launcher buttons invoke persistent windows to perform tasks in Avamar Administrator.

Table 5 Dashboard launcher buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Window</th>
<th>Available tasks in the window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy</td>
<td>Create and manage groups, datasets, schedules, and retention policies.</td>
</tr>
<tr>
<td>Backup &amp; Restore</td>
<td>Backup, Restore and Manage</td>
<td>Perform on-demand backups and restores, and manage completed backups.</td>
</tr>
</tbody>
</table>
Table 5 Dashboard launcher buttons (continued)

<table>
<thead>
<tr>
<th>Button</th>
<th>Window</th>
<th>Available tasks in the window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Administration</td>
<td>Create and manage domains, clients, users, system events, and services.</td>
</tr>
<tr>
<td>Activity</td>
<td>Activity</td>
<td>Monitor backup, restore, backup validation, and replication activity.</td>
</tr>
<tr>
<td>Server</td>
<td>Server</td>
<td>Monitor server activity and client sessions.</td>
</tr>
<tr>
<td>Replication</td>
<td>Replication</td>
<td>Configure policy-based replication.</td>
</tr>
</tbody>
</table>

System Information panel

The **System Information** panel on the Avamar Administrator dashboard provides an overview of important system statistics.

**System State**

The **System State** icon provides a status indicator for overall system status:

- A green checkmark icon indicates that the system is fully operational.
- A yellow caution icon indicates that there is an issue with the system that requires attention, but backups can continue.
- A red x icon indicates that there is a problem with the system that requires immediate attention. Backups cannot occur until you resolve the problem.

Click the arrow icon next to the **System State** field to view more detailed system state information. The following table provides details about system state information in the dashboard.

Table 6 System State fields on the Avamar Administrator dashboard

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Avamar State | Summarizes the current operational state of the Avamar server:  
  - A green checkmark indicates that the Avamar server is fully operational.  
  - A yellow caution icon indicates that there are one or more issues with the Avamar server that require attention, but backups can continue.  
  - A red x icon indicates that the Avamar server is in the Inactive, Offline, Degraded, or Unknown operational state. |
| Capacity State | Summarizes system capacity usage and health:  
  - A green checkmark indicates that the system has used greater than 75% of the total storage capacity.  
  - A yellow caution icon indicates that the system has used greater than 75% but less than 90% of the total storage capacity. Consider adding capacity or deleting old backups.  
  - A red x icon indicates that the system has used more than 90% of the total storage capacity. No new backups can occur until you add capacity or delete old backups. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Events</td>
<td>Summarizes unacknowledged system events:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that there are no critical system events that require acknowledgment.</td>
</tr>
<tr>
<td></td>
<td>- A yellow caution icon indicates that one or more warning events require acknowledgment.</td>
</tr>
<tr>
<td></td>
<td>- A red x icon indicates that one or more system error events require acknowledgment.</td>
</tr>
<tr>
<td>Last Checkpoint</td>
<td>Specifies the amount of time since the last checkpoint occurred:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that a checkpoint successfully completed on this Avamar server within the past 24 hours.</td>
</tr>
<tr>
<td></td>
<td>- A yellow caution icon indicates that a checkpoint successfully completed on this Avamar server between 24 and 48 hours ago.</td>
</tr>
<tr>
<td></td>
<td>- A red x icon indicates that more than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.</td>
</tr>
<tr>
<td>Last Validated Checkpoint</td>
<td>Specifies the amount of time since the last checkpoint validation occurred:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that a checkpoint validation successfully completed on this Avamar server within the past 48 hours.</td>
</tr>
<tr>
<td></td>
<td>- A yellow caution icon indicates that a checkpoint validation successfully completed on this Avamar server between 48 and 72 hours ago.</td>
</tr>
<tr>
<td></td>
<td>- A red x icon indicates that more than 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server.</td>
</tr>
<tr>
<td>Last Garbage Collection</td>
<td>Specifies the amount of time since the last garbage collection occurred:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that garbage collection successfully completed on this Avamar server within the past 30 hours.</td>
</tr>
<tr>
<td></td>
<td>- A yellow caution icon indicates that garbage collection has not successfully completed on this Avamar server within the past 30 hours.</td>
</tr>
<tr>
<td></td>
<td>- A red x icon indicates that garbage collection encountered an error the last time it was run.</td>
</tr>
<tr>
<td>Data Domain System(s) State</td>
<td>Summarizes the operational state of all Data Domain systems that have been added to this Avamar server:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that all Data Domain systems are fully operational.</td>
</tr>
<tr>
<td></td>
<td>- A yellow caution icon indicates that there one or more issues with Data Domain systems that require attention. However, backups can continue.</td>
</tr>
<tr>
<td></td>
<td>- A red x icon indicates that there one or more problems with Data Domain systems that require immediate attention. Backups cannot occur until all problems are resolved.</td>
</tr>
</tbody>
</table>

**Scheduler State**

The **Scheduler State** field indicates whether scheduled activities are running or suspended. Scheduled activities include backups, email notifications, and replications. If
scheduled activities are running, then the activities will occur at the scheduled time. If scheduled activities are suspended, then the activities will not occur until you resume the activities.

Click **Suspend** or **Resume** to suspend or resume scheduled activities.

**Maintenance Activities State**
The **Maintenance Activities State** field indicates whether maintenance activities are running or suspended. Maintenance activities include checkpoints, checkpoint validation, and garbage collection. If maintenance activities are running, then the activities will occur at the scheduled time. If maintenance activities are suspended, then the activities will not occur until you resume the activities from the **Server** window.

**License Expiration**
The **License Expiration** field lists the calendar date on which the license for the Avamar server expires.

**Data Protected**
The **Data Protected** field lists the total amount of client data protected (in bytes).

**Data Protected in last 24 hours**
The **Data Protected in last 24 hours** field lists the total amount of client data protected (in bytes) during the past 24 hours.

### Activities panel

The **Activities** panel in the Avamar Administrator dashboard provides status and detailed information for backup and replication jobs.

**Backup Jobs**
The main status icon for backup jobs in the **Activities** panel indicates whether scheduled backups will occur at the scheduled time or if there is a problem that is preventing scheduled backups from occurring.

Click the arrow button next to the **Backup Jobs** field to display detailed status information. The following table provides details on the status information available for backup jobs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduler State</strong></td>
<td>Specifies whether the scheduler for activities such as backups, email notifications, and replications is running or suspended.</td>
</tr>
<tr>
<td><strong>Dispatcher State</strong></td>
<td>Specifies whether the dispatcher is running or suspended. If the dispatcher is suspended, then the Avamar server has reached the health check limit and no backups will occur until this is resolved. Capacity limits and thresholds on page 210 provides details.</td>
</tr>
<tr>
<td><strong>Backup Groups Enabled</strong></td>
<td>Specifies the number of backup groups that are enabled. Click the window icon to the right of the field to open the <strong>Policy</strong> window and manage groups.</td>
</tr>
</tbody>
</table>

You can also view the total number of backup jobs that:

- Are pending.
- Are currently running.
- Failed within the specified time period.
- Succeeded with exceptions within the specified time period.
Succeeded within the specified time period. Select a value from the Period list to control the time period for the results of completed backups.

Click a numeric button to view detailed information for a backup job in the Activity Monitor.

Replication Jobs
The main status icon for replication jobs in the Activities panel indicates whether replication jobs will occur:

- A green checkmark icon indicates that scheduled replication jobs will occur at the scheduled time.
- A yellow caution icon indicates that one or more replication groups are disabled.
- A red x icon indicates that scheduled replication jobs will not occur. This might be due to the scheduler being in a suspended state, all replication groups being disabled, or some other issue with the system.

Click the window icon to the right of the icon to configure replication groups in the Replication window.

You can also view the total number of replication jobs that:

- Are pending.
- Are currently running.
- Failed within the specified time period.
- Succeeded with exceptions within the specified time period.
- Succeeded within the specified time period.

Select a value from the Period list to control the time period for the results of completed replication jobs.

Click a numeric button to view detailed information for a replication job in the Replication Report.

Capacity panel

The Capacity panel on the Avamar Administrator dashboard provides system capacity usage and forecasting information for the Avamar server and any Data Domain systems that have been added.

Avamar server capacity information
The capacity usage of the Avamar server is shown as a vertical bar with color indicators for usage levels based on the percentage of total capacity.

Text fields list the total capacity of the Avamar server in terabytes (TB), the percentage of used capacity, and a capacity forecast for systems with sufficient historical data. A capacity forecast is the expected amount of time that each system component can consume storage at the current rate.

If the Avamar system configuration includes a Data Domain system, then Avamar server capacity calculations include metadata usage for the Data Domain system.

Click the link on the Avamar server name to view detailed system information in the Server Monitor, including Data Domain metadata utilization, if applicable.

Data Domain system capacity information
Each configured Data Domain system is listed separately in the Capacity panel.

The capacity usage of the Data Domain system is shown as a vertical bar with color indicators for usage levels based on the percentage of total capacity.
Text fields list the total capacity of the Data Domain system in gibibytes (GiB), the amount of used capacity as a percentage and value in GiB, the total amount of available capacity in GiB, and a capacity forecast for systems with sufficient historical data.

Click the link on the Data Domain system name to view the Data Domain Enterprise Manager web page for that system.

**Critical Events panel**

The **Critical Events** panel in the Avamar Administrator dashboard shows the number of unacknowledged serious system errors and warnings that have occurred, as well as certain defined system alerts.

To clear these serious system errors and warnings (that is, reset the count to zero), you must explicitly acknowledge them. **Acknowledging system events on page 191** provides details.

The following table lists the system alerts that may appear in the **Critical Events** panel.

<table>
<thead>
<tr>
<th>Type of alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFS check failures</td>
<td>If the last checkpoint validation failed, then a data integrity alert is generated. Investigate and address the issue as soon as possible. <a href="#">Creating a checkpoint on page 153</a> provides more information.</td>
</tr>
<tr>
<td>Capacity warnings</td>
<td>These alerts warn that the system is approaching critical system storage capacity usage thresholds.</td>
</tr>
<tr>
<td>Capacity usage warnings</td>
<td>These alerts warn that the system is approaching critical system storage capacity forecasting thresholds.</td>
</tr>
</tbody>
</table>

**Avamar Administrator user interface elements**

All of the primary windows in the Avamar Administrator user interface share several elements and functionality in common, including the status bar, navigation tree features, and mouse shortcuts.

**Status bar**

The status bar at the bottom of each Avamar Administrator persistent window conveys status information and provides a single-click shortcut to specific features and functions.

**Figure 6** Avamar Administrator status bar

![Status bar](Sch/Disp: Running/Running ▶ No Unacknowledged Events ▶ Server: Full Access)

**Launcher shortcuts**

The shortcut icons on the left side of the status bar provide shortcuts to the six main Avamar Administrator windows.

The following table lists the shortcut icons that are available on the status bar.
Table 9 Launcher shortcut icons on the status bar

<table>
<thead>
<tr>
<th>Button</th>
<th>Window</th>
<th>Available tasks in the window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy</td>
<td>Create and manage groups, datasets, schedules, and retention policies.</td>
</tr>
<tr>
<td>Backup &amp; Restore</td>
<td>Backup, Restore and Manage</td>
<td>Perform on-demand backups and restores, and manage completed backups.</td>
</tr>
<tr>
<td>Administration</td>
<td>Administration</td>
<td>Create and manage domains, clients, users, system events, and services.</td>
</tr>
<tr>
<td>Activity</td>
<td>Activity</td>
<td>Monitor backup, restore, backup validation, and replication activity.</td>
</tr>
<tr>
<td>Server</td>
<td>Server</td>
<td>Monitor server activity and client sessions.</td>
</tr>
<tr>
<td>Replication</td>
<td>Replication</td>
<td>Configure policy-based replication.</td>
</tr>
</tbody>
</table>

Status messages

The right side of the status bar shows status messages for scheduler and backup dispatching, unacknowledged events, and the Avamar server and Data Domain systems.

Scheduler and backup dispatching status

The scheduler controls whether scheduled backups occur. The backup dispatching status indicates whether backups can occur based on whether the health check limit has been reached. The following table lists the available status messages.

Table 10 Scheduler and backup dispatching status messages

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sch/Disp: Running/Running</td>
<td>Backups will occur at the scheduled time. Scheduled backups are enabled, and the health check limit has not been reached.</td>
</tr>
<tr>
<td>Sch/Disp: Running/Suspended</td>
<td>Even though scheduled backups are enabled, backups will not occur at the scheduled time because the health check limit has been reached. Resolve the system capacity issues and acknowledge the system event to resume backups. <a href="#">Capacity Management on page 209</a> and <a href="#">Acknowledging system events on page 191</a> provide details.</td>
</tr>
<tr>
<td>Sch/Disp: Suspended/Running</td>
<td>Even though the health check limit has not been reached, backups will not occur at the scheduled time because scheduled backups are disabled. Backups can resume when you resume scheduled operations.</td>
</tr>
<tr>
<td>Sch/Disp: Suspended/Suspended</td>
<td>Backups will not occur at the scheduled time because scheduled backups are disabled and the health check limit has been reached. <a href="#">Suspending and resuming scheduled operations on page 145</a> provides details on reenabling the scheduler.</td>
</tr>
</tbody>
</table>
Table 10 Scheduler and backup dispatching status messages (continued)

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have Unacknowledged Events</td>
<td>There are entries in the unacknowledged events list that must be explicitly acknowledged by an Avamar server administrator. Click the <strong>Unacknowledged Events</strong> status icon or text label to show the <strong>Administration</strong> window <strong>Unacknowledged Events</strong> pane (tab). Acknowledging system events on page 191 provides details.</td>
</tr>
<tr>
<td>No Unacknowledged Events</td>
<td>There are no entries in the unacknowledged events list.</td>
</tr>
</tbody>
</table>

Unacknowledged events
Certain system events to require acknowledgement by an Avamar server administrator each time they occur. The following table lists the available status messages.

Table 11 Status messages for unacknowledged events

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have Unacknowledged Events</td>
<td>There are entries in the unacknowledged events list that must be explicitly acknowledged by an Avamar server administrator. Click the <strong>Unacknowledged Events</strong> status icon or text label to show the <strong>Administration</strong> window <strong>Unacknowledged Events</strong> pane (tab). Acknowledging system events on page 191 provides details.</td>
</tr>
<tr>
<td>No Unacknowledged Events</td>
<td>There are no entries in the unacknowledged events list.</td>
</tr>
</tbody>
</table>

Avamar server and Data Domain system status
This icon lists the operational status of either the Avamar server or any configured Data Domain systems. The following table lists the available status messages.

Table 12 Operational status messages for Avamar or Data Domain

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: Full Access</td>
<td>Normal operational state for an Avamar server. All operations are allowed.</td>
</tr>
<tr>
<td>Server: Admin</td>
<td>The Avamar server is in an administrative state in which the Avamar server and root user can read and write data; other users are only allowed to read data.</td>
</tr>
<tr>
<td>Server: Admin Only</td>
<td>The Avamar server is in an administrative state in which the Avamar server or root user can read or write data; other users are not allowed access.</td>
</tr>
<tr>
<td>Server: Admin Read Only</td>
<td>The Avamar server is in an administrative read-only state in which the Avamar server or root user can read data; other users are not allowed access.</td>
</tr>
<tr>
<td>Server: Degraded</td>
<td>The Avamar server has experienced a disk failure on one or more nodes. All operations are allowed, but immediate action should be taken to fix the problem.</td>
</tr>
<tr>
<td>Server: Inactive</td>
<td>Avamar Administrator was unable to communicate with the Avamar server.</td>
</tr>
</tbody>
</table>
Table 12 Operational status messages for Avamar or Data Domain (continued)

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: Node Offline</td>
<td>One or more Avamar server nodes are in an OFFLINE state.</td>
</tr>
<tr>
<td>Server: Read Only</td>
<td>The Avamar server is in a read-only administrative state in which all users can read data, but writing data is not allowed.</td>
</tr>
<tr>
<td>Server: Suspended</td>
<td>Avamar Administrator was able to communicate with the Avamar server, but normal operations have been temporarily suspended.</td>
</tr>
<tr>
<td>Server: Synchronizing</td>
<td>The Avamar server is in a transitional state. It is normal for the server to be in this state during startup and for short periods of time during maintenance operations.</td>
</tr>
<tr>
<td>Server: Unknown State</td>
<td>Avamar Administrator could not determine the Avamar server state.</td>
</tr>
<tr>
<td>Data Domain System Unresponsive</td>
<td>Avamar can connect to a Data Domain system, but there is a problem with the connection.</td>
</tr>
<tr>
<td>DD System: Inactive</td>
<td>Avamar cannot connect to a Data Domain system.</td>
</tr>
</tbody>
</table>

To suspend or resume Avamar server activities, click the Server status icon or text label to display the Avamar Server window Session Monitor tab. From there, select Actions > Resume Backups/Restores or Actions > Suspend Backups/Restores to resume or suspend server activities, respectively.

To view additional details about Data Domain system status, open the Server window by clicking Navigation > Server. Select the Server Management tab, and then select the Data Domain system in the tree. The Monitoring Status of the Data Domain system appears in the right pane. The EMC Avamar and EMC Data Domain System Integration Guide provides details on the available detailed status messages.

Navigation tree features

The navigation trees in the Administration, Backup, Restore and Manage, and Replication windows provide several controls to facilitate the location of one or more clients.

Figure 7 Navigation tree features

The upper pane shows the Avamar server domain structure. The lower pane shows contents of any domain selected in the upper pane. You can click the split pane icon to the left of the filter field between the two panes to split the two panes vertically instead of horizontally.

Click the double folder icon to the left of the filter field to show all clients in subfolders.
Mouse shortcuts

The Avamar Administrator user interface supports context-sensitive left-click, right-click, and double-click shortcuts.

**Right-click**
All GUI elements that can enable features or functions when clicked, have right-click support added to them. However, if the GUI element only acts as a navigation mechanism, there is no right-click support. For example, the Policy window client tree has a right-click shortcut menu because specific features and functions become available based on which node of the tree is selected.

**Double-click**
For all tables where properties or edit dialog boxes can be invoked, double-click any row of the table to display the properties or edit dialog box. Additionally, when lists are used rather than tables, double-click an element in the list to display the edit dialog box.

**Column heading sort**
Click a table column heading to sort that column. For example, double-click the Activity Monitor State column to sort the Activity Monitor by the state of each backup.

Press **Shift** and then click any table column heading to reverse sort the values in a table column.
CHAPTER 3

Client Management

This chapter includes the following topics:

- Overview of Avamar clients ....................................................................................50
- Client domains ...................................................................................................... 50
- Client registration .................................................................................................52
- Activating a client .................................................................................................56
- Client paging .........................................................................................................56
- Editing client information ...................................................................................... 58
- Viewing client properties .......................................................................................59
- Enabling and disabling a client .............................................................................. 60
- Moving a client to a new domain ........................................................................... 60
- Retiring a client ...................................................................................................... 61
- Deleting a client ...................................................................................................... 61
Overview of Avamar clients

Avamar clients are networked computers or workstations that access the Avamar server over a network connection.

You can organize and segregate clients by using Avamar domains. Domains provide enhanced security by enabling you to define administrative user accounts on a domain-by-domain basis.

Before Avamar can back up or restore data on a client, you must add, or register, the client with the Avamar server, and then activate the client.

To provide maximum flexibility in deploying Avamar clients, registration and activation are separate events that occur asynchronously. Although they often occur at nearly the same time, they can also occur hours, days, or even weeks apart.

In Avamar Administrator, the client name must always be the client’s hostname. If you need to change the client name in Avamar Administrator because the client hostname changed, you must first shut down the Avamar software on the client computer, change the client name by editing the client information, then restart the Avamar client software. This is the only way to ensure that the client maintains its registration with the Management Console Server (MCS) database, which ensures that past backups continue to be associated with the client.

Client domains

Avamar client domains are distinct zones to organize and segregate clients in the Avamar server. This provides enhanced security by enabling you to define administrative user accounts on a domain-by-domain basis.

Avamar client domains are completely internal to the Avamar server and have nothing to do with Internet domains.

Nested structure
You can nest domains to create a rich tree structure. Consider the following example domain.

Figure 8  Avamar domain example
The root domain, avamar-1.example.com, contains three departmental domains: Accounting, Engineering, and Operations. The Operations domain contains Maintenance and Shipping subdomains.

There is no functional difference between domains and subdomains. Subdomain is merely a term that refers to any domain nested within another higher level domain.

Hierarchical management
The real power of domains is that you can add administrators to a specific level on the client tree. These domain-level administrators can then manage the clients and policies within that domain.

For example, if you add an administrative user to the root domain, then that user can administer clients and policies anywhere in the system. However, if you add an administrative user to a domain, then that user can only administer clients and policies in that domain and its subdomains.

The procedures in this guide assume that you are logged in to the root domain. If you log in to a lower-level domain, you may not have access to specific clients, datasets, groups, and event management features outside that domain.

Special domains
You cannot delete the MC_RETIRED and REPLICATE domains.

The MC_RETIRED domain contains clients that have been retired. Its primary purpose is to facilitate restores from retired client backups.

The REPLICATE domain contains replicated data from other servers.

Creating a domain

Procedure
1. In Avamar Administrator, click the Administration launcher button. The Administration window appears.
2. Click the Account Management tab.
3. In the left pane, select the location in the tree in which to create the domain.
4. From the Actions menu, select Account Management > New Domain. The New Domain dialog box appears.
5. In the New Domain Name box, type the name of the domain. Domain names must be 63 characters or fewer, and must not use any of the following characters: =~!@$%^(){}[]",;:/?<>" &.
6. (Optional) Type the name, telephone number, email address, and location for a contact for the domain in the remaining fields on the New Domain dialog box.
7. Click OK. A confirmation message appears.
8. Click OK.

Editing domain information
You can edit contact and location information for a domain.

Procedure
1. In Avamar Administrator, click the Administration launcher button. The Administration window appears.
2. Click the **Account Management** tab.
3. In the tree, select the domain to edit.
4. From the **Actions** menu, select **Account Management > Edit Domain**.
   The **Edit Domain** dialog box appears.
5. Edit the domain contact information.
6. Click **OK**.
7. Click **OK** on the confirmation message that appears.

### Deleting a domain

When you delete a domain, the process also deletes any clients in the domain. To preserve the clients in the system, move the clients to a new domain before you delete the domain.

In addition, if you use directory service authentication, then Avamar removes the LDAP maps that use that domain for access. The associated directory service groups are otherwise unaffected by the deletion.

#### Procedure

1. (Optional) Move any clients in the domain to a new domain. Moving a client to a new domain on page 60 provides instructions.
2. In Avamar Administrator, click the **Administration** launcher button.
   The **Administration** window appears.
3. Click the **Account Management** tab.
4. In the tree, select the domain to delete.
5. From the **Actions** menu, select **Account Management > Delete Domain**.
   A confirmation message appears.
6. Click **Yes**.
7. Click **OK** on the second confirmation message that appears.

### Client registration

Client registration is the process of establishing an identity with the Avamar server. Once Avamar “knows” the client, it assigns a unique client ID (CID), which it passes back to the client during activation.

There are three ways to register a client:

- Client-side registration
- Interactive server-side registration by using Avamar Administrator
- Batch client registration

#### Client-side registration

The client-side registration process depends on the operating system.

The *EMC Avamar Backup Clients User Guide* describes client-side registration for each supported operating system.

Client-side registration also activates the client at the same time. For this reason, client-side registration is very popular. However, the client is automatically added to the Default
Group and must use the default dataset, schedule, and retention policy. As a result, this method may not provide enough control for some sites.

Registering a client in Avamar Administrator

You can use Avamar Administrator to add a client to the system in a domain and group. This provides a high degree of control. For example, you can assign a specific dataset, schedule, and retention policy. However, it can be very time consuming if you need to add many clients.

Procedure

1. In Avamar Administrator, click the Administration launcher button. The Administration window appears.
2. Click the Account Management tab. In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
3. In the tree, select the domain for the new client.
4. From the Actions menu, select Account Management > New Client. The New Client dialog box appears.
5. From the Client Type list, select Normal.

**NOTICE**
The EMC Avamar for VMware User Guide provides information on VMware vCenter™, Image Proxy, and Virtual Machine client types.

6. In the New Client Name field, type the client name.
7. (Optional) Type the client contact name, telephone number, email address, and location in the remaining fields of the New Client dialog box.
8. Click OK. A confirmation message appears.
9. Click OK.

Batch client registration

To support large sites with many clients, the batch client registration feature enables you to define multiple clients in a single client definition file, then validate and import that file into the Avamar server.

Batch client registration is very popular at large sites because it provides nearly as much control as interactively adding the client using Avamar Administrator but is much faster.

Clients definition files

Avamar supports Extensible Markup Language (XML) and comma-separated values (CSV) formats for the clients definition file for batch client registration.

**XML format**

XML clients definition files must have an .xml file extension and conform to the following structure and format:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<registration_stream>
```
<registrants>
<entry>
    <host_name>MyClient.Example.com</host_name>
    <mcs_domain>clients</mcs_domain>
    <mcs_group>MyGroup</mcs_group>
    <dataset>MyDataset</dataset>
    <retention_policy>MyRetentionPolicy</retention_policy>
    <contact_address>192.168.31.5</contact_address>
    <contact_port>28002</contact_port>
    <access_list>user1@avamar:password, user2@LDAP</access_list>
    <encryption>high</encryption>
    <encryption_override>false</encryption_override>
</entry>
</registrants>

The clients definition file in this topic is for reference purposes only. Do not attempt to copy and paste this example into a clients definitions file. Invisible formatting characters will prevent you from successfully doing so.

Define each client by using a separate <entry> element. The following table describes the available attributes for each <entry> element.

**Table 13 Attributes for each entry in a clients definition file**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_name</td>
<td>Network hostname or IP address for this client.</td>
</tr>
<tr>
<td>mcs_domain</td>
<td>Optional Avamar domain for this client. Specifying a value for this attribute overrides the default clients domain.</td>
</tr>
<tr>
<td>mcs_group</td>
<td>Optional default group for this client. Specifying a value for this attribute overrides assignment to the Default Group.</td>
</tr>
<tr>
<td>dataset</td>
<td>Optional default dataset for this client to use during backups. Specifying a value for this attribute overrides the default dataset that would normally be inherited from the group.</td>
</tr>
<tr>
<td>retention_policy</td>
<td>Optional default backup retention policy for this client. Specifying a value for this attribute overrides the default retention policy that would normally be inherited from the group.</td>
</tr>
<tr>
<td>contact_address</td>
<td>Optional client IP address.</td>
</tr>
<tr>
<td>contact_port</td>
<td>Set this to 28002, the default Avamar data port.</td>
</tr>
<tr>
<td>access_list</td>
<td>Optional list of users who can access the Avamar server from this client. The format is user@authentication:password. If you use the internal authentication system, the word password must follow the colon. This causes the system to prompt users for authentication when they access the system. If you use an external authentication system, omit :password.</td>
</tr>
</tbody>
</table>
### Table 13 Attributes for each entry in a clients definition file (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption</td>
<td>Encryption method for client/server data transfer:</td>
</tr>
<tr>
<td></td>
<td>- High</td>
</tr>
<tr>
<td></td>
<td>- Medium</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
</tbody>
</table>

**Note**

The encryption technology and bit strength for a client/server connection depends on several factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

| encryption_override | Optional encryption override. If **TRUE**, then this client does not use the group encryption method.                                   |

**CSV format**

CSV clients definition files use the same element and attribute names as the XML format. However, you must define each client on a single line and separate each attribute value by a comma, as shown in the following example:

```plaintext
host_name,mcs_domain,mcs_group,dataset,retention_policy,
contact_address,contact_port,access_list,encryption,
encryption_override
```

**Validating and importing a clients definition file**

**Procedure**

1. In Avamar Administrator, click the **Administration** launcher button.
   
The Administration window appears.
2. Click the **Account Management** tab.
3. From the **Actions** menu, select **Account Management > Import Clients from File**.
   
The **Validate** dialog box appears.
4. Browse to and select the saved clients definition file.
5. Click **Validate**.
   
The **Validation Results** dialog box appears.
6. If the clients definition file is error free, click **Commit** to import the client list. Or, of the clients definition file contains errors, correct the errors, save the file again, and repeat the steps in this procedure.
   
The **Validation Results** dialog box closes, and the new clients appear in the **Account Management** tree.
Activating a client

Client activation is the process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

There are two ways to activate a client:

- Initiate activation from the client. The *EMC Avamar Backup Clients User Guide* describes this method.
- Invite the client to activate with the server by using Avamar Administrator.

**NOTICE**

HP-UX, Linux, and Solaris clients can either be activated during installation or by using Avamar Administrator. There is no client-side command to initiate client activation on these computing platforms.

**Procedure**

1. Ensure that the following requirements are met:
   - The client must be present on the network.
   - The Avamar client software must be installed and running on the client.
   - The Avamar server must be able to resolve the hostname that was used to register the client.

2. In Avamar Administrator, click the **Administration** launcher button.
   The **Administration** window appears.

3. Click the **Account Management** tab.
   In the **Account Management** tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

4. In the tree, select the client to activate.

5. From the **Actions** menu, select **Account Management** > **Invite Client**.
   A status message indicates that the client was sent an invitation to activate with the server.

6. Click **OK**.

Client paging

Avamar clients can be either pageable or non-pageable. If a client is pageable you can specify settings to control how the MCS determines the appropriate paging settings for the client. You may need to use workarounds for limitations that exist in environments with non-pageable clients.

Pageable clients

Pageable clients have provided the Avamar server with a page address and port number, which enables performance of on-demand backups and restores. In addition, Avamar
Administrator can browse the client file system during backups and restores in Avamar Administrator.

You can specify one of the following client paging settings to control how the MCS determines the appropriate paging settings for a client:

- **Automatic** — With the default setting of automatic paging, the MCS attempts to automatically determine appropriate paging settings for the client. If the MCS receives updated paging information from the client, it automatically updates the settings.

- **Manual** — With manual paging, you specify the IP address and data port number for client/MCS communications. You may want to use manual paging if you use Network Address Translation (NAT). With NAT, the MCS probably cannot automatically determine the correct client paging settings. In manual mode, the MCS never overwrites the IP address and port number settings for the client.

You can also disable automatic paging without specifying an IP address or data port number for client/MCS communications. Disabling automatic paging might be useful to support clients that are off the network for extended periods of time, as can be the case with laptop computers. These clients must initiate their own on-demand backups. For this reason, you should enable client paging whenever possible.

### Non-pageable clients

A client is non-pageable when the Avamar Administrator server running on the Avamar server utility node or on a single-node server cannot establish a TCP/IP connection to port 28002 on the Avamar client.

**When a client might be non-pageable**

A client might be non-pageable in the following situations:

- The environment (including the client) has firewall rules that prevent incoming connections on port 28002 to the client.

- The client is behind a router that doesn't support port-forwarding for connections initiated from the Avamar server. (This is the common situation that managed service providers could encounter if they deploy Avamar without using VPN, for example.)

- The Avamar Administrator server cannot connect to the Avamar client on the paging address used by the Avamar Administrator server. One example of this is if the client is multi-homed and the paging address used by the Avamar Administrator server to connect to the client does not have a route to the paging address.

- The environment requires authentication to establish a host-to-host connection to port 28002 on the client, and the Avamar Administrator server process is not able to support the required authentication protocol.

- An IPSEC environment. In a Windows environment Microsoft best practices recommend enabling IPSEC, and clients are not pageable in an IPSEC environment.

MCS should automatically detect non-pageable clients and adjust settings. Usually no manual changes are needed in MCS. You can determine whether a client is pageable or non-pageable by viewing the properties for the client on the Client tab in the Policy window of Avamar Administrator. If No appears in the Paging column for the client, then MCS cannot connect to the avagent process on the client and the client is non-pageable.

### Limitations in environments with non-pageable clients

You can use Avamar Administrator to perform backups or restores, or define policies in environments with non-pageable clients. In some cases you must enter explicit path names.

The following limitations apply when the client is non-pageable:
• If the MCS cannot page the client on port 28002, then Avamar cannot invite the client to activate by using Avamar Administrator.

• You cannot browse the client file system when defining datasets or when browsing to select a target for restore. To work around this limitation, explicitly define the backup dataset without browsing a client. During a restore, explicitly type the restore target path.

• You cannot view client logs by double-clicking on the Activities view. To work around this limitation, get the logs from the client computer.

• You cannot page the client when there is a work order waiting for the client. In this case, the client connects to the MCS and polls for the existence of a work order approximately once every minute.

If you are backing up several hundred or more non-pageable clients, you may need to increase the polling interval. The default polling interval is 60 seconds. If MCS performance is slowing down, increase the polling interval until you achieve acceptable performance.

Editing client paging settings

The MCS can automatically determine client paging settings, or you can manually specify paging settings for a client. You may need to manually specify paging settings if you use NAT.

Procedure

1. In Avamar Administrator, click the Policy launcher button.

   The Policy window appears.

2. Click the Policy Management tab.

3. Click the Clients tab.

4. Select the client.

5. From the Actions menu, select Client > Edit Client.

   The Edit Client window appears.

6. Click the Properties tab.

7. Select either the Automatic or Manual paging mode.

8. If you selected Manual, specify the client information for client/MCS communications:

   • If the MCS is unable to automatically determine a hostname for this client in automatic mode, type a valid (un-NAT’d) IP address for the client in the Address box.

   • In the Port Number box, specify the data port number. The default data port is 28002.

9. Click OK.

Editing client information

You can edit the name, contact information, or location information for a client in Avamar Administrator.

In Avamar Administrator, the client name must always be the client hostname. If you need to change the client name in Avamar Administrator because the client hostname changed, you must first shut down the Avamar software on the client computer, change the client name by way of this procedure, then restart the Avamar client software. This is the only way to ensure that the client maintains its registration with the Management
Console Server (MCS) database, which ensures that past backups continue to be associated with the client.

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the Account Management tab.
   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
3. In the tree, select the client to edit.
4. From the Actions menu, select Account Management > Edit Client.
   The Edit Client dialog box appears.
5. Edit the name, contact information, or location information for the client.
6. Click OK.
   A confirmation message appears.
7. Click OK.

Viewing client properties

Procedure

1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Clients tab.
4. Select the client.
   The client properties described in the following table appear in the main pane of the window.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Descriptive client name.</td>
</tr>
<tr>
<td>Backups Disabled</td>
<td>Whether Avamar can perform backups for the client. Regardless of this setting, the client can restore files as long as a previous backup exists in the system.</td>
</tr>
<tr>
<td>Activated</td>
<td>Whether the client is activated with the Avamar server.</td>
</tr>
<tr>
<td>Domain</td>
<td>The Avamar domain for the client.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system on the client.</td>
</tr>
<tr>
<td>Paging</td>
<td>Whether the client has provided the Avamar server with a page address and port number, thereby allowing it to perform on-demand backups and restores. In addition, Avamar Administrator can browse its file system during Avamar Administrator-initiated backups and restores.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of Avamar client software on the client.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Check-in</td>
<td>The date and time that the Avamar client agent last checked in with the Avamar server.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The encryption method used for client/server data transfer.</td>
</tr>
<tr>
<td>CID</td>
<td>The Client ID, a unique identifier for this client in the Avamar server. CIDs are assigned during client activation.</td>
</tr>
</tbody>
</table>

## Enabling and disabling a client

You can disable a client so that it cannot use the Avamar server to back up files. This is typically done to place the system in a state that supports maintenance activities. If a client has been disabled, you must reenable the client before backups for the client can resume.

**Procedure**

1. In Avamar Administrator, click the **Policy** launcher button.
   - The **Policy** window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select the client to disable or enable.
5. From the **Actions** menu, select **Client > Disable all backups of selected client**.
   - A confirmation message appears.
6. Click **Yes**.
   - When the client is disabled, a checkmark appears next to the **Disable all backups of selected client** option on the **Actions > Client** menu. When the client is enabled, the checkmark does not appear.

## Moving a client to a new domain

**Procedure**

1. In Avamar Administrator, click the **Administration** launcher button.
   - The **Administration** window appears.
2. Click the **Account Management** tab.
3. In the **Account Management** tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
4. In the tree, select the client to move.
5. From the **Actions** menu, select **Account Management > Move Client**.
   - The **Move Client** dialog box appears.
6. Select the new domain for the client.
7. Click **OK**.
Retiring a client

When you retire a client, Avamar does not back up the client. However, old backups associated with a retired client are maintained in the system (subject to backup retention settings), and you can restore files from the client by using Avamar Administrator.

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the Account Management tab.
   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
3. In the tree, select the client to retire.
4. From the Actions menu, select Account Management > Retire Client.
   The Retire Client dialog box appears.
5. Choose how long to keep backups for this client:
   - To keep backups until their existing expiration dates, select Retire client and retain backups with existing expiration date.
   - To keep backups indefinitely, regardless of the existing backup expiration dates, select Retire client and retain all backups indefinitely.
   - To keep backups until a new expiration date, select Retire client and reset backup expiration date and select a new backup expiration date.
6. Click OK.
   A confirmation message appears.
7. Click Yes.

Deleting a client

When you delete a client, Avamar permanently deletes all backups stored for that client. Therefore, you should only delete a client when you are certain that there is no reason to retain the backups. If there is any doubt, retire the client instead.

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the Account Management tab.
   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
3. In the tree, select the client to delete.
4. From the Actions menu, select Account Management > Delete Client.
   A confirmation message appears.
5. Click Yes.
   A second confirmation message appears.
6. Click **OK**.
CHAPTER 4

User Management and Authentication

This chapter includes the following topics:

- Overview of Avamar user accounts ................................................................. 64
- User authentication .......................................................................................... 64
- Roles ................................................................................................................. 75
- Adding a user to a client or domain ................................................................. 79
- Editing user information .................................................................................. 80
- Deleting a user .................................................................................................. 81
Overview of Avamar user accounts

A user account in Avamar can administer a domain or client. The user account defines the authentication system that is used to grant users access to the Avamar server. It also defines the role for the user, which controls the operations that a user can perform.

You can add user accounts to domains or individual clients. When you add a user account to a domain, the account can administer that domain and any subdomains beneath it. When you add a user account to an individual client, the account can perform backups and restores of that client, and access backups belonging to that client in the system.

In Avamar, users are entries in a domain or client access list. When you add a user account to the Avamar system, you are adding a new entry to a domain or client user access list.

In the following example, the user “Gretchen” has been added to both the Accounting domain and her computer. However, the authentication system and role are different. These are in fact two completely separate user accounts that happen to have the same username.

Figure 9  Users in Avamar domains

The following table describes the information that comprises an Avamar user account.

Table 14  Avamar user account information

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username depends on the authentication system and must be in the format that the authentication system accepts. For example, the internal authentication system uses case-sensitive usernames, whereas Windows Active Directory usernames are case-insensitive. Usernames cannot be longer than 31 characters.</td>
</tr>
<tr>
<td>Authentication system</td>
<td>An authentication system is a username/password system that is used to grant users access to the Avamar server.</td>
</tr>
<tr>
<td>Role</td>
<td>Roles define the allowable operations for each user account.</td>
</tr>
</tbody>
</table>

User authentication

An authentication system is a username/password system that is used to grant users access to the Avamar server.

Avamar supports three authentication systems:
- Avamar internal authentication
- Directory service authentication
• Enterprise authentication

Avamar internal authentication

With Avamar internal authentication, you define the username and password for Avamar user accounts, and Avamar stores the information. Usernames are case-sensitive and cannot be longer than 31 characters.

No additional steps are required to use internal Avamar authentication to authenticate user accounts. You define the username and password for each account when you add the user in Avamar Administrator.

Directory service authentication

When you use directory service authentication to authenticate and assign roles to Avamar users, you can take advantage of a directory service that already exists in an organization. You can use any LDAP v.3-compliant directory service, such as Microsoft Active Directory Domain Services. Also, you can use a Network Information Service (NIS) on its own or with the LDAP services.

Avamar products that use directory service authentication

The following Avamar products use existing directory services to authenticate users:

• Avamar Administrator
• Avamar Enterprise Manager
• Avamar Web Restore
• Avamar client web UI

Avamar Web Restore requires the use of existing directory services to authenticate users. The other products also support other authentication methods.

NOTICE

When you delete an Avamar domain, Avamar removes the LDAP maps that rely on that Avamar domain for access. The directory service groups associated with the removed LDAP maps are not affected by the deletion.

LDAP requirements

Avamar directory service authentication supports LDAP v.3-compliant directory services when the following conditions are met:

• LDAP server permits username bind through both of the following formats:
  ▪ username
  ▪ username@domain.com
• LDAP server permits searching for group membership by using a username.
• LDAP server permits searching for groups by using a search string.
• LDAP server account that is provided when adding an LDAP map has permission to run a nested ldapsearch command.

Encrypted communication

Avamar’s directory service authentication uses the Kerberos protocol for all communications with the Key Distribution Center. Avamar automatically encrypts usernames and passwords before sending them to port 88 on the Key Distribution Center.
Preparing to use directory service authentication

To prepare to use directory service authentication, give Avamar access to certain ports on the Key Distribution Center. Also, create the directory service groups that will be associated with Avamar LDAP maps.

Procedure

1. Ensure that Avamar has access to the following recognized ports on the Key Distribution Center (KDC).

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>Kerberos authentication system</td>
</tr>
<tr>
<td>389</td>
<td>Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td>464</td>
<td>Kerberos Change/Set password</td>
</tr>
</tbody>
</table>

The ports are defined in krb5.conf and ldap.properties. Editing the directory service configuration files on page 69 provides instructions on editing these files.

2. Create directory service groups in the directory service (not in Avamar).

Groups can range in size from one member to as many members as the directory service allows.

Ideally, you should create directory service groups specifically for use with an Avamar LDAP map. By doing this, group composition is considered in the context of the level of Avamar access being granted. Also, the group name can include a common character pattern to simplify its discovery during mapping. For example, you could start each group name with the characters `av`, as in `avAdministrators`. This would enable you to search for all groups associated with Avamar by using the wildcard search string `av*`.

After you finish

Complete the following tasks:

- Configure Avamar to use the directory service. Adding directory service information on page 66 provides instructions.
- Create an LDAP map to associate the directory service group to Avamar user information. Adding an LDAP map on page 71 provides instructions.

Adding directory service information

Procedure

1. Log in to the root domain in Avamar Administrator as an administrator.
   
   a. Launch Avamar Administrator.
   
   b. In the **Username** box in the login window, type a username for an account that is assigned the administrator role at the root domain level.
      
      If you already configured a directory service, then you can log in with an account for an LDAP user with the administrator role at the root domain level.
   
   c. In **Password**, type the password for the user account.
   
   d. In **Domain Name**, use the default entry of a single slash (/) character to specify the root domain.
e. In **Avamar Server**, type the IP address or DNS name of the Avamar server.

f. Click **Log On**.

2. In Avamar Administrator, click the **Administration** launcher button.

   The **Administration** window appears.

3. Click the **LDAP Management** tab.

4. Click **Directory Service Management**.

   The **Directory Service Management** dialog box appears.

5. Add the LDAP v.3-compliant directory service:
   a. Click **Add**.

      The **Adding a new Directory Service** section appears.

   b. Select **LDAP**.

   c. In **Enter a fully qualified domain name**, type the fully qualified domain name (FQDN) of a directory server.

   d. (Optional) If this is the server that represents the organization's default directory service domain, then select **Make this the default domain LDAP domain**.

      To allow the Avamar client web UI to authenticate users from Macintosh computers, the LDAP server assigned to Macintosh users must be configured as the default server.

   e. Click **Add**.

      A confirmation message appears.

   f. Click **Yes**.

      A success message appears. If an error message appears instead, then resolve the issue and re-add the directory service. **Error messages during directory service configuration on page 68** provides details.

   g. Click **OK**.

      The changes are applied to the Management Console Server (**mcs**), Enterprise Manager (**em**), and Desktop and Laptop (**dtlt**) services.

6. (Optional) Repeat the previous step to add other authentication domains.

7. Add an NIS directory service:
   a. In the **Directory Service Management** dialog box, click **Add**.

      The **Adding a new Directory Service** section appears.

   b. Select **NIS**.

   c. In **Enter a fully qualified domain name**, type the NIS domain name.

   d. In **NIS Domain IP address**, type the IP address of the NIS server.

   e. Click **Add**.

      A confirmation message appears.

   f. Click **Yes**.

      A success message appears. If an error message appears instead, then resolve the issue and re-add the directory service. **Error messages during directory service configuration on page 68** provides details.
g. Click OK.

The changes are applied to the Management Console Server (mcs), Enterprise Manager (em), and Desktop and Laptop (dtlt) services.

8. Test the directory service entries:
   a. In the Directory Service Management dialog box, select one of the entries from Configured Directory Services.
      The Testing section appears.
   b. In Username, type the username for an account that is authorized to read the directory service database.
   c. In Password, type the password associated with the username.
   d. Click Run Test.
      If an error message appears, then resolve the issue. Error messages during directory service configuration on page 68 provides details.
   e. Click Close to close the Testing section.


Error messages during directory service configuration

Error messages appear when issues occur during the addition or testing of a directory service configuration.

The following table lists some of the potential messages and provides a description of the cause.

Table 15 Error messages during directory service configuration

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot discover KDC</td>
<td>A key distribution center (KDC) could not be found by using the specified domain information.</td>
</tr>
<tr>
<td>No URL is present</td>
<td>The specified domain is not present in the ldap.properties file.</td>
</tr>
<tr>
<td>Parameters are not correct</td>
<td>The directory service domain information in the ldap.properties file is invalid.</td>
</tr>
<tr>
<td>Client not found in Kerberos database</td>
<td>The specified username is invalid.</td>
</tr>
<tr>
<td>Pre-authentication information was invalid</td>
<td>The specified password is incorrect.</td>
</tr>
<tr>
<td>Query fails</td>
<td>The specified user account does not have sufficient privileges to read the directory service database.</td>
</tr>
<tr>
<td>Clock skew too great</td>
<td>The differential between the clock on the Avamar server host and the clock on the directory service host is too large.</td>
</tr>
<tr>
<td>Cannot open LDAP configuration file</td>
<td>The ldap.properties file does not exist or the file permissions prevent access.</td>
</tr>
</tbody>
</table>
Table 15 Error messages during directory service configuration' (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot open Kerberos configuration file</td>
<td>The krb5.conf file does not exist or the file permissions prevent access.</td>
</tr>
<tr>
<td>GSS initiate failed</td>
<td>Credential authentication failed. Usually this is because reverse DNS is improperly configured. Add the KDC host to /etc/hosts on the Avamar server.</td>
</tr>
<tr>
<td>Cannot get kdc for realm</td>
<td>The KDC is improperly configured in the krb5.conf file.</td>
</tr>
<tr>
<td>Domain &lt;domain&gt; exists in ldap.properties file</td>
<td>The specified domain already exists in the ldap.properties file.</td>
</tr>
</tbody>
</table>

Editing the directory service configuration files

The LDAP Management tool provides you with the ability to manually edit the ldap.properties and krb5.conf directory service configuration files. Manually edit these files to configure non-standard settings and to resolve problems that occur when configuring Avamar to use a directory service.

Before you begin
Determine the correct format for keys and values in the configuration files.

Procedure
1. Log in to the root domain in Avamar Administrator as an administrator.
   a. Launch Avamar Administrator.
   b. In the Username box in the login window, type a username for an account that is assigned the administrator role at the root domain level.
      If you already configured a directory service, then you can log in with an account for an LDAP user with the administrator role at the root domain level.
   c. In Password, type the password for the user account.
   d. In Domain Name, use the default entry of a single slash (/) character to specify the root domain.
   e. In Avamar Server, type the IP address or DNS name of the Avamar server.
   f. Click Log On.
2. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
3. Click the LDAP Management tab.
4. Click Edit LDAP file to edit ldap.properties or Edit KRB5 file to edit krb5.conf.
5. Type additions and changes directly in the Edit file window.
6. Click Save, and then click Close.

Format requirements and settings for ldap.properties
The LDAP Management tool in Avamar Administrator creates a properly formatted ldap.properties file. When you edit the file by using the LDAP Management tool, the
format must comply with the required key/value (KV) pair rules. You can manually add other settings to ldap.properties to meet your organization's authentication requirements.

**KV pair rules**
The following table lists the KV pair rules.

### Table 16 Key/value pair rules for ldap.properties

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>One LDAP URL KV pair for each LDAP server</td>
<td>The LDAP URL KV pair maps an LDAP server to a specific domain controller.</td>
<td>ldap.url.ds.example.abc.com=ldap://dchost.r1.example.abc.com:389 where: • ds.example.abc.com is the FQDN of the LDAP server. • dchost.example.abc.com is the FQDN of the domain controller for the LDAP server. • 389 is the port used by the LDAP service.</td>
</tr>
<tr>
<td>Exactly one default server KV pair</td>
<td>The default server KV pair is used during authentication of users on clients that are not mapped to a specific domain, such as local users and users logging in from an AIX, FreeBSD, HP-UX, Linux, SCO, or Solaris computer.</td>
<td>ldap.qualified-name-default=dhost.example.abc.com where dhost.example.abc.com is the FQDN of the default LDAP server.</td>
</tr>
</tbody>
</table>

### Additional KV pair settings
You can add other settings in the form of KV pairs to ldap.properties by using the LDAP Management tool in Avamar Administrator. The following table lists the available settings.

### Table 17 Key/value pairs in ldap.properties

<table>
<thead>
<tr>
<th>Key</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| ldap.auth.domain.login-domain-suffix | Specifies a login domain name suffix that is included as part of the username value when authenticating through LDAP, where login-domain-suffix is the login domain name suffix and the value is an authentication domain.  
For example, where this key is set as follows:  

```yaml
ldap.auth.domain.boston=boston.edu
``` |
Table 17 Key/value pairs in ldap.properties (continued)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can log in using either: username@boston or <a href="mailto:username@boston.edu">username@boston.edu</a>. Use this key in conjunction with the next key, ldap.query.domain, to map multiple authentication domains to a single login domain name suffix.</td>
<td></td>
</tr>
<tr>
<td>ldap.query.domain.login-domain-suffix</td>
<td>Maps additional authentication domains to a single login domain suffix, where login-domain-suffix is defined by the ldap.auth.domain key, and the ldap.query.domain values are additional authentication domains within the organization’s intranet. For example, where the two keys are set as follows: ldap.auth.domain.boston=boston.edu ldap.query.domain.boston=science.boston.edu,art.boston.edu Users from either of the listed authentication domains log in using the format username@boston.</td>
</tr>
</tbody>
</table>
| user-login-module | Controls the authentication mechanism. The following values are available:  
  * kerberos — LDAP authentication with Kerberos encryption. This is the default value when the key is missing from the configuration file.  
  * ldap — Plaintext LDAP authentication.  
  * avamar — Avamar authentication.  
  * mix — Both kerberos and avamar. |
| avamar-authentication-domains | Required when user-login-module=mix.  
The value is a comma-separated list of domains. Avamar authentication is applied to users from each listed domain. LDAP authentication is applied to all other users. |
| support-nis-authentication | Enables (true) or disables (false) NIS authentication support. When the key is missing from the configuration file, false is the default value. |
| nis.qualified-name-default | Specifies the FQDN of the NIS domain server. |
| nis.url.nisdomainname | Specifies the IP address of the NIS domain server, where nisdomainname is the value of nis.qualified-name-default. |

Adding an LDAP map

Create an LDAP map to associate the directory service group to Avamar user information. An LDAP map is a database construct that ties a group of users to an authentication system, domain or subdomain access list, and role.

**Before you begin**

Add directory service domains to the Avamar configuration.
Procedure
1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the Account Management tab.
3. Click the LDAP Maps tab.
4. In the left-pane hierarchical tree, select a domain or a subdomain to specify the access level of the directory service group.
5. Select Actions > Account Management > New LDAP Map.
   The New LDAP Group Map dialog box appears.
6. From the LDAP Domains list, select a directory service domain to map.
7. In the Group Search box, type a search string specific to the group being mapped.
   You can use an asterisk (*) as a wildcard that represents one or more alphanumeric characters.
8. Click Search.
   The Directory Service Authentication dialog box appears.
9. Specify the authentication information required for querying the directory service.
   Authentication can be through a domain different from the one being mapped, as long as there is a trust relationship between the two domains.
   a. From the Auth Domain list, select a domain to use for authentication.
   b. In the User Name box, type a username for an account that has Read privileges for the domain.
   c. In the Password box, type the password for the username.
   d. Click OK.
   The Directory Service Authentication dialog box closes and the search starts. The Search button on the New LDAP Group Map dialog box changes to Stop.
   To terminate a search, click Stop. Searching a directory service can take a long time.
   The search is complete when groups appear in the LDAP Groups list.
10. From the LDAP Groups list, select the group to map.
11. From the Role list, select a role for the group.
12. Click OK.
   The group is mapped and the New LDAP Group Map dialog closes. Select the appropriate administrative node to see the mapping on the LDAP Maps tab.

Editing the role for an LDAP map

Procedure
1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the Account Management tab.
3. Click the LDAP Maps tab.
4. In the left-pane hierarchical tree, select a domain or a subdomain.
   The maps for the domain or subdomain appear in the LDAP Maps area.
5. Select the map to edit.

6. Select Actions › Account Management › Edit LDAP Map.

The Edit LDAP Map dialog appears.

7. In Role, select a new role to assign to the map.

8. Click OK.

The map is assigned the new role. Group members are assigned the new role in all subsequent sessions.

Deleting an LDAP map

Procedure

1. In Avamar Administrator, click the Administration launcher button.

   The Administration window appears.

2. Click the Account Management tab.

3. Click the LDAP Maps tab.

4. In the left-pane hierarchical tree, select a domain or a subdomain.

   The maps for the domain or subdomain appear in the LDAP Maps area.

5. Select the map to delete.

6. Select Actions › Account Management › Delete LDAP Map.

   The Delete LDAP Map dialog appears.

7. Click Yes.

Editing the time-out value for directory service processes

Directory service processes wait as long as five minutes for a response from the directory service. After this time period, the attempt is discarded and a time-out message appears. You can edit the time-out value.

The time-out value is used by the following directory service authentication processes:

- Authentication requests through the directory service
- Addition of a directory service to the Avamar configuration
- Testing of a directory service in the Avamar configuration

Procedure

1. Open a command shell and log in by using one of the following methods:

   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.

2. Stop the Management Console Server (mcs) service by typing `dpnctl stop mcs`.

3. Change the working directory by typing the following command:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

User Management and Authentication
4. Open mcserver.xml in a text editor.
5. Find the <node name="ldap"> node.
6. Change the value of <entry key="ldap_services_timeout_seconds" value="n" /> to a new time-out value in seconds, where \( n \) is the new value.
   The default value is 300 seconds (five minutes).
7. Save the change and close the file.
8. Start the MCS and the scheduler by typing:
   ```
   dpnctl start mcs
   dpnctl start sched
   ```
9. Close the command shell.

**Enterprise authentication**

With enterprise authentication, Avamar uses the Pluggable Authentication Module (PAM) library of the host Linux operating system to provide access to external authentication databases.

Enterprise authentication, which is described in the *EMC Avamar Product Security Guide*, is deprecated and will be removed in future releases. By default, you cannot select an enterprise authentication domain when you add a user to a domain or client in this Avamar release. However, if you upgraded to this release and you want to continue to use enterprise authentication, you can configure the system to enable selection of enterprise authentication when you add a user by changing the enterprise authentication selection setting in mcserver.xml.

**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.
2. Stop the Management Console Server (mcs) service by typing `dpnctl stop mcs`.
3. Change the working directory by typing the following command:
   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
4. Open mcserver.xml in a text editor.
5. Find the <node name="ldap"> node.
6. Change the value of <entry key="enable_new_user_authentication_selection" value="false" /> from false to true.
7. Save the change and close the file.
8. Start the MCS and the scheduler by typing:
How Avamar authenticates users and assigns roles

To provide backwards compatibility with enterprise authentication and to account for the possibility of users in more than one LDAP mapped group, Avamar uses the following authentication and role assignment sequence for each login attempt:

1. When the username is in the format `user`, where `user` is a username without `@server` appended, then Avamar checks the internal Avamar authentication database. If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database. If they do not match, then the login fails.

2. When the username is in the format `user@server`, where `user` is a username and `server` is the fully qualified domain name of the authentication server, then Avamar checks the login information by using enterprise authentication. If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database. If there is no match, then the evaluation continues.

3. When the username is in the format `user@server` and authentication by using enterprise authentication fails, then Avamar checks the LDAP mapping system. The login attempt is checked against all mapped groups for a match of each of the following identifiers:
   - Username, the portion of the User Name field entry before the @ symbol.
   - Password, as entered in the Password field.
   - Avamar domain, as entered in the Domain Name field.
   - Directory service domain, the portion of the User Name field entry after the @ symbol.

   When all identifiers match, the login is successful and Avamar assigns the user a role from the mapped group.

   A user can be the member of mapped groups in different directory service domains. The role of the mapped group that matches the directory service domain provided during login is assigned to the user for that session.

   When the user is a member of more than one mapped group in the same directory service domain, the role with the greatest authority is assigned.

4. When the login information does not meet the requirements of any of the previous steps, then the login fails and a failure message appears.

Roles

Roles define the allowable operations for each user account.

There are three types of roles:

- Administrator roles
- Operator roles
- User roles
Administrator roles

Administrators are generally responsible for maintaining the system.

You can only assign the role of administrator to user accounts at a domain level. This includes the top-level (root) domain or any other domain or subdomain. You cannot assign this role to user accounts at a client level.

You can assign the administrator role to users at the top-level (root) domain or to a specific domain or subdomain.

Table 18 Administrator roles

<table>
<thead>
<tr>
<th>Administrator type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root administrators</td>
<td>Administrators at the top-level (root) domain have full control of the system. They are sometimes referred to as “root administrators.”</td>
</tr>
<tr>
<td>Domain administrators</td>
<td>Administrators at domains other than root generally have access to most of the features described in this guide, but typically can only view or operate on objects (backups, policy objects, and so forth) in that domain. Any activity that might allow a domain administrator to view data outside that domain is disallowed. Therefore, access to server features of a global nature (for example, suspending or resuming scheduled operations, changing runtimes for maintenance activities, and so forth) is disallowed. Furthermore, domain administrators:</td>
</tr>
<tr>
<td></td>
<td>• Cannot add or edit other subdomain administrators.</td>
</tr>
<tr>
<td></td>
<td>• Cannot change their assigned role.</td>
</tr>
<tr>
<td></td>
<td>• Can change their password.</td>
</tr>
</tbody>
</table>

Operator roles

Operator roles are generally implemented to allow certain users limited access to certain areas of the system to perform backups and restores, or obtain status and run reports. These roles allow greater freedom in assigning backup, restore, and reporting tasks to persons other than administrators.

You can only assign operator roles to user accounts at the domain level. You cannot assign these roles to user accounts at the client level. To add the user account to subdomains, you must have administrator privileges on the parent domain or above.

Users with an operator role do not have access to all features in Avamar Administrator. Instead, after login, they are presented with a single window that provides access to the features that they are allowed to use.

The following table describes the four operator roles.
## Table 19 Operator roles

<table>
<thead>
<tr>
<th>Operator type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Restore only operator**| Restore only operators are generally only allowed to perform restores and to monitor those activities to determine when they complete and if they completed without errors. Restore only operators at the top-level (root) domain can perform restores for any client in the system. Restore only operators at a domain other than root can only perform restores for clients in that domain. Restore only operators can restore backup data and monitor activities in the assigned domain. By default, restore only operators cannot browse backups from the command line or the Avamar Web Restore interface. To enable these activities for a restore only operator, add the `noticketrequired` privilege by using the `avmgr chgv` command:  
  
  `avmgr chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,noticketrequired"
  
  where `location` is the subdomain of the operator, `name` is the Avamar username of the user, and `auth` is the external authentication system used to authenticate the user. |
| **Back up only operator**| Back up only operators are generally only allowed to perform backups and to monitor those activities to determine when they complete and if they completed without errors. Back up only operators at the top-level (root) domain can perform backups for any client or group in the system. Back up only operators at domains other than root can only perform backups for clients or groups in that domain. Back up only operators can perform on-demand backups of a client or a group, as well as monitor activities in the assigned domain. By default, back up only operators cannot perform backups from the command line. To enable command line backups for a back up only operator, add the `noticketrequired` privilege by using the `avmgr chgv` command:  
  
  `avmgr chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,backup,noticketrequired"
  
  where `location` is the subdomain of the operator, `name` is the Avamar username of the user, and `auth` is the external authentication system used to authenticate the user. |
| **Back up/restore operator**| Back up/restore operators are generally only allowed to perform backups or restores and to monitor those activities to determine when they complete and if they completed without errors. As with roles assigned to other domain user accounts, back up/restore operators at the top-level (root) domain can perform backups and restores for any client or group in the system. Back up/restore operators at domains other than root can only perform backups and restores for clients or groups in that domain. Back up/restore operators can perform the following tasks in the assigned domain:  
  
  - Perform on-demand backups for a client or group.  
  - Perform restores. |
Table 19 Operator roles (continued)

<table>
<thead>
<tr>
<th>Operator type</th>
<th>Description</th>
</tr>
</thead>
</table>
|               | • Monitor activities. By default, back up/restore operators cannot browse backups from the command line or using the Avamar Web Restore interface, and cannot perform backups from the command line. To enable these activities, add the `noticketrequired` privilege by using the `avmgr chgv` command:  
  ```
vmsg chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,backup,noticketrequired"
  ```  
  where `location` is the subdomain of the operator, `name` is the Avamar username of the user, and `auth` is the external authentication system used to authenticate the user. |

Activity operator  
Activity operators are generally only allowed to monitor backup and restore activities and to create certain reports.  
Activity operators at the top-level (root) domain can view or create reports for backup and restore activities in all domains and subdomains. Activity operators at domains other than root can only view or create reports for backup and restore activities in that domain.  
Activity operators can perform the following tasks in the assigned domain:  
• Monitor activities.  
• View the group status summary.  
• View the Activity Report.  
• View the Replication Report. |

User roles

User roles limit the operations allowed for a user account to a specific client.  
Users assigned to one of the user roles cannot log in to Avamar Administrator, Avamar Enterprise Manager, or the Avamar client web UI.  
The following table describes the four user roles.

Table 20 User roles

<table>
<thead>
<tr>
<th>User type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Up Only User</td>
<td>Users assigned this role can initiate backups directly from the client by using the <code>avtar</code> command line.</td>
</tr>
<tr>
<td>Restore (Read) Only User</td>
<td>Users assigned this role can initiate restores directly from the client by using the <code>avtar</code> command line or MCS web services.</td>
</tr>
<tr>
<td>Back Up/Restore User</td>
<td>Users assigned this role can initiate backups and restores directly from the client by using the <code>avtar</code> command line or MCS web services.</td>
</tr>
</tbody>
</table>
### Table 20 User roles (continued)

<table>
<thead>
<tr>
<th>User type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Restore (Read) Only/Ignore File Permissions | This role is similar to the Restore (Read) Only User role except that operating system file permissions are ignored during restores, thereby effectively allowing this user to restore any file stored for that Avamar client. This role is only available when you use internal authentication. Windows client user accounts should be assigned this role to ensure trouble-free restores, only if both of the following are true:  
  * Users are authenticated using Avamar internal authentication.  
  * The user will not access the Avamar client web UI. |

---

### Adding a user to a client or domain

You can add a user account to a client or domain when the user account is authenticated by using Avamar internal authentication or the deprecated enterprise authentication system.

[Preparing to use directory service authentication on page 66](#) provides details on adding a user that uses an existing directory service for authentication.

**Procedure**

1. Review Roles on page 75 to ensure that you will assign the correct role to this user.
2. In Avamar Administrator, click the **Administration** launcher button. The **Administration** window appears.
3. Click the **Account Management** tab.
4. Click the **Users** tab.
5. In the left-pane hierarchical tree, select the domain or client for the new user.

**Note**

You cannot add user accounts to the **MC_RETIRED** domain or to clients in the **MC_RETIRED** domain.

6. From the **Actions** menu, select **Account Management** > **New User(s)**. The **New User(s)** dialog box appears.
7. (Optional) From the **Authentication System** list, select an authentication system.

   The **Authentication System** list normally appears in a dimmed state, with **Axion Authentication System** (the internal system) selected. This indicates that the ability to select an enterprise authentication system is not currently enabled.

   The enterprise authentication system, which is described in the *EMC Avamar Product Security Guide*, is deprecated and will be removed in future releases. However it can be used with this release. To enable the ability to select an enterprise authentication system, complete the procedure described in **Enterprise authentication on page 74**.

   For a more robust alternative to enterprise authentication, use the method described in **Preparing to use directory service authentication on page 66**.
8. (Optional) If you select the enterprise authentication system, select the Everyone option to designate roles for all users on this client or domain.

9. Select the User Name option and type the new username.
   
   The username must meet the following requirements:
   
   - If you use enterprise authentication, this must be the username assigned by that system.
   - The username cannot contain more than 31 characters.
   - The username cannot contain any of the following characters: `~!@#$%^(){}[]\;\|,:?><'"& .

10. From the Role list, select a role for the user.

11. In the Password box, type a password for the user.

   Passwords are case-sensitive and must meet the following requirements:
   
   - The password must be between six and 31 characters in length.
   - The password must contain only alphanumeric, hyphen, period, or underscore characters.
   - The password must contain at least one alphabetic character.

   This field is not used with enterprise authentication.

12. In the Confirm box, retype the password.

   This field is not used with enterprise authentication.

13. Click OK.

   A confirmation message appears.

14. Click OK.

---

**Editing user information**

**Procedure**

1. In Avamar Administrator, click the Administration launcher button.

   The Administration window appears.

2. Click the Account Management tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the left-pane hierarchical tree, select the domain or client with the user.

4. Select the user.

5. From the Actions menu, select Account Management > Edit User.

   The Edit User dialog box appears.

6. Select the role for the user.

7. (Optional) Change the password for the user:

   a. Click Set Password.

      The Set Password dialog box appears.

   b. Type the new password into both the New Password and Confirm Password boxes.
c. Click OK on the Set Password dialog box.

8. Click OK.
   A confirmation message appears.

9. Click OK.

Deleting a user

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.

2. Click the Account Management tab.

3. In the left-pane hierarchical tree, select the domain or client with the user.

4. Select the user.

5. From the Actions menu, select Account Management > Delete User.
   A confirmation message appears.

6. Click Yes.
   A second confirmation message appears.

7. Click OK.
User Management and Authentication
CHAPTER 5
Backup

This chapter includes the following topics:

- Performing on-demand backups.................................................................84
- Scheduling backups....................................................................................85
- Monitoring backups....................................................................................110
- Canceling backups.....................................................................................110
- Managing completed backups.......................................................................111
Performing on-demand backups

You can perform an on-demand backup of an individual client. If you configure scheduled backups for a group of clients, then you can also perform an on-demand backup of a group or an on-demand backup of a single client by using group policy settings.

An on-demand backup is a one-time backup of data on an Avamar client computer. You may want to perform an on-demand backup for the first backup of the client immediately after you install the Avamar client software. You should also perform an on-demand backup before system maintenance, software installations, or software upgrades.

Performing an on-demand backup of a client

Procedure

1. In Avamar Administrator, click the Backup & Restore launcher button.
   
   The Backup, Restore and Manage window appears.

2. In the domain tree, select the domain for the client.

3. From the list of clients, select the client computer to back up.
   
   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.

4. Click the Backup tab.
   
   A list of plug-ins on the client appears in the left pane of the Backup tab.

5. Browse to and select the checkbox next to the data to back up.

6. If you browse the client file system, specify a valid client username and password, then click OK.
   
   The username and password must have read permissions on the files and directories that you select for backup.

7. (Optional) To view a summary of all directories and files that you selected for backup, select Actions > Preview List.

8. Select Actions > Back Up Now.
   
   The On Demand Backup Options dialog box appears.

9. Select the backup retention setting:
   
   - To automatically delete this backup from the Avamar server after a specific amount of time, select Retention period and then specify the number of days, weeks, months, or years for the retention period.
   
   - To automatically delete this backup from the Avamar server on a specific calendar date, select End date and browse to that date on the calendar.
   
   - To keep this backup for as long as this client remains active in the Avamar server, select No end date.

10. From the Avamar encryption method list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.
   
   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The EMC Avamar Product Security Guide provides additional information.

11. Click More Options.
   
   The Backup Command Line Options dialog box appears.
Performing an on-demand group backup

On-demand group backups enable you to back up an entire group of clients, or an individual client with group policy settings at some time other than the regularly scheduled time.

While you can perform individual on-demand backups for each client, this can be time-consuming if there are many clients. Furthermore, you cannot manage on-demand backups by using advanced retention settings; they can only be assigned a static expiration date. Instead, you can perform an on-demand group backup, which may take less time and also enables you to manage the backups using advanced retention settings.

Procedure

1. In Avamar Administrator, click the Policy launcher button. The Policy window appears.
2. Click the Policy Management tab.
3. Select the group or client to back up:
   - To back up a group, click the Groups tab and then select the group from the list.
   - To back up a client, click the Clients tab and then select the client from the list.
4. Click the Back Up.
5. Click OK on the confirmation message.

Scheduling backups

Scheduled backups run automatically to ensure that backups occur on an ongoing basis. You can schedule backups to run daily, weekly, or monthly. The scheduled backup can include multiple clients or a single server.

Procedure

1. Create a dataset to define the data that is included in the backups.
2. Create a schedule for when the backups should occur.
3. Create a retention policy to define how long to keep the backups in the system.
4. Create a group for the backups.
   a. Assign the new dataset to the new group.
   b. Assign a schedule to the new group.
   c. Assign a retention policy to the new group.
   d. Add one or more clients to the new group.
5. Enable scheduling for the group.

Datasets

When you perform an on-demand backup, the selection of directories and files in a client file system for the backup is valid only for that backup. In other words, it is not saved for future backups. An Avamar dataset is a list of directories and files to back up from a client. Assigning a dataset to a client or group enables you to save backup selections.

Each dataset defines:

- Source data list
- Exclusion list
- Inclusion list
- Plug-in options

**Source data list**

Dataset definitions start with a source data list that consists of:

- Data from one or more plug-ins
- A defined file system hierarchy, either the entire file system or selected directories, within each plug-in

**Exclusion and inclusion lists**

Datasets can also narrow the scope of the source data list by explicitly defining certain directories and file types to exclude or include in each backup.

Because default dataset behavior is to include everything in the source data list, the explicit exclusion and inclusion lists typically contain only a few entries.

When you specify exclusions and inclusions, case-sensitivity varies according to the target computing platform for the backup. Exclusions and inclusions for Windows platforms are not case-sensitive, while exclusions and inclusions for most other platforms are case-sensitive.

**NOTICE**

You cannot define inclusion and exclusion lists for several plug-ins, including the Exchange VSS plug-in, the SharePoint VSS plug-in, and VMware Image Backups.

**Processing relationship**

Avamar processes these dataset elements in the following order:

1. **Source data**—Source data from one or more plug-ins is defined. The default behavior is to include all data from all defined plug-ins.
2. **Exclusion list**—Next, the exclusion list is used to eliminate certain directories and file types from the dataset.
3. **Inclusion list**—Finally, the inclusion list is used to add back any files that were eliminated from the dataset in the exclusion list.

**Plug-in options**

Plug-in options enable you to further customize the behavior of a dataset. The user guide for each plug-in provides details on the options available for the plug-in.
Dataset catalog

The Avamar system includes a set of preconfigured datasets by default. You can use these datasets for scheduled backups of clients, or you can create a custom dataset.

**Base Dataset**
The Base Dataset defines a set of minimum, or baseline, backup requirements. The initial settings in the Base Dataset are:

- No source data plug-ins
- No explicit exclusion or inclusion list entries

This is essentially an empty dataset.

**Default Dataset**
The Default Dataset defines persistent backup selections for the Default Group. The initial settings in the Default Dataset are:

- All available source data plug-ins
- No explicit exclusion or inclusion list entries

This ensures that all members of the Default Group can back up their client computers regardless of platform type.

If you edit these settings, the changes are enforced on all members of the Default Group, unless you override the group settings and assign another dataset at the client level.

The directories listed in the following table are also inherently excluded from all backups, even though they do not explicitly appear in the exclusion list.

**Table 21 Directories excluded from Default Dataset backups**

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.snapshot/</td>
<td>NetApp mounts</td>
</tr>
<tr>
<td>VARDIR/f_cache.dat</td>
<td>Local avtar file cache</td>
</tr>
<tr>
<td>VARDIR/p_cache.dat</td>
<td>Local avtar &quot;is present&quot; cache</td>
</tr>
</tbody>
</table>

**Unix Dataset**
The Unix Dataset is optimized for use with AIX, FreeBSD, HP-UX, Linux, and Solaris clients. The initial settings in the Unix Dataset are:

- Only the AIX, FreeBSD, HP-UX, Linux, Macintosh OS X, and Solaris file system source data plug-ins
- Explicit exclusion of various temp directories (/tmp, /var/tmp, /usr/tmp), core dump files (core), and local cache files (*cache.dat, *scan.dat)
- No explicit inclusion list entries

The directories listed in the following table are also inherently excluded from all Unix Dataset backups, even though they do not explicitly appear in the exclusion list.

**Table 22 Directories excluded from Unix Dataset backups**

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.snapshot/</td>
<td>NetApp mounts</td>
</tr>
</tbody>
</table>
Table 22 Directories excluded from Unix Dataset backups (continued)

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VARDIR/f_cache.dat</td>
<td>Local avatar cache files</td>
</tr>
<tr>
<td>VARDIR/p_cache.dat</td>
<td>Local avatar cache files</td>
</tr>
<tr>
<td>/proc</td>
<td>Pseudo file system that cannot be restored</td>
</tr>
<tr>
<td>/dev</td>
<td>Excluded only if not running as root</td>
</tr>
<tr>
<td>/devices</td>
<td>Excluded only for Solaris</td>
</tr>
</tbody>
</table>

Windows Dataset

The Windows Dataset is optimized for use with Microsoft Windows clients. The initial settings in the Windows Dataset are:

- Only Windows file system source data plug-in
- No explicit exclusion or inclusion list entries

The directories listed in the following table are also inherently excluded from all Windows Dataset backups, even though they do not explicitly appear in the exclusion list.

Table 23 Directories excluded from Windows Dataset backups

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.snapshot/</td>
<td>NetApp mounts</td>
</tr>
<tr>
<td>VARDIR/f_cache.dat</td>
<td>Local avatar cache files</td>
</tr>
<tr>
<td>VARDIR/p_cache.dat</td>
<td>Local avatar cache files</td>
</tr>
<tr>
<td>All files referenced by the following registry keys:</td>
<td>Files explicitly designated by Microsoft to exclude from backups</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control \BackupRestore\FilesNotToBackup</td>
<td></td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\SYSTEM \CurrentControlSet\Control \BackupRestore\FilesNotToBackup</td>
<td></td>
</tr>
<tr>
<td>Temporary Internet files</td>
<td>Internet Explorer temporary files</td>
</tr>
<tr>
<td>outlook.ost</td>
<td>Outlook local cache files</td>
</tr>
<tr>
<td>outlook*.ost</td>
<td>Outlook local cache files</td>
</tr>
</tbody>
</table>

VMware Image Dataset

The VMware Image Dataset is the default dataset for protecting VMware entities with image backup. In many respects, the VMware Image Dataset is simpler than most other datasets:

- The only available source data plug-ins are Linux and Windows virtual disks, and both are selected by default.
- The Select Files and/or Folders option, as well as the Exclusions and Inclusions tabs, are disabled.
• Change block tracking is enabled by default using an embedded 
utilize_changed_block_list=true plug-in option statement.

The *EMC Avamar for VMware User Guide* provides details on using the VMware Image Dataset to back up VMware entities.

Creating a dataset

**Procedure**

1. In Avamar Administrator, select Tools › Manage Datasets.
   
   The Manage All Datasets window appears.

2. Click New.
   
   The New Dataset dialog box appears.

3. In the Name box, type a name for the dataset.
   
   The name can include alphanumeric characters (A-Z, a-z, 0-9) and the following special characters: period (.), hyphen (-), and underscore (_). Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?

4. Click the Source Data tab, and then define the source data plug-ins that contribute data to this dataset.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Include data from all plug-ins on the client</strong></td>
<td>Select Select All Data for All Local File Systems.</td>
</tr>
</tbody>
</table>
   | **Include data only from a specific plug-in and limit the dataset to specific data** | a. Select Enter Explicitly.  
b. From the Select Plug-In Type list, select the plug-in to use for the backups.  
Additional options may appear below the Select Plug-In Type list.  
c. Select the option to back up all available data with the plug-in, or select Select Files and/or Folders and then browse to the data to include in the backups. |

   **Note**
   
   You can also type the path to the data to back up. Typing the data path for a dataset on page 90 provides guidelines for typing the path.

5. Click the Exclusions tab, and then define the data to exclude from the dataset:
   
   a. Select the plug-in that you are using for the backups from the Select Plug-In Type list.
   
   b. Type the path to the data to exclude, or click ... to browse to the data.
   
   c. Click +.
   
   d. Repeat these steps for each data path to exclude from the backups.

   Typical exclusion lists include /temp files and directories and UNIX core dumps.
You cannot define inclusion and exclusion lists for several plug-ins, including the Exchange VSS plug-in, the SharePoint VSS plug-in, and VMware Image Backups.

6. Click the **Inclusions** tab, and then define the data to include in the dataset that otherwise would be excluded based on the selections on the **Exclusions** tab:
   a. Select the plug-in that you are using for the backups from the **Select Plug-in Type** list.
   b. Type the path to the data to include, or click ... to browse to the data.
   c. Click +.
   d. Repeat these steps for each data path to include in the backups.

7. Click the **Options** tab, and then set plug-in options either by using the graphical controls or by typing option names and values as text entries.

   The user guide for each plug-in provides details on the available options.

8. Click **OK**.

**Typing the data path for a dataset**

You can limit scheduled backups to a set of data by specifying the path to the data in the dataset. You can browse to or type the path to the data. Several rules apply when you type the path.

**Wildcards**

If you are using a file system plug-in, then the first occurrence of an asterisk (*) in a path is treated as a folder wildcard. For example, to specify the My Documents folder for all users on a Windows computer, type C:\Documents and Settings\*\My Documents.

To specify the Documents folder for all users on a Macintosh, type /Users/*/Documents.

**NOTICE**

When you specify a data path, only the first occurrence of an asterisk is treated as a folder wildcard. Subsequent occurrences are interpreted literally.

**Supported characters in the data path**

The path can include alphanumeric characters (A-Z, a-z, 0-9) and an asterisk (*) as a wildcard. Do not use any of the following characters in the data path: ~!@#$%^(){}[]\|,`;:*<>''&.

**Editing a dataset**

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Datasets**.

   The **Manage All Datasets** window appears.

2. Select a dataset and click **Edit**.

   The **Edit Dataset** dialog box appears.

3. Edit the dataset settings.

4. Click **OK**.

   Dataset changes take effect on the next scheduled backup. Backups that have already begun or have been completed are not affected.
Copying a dataset

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Datasets**.
   The *Manage All Datasets* window appears.
2. Select the dataset and click **Copy**.
   The *Save As* dialog box appears.
3. Type a name for the new dataset and click **OK**.

Deleting a dataset

**Before you begin**

Ensure that the dataset is not currently assigned to a client or group. You cannot delete a dataset if it is currently assigned to a client or group.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Datasets**.
   The *Manage All Datasets* window appears.
2. Select the dataset and click **Delete**.
3. Click **Yes** on the confirmation message.

Schedules

Schedules are reusable objects that control when group backups, custom event profile email notifications, and policy-based replication occur.

**Schedule types**

You can configure an Avamar schedule to repeat a system activity at one of the intervals listed in the following table.

**Table 24 Schedule types**

<table>
<thead>
<tr>
<th>Schedule type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>Repeats a system activity every day at one or more times of the day. With daily schedules, you must also limit the duration of the activity to prevent job overlap.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Repeats a system activity every week on one or more days of the week. With weekly schedules, you must also define the earliest start time for the activity, as well as the time at which the activity is stopped, even if it is still in progress.</td>
</tr>
<tr>
<td>Monthly</td>
<td>Repeats a system activity on a specific calendar date or on a designated day of the week each month, such as the first Sunday of every month. With monthly schedules, you must also define the earliest start time for the activity, as well as the time at which the activity is stopped, even if it is still in progress.</td>
</tr>
<tr>
<td>On-demand</td>
<td>Defines a schedule that does not run automatically. This option is useful for creating schedules that you can assign today but activate in the future, or to create schedules that are assigned to groups that only perform on-demand backups, such as groups that contain only laptop clients.</td>
</tr>
</tbody>
</table>
Schedule start time, end time, and duration

When you create a schedule, you also define when the schedule should take effect, and when it should be discontinued. For example, if you know that client computers used for a specific development project will be obsolete at a specific future date, you could create a schedule for those group backups that would automatically cease backups on a certain date. Similarly, if you are administering a large site, you could create schedules ahead of time, assign them to groups, and then activate them on a certain date. These group backups would not occur until the schedule took effect.

Because scheduled activities often straddle two calendar days, it is important to understand that Avamar allocates the full window of time to any activity initiated by a schedule. For example, consider a schedule with an earliest start time of 10 p.m., a latest end time of 6 a.m. (the following morning), and an end after date of December 31 of the current calendar year. On the evening of December 31, the activity starts as expected and runs until completed, typically sometime during the morning of January 1 the following year. However, beginning January 1, no new scheduled activities are initiated by this schedule.

The following figure illustrates how the start time, end time, and duration of a schedule interact with one another, using the initial settings of the Default schedule.

**Figure 10** Schedule start time, end time, and duration

![Backup Window Duration](image)

This system activity would begin at 10 p.m. (22:00), and could run until 6 a.m. (06:00) the next day. This creates an effective eight-hour duration.

In practice, scheduled activities rarely start or end precisely on time. Actual start times are affected by server load, and actual end times are affected by the complexity of the activity. The complexity of the activity involves, for example, the amount of new client data that must be backed up, the number of group backups initiated, the number of email messages that must be sent, and so forth.

It must therefore be understood that specifying a schedule start time means that this is the earliest possible time that the system activity can begin. In addition, specifying a duration or end time establishes the latest possible end time for the system activity.

Schedule time zones

When you create or edit schedules, all times are shown relative to the local time zone for the Avamar Administrator client. For example, if you create a schedule in the Pacific Standard Time zone with a next runtime of 10 p.m., then the next runtime for the schedule appears as 1 a.m. the following day (3 hours later) for an administrative user in the Eastern Standard Time zone.

Schedule catalog

The Avamar system includes a set of preconfigured schedules by default. You can use these schedules or create a custom schedule.

The following schedules are available by default.
Table 25 Schedule catalog

<table>
<thead>
<tr>
<th>Schedule name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Schedule</td>
<td>Controls backup scheduling for the Default Group. It is initially configured to run once per day at 10 p.m. If you edit these settings, the changes are enforced on all members of the Default Group.</td>
</tr>
<tr>
<td>Default Replication</td>
<td>Controls replication for replication groups.</td>
</tr>
<tr>
<td>Daily Schedule</td>
<td>Avamar supplies a predefined Daily Schedule.</td>
</tr>
<tr>
<td>Evaluation Schedule</td>
<td>Controls when the Evaluation Profile email notification is sent. It is initially configured to run every Monday at 6 a.m.</td>
</tr>
<tr>
<td>Notification Schedule</td>
<td>Controls when custom event profile email notification messages are sent.</td>
</tr>
<tr>
<td>Override Daily Schedule</td>
<td>Defines the available start times for clients that have the Override group schedules setting enabled. This schedule is editable. Copies of this schedule are not used with the Override group schedules setting.</td>
</tr>
<tr>
<td>Statistics Schedule</td>
<td>Controls how often various Avamar server statistics (for example, the Avamar server detail Bytes protected value) are retrieved or calculated. The default setting for this schedule is hourly.</td>
</tr>
</tbody>
</table>

Creating a schedule

Procedure

1. In Avamar Administrator, select Tools > Manage Schedules.
   The Manage All Schedules window appears.
2. Click New.
   The New Schedule dialog box appears.
3. In the Name box, type a name for the schedule.
   Do not use any of the following characters in the name: ~!@#$%^(){}[]\|';
   \/:*'<>"&.
4. In the Repeat this schedule section, choose the schedule type:
   - Daily
   - Weekly
   - Monthly
   - On-Demand
5. Specify the schedule settings.

<table>
<thead>
<tr>
<th>Schedule type</th>
<th>Schedule settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>a. Use the Select Daily Times lists to specify the time of day at which the schedule should run, and then click Add to add the time to the Scheduled Times list.</td>
</tr>
<tr>
<td></td>
<td>b. Repeat the previous step for each time at which the schedule should run each day.</td>
</tr>
</tbody>
</table>
### Schedule settings

<table>
<thead>
<tr>
<th>Schedule type</th>
<th>Weekly</th>
<th>Monthly</th>
</tr>
</thead>
<tbody>
<tr>
<td>c. (Optional) To remove a time from the <strong>Scheduled Times</strong> list, select the time and click <strong>Remove</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Limit the duration of scheduled system activities to prevent job overlap by selecting a time limit from the <strong>Limit each run to (hours)</strong> list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. From the <strong>Delay until</strong> list, select the date when the schedule should take effect. To make a schedule effective immediately, select the current date from the list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Choose when to discontinue the schedule:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• To enable a schedule to run indefinitely, select <strong>No End Date</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• To discontinue a schedule on a specific date, select <strong>End after</strong> and then select a date from the list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weekly</td>
<td>a. Select the checkbox next to the days of the week on which the schedule should run.</td>
<td>a. Choose whether to repeat the activity on a specific calendar date or on a designated day of the week each month:</td>
</tr>
<tr>
<td></td>
<td>b. Define the activity operating hours by using the <strong>Earliest start time</strong> and <strong>End no later than</strong> boxes. You can type the times, or select the time and use the arrow buttons to change the times.</td>
<td>• To repeat the activity on a specific calendar date, select <strong>Day of every month</strong>, and then select the day from the list.</td>
</tr>
<tr>
<td></td>
<td>Server workload affects the start time for an activity. In addition, the first time that a backup is performed for any client, the backup is allowed to continue past the specified end time. This is because initial backups can take significantly longer than subsequent backups of the same client.</td>
<td>• To repeat the activity on a designated day of the week each month, select <strong>The ... of every month</strong> and then select the day from the lists.</td>
</tr>
<tr>
<td></td>
<td>From the <strong>Delay until</strong> list, select the date when the schedule should take effect. To make a schedule effective immediately, select the current date from the list.</td>
<td>b. Define the activity operating hours by using the <strong>Earliest start time</strong> and <strong>End no later than</strong> boxes. You can type the times, or select the time and use the arrow buttons to change the times.</td>
</tr>
<tr>
<td></td>
<td>Choose when to discontinue the schedule:</td>
<td>Server workload affects the start time for an activity. In addition, the first time that a backup is performed for any client, the backup is allowed to continue past the specified end time. This is because initial backups can take significantly longer than subsequent backups of the same client.</td>
</tr>
<tr>
<td></td>
<td>• To enable a schedule to run indefinitely, select <strong>No End Date</strong>.</td>
<td>c. From the <strong>Delay until</strong> list, select the date when the schedule should take effect. To make a schedule effective immediately, select the current date from the list.</td>
</tr>
<tr>
<td></td>
<td>• To discontinue a schedule on a specific date, select <strong>End after</strong> and then select a date from the list.</td>
<td>d. Choose when to discontinue the schedule:</td>
</tr>
<tr>
<td>Schedule type</td>
<td>Schedule settings</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
<td></td>
</tr>
</tbody>
</table>
|               | • To enable a schedule to run indefinitely, select **No End Date**.  
|               | • To discontinue a schedule on a specific date, select **End after** and then select a date from the list. |
| On-demand     | There are no additional settings for on-demand schedules. |

6. Ensure that the date and time listed next to **Next Run Time** near the top of the **New Schedule** dialog box are correct.

7. Click **OK**.

Editing a schedule

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Schedules**.  
The **Manage All Schedules** window appears.

2. Select a schedule and click **Edit**.  
The **Edit Schedule** dialog box appears.

3. Edit the schedule settings.

4. Click **OK**.

Editing the start times for client overrides of group schedules

When you allow users to override group backup schedules by using the web UI, you must configure the start times that are available for clients to use. To configure the start times, add entries to the Override Daily Schedule.

Access to the web UI is part of the enhanced features for enterprise desktop and laptop computers.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Schedules**.  
The **Manage All Schedules** window appears.

2. From the list of schedules, select **Override Daily Schedule** and click **Edit**.  
The **Edit Schedule** dialog box appears.

3. Use the **Select Daily Times** lists to specify a time of day to add to the selection list available to users on the web UI, and then click **Add** to add the time to the **Scheduled Times** list.

   To remove a time from the **Scheduled Times** list, select the time and click **Remove**.

4. Repeat the previous step to add time entries to the selection list available to users.

5. Limit the duration of scheduled system activities to prevent job overlap by selecting a time limit from the **Limit each run to (hours)** list.

6. Click **OK**.
Copying a schedule

**Procedure**
1. In Avamar Administrator, select **Tools > Manage Schedules**.
   The **Manage All Schedules** window appears.
2. Select the schedule and click **Copy**.
   The **Save As** dialog box appears.
3. Type a name for the new schedule and click **OK**.

Running a schedule on-demand

You can initiate scheduled operations immediately on an on-demand basis. The scheduler does not need to be running when you run a schedule on-demand.

**Procedure**
1. In Avamar Administrator, select **Tools > Manage Schedules**.
   The **Manage All Schedules** window appears.
2. Select a schedule and click **Run Now**.

Deleting a schedule

**Before you begin**
Ensure that the schedule is not currently assigned to a group. You cannot delete a schedule if it is currently assigned to a group.

**Procedure**
1. In Avamar Administrator, select **Tools > Manage Schedules**.
   The **Manage All Schedules** window appears.
2. Select the schedule and click **Delete**.
3. Click **Yes** on the confirmation message.

Retention policies

Backup retention policies enable you to specify how long to keep a backup in the system. A retention policy is assigned to each backup when the backup occurs. You can specify a custom retention policy when you perform an on-demand backup, or you can create a retention policy that is assigned automatically to a group of clients during a scheduled backup.

When the retention for a backup expires, then the backup is automatically marked for deletion. The deletion occurs in batches during times of low system activity.

If necessary, you can manually change the retention setting for an individual backup that has already occurred. Changing the retention type for a backup on page 113 provides instructions. If you change a configured retention policy, however, the change applies only to backups that occur after the change. The retention setting remains the same for backups that have already been performed. Therefore, it is very important to carefully consider and implement the best retention policy for a site before too many backups occur.

There are two types of retention settings:
- Basic retention settings specify a fixed expiration date.
Advanced retention settings specify the number of daily, weekly, monthly, and yearly backups to keep.

Basic retention settings
Basic retention settings are used to assign a fixed expiration date to a backup using one of the settings in the following table.

Table 26 Basic retention settings

<table>
<thead>
<tr>
<th>Retention setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention period</td>
<td>Enables you to define a fixed retention period in days, weeks, months, or years after the backup is performed. For example, you could specify that backups expire after 6 months.</td>
</tr>
<tr>
<td>End date</td>
<td>Enables you to assign a calendar date as the expiration date. For example, you could specify that backups expire on December 31, 2013.</td>
</tr>
<tr>
<td>No end date</td>
<td>Enables you to keep backups indefinitely. This setting is useful for ensuring that all backups that are assigned this retention policy are retained for the life of the system.</td>
</tr>
</tbody>
</table>

NOTICE

For backups of 32-bit Windows or 32-bit Linux client computers, do not assign a retention period for a date after February 7, 2106. If you assign an extended retention period to a 32-bit Windows client, the backup completes with exceptions. For 32-bit Linux clients, the backups complete but do not appear in Avamar Administrator.

Advanced retention settings
With advanced retention settings, you can dynamically assign backup expiration dates based on the number of daily, weekly, monthly, and yearly backups to retain in the system.

When you perform scheduled daily backups on a regular basis, some backups are automatically assigned an advanced retention type:

- The first successful scheduled backup each day is designated as the daily backup.
- The first successful scheduled backup each week is designated as the weekly backup.
- The first successful scheduled backup each month is designated as the monthly backup.
- The first successful scheduled backup each year is designated as the yearly backup.

For the purpose of assigning advanced retention types, each day begins at 00:00:01 GMT, each week begins on Sunday, each month begins on the first calendar day of that month, and each year begins on January 1.

NOTICE

You cannot apply advanced retention settings to on-demand backups. On-demand backups can occur at any time, and are therefore inherently asynchronous—the system cannot tag them as daily, weekly, monthly, or yearly.

You should always use retention policies with advanced retention settings in conjunction with daily scheduled backups. The reason for this is that the Always keep: n weeks of daily backups setting has no effect unless there are daily backups in the system. However, depending on which schedule you use, this may not always be the case. For
example, if you assign a schedule to a group that only performs weekly backups, then there are no daily backups in the system.

Retention policy catalog

The Avamar system includes a set of preconfigured retention policies by default. You can use these retention policies for scheduled backups of clients, or you can create a custom retention policy.

The retention policies in the following table are available by default.

Table 27 Retention policy catalog

<table>
<thead>
<tr>
<th>Retention policy name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal Retention</td>
<td>Enables you to enforce a minimum basic retention setting across an entire site. For example, you can keep all backups for at least 90 days regardless of what other retention policies specify. This feature is intended to address the need of some enterprises to enforce site-wide minimum retention standards regardless of what individual organizations might decide to implement with other retention policies. The Minimal Retention policy is a global system object that controls only the minimal retention setting. Therefore, you cannot assign the Minimal Retention policy to a group.</td>
</tr>
<tr>
<td>Default Retention</td>
<td>Defines backup retention settings for the Default Group. By default, the Default Retention policy assigns a retention period of 60 days and retains 60 days of daily backups.</td>
</tr>
<tr>
<td>End User On Demand Retention</td>
<td>Controls the retention settings for on-demand backups initiated by the client, such as when you use the Back Up Now command on the Avamar Windows client. Advanced retention settings are disabled on this retention policy because advanced retention settings never apply to on-demand backups. The End User On Demand Retention policy is a global system object that only controls retention for on-demand backups initiated by the client. Therefore, you cannot assign the End User On Demand Retention policy to a group.</td>
</tr>
<tr>
<td>Monthly Retention policy</td>
<td>Sets the expiration date to one month after the backup is performed.</td>
</tr>
<tr>
<td>Weekly Retention policy</td>
<td>Sets the expiration date to one week after the backup is performed.</td>
</tr>
</tbody>
</table>

Creating a retention policy

Procedure

1. In Avamar Administrator, select Tools > Manage Retention Policies. The Manage All Retention Policies window appears.
3. In the Name box, type a name for the retention policy.
Do not use any of the following characters in the retention policy name: ~!@#$%^(){}[],\;:\""'.

4. Specify either basic or advanced retention settings for the policy.

<table>
<thead>
<tr>
<th>Retention setting</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Select one of the following settings:</td>
</tr>
<tr>
<td></td>
<td>• To automatically delete backups after a specific number of days, weeks, months, or years, select <strong>Retention period</strong> and specify the number of days, weeks, months, or years.</td>
</tr>
<tr>
<td></td>
<td>• To automatically delete backups on a specific calendar date, select <strong>End date</strong> and then browse to that date on the calendar.</td>
</tr>
<tr>
<td></td>
<td>• To keep backups for as long as a client remains active, select <strong>No end date</strong>.</td>
</tr>
<tr>
<td></td>
<td>The best practice is to specify a retention that is greater than or equal to 14 days. When you create a retention policy for less than 14 days, an alert appears.</td>
</tr>
<tr>
<td>Advanced</td>
<td>a. Select <strong>Override basic retention policy for scheduled backups</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Advanced</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Edit Advanced Retention Policy</strong> dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>c. Specify the maximum number of daily, weekly, monthly, and yearly backups to retain.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong> on the <strong>Edit Advanced Retention Policy</strong> dialog box.</td>
</tr>
</tbody>
</table>

5. Click **OK** on the **New Retention Policy** dialog box.

Editing a retention policy

**Procedure**

1. In Avamar Administrator, select **Tools** > **Manage Retention Policies**.

   The **Manage All Retention Policies** window appears.

2. Select a retention policy and click **Edit**.

   The **Edit Retention Policy** dialog box appears.

3. Edit the retention policy settings.

   Click **OK**.

Copying a retention policy

**Procedure**

1. In Avamar Administrator, select **Tools** > **Manage Retention Policies**.

   The **Manage All Retention Policies** window appears.

2. Select a retention policy and click **Copy**.

   The **Save As** dialog box appears.

3. Type a name for the new retention policy and click **OK**.
Deleting a retention policy

**Before you begin**

Ensure that the retention policy is not currently assigned to a client or group. You cannot delete a retention policy if it is currently assigned to a client or group.

**Procedure**

1. In Avamar Administrator, select *Tools > Manage Retention Policies*.
   The *Manage All Retention Policies* window appears.
2. Select the retention policy and click *Delete*.
3. Click *Yes* on the confirmation message.

Enforcing a minimum retention setting

Minimal retention enables you to enforce a minimum basic retention setting across an entire site. For example, you can keep all backups for at least 90 days regardless of what other retention policies specify.

This feature is intended to address the need of some enterprises to enforce site-wide minimum retention standards regardless of what individual organizations might decide to implement with other retention policies.

To enforce minimal retention, enable and configure the Minimal Retention policy, which is a default retention policy in the system. The Minimal Retention policy is a global system object that controls only the minimal retention setting. Therefore, you cannot assign the Minimal Retention policy to a group.

**Procedure**

1. In Avamar Administrator, select *Tools > Manage Retention Policies*.
   The *Manage All Retention Policies* window appears.
2. Select the *Minimal Retention* policy and click *Edit*.
   The *Edit Retention Policy* dialog box appears.
3. Select *Retention period*.
4. Specify the number of days, weeks, months, or years to ensure that backups are retained.
5. Click *OK*.

Automatically retaining the last backup

To retain the last backup of all clients, even after the backup exceeds its retention period, enable last backup retention. Last backup retention changes the default retention behavior for client backups that occur after it is enabled. With last backup retention, the last backup of a client is not marked for deletion when its retention period expires. When a new backup runs, the new backup becomes the “last backup” and the previous “last backup” expires or is retained according to its retention policy.

Last backup retention is designed for clients that do not back up frequently. For those clients, the default behavior can lead to the last backup expiring before a new backup occurs. This could result in clients that do not have an available backup.

Clients that are not permanently connected to a domain, such as remote desktops and laptops, may encounter this situation more frequently than clients that have uninterrupted server access.
When you enable last backup retention, Avamar retains a single backup for each client, even if you perform multiple types of backups of a client. For example, if you perform both file system and application backups of a client, and the file system backup is the last backup, then all application backups can expire.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press Enter.
2. Change directories by typing:
   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
3. Open `mcserver.xml` in a text editor.
4. Find the `dpn` node.
5. In the `dpn` node, change the value of the `keep_last_backup` entry key from `false` to `true`.
6. Save the change and close the text editor.
7. Stop and restart the MCS, and start the scheduler by typing the following commands:
   ```
   dpnctl stop mcs
   dpnctl start mcs
   dpnctl start sched
   ```
8. Close the command shell.

Groups

Avamar uses groups to implement various policies to automate backups and enforce consistent rules and system behavior across an entire segment, or group, of the user community.

Group members

Group members are client machines that have been added to a particular group for the purposes of performing scheduled backups. Because the normal rules for domain administrators apply, these clients must be located within the same domain or within a subdomain of where the group exists.

Group policy

When you create a group, you specify the dataset, schedule, and retention policy for the group. These three objects comprise the group policy. The group policy controls backup behavior for all members of the group.

You can override group dataset and retention policy settings for a client by making explicit dataset or retention policy assignments for the client. However, schedules apply only to groups, not individual clients.
**Default Group**

The Avamar system includes a Default Group. In the default Avamar server configuration, the Default Group always uses the system default dataset, schedule, and retention policy. You cannot change these system default assignments. However, you can edit the settings within the system default dataset, schedule, and retention policy.

If you do not create any other groups, then new clients are automatically added to the Default Group.

**VMware groups**

The following table describes the special groups that apply to VMware environments.

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Proxy Group</td>
<td>The Default Proxy Group is the default group for VMware Image Proxy clients. You cannot delete the Default Proxy Group. Enabling the Default Proxy Group does not conflict with scheduled backups performed by other plug-ins configured on the proxy client.</td>
</tr>
<tr>
<td>Default Virtual Machine Group</td>
<td>New virtual machine clients are automatically added to the Default Virtual Machine Group when they are registered. You cannot manually delete the Default Virtual Machine Group, but it is automatically deleted if you delete the vCenter domain.</td>
</tr>
<tr>
<td>VM Backup Validation groups</td>
<td>VM Backup Validation groups are used to implement the restore rehearsal feature for VMware virtual machines.</td>
</tr>
</tbody>
</table>

The *EMC Avamar for VMware User Guide* provides additional details on each of these groups.

### Creating a group

When you create a group, you define the dataset, schedule, and retention policy, which together comprise the group policy for scheduled backups of all members of the group. A group must contain at least one Avamar client. If the group contains two or more clients, then the clients must belong to the same Avamar domain. You can override group policy settings at the client level.

**Before you begin**

You cannot edit schedules or retention policies when you use the **New Group** wizard to create a group. Review existing schedules and retention policies. If required, create new ones before you create the group.

**Procedure**

1. In Avamar Administrator, click the **Policy** launcher button.

The **Policy** window appears.

2. Click the **Policy Management** tab.

3. Click the **Groups** tab.

4. Select the domain for the group.

The **Policy** window displays a table that contains groups for the domain.

5. Select **Actions**  >  **Group**  >  **New**  >  **Backup Group**.

The **New Group** wizard appears.
6. Type a name for the new group in the **Name** box.

   The name can include alphanumeric characters (A-Z, a-z, 0-9) and the following special characters: period (.), hyphen (-), and underscore (_). Do not use Unicode characters or the following special characters: ` ~ ! # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?

7. Clear the **Disabled** checkbox to use this group for scheduled client backups.

   Selecting the checkbox disables backups for the group.

8. From the **Avamar encryption method** list, select an encryption method to use for data transfer between the Avamar server and the client during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

9. (Optional) Select **Override Schedule** to override the assigned schedule for this group:

   - To skip the next scheduled backup, select **Skip Next Backup**.
   - To perform the next scheduled backup one time only, select **Run Next Backup Once**.

10. Click **Next**.

    The next **New Group** wizard page appears with dataset information.

11. From the **Select An Existing Dataset** list, select the dataset that you created, and then click **Next**.

    The next **New Group** wizard page appears with schedule information.

12. Select a schedule from the **Select An Existing Schedule** list, and click **Next**.

    The next **New Group** wizard page appears with retention policy information.

13. Select a retention policy from the **Select an Existing Retention Policy** list, and click **Next**.

    The final **New Group** wizard page appears. A list of domains appears in the **Choose Domain** pane.

14. Select the domain for the client.

    A list of Avamar clients appears in the pane below the **Choose Domain** pane.

15. Select the checkbox next to the clients to include in the group.

    The clients appear in the **Members** pane.

16. (Optional) To remove a client from the group, select the client from the **Members** list, and then click the red X.

17. Click **Finish**.

**Managing group membership**

You can manage group membership in Avamar Administrator either by adding or removing members for a group or adding or removing groups to which a client belongs.

The method that you use to manage group membership depends on the situation. For example, if you are adding or deleting multiple clients from a single group, then the group-centric method is efficient. Conversely, if you are adding or removing a single client from multiple groups, then the client-centric method is most efficient.
Editing membership for a group

Procedure
1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Groups tab.
4. Select the group.
5. Select Actions > Group > Edit Group.
   The Edit Group dialog box appears.
6. Click the Members tab.
7. Add or remove members for the group.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add members to the group</td>
<td>Select the checkboxes next to the clients to add.</td>
</tr>
<tr>
<td>Remove members from the</td>
<td>Select the clients to remove and click X.</td>
</tr>
<tr>
<td>group</td>
<td></td>
</tr>
<tr>
<td>Move members to another</td>
<td>Select the client from the Member(s) list and click Move. In the</td>
</tr>
<tr>
<td>group</td>
<td>Move Group Members dialog box, select the new group for the client</td>
</tr>
<tr>
<td></td>
<td>and click OK.</td>
</tr>
</tbody>
</table>

8. Click OK.

Editing the groups for a client

Procedure
1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Clients tab.
4. Select the client to edit.
5. Select Actions > Group > Edit Client.
   The Edit Client dialog box appears.
6. Click the Groups tab.
7. Add and remove groups for the client:
   • To add groups, click Add, select the groups, and then click OK.
   • To remove groups, select the groups from which to remove the client, and click Remove.
8. Click OK.

Monitoring groups

You can monitor groups by using the Group Summary Reports and Group Status Summary.
Procedure

- To view the Group Summary Reports, click the Policy launcher button in Avamar Administrator, and then click the Group Summary Reports tab on the Policy window.

  The Group Summary Reports are a combined “at a glance” view of all current group properties and settings, including group policy overrides. The reports also display the datasets, schedules, and retention policies assigned to various groups.

- To view the Group Status Summary, click the Activity launcher button in Avamar Administrator, and then click the Group Status Summary tab on the Activity window.

  The Group Status Summary is a simplified presentation of all backup activity initiated as a result of group policies, including the total number of backups initiated by way of the group policy, as well as the number of active, successfully completed, canceled, and failed backups.

Editing group properties

You can edit properties for a single group or for multiple groups. When you select multiple groups, you cannot edit all group properties.

The Default Proxy Group and the Default Virtual Machine Group contain special settings that are only of interest to persons managing the VMware Image backup and restore feature. The EMC Avamar for VMware User Guide provides details on these settings.

Procedure

1. In Avamar Administrator, click the Policy launcher button.

   The Policy window appears.

2. Click the Policy Management tab.

3. Click the Groups tab.

4. Select one or more groups to edit.

5. Select Actions > Group > Edit Group.

   If you selected a single group, then the Edit Group dialog box appears. If you selected multiple groups, then the Edit Multiple Groups dialog box appears.

6. Edit the group information:

   - When you edit a single group, you can edit only basic group properties, such as the name, client list, and the dataset, schedule, and retention policy that are assigned to the group. You cannot edit the settings for the assigned dataset, schedule, and retention policy.

   - When you edit the Default Group, you cannot edit Default Group policy object assignments. The Default Group always uses the default dataset, default schedule, and default retention policy. Therefore, the Dataset, Schedule, and Retention Policy tabs do not appear when you edit the Default Group.

   - When you edit multiple groups, select the new settings from the lists, or select Don’t Change to leave a setting unchanged for the selected groups. You can edit only basic group properties, such as whether the group is enabled or disabled, the encryption setting, and the dataset, schedule, and retention policy that are assigned to the groups. You cannot edit the settings for the assigned dataset, schedule, and retention policy.

7. Click OK.
Copying a group

You must copy groups within the same domain. You cannot copy a group to another domain.

Procedure

1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Groups tab.
4. Select the group to copy.
5. Select Actions > Group > Copy Group.
   The Save As dialog box appears.
6. Type a name for the new group.
7. Select the Include Client Members to copy the entire client list to this new group.
8. Click OK.

Enabling and disabling a group

You can disable a group to prevent scheduled backups from occurring for the group. This is typically done to place the system in a state that supports various maintenance activities.

If you disable a group, you must re-enable the group to resume scheduled group backups.

Procedure

1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Groups tab.
4. Select the group to enable or disable.
5. Right-click the group and select Disable Group.
   If the group is disabled, this action clears the checkmark and enables the group. If the group is enabled, this action sets the checkmark and disables the group.
6. Click Yes.

Deleting a group

Before you begin

Assign the clients in the group to a different group so that scheduled backups for the clients can continue uninterrupted.

Procedure

1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Groups tab.
4. Select the group to delete.
5. Select Actions > Group > Delete Group.
6. Click Yes on the confirmation message. A second confirmation message appears.
7. Click OK.

Overriding group policy settings for a client

You can override group policy settings for a single client, including the dataset, schedule, and encryption method for client/server data transfers. You also can allowing users to initiate on-demand backups from the client by using the Avamar client web UI, or specify a maximum size in MB for backups from the client.

**NOTICE**

Too many overrides can make group policies less effective. Instead, implement a new group policy rather than repeatedly overriding an existing policy at the client level.

**Procedure**

1. In Avamar Administrator, click the Policy launcher button. The Policy window appears.
2. Click the Policy Management tab.
3. Click the Clients tab.
4. In the left pane, select the domain for the client.
5. In the right pane, select the client.
6. Click Edit. The Edit Client window appears.
7. Click the Properties tab.
8. To allow users on the client to initiate on-demand backups, select Allow client initiated backups.
   
   If no additional configuration is performed, backups initiated by this client include only those files selected by the user at the time the backup is started. In addition, End User On-Demand Retention is applied. However, you can enforce the use of a particular dataset and retention policy for all client-initiated backups.

9. To allow users to create sets of folders and files to back up through an on-demand backup by using the Avamar client web UI, select Allow file selection on client initiated backups.

   When this feature is enabled, users can:
   
   - Specify the folders and files to include in a backup set.
   - Create multiple backup sets.
   - Save backup sets for reuse.
   - Perform an on-demand backup of the folders and files in the backup sets they create.

**NOTICE**

Folders and files selected through this feature are not subject to group dataset source limits, exclusions, or inclusions. In addition, automatic backup of clients according to their group policies is not affected by this feature.
Note

Windows, Mac, and Linux clients that use the desktop and laptop client enhancements require an additional configuration step to enable this setting. Allowing users to create on-demand backup sets on page 342 provides more information.

10. Choose whether to override the group schedule duration setting for a client by selecting a value from the **Overtime** list:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No overtime allowed</td>
<td>Scheduled group backups are never allowed to run past the schedule duration setting.</td>
</tr>
<tr>
<td>Overtime on next backup only</td>
<td>Only the next scheduled group backup is allowed to run past the schedule duration setting.</td>
</tr>
<tr>
<td>Overtime until successful backup</td>
<td>Scheduled group backups are allowed to run past the schedule duration setting until a successful backup completes.</td>
</tr>
<tr>
<td>Always allow overtime</td>
<td>Scheduled group backups are always allowed to run past the schedule duration setting.</td>
</tr>
</tbody>
</table>

11. Select **Override group encryption to**, and then select the encryption setting to use for client/server data transfer for the client.

The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The **EMC Avamar Product Security Guide** provides details.

12. To allow users in the Avamar client web UI to select a different backup start time for daily backups from a list of available times that you specify, select **Allow override of group’s daily schedule**.

Editing the start times for client overrides of group schedules on page 95 provides more information on specifying the list of available times.

13. To specify a maximum allowed size in MB for the client’s backups, type an integer between 1 and 99999 in **Hard limit (MB)**.

Backups from the client that exceed that size are canceled. The Activity Report entry for the backup displays **True** in the `hard_limit_exceeded` column, and the status entry **Hard limit exceeded** appears in the Activity Monitor.

14. To specify a maximum size in MB beyond which the client's backups are flagged for excessive size, type an integer between 1 and 99999 in **Soft limit (MB)**.

Backups from the client that exceed that size are allowed, but the Activity Report entry for the client’s backup displays **True** in the `soft_limit_exceeded` column, and the status entry **Completed** appears in the Activity Monitor.

15. If you allow users on the client to initiate on-demand backups, select the retention policy for all client-initiated backups:

a. Click the **Retention Policy** tab.

b. Choose whether to use the group retention policy or a different retention policy for all client-initiated backups by selecting or clearing the **Override group retention policy** checkbox. Clear the checkbox to use the retention policy assigned to the group, or select the checkbox to use a different retention policy.
c. If you select the checkbox to use a different retention policy, select the **Override retention policy on client initiated backups** checkbox, and then select the retention policy from the **Select an Existing Retention Policy** list.

16. To assign separate override datasets for each group in which the client is a member:
   a. Click the **Groups** tab.
   b. For each group in which the client is a member, select a dataset from the list in the **Override Dataset** column.

17. To allow users use the Avamar client web UI to add folders to the source data for the group datasets assigned to the users’ clients, click the **Dataset Additions** tab and then select **Allow additions to source data**.

   The added data is included in every automatic and on-demand backup for every group assigned to the client, and group exclusion and inclusion lists are applied to the added data.

18. Click **OK**.

**Overriding group policy settings for multiple clients**

You can override group policy settings for multiple clients at a time, including the encryption method, whether backups can run beyond the schedule end time, and whether users on the client can initiate on-demand backups and select a different backup start time.

**Procedure**

1. In Avamar Administrator, click the **Policy** launcher button.
   
   The **Policy** window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select the clients.
5. Click **Edit**.
   
   The **Edit Multiple Clients** dialog box appears.
6. Select an override value from the list, and select **Apply the change**.
   
   **Overriding group policy settings for a client on page 107** provides more information on each of the settings.
7. Click **OK**.

**Enabling scheduled backups**

Scheduled backups occur only for enabled groups. Groups are disabled by default unless you select the **Enabled** checkbox on the first page of the **New Group** wizard. If you did not enable the group when you created it, use the menu options in the **Policy** window to enable backups.

**Procedure**

1. In Avamar Administrator, click the **Policy** launcher button.
   
   The **Policy** window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group that you created.
5. Enable the group by selecting Actions > Group > Disable Group. Perform this step only if a check mark appears next to the Disable Group menu option.
6. Click Yes to enable this group.

Monitoring backups

You can monitor backups to ensure that the backups complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for both on-demand and scheduled backups.

Procedure
1. In Avamar Administrator, click the Activity launcher button. The Activity window appears.
2. Click the Activity Monitor tab. A list of all activities appears.
3. To filter the results to display only backup activity, select Actions > Filter. The Filter Activity dialog box appears.
4. Select All Backups from the Type list.
5. Click OK.

Canceling backups

You can cancel a backup any time before it completes. The cancellation might take five minutes or longer. The backup may complete before the cancellation finishes.

Procedure
1. In Avamar Administrator, click the Activity launcher button. The Activity window appears.
2. Click the Activity Monitor tab. A list of all activities appears.
3. Select the backup from the list.
4. Select Actions > Cancel Activity. A confirmation message appears.
5. Click Yes.
Managing completed backups

After you perform an on-demand or scheduled backup, you can validate the backup, change settings for the backup, or delete the backup.

Finding a completed backup to manage

You can find a completed backup by searching for a backup that occurred on a specific calendar date or during a specific date range, or by searching for a backup with a specific retention type.

**NOTICE**

Avamar generally supports the use of specific supported international characters in directory, folder, and filenames. However, proper display of international language characters is contingent on the client computer’s Java locale and installed system fonts being compatible with the original language. If you browse backups that were created with international characters and a compatible font is not installed, then any characters that cannot be resolved by the system appear as rectangles. This is a normal limitation of that particular situation and does not affect the ability to restore these directories, folders, or files. The *EMC Avamar Release Notes* provide additional international language support information.

**Procedure**

1. In Avamar Administrator, click the `Backup & Restore` launcher button. The `Backup, Restore and Manage` window appears.
2. In the clients tree, browse to and select the client with the backups to manage.
3. Click the `Manage` tab.
4. Find the backup either by date, date range, or retention type.

<table>
<thead>
<tr>
<th>Search method</th>
<th>Steps</th>
</tr>
</thead>
</table>
| By date           | a. Select **By day**.  
b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight. |
| By date range     | a. Select **By date range**.  
b. Click the **From Date** list, and browse the calendar for the start date for the range.  
c. Click the **To Date** list, and browse the calendar for the end date for the range.  
d. Click **Retrieve**. |
| By retention type | a. Select **By retention**.  
b. Select the checkbox next to the retention type for the backup.  
c. Click **Retrieve**. |
A list of backups on that date, within that date range, or with the retention type appears in the Backup History list.

Validating a backup

You can verify that files can be restored from a backup. This validation initiates a “virtual” restore of all files in the backup, but does not actually restore any files to the client file system.

Procedure

1. In Avamar Administrator, click the Backup & Restore launcher button.
   The Backup, Restore and Manage window appears.

2. Find the backup. Finding a completed backup to manage on page 111 provides instructions.

3. In the Backup History list, select the backup to validate.

4. Select Actions > Validate Backup.
   The Select Client to Perform Validation dialog box appears.

5. Select the client on which to validate the backup:
   • To validate the backup on the same client from which the backup was originally performed, select Validate using the backup client.
   • To validate the backup on a different client, select Validate using a different client, and then click Browse to browse to the client.

6. From the Validation Plug-in Type list, select the plug-in on which to validate the backup. Only the plug-ins that are installed on the selected client appear in the list.

7. From the Avamar encryption method list, select the encryption method to use for client/server data transfer during the validation.

   Note
   The default encryption setting for backup validations is high, regardless of the encryption setting used for the original backup.

8. Click OK.
   A confirmation message appears.

9. Click OK.

After you finish

Backup validations appear as activities in the Activity window. You can monitor and cancel the backup validation activity the same way that you monitor or cancel a backup. Monitoring backups on page 110 and Canceling backups on page 110 provide instructions.

Changing the expiration date for a backup

You can change the date that a backup expires. When the backup expires, Avamar users cannot recover data from the expired backup. A garbage collection process runs on a nightly basis to clean up and reclaim space from orphaned data (data that is unique to the expired backups).

The expiration date can be a specific date that you select or a retention period of a certain number of days, weeks, months, or years. You also can configure a backup to remain in backup storage for as long as the client remains active on the Avamar server.
Procedure

1. In Avamar Administrator, click the **Backup & Restore** launcher button.
   The **Backup, Restore and Manage** window appears.

2. Find the backup. Finding a completed backup to manage on page 111 provides instructions.

3. In the **Backup History** list, select the backup to manage. To select multiple backups, press Ctrl while you select the backups.

4. Select **Actions** > **Change Expiration Date**.
   The **Change Expiration Date** dialog box appears.

5. Select the new expiration date:
   - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period** and then specify the number of days, weeks, months, or years for the retention period.
   - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
   - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.

6. Click **OK**.
   A confirmation message appears.

7. Click **Yes**.
   An event code dialog box appears.

8. Click **OK**.

9. Click **OK** on the confirmation message.

Changing the retention type for a backup

To support certain advanced features, Avamar Administrator automatically assigns one or more retention types to every backup. For example, the first backup created on an Avamar system is tagged as a daily, weekly, monthly, or yearly. You can manually change the retention types assigned to a backup.

When you manually change the retention types assigned to a backup, especially one that has multiple retention types, be certain that you are not inadvertently removing a weekly, monthly, or yearly backup that you need to retain. For example, consider a backup that is assigned daily, weekly, monthly, and yearly retention types. If you remove the yearly retention type designation, you might not have another yearly backup in the system for quite a long time.

Procedure

1. In Avamar Administrator, click the **Backup & Restore** launcher button.
   The **Backup, Restore and Manage** window appears.

2. Find the backup. Finding a completed backup to manage on page 111 provides instructions.

3. In the **Backup History** list, select the backup to manage. To select multiple backups, press Ctrl while you select the backups.

4. Select **Actions** > **Change Retention Type**.
   The **Change Retention Type** dialog box appears.
5. Select one of the following retention types for the backups:
   • To explicitly assign a daily, weekly, monthly or yearly retention type to this backup, select Tags and then select the checkbox next to the retention types.
   • If you do not want to explicitly assign a daily, weekly, monthly, or yearly retention type to the backup, select Not tagged. The backup is designated as untagged.

6. Click OK.
   A confirmation message appears.

7. Click Yes.
   A second confirmation message appears.

8. Click OK.

Viewing backup statistics

You can view detailed statistics for completed backups from both the Activity window and the Manage tab of the Backup, Restore and Manage window.

The Manage tab of the Backup, Restore and Manage window provides statistics for any stored backup. The Activity window shows only recent backup activity. Typically, only the backups within the past 72 hours appear in the Activity window.

The same statistics appear for each backup, regardless of whether you view the statistics from the Backup, Restore and Manage window or the Activity window.

Procedure

1. Find the backup in either the Backup, Restore and Manage window or the Activity window.

<table>
<thead>
<tr>
<th>Window</th>
<th>Steps to find the backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup, Restore and Manage window</td>
<td>a. In Avamar Administrator, click the Backup &amp; Restore launcher button. The Backup, Restore and Manage window appears.</td>
</tr>
<tr>
<td></td>
<td>b. Find the backup. Finding a completed backup to manage on page 111 provides instructions.</td>
</tr>
<tr>
<td></td>
<td>c. In the Backup History list, select the backup.</td>
</tr>
<tr>
<td>Activity window</td>
<td>a. In Avamar Administrator, click the Activity launcher button. The Activity window appears.</td>
</tr>
<tr>
<td></td>
<td>b. Click the Activity Monitor tab.</td>
</tr>
<tr>
<td></td>
<td>c. Select a backup activity from the list.</td>
</tr>
</tbody>
</table>

2. Select Actions > View Statistics.

   The Backup Statistics dialog box appears. The following information is available on the tabs of the Backup Statistics dialog box.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Detailed information from the v_activities_2 database view. The EMC Avamar Reports Guide provides more information about the v_activities_2 database view.</td>
</tr>
<tr>
<td>Files</td>
<td>A list of files included in the backup.</td>
</tr>
</tbody>
</table>
3. (Optional) To export the data on a tab of the **Backup Statistics** dialog box to a comma-separated values (`.csv`) file, click **Export** and then specify the location and filename for the file.

4. Click **Close**.

### Deleting a backup

When you delete a backup, Avamar immediately and permanently deletes all data in that backup from the server.

**Procedure**

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup, Restore and Manage** window appears.

2. Find the backup to delete. [Finding a completed backup to manage](#) provides instructions.

3. In the **Backup History** list, select the backup to delete.

4. Select **Actions > Delete Backup**.

   A confirmation message appears.

5. Click **OK**.
Backup
CHAPTER 6

Restore and Recovery

This chapter includes the following topics:

- Restoring data from a backup ................................................................. 118
- Monitoring restores .................................................................................. 123
- Canceling restores .................................................................................... 123
- Windows client system recovery ................................................................. 124
- Red Hat and CentOS Linux system recovery ............................................. 124
- SUSE Linux system recovery .................................................................... 130
- Oracle Solaris system recovery .................................................................. 137
Restoring data from a backup

You can find a backup to restore either by date or by the contents of the backup. When you perform the restore, you can restore to either the original location, a different location, or multiple locations.

**NOTICE**

The options for the restore destination depend on the plug-in type. For example, the SQL Server plug-in enables you to restore to a file instead of to SQL Server, and you cannot restore to multiple locations with the Oracle plug-in. The user guide for each plug-in provides details on the available options and how to perform each available type of restore.

Finding a backup

The first step to restore data is to find the backup with the data that you want to restore. You can find Avamar client backups by searching either for a specific date or for specific content.

Locate backups by date when one or more of the following situations apply:

- You save all data for the client in a single backup set.
- The exact pathname or name of the data to restore is unknown.
- The backup you want to restore is before a specific date or event. For example, you know the approximate date when data was lost or corrupted. You can search for a backup before that date.
- The specific types of backups are known. For example, you run scheduled disaster recovery backups every Wednesday and Saturday night, and you run full volume backups daily. When you need to rebuild a server, select the disaster recovery backup with the date closest to the event that caused the loss of data.

Locate backups by the content of the backup when one or more of the following situations apply:

- You back up data on the client in separate backup sets.
- You want to view multiple versions of the same file so that you can decide the version to restore.
- The date of the backup or the content of a backup is unknown, but you know the name of the data to restore.

**NOTICE**

Avamar generally supports the use of specific supported international characters in directory, folder, and filenames. However, proper display of international language characters is contingent on the client computer's Java locale and installed system fonts being compatible with the original language. If you browse backups that were created with international characters and a compatible font is not installed, then any characters that cannot be resolved by the system appear as rectangles. This is a normal limitation of that particular situation and does not affect the ability to restore these directories, folders, or files. The EMC Avamar Release Notes provide additional international language support information.
Finding a backup by date

Procedure
1. In Avamar Administrator, click the **Backup & Restore** launcher button.
   
The *Backup, Restore and Manage* window appears.
2. Click the **Restore** tab.
   
The upper left pane contains a list of domains.
3. Select the domain that contains the client.
   
You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.
   
A list of Avamar clients appears in the pane under the domains list.
4. Select the client from the list.
5. Click the **By Date** tab.
6. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.
   
A list of backups on that date appears in the **Backups** table next to the calendar.
7. Select the backup to restore from the **Backups** table.
8. Select the data to restore from the **Contents of Backup** pane at the bottom of the **Select for Restore** tab.
9. If you browse the client file system, specify a valid client username and password, then click **OK**.
   
The username and password must have read permissions on the files and directories that you select for restore.
10. Select **Actions** ⇒ **Restore Now**.

Finding a backup by content

Procedure
1. In Avamar Administrator, click the **Backup & Restore** launcher button.
   
The *Backup, Restore and Manage* window appears.
2. Click the **Restore** tab.
   
The upper left pane contains a list of domains.
3. Select the domain that contains the client.
   
You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.
   
A list of Avamar clients appears in the pane under the domains list.
4. Select the client from the list.
5. Click the **By File/Folder** tab.
6. In the **Enter path to retrieve history for** text box, specify the pathname to the content by using one of the methods in the following table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type the path</strong></td>
<td>Type the full pathname to the content in the <strong>Enter path to retrieve history for</strong> box.</td>
</tr>
</tbody>
</table>
| **Browse**   | a. Click **Browse**. The **Select File or Folder** window appears.  
|              | b. Select the client.  
|              | c. Select the plug-in. A list of folders appears in a table to the right of the plug-ins pane.  
|              | d. Select the content to restore.  
|              | e. Click **OK**. The selected content appears in the **Enter path to retrieve history for** box.                                             |

7. Click **Retrieve**.

The **Version History** table lists all versions and sizes of the content in backups for the client.

8. Select the version in the **Version History** table.

All backups for the client that contain the version appear in the **Backups** table next to the **Version History** table.

9. Select the data to restore from the **Contents of Backup** pane at the bottom of the **Select for Restore** tab.

10. If you browse the client file system, specify a valid client username and password, then click **OK**.

The username and password must have read permissions on the files and directories that you select for restore.

11. Select **Actions** › **Restore Now**.

**Restoring to the original location**

**Procedure**

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

The **Backup, Restore and Manage** window appears.

2. Find the backup to restore:

   - **Finding a backup by date on page 119**
   - **Finding a backup by content on page 119**

   The backup to restore is selected in the **Backups** table.

3. Select **Actions** › **Restore Now**.

   The **Restore Options** dialog box appears.

4. Leave the default selection of the original client in the **Restore Destination Client** box.

5. Leave the default selection of the original backup plug-in in the **Restore Plug-in** list.

6. From the **Avamar encryption method** list, select an encryption method for client/server data transfers during this restore.
Note
The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

7. Select **Restore everything to its original location**.

8. To include plug-in options with this restore, click **More Options**, and then configure the settings. The user guide for each plug-in provides details on each plug-in option.

9. Click **OK** on the **Restore Options** dialog box.

   The **Restore Request** dialog box indicates that the restore was initiated.

10. Click **Close**.

**Restoring to a different location**

**Procedure**

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup, Restore and Manage** window appears.

2. Find the backup to restore:

   - **Finding a backup by date on page 119**
   - **Finding a backup by content on page 119**

   The backup to restore is selected in the **Backups** table.

3. Select **Actions > Restore Now**.

   The **Restore Options** dialog box appears.

4. Select the destination client for the data to restore:

   - To restore to a different location on the same client, leave the default selection of the original client in the **Restore Destination Client** box.
   - To restore to a different client, click the **Browse** button next to the **Restore Destination Client** box, and then browse to and select the destination client.

5. Select the plug-in to use for the restore from the **Restore Plug-in** list.

6. From the **Avamar encryption method** list, select an encryption method for client/server data transfers during this restore.

---

**Note**

The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

7. Select **Restore everything to a different location**.

---

**NOTICE**

When you restore a single directory to a different location, Avamar restores only the contents of the directory. Avamar does not restore the original parent directory.

8. Select the destination directory on the client for the data to restore:

   a. Click **Set Destination** below the items **Marked for Restore** list.

      The **Set Destination** dialog box appears.
b. Type the path to the destination directory in the **Save Target(s) in Directory** box, or click **Browse** to browse to a directory.

If you type a path and the directory does not already exist, then the restore process creates the directory.

c. Click **OK** on the **Set Destination** dialog box.

When a file with the same name already exists in the path to which you are restoring a file, use the **Overwrite Existing Files** option on the **Restore Command Line Options** dialog box to control whether the restore process overwrites the file.

9. To include plug-in options with this restore, click **More Options**, and then configure the settings. The user guide for each plug-in provides details on each plug-in option.

10. Click **OK** on the **Restore Options** dialog box.

The **Restore Request** dialog box indicates that the restore was initiated.

11. Click **Close**.

## Restoring to multiple locations

You can restore backup data to multiple locations on a destination client.

### Procedure

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup, Restore and Manage** window appears.

2. Find the backup to restore:
   - Finding a backup by date on page 119
   - Finding a backup by content on page 119

   The backup to restore is selected in the **Backups** table.

3. Select **Actions** > **Restore Now**.

   The **Restore Options** dialog box appears.

4. Select the destination client for the data to restore:
   - To restore to multiple locations on the same client, leave the default selection of the original client in the **Restore Destination Client** box.
   - To restore to multiple locations on a different client, click the **Browse** button next to the **Restore Destination Client** box and then browse to and select the destination client.

5. Select the plug-in to use for the restore from the **Restore Plug-in** list.

6. From the **Avamar encryption method** list, select an encryption method for client/server data transfers during this restore.

   __Note__

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

7. Select **Restore everything to multiple locations**.

   __NOTICE__

   When you restore multiple directories to multiple locations, Avamar restores only the contents of the directory. Avamar does not restore the original parent directory.
8. Select the destination directories on the client for the data to restore:
   a. Click Set Destination below the Items Marked for Restore list.
      The Set Destination dialog box appears.
   b. Select a row in the list.
   c. Type the path to the destination directory in the Destination (Save As) column in the list, or click Browse to browse to a directory.
      If you type a path and the directory does not already exist, then the restore process creates the directory.
   d. Repeat the previous two steps for each row in the list on the Set Destination dialog box.
   e. Click OK on the Set Destination dialog box.
      When a file with the same name already exists in the path to which you are restoring a file, use the Overwrite Existing Files option on the Restore Command Line Options dialog box to control whether the restore process overwrites the file.
9. To include plug-in options with this restore, click More Options, and then configure the settings. The user guide for each plug-in provides details on each plug-in option.
10. Click OK on the Restore Options dialog box.
    The Restore Request dialog box indicates that the restore was initiated.
11. Click Close.

Monitoring restores

You can monitor restores to ensure that the restores complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for restores.

Procedure
1. In Avamar Administrator, click the Activity launcher button.
   The Activity window appears.
2. Click the Activity Monitor tab.
   A list of all activities appears.
3. To filter the results to display only restore activity, select Actions > Filter.
   The Filter Activity dialog box appears.
4. Select Restore from the Type list.
5. Click OK.

Canceling restores

You can cancel a restore any time before the restore completes. The cancellation might take five minutes or longer. The restore may complete before the cancellation finishes.

Procedure
1. In Avamar Administrator, click the Activity launcher button.
   The Activity window appears.
2. Click the Activity Monitor tab.  
   A list of all activities appears.
3. Select the restore from the list.
4. Select Actions > Cancel Activity.  
   A confirmation message appears.
5. Click Yes.

Windows client system recovery  
Comprehensive details about the necessary backups for Windows client system recovery and the procedures to perform the recovery are available in the *EMC Avamar for Windows Server User Guide*.

Red Hat and CentOS Linux system recovery  
The following topics describe how to restore a Red Hat or CentOS Linux client system to its original system state.

Reconstructing the partition table  
Before you perform system recovery of a Linux client, you must reconstruct the partition table used in the original Avamar backup by running an `avtar --showlog mounts` command on a temporary client computer, then examining the output to determine the number and size of partitions to create when you install the operating system on the target recovery client.

**Procedure**
1. Locate the backup to use for the system state recovery:
   a. In Avamar Administrator, click the **Backup & Restore** launcher button.
      The **Backup, Restore and Manage** window appears.
   b. Click the **Restore** tab.
   c. In the clients tree, select the original Linux client.
   d. Find the full system backup to use to recover the system state.
   e. Note the backup label number.
   f. Leave Avamar Administrator open for the remainder of the system state recovery procedure.
2. On a temporary client computer with network connectivity to the Avamar server, open a command shell and log in as root.
3. Type the following command:
   ```
   /usr/local/avamar/bin/avtar --avamaronly --showlog mounts --server=Avamar_server --id=username --ap=password --path=/domain/client --labelnumber=n
   ```
   where:
   - *Avamar_server* is the IP address or fully qualified hostname as defined in DNS for the Avamar server.
- *username* and password are the login credentials for a user account with a sufficient role and privileges to perform a restore.
- */domain/client* is the full location of the original Linux client on the Avamar server.
- *n* is the label number of the backup to use for the system state recovery.

4. Examine the command output to locate entries beginning with `mount_decision`. For example:

```plaintext
mount_decision: reason="starting_point" fstype="ext3" path="/"
mount_decision: reason="default_backup" fstype="ext3" path="/boot"
mount_decision: reason="default_backup" fstype="ext3" path="/home"
```

These are entries for the mount points on the original system. Earlier in the output, there are entries for each of these mount points. For example:

```plaintext
mount: status="user_directed_backup" path="/" hdev="/dev/root" kind="ext3" blksize=4096 freeblks=1189334 maxblks=2405872 freefiles=2259654 maxfiles=2432000 dev=2050
mount: status="default_backup" path="/boot" hdev="/dev/sda1" kind="ext3" blksize=1024 freeblks=183371 maxblks=194442 freefiles=50167 maxfiles=50200 dev=2049
mount: status="default_backup" path="/home" hdev="/dev/sdb1" kind="ext3" blksize=4096 freeblks=1027161 maxblks=5158925 freefiles=2530548 maxfiles=2621440 dev=2065
```

These entries contain mount point size and path information.

5. Calculate the original file system size or each mount point in bytes by multiplying the `blksize` value by the `maxblks` value.

**NOTICE**

Multiplying the `blksize` value by the `maxblks` value calculates the free space used on the original device. However, you should create the root partition with an additional 2 GB to 3 GB of free space to ensure sufficient space for the minimal install used for the restore process.

6. Note which paths are mounted from separate file systems. This information is required later in the restore process.

**Preparing the target recovery client**

**Procedure**

1. Ensure that the recovery destination disk is connected to the target recovery client.

2. Perform a minimal installation of a compatible operating system. For the purposes of this procedure:
   - Minimal installation means that desktop environment entries such as Desktop - Gnome should not be selected for installation.
   - In the **Customize Now** dialog box **Base System** category, select the **Base** option. Leave all other options disabled.
   - Compatible operating system means the same version. For example, if the original client backup on the Avamar server was performed on an RHEL3 client, then you must install RHEL3 on the target recovery client.
Use the information that you gathered during Reconstructing the partition table on page 124 to create as many partitions as necessary to replicate the original configuration.

3. (Optional) Save a copy of the /etc/fstab file so that you can compare it to the restored /etc/fstab file.

4. Install the Avamar Client for Linux. The *EMC Avamar Backup Clients User Guide* provides instructions.

Performing system recovery of a RedHat or CentOS Linux client

**Before you begin**

Perform the steps in Reconstructing the partition table on page 124 and Preparing the target recovery client on page 125.

**Procedure**

1. Start the recovery target client from the install media (first CD/DVD):
   - On Red Hat or CentOS 4 or 5, type `linux rescue` at the command prompt.
   - On Red Hat or CentOS 6.0 or later, select Rescue installed system.

2. Follow the onscreen instructions.
   
   Be sure to enable networking by providing IP address, network mask, default gateway, and DNS server values when prompted. You can use a temporary hostname and IP, or the original information from the machine that you are restoring.

3. Allow the installer to search for installations and mount the /mnt/sysimage file system as read-write.

   This is the target of the restore, and is also referred to as the *recovery destination disk*.

   **Note**

   You cannot restore the root file system directly to /mnt/sysimage because there is currently no method to restrict the restore operation to only the local partition without traversing network mount points. Therefore, a restore directly to /mnt/sysimage might copy files from all the partitions, and /mnt/sysimage could fill up before all required files were restored.

4. Ensure that the following directories are all present in the `LD_LIBRARY_PATH` system variable:
   - /lib
   - /lib64
   - /usr/lib
   - /usr/lib64
   - /mnt/sysimage/lib
   - /mnt/sysimage/lib64
   - /mnt/sysimage/usr/local/avamar/lib

   If any directories are missing from `LD_LIBRARY_PATH`, add them.

5. Create a temporary /tmp/avtar.cmd flag file with a UNIX text editor. For example:

   ```
   cd /tmp
   vi avtar.cmd
   ```
---bindir=/mnt/sysimage/usr/local/avamar/bin
--vardir=/mnt/sysimage/usr/local/avamar/var
--sysdir=/mnt/sysimage/usr/local/avamar/etc
--server=Avamar_server
--account=/domain/client
--id=username
--ap=password
--target=.

where:

- **Avamar_server** is the Avamar server IP address or fully qualified hostname as defined in DNS.
- **/domain/client** is the full location of the original Linux client on the Avamar server.
- **username** and **password** are the login credentials for a user account with sufficient role and privileges to perform the restore.

6. Restore most of the directories that originally existed under root (/):

**NOTICE**

Do not restore files located on file systems other than the root file system at this time. These directories and files are restored later in this procedure.

a. Create a temporary restore directory under the client /mnt/sysimage directory and change directory to it by typing commands similar to the following examples:

```bash
mkdir /mnt/sysimage/restore
cd /mnt/sysimage/restore
```

b. Restore the contents of the root file system from the backup by typing the following command on a single command line:

```bash
/mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd --labelnumber=n [--exclude=./boot --exclude=./home] /
```

where **n** is the label number of the backup to use for the system state recovery.

Use **--exclude=path** options to exclude paths that were identified as separate mount points. These directories and files are separately restored later in this procedure.

The first two **--exclude** options in the previous command are included as an example. You must replace the values with options appropriate to the system that you are restoring. You must specify exclude options relative to the root of the original backup. For example, **--exclude=./boot** instead of **--exclude=/boot**.

c. For each directory that was restored, delete the original directory from /mnt/sysimage, and move the restored directory from the /mnt/sysimage/restore directory to /mnt/sysimage by typing commands similar to the following examples:

```bash
rm -rf /mnt/sysimage/etc
mv /mnt/sysimage/restore/etc /mnt/sysimage/etc
```

d. Repeat the previous step for each directory that successfully restored to /mnt/sysimage/restore.

7. Restore individual files in the root (/) directory:
a. Change directory to `/mnt/sysimage/restore` by typing the following command:

    cd /mnt/sysimage/restore

b. Restore the individual files in the root (/) directory by typing the following commands:

    mv ./* /mnt/sysimage
    mv ./.* /mnt/sysimage

8. Restore other mount points:

a. Check that file systems are mounted as expected by typing `df -h` on the command line.

b. Compare the output to the expected set of mounted file systems. If there are discrepancies, mount the devices onto the appropriate mount points.

c. Change directory to each mount point by typing a command similar to the following example:

    cd /mnt/sysimage/home

d. Create a temporary restore directory, then change directory to it by typing commands similar to the following examples:

    mkdir ./restore
    cd ./restore

e. Restore the contents of the mount point by typing the following command:

    /mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd --labelnumber=n /home

    where n is the label number of the backup to use for the restore, and `/home` is an example mount point.

f. Return to the mount point directory, and delete all files except for the restore directory by typing commands similar to the following examples:

    alias ls=/usr/bin/ls
    cd /mnt/sysimage/home; rm -rf `ls --hide restore`
    rm -rf ./.*

g. Change directory to the `restore` directory, then move the contents into the appropriate place in the mount point by typing the following command:

    cd ./restore;mv `ls -A ./` ..

h. Remove the `restore` directory by typing the following commands:

    cd ..
    rmdir restore

i. Repeat steps d through i for each remaining mount point.

9. Perform final system checks:

a. Inspect `/mnt/sysimage/etc/fstab`, and verify that there are valid statements for each file system to be mounted on the new system.

    There are three ways that devices might be listed in the `fstab` file: device path, volume label, and Universally Unique Identifier (UUID).
You can determine this information about the file systems by typing `/mnt/sysimage/lib/udev/vol_id device_path`, where `device_path` is the `/dev` path to the device.

If that program is not present on the system, type `/mnt/sysimage/sbin/blkid device_path`.

If you had to manually re-create partitions during the minimal system install, the device UUIDs might have changed. Update the device UUIDs in `/mnt/sysimage/etc/fstab`. If some volumes are missing expected labels, set the label by typing `/mnt/sysimage/sbin/e2label device_path label`.

b. Re-examine the `fstab` carefully.

The restored system does not boot properly if the `fstab` entries do not exactly match the storage device configuration, and the rescue system on the install media has difficulty discovering which file systems to mount to `/mnt/sysimage`.

---

**Note**

If you saved a reference copy of the `fstab` file when you were preparing the target client for recovery, then you may be able to find the disk information in that file. For systems with few manual modifications to the restored `fstab` file, it might be possible to use the reference `fstab` file instead of the restored copy of the file.

c. Verify that no more files are present in `/mnt/sysimage/restore` by typing the following command:

```
ls -al /mnt/sysimage/restore
```

d. If the directory is empty, remove it by typing the following command:

```
rmdir /mnt/sysimage/restore
```

e. If the command fails because the directory is not empty, then there might be directories that you failed to move in when you restored most of the directories in root (`/`). If this is the case, then move the directories to the proper restore locations.

10. Exit the command shell and reboot the system by typing `exit`.

   If you are rebooting a Red Hat or CentOS 6 system, a menu appears.

11. Select `reboot`, then `OK` and press `Enter`.

   The system restarts.

12. Eject the install media and boot normally.

13. Confirm correct client operation.
Troubleshooting system recovery of a RedHat or CentOS Linux client

The following topics provide details on troubleshooting issues that may occur after you perform system recovery of a RedHat or CentOS Linux client.

Troubleshooting a boot failure after system recovery

If the restored system does not boot at the end of the restore procedure, then the version of GRUB installed by the minimal OS might be too dissimilar to the version previously used on the machine. You must boot into the restore environment and reinstall GRUB.

Procedure

1. Boot into the restore environment by starting the client from the install media with the rescue option.
2. If the startup process cannot find the restored operating system, then its `fstab` is probably configured incorrectly. Mount the partitions manually, and correct the contents of the file.
3. Reinstall GRUB by typing the following commands:

   ```bash
   chroot /mnt/sysimage
   grub-install device
   ```

   where `device` is the boot device (for example, `/dev/sda`).
4. Exit the chroot environment by typing `exit`.
5. Exit the command shell and reboot the system by typing `exit`.

   If you are rebooting a Red Hat or CentOS 6 system, a menu appears.
6. Select `reboot`, then `OK` and press `Enter`.

   The system restarts.
7. Eject the install media and boot normally.

Restoring network settings after system recovery of a RedHat or CentOS Linux client

If the operating system detects that you have restored the system to new hardware, it might revert the network settings to defaults (for example, DHCP name resolution instead of static IP). You can recover the previous network settings by manually reconfiguring the settings.

To examine the previous settings, open the `.bak` files in `/etc/sysconfig/network-scripts` in a text editor. These files contain useful information, but should not be used in the current configuration in an unmodified form, since they include MAC address information from the previous hardware.

SUSE Linux system recovery

The following topics describe how to restore a SUSE Linux client system to its original system state.

Reconstructing the partition table

Before you perform system recovery of a Linux client, you must reconstruct the partition table used in the original Avamar backup by running an `avtar --showlog mounts` command on a temporary client computer, then examining the output to determine the
number and size of partitions to create when you install the operating system on the target recovery client.

**Procedure**

1. Locate the backup to use for the system state recovery:
   a. In Avamar Administrator, click the **Backup & Restore** launcher button. The **Backup, Restore and Manage** window appears.
   b. Click the **Restore** tab.
   c. In the clients tree, select the original Linux client.
   d. Find the full system backup to use to recover the system state.
   e. Note the backup label number.
   f. Leave Avamar Administrator open for the remainder of the system state recovery procedure.

2. On a temporary client computer with network connectivity to the Avamar server, open a command shell and log in as root.

3. Type the following command:

   ```
   /usr/local/avamar/bin/avtar --avamaronly --showlog mounts --
   server=Avamar_server --id=username --ap=password --path=/domain/
   client --labelnumber=n
   ```

   where:
   - **Avamar_server** is the IP address or fully qualified hostname as defined in DNS for the Avamar server.
   - **username** and password are the login credentials for a user account with a sufficient role and privileges to perform a restore.
   - **/domain/client** is the full location of the original Linux client on the Avamar server.
   - **n** is the label number of the backup to use for the system state recovery.

4. Examine the command output to locate entries beginning with **mount_decision**.

   For example:

   ```
   mount_decision: reason="starting_point" fstype="ext3"
   path="/"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/boot"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/home"
   ```

   These are entries for the mount points on the original system. Earlier in the output, there are entries for each of these mount points. For example:

   ```
   mount: status="user_directed_backup" path="/" hdev="/dev/
   root" kind="ext3" bksize=4096 freeblks=1189334
   maxblks=2405872 maxfiles=2259654 dev=2050
   mount: status="default_backup" path="/boot" hdev="/dev/sda1"
   kind="ext3" bksize=1024 freeblks=183371 maxblks=194442
   freefiles=50167 maxfiles=50200 dev=2049
   mount: status="default_backup" path="/home" hdev="/dev/sdb1"
   kind="ext3" bksize=4096 freeblks=1027161 maxblks=5158925
   freefiles=2530548 maxfiles=2621440 dev=2065
   ```
These entries contain mount point size and path information.

5. Calculate the original file system size or each mount point in bytes by multiplying the `blksize` value by the `maxblks` value.

   **NOTICE**

   Multiplying the `blksize` value by the `maxblks` value calculates the free space used on the original device. However, you should create the root partition with an additional 2 GB to 3 GB of free space to ensure sufficient space for the minimal install used for the restore process.

6. Note which paths are mounted from separate file systems. This information is required later in the restore process.

### Preparing the target recovery client

**Procedure**

1. Ensure that the recovery destination disk is connected to the target recovery client.

2. Perform a minimal installation of a compatible operating system. For the purposes of this procedure:
   - Minimal installation means that only **Base System** and **Minimal System (Appliances)** packages are installed from the **Software selection** page. All other packages should be deselected so that they are not installed.
   - Compatible operating system means the same version. For example, if the original client backup on the Avamar server was performed on a SLES10 client, then you must install SLES10 on the target recovery client.
   - Use the information that you gathered during Reconstructing the partition table on page 124 to create as many partitions as necessary to replicate the original configuration.

3. (Optional) Save a copy of the `/etc/fstab` file so that you can compare it to the restored `/etc/fstab` file.

4. Install the Avamar Client for Linux. The **EMC Avamar Backup Clients User Guide** provides instructions.

### Performing system recovery of a SUSE Linux client

**Before you begin**

Perform the steps in Reconstructing the partition table on page 124 and Preparing the target recovery client on page 132.

**Procedure**

1. Start the recovery target client from the install media (first CD/DVD) and select **Rescue System**.

2. Open a command shell on the recovery target client and log in as root.

3. Mount the root partition created in the minimal install to `/mnt` by typing the following command:

   ```
   mount /dev/sda# /mnt
   
   where `/dev/sda#` is the device that contains the root file system. If the drive was configured to use Linux Logical Volume Management, then the root device might be in the form of `/dev/VolGroup##/LogVol##`. ```
4. Rebind the pseudo-file systems into the /mnt tree by typing the following commands:

```bash
mount --rbind /proc /mnt/proc
mount --rbind /sys /mnt/sys
mount --rbind /dev /mnt/dev
```

5. Change the current file system root by typing the following command:

```
chroot /mnt
```

6. Start the network as configured in the prerequisites by typing the following command:

```
rcnetwork start
```

7. Mount the auto-mount file systems and verify that the correct file systems were mounted by typing the following command:

```
mount -a; df -h
```

8. If any file systems are missing (for example, if /boot is not set to auto-mount), then manually mount them to the correct locations by using additional `mount` commands.

9. Exit the chroot environment by typing `exit`.

10. Copy the network name resolution file from the chroot environment into the working restore environment by typing the following command:

```
cp /mnt/etc/resolv.conf /etc/resolv.conf
```

11. Ensure that the following directories are all present in the `LD_LIBRARY_PATH` system variable:

- /lib
- /lib64
- /usr/lib
- /usr/lib64
- /mnt/lib
- /mnt/lib64
- /mnt/usr/local/avamar/lib

If any directories are missing from `LD_LIBRARY_PATH`, add them.

12. Create a temporary `/tmp/avtar.cmd` flag file with a UNIX text editor. For example:

```bash
cd /tmp
vi avtar.cmd
```

```
--bindir=/mnt/usr/local/avamar/bin
--vardir=/mnt/usr/local/avamar/var
--sysdir=/mnt/usr/local/avamar/etc
--server=Avamar_server
--account=/domain/client
--id=username
--ap=password
--target=
```

where:

- `Avamar_server` is the Avamar server IP address or fully qualified hostname as defined in DNS.
- `/domain/client` is the full location of the original Linux client on the Avamar server.
username and password are the login credentials for a user account with sufficient role and privileges to perform the restore.

13. Restore most of the directories that originally existed under root (/):

NOTICE

Do not restore files located on file systems other than the root file system at this time. These directories and files are restored later in this procedure.

a. Create a temporary restore directory under the client /mnt directory and change directory to it by typing commands similar to the following examples:

   mkdir /mnt/restore
   cd /mnt/restore

b. Restore the contents of the root file system from the backup by typing the following command on a single command line:

   /mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd --labelnumber=n [--exclude=./boot --exclude=./home] /

   where n is the label number of the backup to use for the system state recovery.

   Use --exclude=path options to exclude paths that were identified as separate mount points. These directories and files are separately restored later in this procedure.

   The first two --exclude options in the previous command are included as an example. You must replace the values with options appropriate to the system that you are restoring. You must specify exclude options relative to the root of the original backup. For example, --exclude=./boot instead of --exclude=/boot.

c. For each directory that was restored, delete the original directory from /mnt, and move the restored directory from the /mnt/restore directory to /mnt by typing commands similar to the following examples:

   rm -rf /mnt/etc
   mv /mnt/restore/etc /mnt/etc

d. Repeat the previous step for each directory that successfully restored to /mnt/restore.

14. Restore individual files in the root (/) directory:

a. Change directory to /mnt/restore by typing cd /mnt/restore.

b. Restore the individual files in the root (/) directory by typing the following commands:

   mv ./* /mnt
   mv ./.* /mnt

15. Restore other mount points:

a. Check that file systems are mounted as expected by typing df -h on the command line.

b. Compare the output to the expected set of mounted file systems. If there are discrepancies, mount the devices onto the appropriate mount points.

c. Change directory to each mount point by typing a command similar to the following example:

   cd /mnt/home
d. Create a temporary restore directory, then change directory to it by typing commands similar to the following examples:

```
mkdir ./restore
cd ./restore
```

e. Restore the contents of the mount point by typing the following command:

```
/mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd
--labelnumber=n /home
```

where \( n \) is the label number of the backup to use for the restore, and \( /home \) is an example mount point.

f. Return to the mount point directory, and delete all files except for the restore directory by typing commands similar to the following examples:

```
alias ls=/usr/bin/ls
cd /mnt/home; rm -rf `ls --hide restore`
rm -rf ./.*
```

g. Change directory to the restore directory, then move the contents into the appropriate place in the mount point by typing the following command:

```
cd ./restore;mv `ls -A ./` ..
```

h. Remove the restore directory by typing the following commands:

```
cd ..
rmdir restore
```

i. Repeat steps d through i for each remaining mount point.

16. Perform final system checks:

a. Inspect \( /mnt/etc/fstab \), and verify that there are valid statements for each file system to be mounted on the new system.

There are three ways that devices might be listed in the \( fstab \) file: device path, volume label, and Universally Unique Identifier (UUID).

You can determine this information about the file systems by typing \( /mnt/lib/udev/vol_id \) \( device_path \), where \( device_path \) is the \( /dev \) path to the device.

If you had to manually re-create partitions during the minimal system install, the device UUIDs might have changed. Update the device UUIDs in \( /mnt/etc/fstab \). If some volumes are missing expected labels, set the label by typing \( /mnt/sbin/e2label device_path label \).

b. Re-examine the \( fstab \) carefully.

The restored system does not boot properly if the \( fstab \) entries do not exactly match the storage device configuration, and the rescue system on the install media has difficulty discovering which file systems to mount to \( /mnt \).

---

**Note**

If you saved a reference copy of the \( fstab \) file when you were preparing the target client for recovery, then you may be able to find the disk information in that file. For systems with few manual modifications to the restored \( fstab \) file, it might be possible to use the reference \( fstab \) file instead of the restored copy of the file.
c. Verify that no more files are present in /mnt/sysimage/restore by typing the following command:

```
ls -al /mnt/restore
```

d. If the directory is empty, remove it by typing the following command:

```
rmdir /mnt/restore
```

e. If the command fails because the directory is not empty, then there might be directories that you failed to move in when you restored most of the directories in root (/). If this is the case, then move the directories to the proper restore locations.

17. Reboot the system by typing `reboot`.

18. Eject the install media and boot normally.

19. Confirm correct client operation.

**Troubleshooting system recovery of a SUSE Linux client**

The following topics provide details on troubleshooting issues that may occur after you perform system recovery of a SUSE Linux client.

**Troubleshooting a boot failure after system recovery**

If the restored system does not boot at the end of the restore procedure, then the version of GRUB installed by the minimal OS might be too dissimilar to the version previously used on the machine. You must boot into the restore environment and reinstall GRUB.

**Procedure**

1. Boot into the restore environment:
   a. Start the recovery target client from the install media (first CD/DVD) and select Rescue System.
   b. Open a command shell on the recovery target client and log in as root.
   c. Mount the root partition created in the minimal install to /mnt by typing the following command:

      ```
mount /dev/sda#/ /mnt
```

      where `/dev/sda#` is the device that contains the root file system. If the drive was configured to use Linux Logical Volume Management, then the root device might be in the form of `/dev/VolGroup##/LogVol##`.

d. Rebind the pseudo-file systems into the /mnt tree by typing the following commands:

   ```
   mount --rbind /proc /mnt/proc
   mount --rbind /sys /mnt/sys
   mount --rbind /dev /mnt/dev
   ```

e. Change the current file system root by typing the following command:

   ```
   chroot /mnt
   ```

f. Start the network as configured in the prerequisites by typing the following command:

   ```
   rnetwork start
   ```
g. Mount the auto-mount file systems and verify that the correct file systems were mounted by typing the following command:

```
mount -a; df -h
```

h. If any file systems are missing (for example, if `/boot` is not set to auto-mount), then manually mount them to the correct locations by using additional `mount` commands.

2. Reinstall GRUB by typing the following commands:

```
chroot /mnt
grub-install device
```

where `device` is the boot device (for example, `/dev/sda`).

3. Exit the chroot environment by typing `exit`.

4. Reboot the system by typing `reboot`.

5. Eject the install media and boot normally.

Restoring network settings after system recovery of a RedHat or CentOS Linux client

If the operating system detects that you have restored the system to new hardware, it might revert the network settings to defaults (for example, DHCP name resolution instead of static IP). You can recover the previous network settings by manually reconfiguring the settings.

To examine the previous settings, open the `.bak` files in `/etc/sysconfig/network-scripts` in a text editor. These files contain useful information, but should not be used in the current configuration in an unmodified form, since they include MAC address information from the previous hardware.

Oracle Solaris system recovery

The following topics describe how to restore an Oracle Solaris client system to its original system state.

Preparing for Oracle Solaris system recovery

Ensure that the environment meets the following prerequisites before you perform system recovery for an Oracle Solaris system.

Available backup with critical system files

To successfully restore an Oracle Solaris client system to its original system state, you must have an Avamar backup of the entire local file system and the following critical system files and virtual file systems. This is accomplished by forcing traversal of the targets listed in the following table during a backup.

<table>
<thead>
<tr>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mntfs</td>
<td><code>/etc/svc/volatile</code></td>
</tr>
<tr>
<td>tmpfs</td>
<td><code>/etc/mnttab</code></td>
</tr>
<tr>
<td>cachefs</td>
<td>Solaris Cache File System</td>
</tr>
<tr>
<td>fdfs</td>
<td>Solaris File Descriptor File System</td>
</tr>
</tbody>
</table>

Table 29 Target locations for system recovery backups of an Oracle Solaris client
Table 29 Target locations for system recovery backups of an Oracle Solaris client (continued)

<table>
<thead>
<tr>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fifofs</td>
<td>Solaris FIFO File System</td>
</tr>
<tr>
<td>namefs</td>
<td>Solaris Name File System</td>
</tr>
<tr>
<td>specfs</td>
<td>Solaris Device Special File System</td>
</tr>
<tr>
<td>swapfs</td>
<td>Solaris Swap File System</td>
</tr>
<tr>
<td>tfs</td>
<td>Solaris Translucent File System</td>
</tr>
</tbody>
</table>

Use one of the following backup methods to ensure that these targets are included in a backup:

- In Avamar Administrator, explicitly add these targets in an on-demand backup or dataset by specifying `mntfs,tmpfs,cachefs,fdfs,fifofs,namefs,specfs,swapfs,tfs` in the Force traversal of the specified file system type(s) box in the plug-in options.
- Specify `--forcefs="mntfs,tmpfs,cachefs,fdfs,fifofs,namefs,specfs,swapfs,tfs"` on the `avtar` command line.

Available /var and /opt file systems

The original file system tables must have partitions for /opt and /var. The partitions for /opt and /var are mounted when you boot Solaris in read-only mode.

If the partitions do not mount, then you must create new, temporary file systems for /opt and /var when you install a minimal version of Solaris on the client.

Other file systems

If you are using zfs or any other add-on file system, ensure that these file systems are properly re-created and mounted before beginning system recovery.

Installation of a minimal version of Solaris

Create a file system layout that matches the original system as closely as possible. Ensure that there are separate file systems for /opt and /var.

Performing system recovery of an Oracle Solaris client

Before you begin

Perform the steps in Preparing for Oracle Solaris system recovery on page 137.

Procedure

1. Boot from CDROM by typing `reboot -- cdrom` or by changing the boot order in the BIOS menu, depending on the platform.
2. (Solaris 11 and 10 only) At the boot options menu, select one of the following options:
   - 3. Solaris Interactive Text (Desktop session)
   - 4. Solaris Interactive Text (Console session)
3. Proceed through the prompts, providing the client hostname, IP address, default gateway, and corporate DNS server name when prompted to do so.
4. Exit the system prompt and return to a shell prompt:
On Solaris 8, press ! when you are prompted to install software for Solaris with Solaris Web Start.

On Solaris 10 or 11, press F5 to exit when you are prompted to select an installation type, and then press F2 to confirm the exit.

5. Mount the / partition under /a as the target of the restore by typing the following command:

   ```bash
   mount /dev/dsk/c1t0d0s0 /a
   ```

   Use the correct site-specific disk partition and mount parameters for the root volume.

6. Mount the /opt partition under /opt by typing the following command:

   ```bash
   mount /dev/dsk/c1t0d0s5 /opt
   ```

   Use the correct site-specific disk partition and mount parameters for the /opt volume.

7. Mount the /var partition under /var by typing the following command:

   ```bash
   mount /dev/dsk/c1t0d0s4 /var
   ```

   Use the correct site-specific disk partition and mount parameters for the /var volume.

8. Mount any additional file systems in their respective mountpoints under /a.

   If the mount point does not exist, create it. For example, to mount file system /data01 on c1t0d0s7, type the following command:

   ```bash
   mount /dev/dsk/c1t0d0s7 on /a/data01
   ```

9. Install the proper version of the Avamar Client for Solaris software by using the instructions in the *EMC Avamar Backup Clients User Guide*.

   **NOTICE**

   The installation program displays a warning about root (/) having 0 free bytes, as well as errors related to read-only file systems when trying to create /etc/init.d/avagent and various links in /usr/bin and /etc/rc.d/rcX.d. However, despite these warnings, all the binaries are correctly installed in /opt/AVMRclnt/bin.

10. Restore /etc to /a/etc by typing the following commands:

    ```bash
    cd /a/etc
    /opt/AVMRclnt/bin/avtar -x --server=Avamar_server --id=username --password=password --account=/domain/client --target=../ /etc --labelnumber=n --overwrite=always
    ```

    where:

    - *Avamar_server* is the hostname or IP address of the Avamar server.
    - *username* and *password* are the Avamar login credentials for a user with a role that allows access to the backups for this client.
    - */domain/client* is the Avamar domain and Solaris client to restore.
    - *n* is the label number of the backup to restore. If you do not specify a label number, then the most recent backup is used for the restore.
NOTICE

You cannot restore the root file system directly to /a, because there is currently no way to restrict the restore operation to only the local partition without traversing network mount points. A restore directly to /a might copy files from all partitions, causing /a to fill up before all required files are restored.

11. Inspect /a/etc/vfstab to verify the original mount points for the local file system.

12. In Avamar Administrator, click the Backup & Restore launcher button.

   The Backup, Restore and Manage window appears.

13. Click the Restore tab.

14. In the clients tree, select the original Solaris client.

15. Find and select the backup to use for the restore.

16. Examine the directories and files that originally existed under root (/).

17. For each directory that originally existed under root (/), perform the following steps:

   a. If the directory does not already exist, then manually create an empty directory with the same name under /a.

   b. Change directory to that directory.

   c. From the command line, restore the contents of the directory from the backup.

   For example, consider the following commands to restore /usr:

   ```
   mkdir /a/usr; cd /a/usr
   /opt/AVMRclnt/bin/avtar -x --server=Avamar_server --id=username --password=password --account=/domain/client --labelnumber=n --overwrite=always --target=. /usr
   ```

   If /opt and /var were originally on the root partition, then you can restore to /a/opt and /a/var. If /opt and /var were separate file systems, then restore to new, temporary locations, such as /a/newopt and /a/newvar. After all of the restores complete, you can move the contents of /a/newopt to /opt and /a/newvar to /var.

18. To restore the individual files that originally existed under root, run the restore command with the --norecursion option to restore files without descending into subdirectories:

   ```
   /opt/AVMRclnt/bin/avtar -x --server=Avamar_server --id=username --password=password --account=/domain/client --labelnumber=n --norecursion --overwrite=always --target=. /
   ```

19. Reboot the client normally and confirm correct operation.
CHAPTER 7

Server Administration

This chapter includes the following topics:

- Server shutdown and restart ................................................................. 142
- Suspending and resuming server activities ........................................... 145
- Managing client sessions ..................................................................... 145
- Managing client agents and plug-ins ...................................................... 148
- Backup and maintenance windows ......................................................... 150
- Checkpoints .......................................................................................... 152
- Generating and installing a server license ............................................. 155
- Managing services ................................................................................ 158
- Changing server passwords and OpenSSH keys .................................... 159
- MCS configuration settings .................................................................. 160
- Using network address translation (NAT) .............................................. 164
- Editing network settings for a single-node server ................................. 165
- Adding a custom security notification for web browser logins ............... 165
- Viewing and editing server contact information .................................... 166
Server shutdown and restart

The dpnctl program enables you to gracefully shut down and restart the entire Avamar server or selected subsystems.

Shutting down the server

Before you begin

Ensure that there is a recent and validated checkpoint before you perform a full system shutdown.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.

2. Type `dpnctl stop`.
   
   A confirmation message prompts whether to shut down the local instance of EMS.

3. Type `y` to shut down the local EMS instance, and then press Enter.
   
   The output displays the status of the shutdown process until the shut down is complete.

Restarting the server

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.

2. Type `dpnctl start`.
   
   The output displays a confirmation message.

3. Type `y` to proceed with restarting the server, and then press Enter.
   
   The output displays the status of the restart process until the restart is complete.
Stopping the MCS

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press Enter.
2. Type `dpntcl stop mcs`.

Starting the MCS

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press Enter.
2. Type `dpntcl start mcs`.
3. Resume scheduled operations by typing `dpntcl start sched`.

Getting MCS status

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press Enter.
2. Type `dpntcl status mcs`. 
Stopping the EMS

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Type `dpnctl stop ems`.

Starting the EMS

Before you begin
Ensure that Avamar Enterprise Manager has been properly shut down.

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Type `dpnctl start ems`.

Stopping the Avamar Desktop/Laptop server

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Type `dpnctl stop dtlt`.

Starting the Avamar Desktop/Laptop server

When you restart the Avamar utility node, the Avamar Desktop/Laptop server restarts automatically. If necessary, you can manually start the Avamar Desktop/Laptop server.

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Type `dpnctl start dtlt`.

Getting Avamar Desktop/Laptop server status

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Type `dpnctl status dtlt`.
Suspending and resuming server activities

You can suspend and resume backups and restores, scheduled operations, and maintenance activities.

Suspending and resuming backups and restores

Procedure
1. In Avamar Administrator, click the Server launcher button. The Server window appears.
2. Click the Server Management tab.
3. In the left pane, select the Avamar server node.
4. Open the Actions menu and select Suspend Backups/Restores or Resume Backups/Restores.
   - A confirmation message appears.
5. Click Yes.

Suspending and resuming scheduled operations

Procedure
1. In Avamar Administrator, select Tools > Manage Schedules. The Manage All Schedules window appears.
2. Click Suspend All or Resume All.

Suspending and resuming maintenance activities

Procedure
1. In Avamar Administrator, click the Server launcher button. The Server window appears.
2. Open the Actions menu and select Suspend Maintenance Activities or Resume Maintenance Activities.
   - A confirmation message appears.
3. Click OK.

Managing client sessions

You can view a detailed log of a client session to perform troubleshooting or analysis of a backup or restore. If necessary, you can cancel a client session or reset a client when unexpected system behavior occurs.

Monitoring client sessions

The Session Monitor displays a list of active client backup and restore sessions.

Procedure
1. In Avamar Administrator, click the Server launcher button. The Server window appears.
2. Click the **Session Monitor** tab.

The information in the following table appears for each session in the Session Monitor.

**Table 30** Session Monitor tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>Avamar user ID (account name).</td>
</tr>
<tr>
<td>User</td>
<td>Specifies a hierarchical location in the Avamar server. This option is relative to the user's home location unless slash (/) is prefixed to the path designation, in which case an absolute path is assumed.</td>
</tr>
<tr>
<td>Path</td>
<td>Avamar domain where this user resides.</td>
</tr>
<tr>
<td>Domain</td>
<td>Unique identifier for this client session.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Unique identifier for this activity.</td>
</tr>
<tr>
<td><strong>Session</strong></td>
<td>This activity is either avtarbackup or avtarrestore.</td>
</tr>
<tr>
<td>Type</td>
<td>Top level of the file system being backed up, restored, or validated.</td>
</tr>
<tr>
<td>Root</td>
<td>Date and time that this client session started.</td>
</tr>
<tr>
<td>Start time</td>
<td>Plug-in used for this activity.</td>
</tr>
<tr>
<td>Plug-in</td>
<td>Unique identifier for this client session.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Unique identifier for this activity.</td>
</tr>
<tr>
<td>Work order ID</td>
<td>Length of time that this client session has been running.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>Total number of bytes examined during this activity.</td>
</tr>
<tr>
<td>Progress bytes</td>
<td>Percentage of new bytes backed up to either the Avamar server or a Data Domain system. Low numbers indicate high levels of data deduplication.</td>
</tr>
<tr>
<td>New bytes</td>
<td>Client hostname.</td>
</tr>
<tr>
<td>Name</td>
<td>Operating system used by this client.</td>
</tr>
<tr>
<td>OS name</td>
<td>Avamar client software version.</td>
</tr>
</tbody>
</table>

**Viewing a detailed client session log**

You can view a detailed log of a client session to perform troubleshooting or analysis.

**Procedure**

1. In Avamar Administrator, click the **Activity** launcher button.

   The **Activity** window appears.

2. Click the **Activity Monitor** tab.

   By default, the Activity Monitor shows a detailed log of all client backup activity for the past 72 hours.

3. Specify the session log options:
a. Select Action > Session Log Options.
   The Session Log Options dialog box appears.

b. Select Show HTML logs to view the session log summary in HTML format, or Show raw logs to view the session log summary as unformatted text.

c. (Optional) If you select the HTML log format, select the Show debug information checkbox to include debug information in the session log summary.

d. Click OK.

4. Select an activity in the list.

5. Select Actions > View Session Log.
   The Activity Session Drill-down dialog box appears.

6. Perform any of the following tasks in the session log summary:
   • (HTML format only) In the Log Files section, click a hyperlink to go to the log file.
   • Search for a specific text string in the session log summary by typing a text string in the Find field and then clicking Next or Previous.
   • Return to the top of the session log summary by clicking Back to Top.
   • Export the session log summary to a file by clicking Export, specifying a location for the file, and clicking Save.
   • Update the contents in the session log summary by clicking Refresh.

7. Click Close.

Creating a Zip file for EMC Customer Support

The Activity window enables you to create a Zip file of session log information for EMC Customer Support and upload the Zip file to the Avamar server.

Procedure

1. In Avamar Administrator, click the Activity launcher button.
   The Activity window appears.
2. Select an activity in the list.
3. Select Actions > Download Support Bundle.
   The Download Support Bundle dialog box appears.
4. Navigate to a directory for the zip file.
5. Click Save.
   A progress dialog box displays the status of the operation.
6. When the operation completes, click Close on the progress dialog box.
7. To create a Zip file and copy it to the Avamar server, select Actions > Upload Support Bundle to Server.
   The upload process creates a Zip file for session log summary information and copies the Zip file to the /tmp folder on the Avamar server. A progress dialog box displays the status of the operation.
Canceling a client session

 Occasionally, a client might experience unexpected system behavior while it is performing a backup or restore. In these cases, it might be necessary to force an end to these client sessions from Avamar Administrator.

**Procedure**

1. In Avamar Administrator, click the Server launcher button.
   
   The Server window appears.
2. Click the Session Monitor tab.
   
   A list of active client sessions appears.
3. Select the client session to cancel.
4. Select Actions > Cancel Session.
   
   A dialog box shows the progress of the cancellation.
5. When the cancellation is complete, click Close.

**After you finish**

If you cannot cancel the client session, reset the client. This immediately and forcibly terminates active avtar sessions on the client.

Resetting a client

Resetting a client immediately and forcibly terminates active client avtar sessions on that client. In most cases, you should try to cancel the client session before resetting it.

**Procedure**

1. In Avamar Administrator, click the Policy launcher button.
   
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Clients tab.
4. Select the client to reset.
5. From the Actions menu, select Client > Reset Client.

Managing client agents and plug-ins

Each time a client communicates with an Avamar server, it identifies itself by sending the client ID, the specific agent version and build running on that client, and a list of plug-ins (version and build) currently installed on that client. Occasionally, because of known incompatibilities, you may want to deny Avamar server access to all clients running a specific version (all builds) or a specific build of a client agent or plug-in.

You can also selectively allow or disallow the following plug-in operations for all clients running a specific plug-in version (all builds) or build:

- Client activations initiated from the client
- On-demand backups initiated from the client
- Scheduled backups
- Restores
Backup validation

Ability to browse stored backups on the server

Any specific version (all builds) or build that is designated as obsolete is denied access to the Avamar server. A build is designated as obsolete only in cases of known incompatibility between the client agent or plug-in and the specific version of server software that was installed. Therefore, to prevent potential problems, this obsolete designation cannot be overridden using the feature to edit properties for that version or build.

Adding a build record

You can add an MCS database record for a specific client agent or plug-in build. You can only add records at the build level. New version records are automatically added after Avamar server software upgrades.

Procedure

1. In Avamar Administrator, select Tools > Manage Agents & Plug-ins.
   The Manage All Agents & Plug-ins window appears.
2. In the left pane, select the agent or plug-in version for the build.
3. Click New.
   The New Build dialog box appears.
4. In the Build box, type a valid agent or plug-in build number.
5. To deny Avamar server access to clients with this agent or plug-in build, select the Disable checkbox.
6. (Optional) Type a descriptive comment in the Comment box.
7. Click OK.

Editing version or build records

Procedure

1. In Avamar Administrator, select Tools > Manage Agents & Plug-ins.
   The Manage All Agents & Plug-ins window appears.
2. In the left pane, select the agent or plug-in.
3. In the right pane, select the version or build to edit.
4. Click Edit.
   The Edit Build dialog box appears.
5. To deny Avamar server access to clients with this agent or plug-in build, select the Disable checkbox.
6. (Optional) Type a descriptive comment in the Comment box.
7. Click OK.
Deleting a build record

You can delete an MCS database record for a specific client agent or plug-in build. You cannot delete a record for an entire version.

Procedure
1. In Avamar Administrator, select Tools > Manage Agents & Plug-ins.
   The Manage All Agents & Plug-ins window appears.
2. In the left pane, select the agent or plug-in.
3. In the right pane, select the build to delete.
   Click Delete.

Disabling all client initiated activations

You may want to temporarily prevent clients from activating with the Avamar server to place the system in a state that supports maintenance activities.

Procedure
1. In Avamar Administrator, select Tools > Manage Agents & Plug-ins.
   The Manage All Agents & Plug-ins window appears.
2. Click Disable All Client Initiated Activations.
3. To re-enable client initiated activations, click Enable All Client Initiated Activations.

Disabling all client initiated backups

You can temporarily prevent Avamar clients from initiating on-demand backups to place the system in a state that supports various maintenance activities.

Procedure
1. In Avamar Administrator, select Tools > Manage Agents & Plug-ins.
   The Manage All Agents & Plug-ins window appears.
2. Click Disable All Client Initiated Backups.
3. To re-enable client initiated on-demand backups, click Enable All Client Initiated Backups.

Backup and maintenance windows

Each 24-hour day is divided into two operational windows, the backup window and the maintenance window.

The following figure shows the default backup and maintenance windows.
Backup window
The backup window is that portion of each day reserved to perform normal scheduled backups. No maintenance activities are performed during the backup window.

The default backup window begins at 8 p.m. local server time and continues uninterrupted for 12 hours until 8 a.m. the following morning. You can customize the backup window start time and duration.

Maintenance window
The maintenance window is that portion of each day reserved to perform the routine server maintenance activities in the following table.

Table 31 Avamar server maintenance activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkpoint</td>
<td>A snapshot of the Avamar server taken for the express purpose of facilitating server rollbacks.</td>
</tr>
<tr>
<td>Checkpoint validation</td>
<td>An internal operation that validates the integrity of a specific checkpoint. Checkpoint validation is also known as a Hash File System (HFS) check. After a checkpoint passes an HFS check, it can be considered reliable enough to be used for a server rollback.</td>
</tr>
<tr>
<td>Garbage collection</td>
<td>An internal operation that recovers storage space from deleted or expired backups.</td>
</tr>
</tbody>
</table>

Although you can perform backups and restores during the maintenance window, doing so impacts the backup, restore, and maintenance activities. For this reason, minimize
any backup, restore, or administrative activities during the maintenance window. There
might be brief periods of time when backup or administrative activities are not allowed.
The default maintenance window begins at 8 a.m. local server time and continues
uninterrupted for 12 hours until 8 p.m. Although you cannot directly customize the
maintenance window, its start time and duration are derived from backup window
settings.

**Editing the backup and maintenance windows**

You can edit the backup and maintenance windows by setting the backup window start
time and duration, as well as the time zone for the backup and maintenance windows.
Any changes to the backup window duration also affect the maintenance window
duration. For example, changing the backup window duration from 12 hours to 14 hours
reduces the maintenance window duration by 2 hours.
The following best practices apply when you schedule system activities:

- **Limit on-demand backups during the maintenance window**
  You might want to advise users to avoid initiating any on-demand backups from their
  client computers during the first hour and thirty minutes of the maintenance window
  (8 a.m. to 8 p.m. local time for most systems).

- **Avoid initiating on-demand maintenance activities**
  Manually initiating maintenance activities such as checkpoints, checkpoint
  validation, or garbage collection temporarily disables all scheduled maintenance
  activities until the manually initiated operation completes. Unless there is a pressing
  need to initiate an on-demand maintenance activity, it is best to rely on scheduled
  maintenance activities to ensure that sufficient time is allocated for each activity
daily.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Schedules**.
   The **Manage All Schedules** window appears.
2. Click the **Maintenance Window** tab.
3. Change the backup window start time, duration, or time zone by selecting a new value
   from the corresponding list.
4. Click **OK**.

**Checkpoints**

Checkpoints are system-wide backups taken for the express purpose of assisting with
disaster recovery.

A checkpoint occurs automatically during the maintenance window. You can also
manually initiate checkpoints at any time.

You can delete checkpoints to reclaim server storage capacity.

The **Checkpoint Management** tab on the **Server** window in Avamar Administrator displays
the status of individual checkpoints. The following table provides the possible states for
a checkpoint.
Creating a checkpoint

A checkpoint occurs automatically during the maintenance window. You can also manually initiate checkpoints at any time.

Procedure

1. In Avamar Administrator, click the **Server** launcher button. The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select **Actions > Create Checkpoint**. A progress dialog box displays the status of the operation.
4. When the checkpoint completes, click **Close**.

Deleting a checkpoint

You can delete checkpoints to reclaim additional server storage capacity. Generally, it is best to delete unvalidated checkpoints before you delete validated checkpoints.

Procedure

1. In Avamar Administrator, click the **Server** launcher button. The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select the checkpoint and select **Actions > Delete Checkpoint**. A confirmation message appears.
4. Click **OK**.

Rolling back to a checkpoint

Rollback is the process of restoring the Avamar server to a known good state using data stored in a validated checkpoint. You cannot roll back an Avamar 7.1 server to a version 4.x or earlier checkpoint.

Before you begin

If you added nodes to the Avamar server after the checkpoint occurred, remove the entries for the nodes from the **probe.out** file.

You can use only a validated checkpoint for rollback. Checkpoint validation occurs during each maintenance window.

---

**Table 32 Checkpoint states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>The checkpoint failed validation or was canceled before it could complete.</td>
</tr>
<tr>
<td>🔄</td>
<td>The checkpoint has not yet been validated.</td>
</tr>
<tr>
<td>🔄</td>
<td>Validation is currently being performed on this checkpoint.</td>
</tr>
<tr>
<td>✔️</td>
<td>The checkpoint passed validation.</td>
</tr>
</tbody>
</table>

---

Creating a checkpoint

A checkpoint occurs automatically during the maintenance window. You can also manually initiate checkpoints at any time.

Procedure

1. In Avamar Administrator, click the **Server** launcher button.
   
   The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select **Actions > Create Checkpoint**.
   
   A progress dialog box displays the status of the operation.
4. When the checkpoint completes, click **Close**.

Deleting a checkpoint

You can delete checkpoints to reclaim additional server storage capacity. Generally, it is best to delete unvalidated checkpoints before you delete validated checkpoints.

Procedure

1. In Avamar Administrator, click the **Server** launcher button.
   
   The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select the checkpoint and select **Actions > Delete Checkpoint**.
   
   A confirmation message appears.
4. Click **OK**.

Rolling back to a checkpoint

Rollback is the process of restoring the Avamar server to a known good state using data stored in a validated checkpoint. You cannot roll back an Avamar 7.1 server to a version 4.x or earlier checkpoint.

Before you begin

If you added nodes to the Avamar server after the checkpoint occurred, remove the entries for the nodes from the **probe.out** file.

You can use only a validated checkpoint for rollback. Checkpoint validation occurs during each maintenance window.

---

Creating a checkpoint

A checkpoint occurs automatically during the maintenance window. You can also manually initiate checkpoints at any time.

Procedure

1. In Avamar Administrator, click the **Server** launcher button.
   
   The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select **Actions > Create Checkpoint**.
   
   A progress dialog box displays the status of the operation.
4. When the checkpoint completes, click **Close**.

Deleting a checkpoint

You can delete checkpoints to reclaim additional server storage capacity. Generally, it is best to delete unvalidated checkpoints before you delete validated checkpoints.

Procedure

1. In Avamar Administrator, click the **Server** launcher button.
   
   The **Server** window appears.
2. Click the **Checkpoint Management** tab.
3. Select the checkpoint and select **Actions > Delete Checkpoint**.
   
   A confirmation message appears.
4. Click **OK**.

Rolling back to a checkpoint

Rollback is the process of restoring the Avamar server to a known good state using data stored in a validated checkpoint. You cannot roll back an Avamar 7.1 server to a version 4.x or earlier checkpoint.

Before you begin

If you added nodes to the Avamar server after the checkpoint occurred, remove the entries for the nodes from the **probe.out** file.

You can use only a validated checkpoint for rollback. Checkpoint validation occurs during each maintenance window.
**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the `admin_key` passphrase and press `Enter`.

2. Shut down the server by typing `dpnctl stop`.

3. Display a list of checkpoints by typing `cplist`.
   
   The checkpoint list appears similar to the following example:
   ```
   cp.20140106170113 Fri Jan 6 17:01:13 2014 valid hfs del
   nodes 4 stripes 396
   cp.20140107170042 Sat Jan 7 17:00:42 2014 valid hfs del
   nodes 4 stripes 396
   cp.20140108170040 Sun Jan 8 17:00:40 2014 valid hfs ...
   nodes 4 stripes 396
   cp.20140109170043 Mon Jan 9 17:00:43 2014 valid hfs ...
   nodes 4 stripes 396
   ```
   
   where:
   - `cp.yyyymmddhhmmss` is the checkpoint ID.
   - `valid hfs` indicates a validated checkpoint.
   - `valid par` indicates a partially validated checkpoint.

4. Note the checkpoint ID of the checkpoint that you plan to use for the checkpoint.
   Generally, you should roll the system back to the most recent fully validated checkpoint unless you have a good reason to roll back to an earlier checkpoint.

5. Initiate the rollback by typing the following command:
   ```
   rollback.dpn --cpty=checkpoint_id >& file
   ```
   where `checkpoint_id` is the checkpoint ID and `file` is a temporary file.

6. Wait for the rollback to complete. The rollback might take as long as one hour, depending on the amount of data present in the Avamar server.
   When the rollback is complete, the command prompt returns.

7. Open the user-defined temporary file that was created during the rollback, and verify that the rollback successfully completed without errors.
   The server automatically restarts after a successful rollback.
Clearing a data integrity alert

To ensure data integrity, the Avamar server issues an alert any time a checkpoint validation fails. The only way to clear this alert is to contact EMC Customer Support to obtain a reset code, and then input that code in the Clear Data Integrity Alert dialog box.

**Before you begin**

Obtain a reset code from EMC Customer Support.

**Procedure**

1. In Avamar Administrator, click the Administration launcher button.
   
   The Administration window appears.

2. Click the Event Management tab.

3. Click the Unacknowledged Events tab near the bottom of the window.

4. Select Actions › Event Management › Clear Data Integrity Alert.
   
   The Clear Data Integrity Alert dialog box appears.

5. Enter reset code in the Enter reset code field and click OK.

Generating and installing a server license

The Avamar server requires a license key for permanent operation. Otherwise, the Avamar server stops performing several functions after a 30-day grace period. To avoid interruptions to the Avamar server functioning, generate and install a permanent license.

**Procedure**

1. Obtain the assigned license key for the Avamar server software.

2. Use the gathergsankeydata utility to generate a gsankeydata.xml license key information file.
   
   If you already generated the gsankeydata.xml file during the Avamar server software installation and configuration, then skip this step.

3. Generate a permanent license key file.

4. Install and activate the license on the Avamar server.

Obtaining assigned license keys

The assigned license key for the Avamar server software includes the customer account identification number and the Avamar system asset identification number. These values are required to generate a permanent license.

The following example is an assigned license key:

EMC Avamar Software License Key Information
Avamar System Customer Account ID: CN-10062734404
Avamar System Asset ID: A-2010014578

**Procedure**

- Find the assigned license keys on EMC Online Support on the license management page.

  To access EMC Online Support, type the login credentials provided in the EMC License Authorization (LAC) email sent to you from licensingnorthamerica@emc.com,
licensingemea@emc.com, or licensingapj@emc.com. If you cannot find the email, send an email to licensing@emc.com to request that the EMC License Authorization email be resent. Include the EMC product SO number in the email. The EMC product SO number is required.

To access the license management page on EMC Online Support, click the Get and Manage Licenses link below the Service Center section of the home page.

### Generating a license key information file

**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
       ```
       ssh-agent bash
       ssh-add ~admin/.ssh/admin_key
       ```
     c. When prompted, type the admin_key passphrase and press Enter.
2. Type `gathergsankeydata`.
   The output prompts you to specify the customer account number.
3. Type the Avamar system customer account number and press Enter.
   A valid Avamar system customer account number (account ID) conforms to the format CN-yymmddnnnnn, where yymmdd is a year, month, and day, and nnnnn is a five-digit numerical sequence.
   The output prompts you to specify the Avamar system asset ID number.
4. Type the Avamar system asset ID number and press Enter.
   A valid Avamar system asset ID number (asset reference ID) conforms to the format A-yyyyynnnnnn, where yyyy is a year and nnnnnn is a six-digit numerical sequence.
   The output prompts you to specify the Internet domain for the account.
5. Type the Internet domain and press Enter.
   The output prompts you to confirm the data that you specified.
6. Type y and press Enter.
   The local directory contains the gsankeydata.xml license key information file. This file is used to generate the permanent license key.

### Generating a permanent license key file

**Procedure**

1. Access EMC Online Support (https://support.EMC.com) and type the login credentials from the EMC License Authorization (LAC) email that licensingnorthamerica@emc.com, licensingemea@emc.com, or licensingapj@emc.com sent to you.
   The Welcome to the EMC Online Support Site page appears.
Note

If you cannot find the email from LAC, send an email to licensing@emc.com to request that the LAC email be resent. Include the EMC product SO number in the email. The EMC product SO number is required.

2. To access the license management page on EMC Online Support, click **Get Manage License**, below the **Service Center** section.

   The **Manage Licenses** page appears.

3. Click **Avamar** from the list of products.

4. Click **Activate Licenses** and upload the gsankeydata.xml file.

5. In the **Qty** box, type the authorized quantity of terabyte licenses to allocate to the system.

6. Click **Next**.

   This process creates the XML file that contains an activated license key.

7. Save the XML file to a local drive.

   You can also email the XML to one or more email addresses.

**Installing and activating a license**

After you receive the license key file from EMC Licensing, install and activate the license on the Avamar server.

**Procedure**

1. Log in to the email account to which the license key file was sent.

2. Open the email message from info@Avamar.com with a subject line of **EMC Avamar Key Information**.

   The email message contains the license key file as an attached XML file named asset_Key.xml, where **asset** is the DNS name of the Avamar server.

3. Save the attachment to a temporary directory.

4. Use WinSCP or an equivalent program to copy the asset_Key.xml file to the /tmp directory on a single-node server or to the /tmp directory on the utility node in a multi-node server.

5. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

        `ssh-agent bash
        ssh-add ~admin/.ssh/admin_key`

     c. When prompted, type the **admin_key** passphrase and press Enter.

6. Ensure that the Avamar server subsystem (also known as GSAN) is running by typing `dpnctl status gsan`.

   If GSAN is running, the output displays a status of **ready**.

7. Change file permissions on the asset_Key.xml file and activate the license.
Server status | Commands to change file permissions on the license key file
--- | ---
Running | chmod 644 /tmp/asset_key.xml
avmaint license /tmp/asset_key.xml --avamaronly
where asset_key.xml is the license key file.
Not running | cd /usr/local/avamar/etc
mv license.xml license.xml.old
cp /tmp/asset_key.xml license.xml
chmod 644 license.xml
where asset_key.xml is the license key file.

8. If the Avamar server is not running, start it by typing `dpncctl start`.

9. After the Avamar server restarts, verify that the server license is correctly installed by typing the following command:

```
avmaint license --avamaronly
```
License information appears in the command shell.

Managing services

The Services Administration tab on the Administration window in Avamar Administrator enables you to start, stop, suspend, or resume individual services on the Avamar server.

**Procedure**

1. In Avamar Administrator, click the Administration launcher button.

   The Administration window appears.

2. Click the Services Administration tab.

   The following information appears on the Services Administration tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>DNS name of the Avamar server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the Avamar server.</td>
</tr>
<tr>
<td>Load Average</td>
<td>Average number of CPU threads over the past minute.</td>
</tr>
<tr>
<td>Last Administrator Datastore Flush</td>
<td>Date and time of the last MCS flush.</td>
</tr>
<tr>
<td>PostgreSQL database</td>
<td>Status of the MCS database.</td>
</tr>
<tr>
<td>Web Services</td>
<td>Status of MCS web services.</td>
</tr>
<tr>
<td>Web Restore Disk Space Available</td>
<td>Number of hard drive bytes that MCS web services can use to create the restore ZIP file.</td>
</tr>
<tr>
<td>Login Manager</td>
<td>Status of the Avamar Login Manager service.</td>
</tr>
<tr>
<td>snmp sub-agent</td>
<td>Status of the Avamar SNMP sub-agent service.</td>
</tr>
<tr>
<td>ConnectEMC</td>
<td>Status of the ConnectEMC service.</td>
</tr>
</tbody>
</table>
### Changing server passwords and OpenSSH keys

The `change-passwords` utility enables you to change operating user account and Avamar server user account passwords, as well as create new OpenSSH keys.

The `change-passwords` utility guides you through the following operations:

- Changing operating system login passwords for the admin, dpn, and root accounts
- Creating new admin and dpnid OpenSSH keys
- Changing internal Avamar server passwords for the root and MCUUser accounts

**Procedure**

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as dpn.
   - To log in to a multi-node server, log in to the utility node as dpn.
   Start the utility by typing `change-passwords`.
   On a multi-node server, the output prompts you to specify whether to change passwords on all nodes or selected nodes.
2. Type `y` to change passwords on all nodes or `n` to change passwords on selected nodes, and then press Enter.
   The output prompts you to indicate whether you plan to specify SSH private keys that are authorized for root operations.
3. Type `n` and press Enter.
   The output prompts you to specify whether to change admin, dpn, or root operating system user account passwords.
4. Type `y` to change the passwords or `n` to skip the process of changing the passwords, and then press Enter.
5. If you typed `y` in the previous step, then follow the system prompts to change the passwords for one or more of the admin, dpn, or root operating system user accounts. The output prompts you to specify whether to change SSH keys.

6. Type `y` to change or create new admin or dpnid OpenSSH keys, or type `n` if you do not want to change or create the keys, and then press Enter.

7. If you typed `y` in the previous step, then follow the system prompts to change or create the keys. The output prompts you to specify whether to change Avamar server passwords.

8. Type `y` to change the MCUser or internal root Avamar server user account passwords, or type `n` if you do not want to change the passwords, and then press Enter.

9. If you typed `y` in the previous step, then follow the system prompts to change the passwords.

   **NOTICE**
   
   You must specify the current root password for the Avamar server to change the password.

   The output prompts you to specify whether to change the viewuser password.

10. Type `y` to change the viewuser password, or `n` if you do not want to change the password, and then press Enter.

   **NOTICE**
   
   You must specify the current viewuser password to change the password.

11. If you typed `y` in the previous step, then follow the system prompts to change the viewuser password. The output prompts you to specify whether to accept the changes made to passwords or OpenSSH keys during this utility session.

12. Type `y` to accept the changes or type `n` to exit this utility session without making the changes, and then press Enter.

   The output provides the status of the operation.

13. When the operation completes, resume scheduled operations:
   
   a. In Avamar Administrator, select **Tools > Manage Schedules**.
   
   b. Click **Resume All** on the **Manage All Schedules** window.

---

**MCS configuration settings**

Avamar Administrator consists of both client and server software applications. You can independently configure each application by editing either the server or client preferences file.

Changes to the server preferences file, `mcserver.xml`, affect all Avamar Administrator sessions. Changes to a client preferences file, `mcclient.xml`, only affect Avamar Administrator sessions on that client. Both files conform to the `preferences.dtd` XML Document Type Description (DTD) referenced by the JSDK 1.4 API.

**Default and live copies**

Two copies of each of these files are present on the system:
• An initial default copy is used to initialize each application after installation.
• A live copy contains the current settings used by the application.

The default copies are located in the /lib directory for each application. The live copies are located in a “live file” directory. The following table lists the default live file directory for each application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Default live file directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>/usr/local/avamar/var/mc/server_data/prefs</td>
</tr>
<tr>
<td>Client</td>
<td>install_directory/var/mc/gui_data/prefs, where install_directory is typically C:\Program Files\avs\administrator on Microsoft Windows computers and /usr/local/avamar on Linux computers.</td>
</tr>
</tbody>
</table>

Initialization behavior
When either the server or client application is initialized, the respective default preferences file in the /lib directory is loaded into memory and replicated to the live file directory.

Note
Reinitializing a running MCS is highly destructive. It completely overwrites any custom preference settings stored in the live file and reverts the system configuration back to default settings. If this occurs, you must recover custom preference settings from a previous flush (backup) if they are overwritten.

Upgrade behavior
During server upgrades, any mcserver.xml entry that is marked with the merge="delete" attribute in the new default mcserver.xml file is not merged into the new live copy. These entries are obsolete. They are retained in the default mcserver.xml file so that the MCS knows to delete the preferences on an upgraded customer system.

You can manually add a merge="keep" attribute to any entry in the live /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml file. Settings with merge="keep" attributes are retained in the new live copy after the upgrade.

Backing up MCS data
To protect itself from hardware failures, the MCS automatically backs up or flushes its persistent data to the Avamar server hourly and as part of system checkpoints. Flushes are done by way of an avtar client session. You can also force an on-demand flush.

The flush process generates the timestamp files in the following table.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flush.timestamp</td>
<td>Before every flush, flush.timestamp is created in the server_data directory. This file includes the time and date of the flush. On a server rollback, this file is restored and can be used to verify that the rollback was successful to the selected time and date. The contents of</td>
</tr>
</tbody>
</table>
Table 34 MCS backup timestamp files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flush.timestamp</td>
<td>are also accessible by using of the mcserver.sh --status command.</td>
</tr>
<tr>
<td>init.timestamp</td>
<td>During system initialization, the init.timestamp file is created or overwritten in the server_data directory. This file includes the time and date of the system initialization and can be used to verify that initialization was successful on the selected time and date.</td>
</tr>
</tbody>
</table>

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:
        ```bash
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.

2. Type the following command to initiate an on-demand MCS flush:
   ```bash
   mcserver.sh --flush
   ```

Restoring MCS data

Before you begin

If you are planning to restore MCS data to a specific backup instead of the most recent backup, then find the label number for the backup either by browsing for the backup in Avamar Administrator or by using the avtar command:

- In Avamar Administrator, open the Backup, Restore and Manage window, and browse for backups in the /MC_BACKUPS account.
- Type the following command on a single command line:
  ```bash
  avtar --backups --id=root --ap=password --path=/MC_BACKUPS --hfsaddr=Avamar_server --count=n
  ```
  where `password` is the Avamar root user account password (not the operating system root password), `Avamar_server` is the IP address or DNS name of the Avamar server, and `n` is the number of backups to list. A total number of 26 MCS flushes typically occurs each day for an Avamar server — one per hour and one each during the morning and evening system checkpoints. Therefore, to list all MCS backups for a specific past number of days, specify `--count=n` in increments of 26.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
a. Log in to the utility node as admin.
b. Load the admin OpenSSH key by typing:

   ssh-agent bash
   ssh-add ~admin/.ssh/admin_key
c. When prompted, type the admin_key passphrase and press Enter.

2. Stop the MCS by typing `dpnctl stop mcs`.

3. Restore the MCS by typing one of the following commands:
   * To restore to the most recent backup, type `mcserver.sh --restore`.
   * To restore to a specific backup, type `mcserver.sh --restore --labelnum=n`, where n is the label number of the backup.

4. Open `/usr/local/avamar/var/mc/server_log/restore.log` to verify the success of the restore.

5. Start the MCS and the scheduler by typing:

   `dpnctl start mcs`
   `dpnctl start sched`

Reverting to the default MCS configuration settings

Procedure

1. Open a command shell and log in by using one of the following methods:
   * For a single-node server, log in to the server as admin.
   * For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key

     c. When prompted, type the admin_key passphrase and press Enter.

2. Stop the MCS by typing `dpnctl stop mcs`.

3. Change the working directory by typing the following command:

   `cd /usr/local/avamar/var/mc/server_data/prefs`

4. Rename `mcserver.xml` to `old.mcserver.xml` by typing the following command:

   `mv mcserver.xml old.mcserver.xml`

5. Copy the default server preferences file to the current directory by typing the following command on a single command line:

   `cp /usr/local/avamar/lib/mcserver.xml /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`

6. Start the MCS and the scheduler by typing:

   `dpnctl start mcs`
   `dpnctl start sched`
Using network address translation (NAT)

Avamar clients can access Avamar storage nodes by using a set of addresses that undergo NAT.

To make NAT information known to the Avamar server, the `probe.xml` file must contain `nat-address` elements for storage nodes. After a client makes initial contact with the utility node on the Avamar server, the Avamar server provides a set of routable addresses for the storage nodes to each client. In the absence of a `nat-address` element, a client uses a pre-configured "real" (untranslated) network interface address.

The following figure illustrates an example of a 1x4 multi-node server configuration in which Avamar uses NAT.

**Figure 12** Multi-node server configuration with NAT

The following instructions assume that each Avamar node has a unique address (from the Avamar client perspective), and that you configure a router on the network to apply transparent one-to-one network address translation. You can also use these instructions to enable NAT for use in a single-node server configuration.

**Procedure**

1. Use either the `dpnnetutil` or `nodedb` program to add NAT addresses to `probe.xml`.

<table>
<thead>
<tr>
<th>Command name</th>
<th>Example command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dpnnetutil</code></td>
<td><code>su - root</code></td>
</tr>
<tr>
<td></td>
<td><code>dpnnetutil</code></td>
</tr>
<tr>
<td></td>
<td>Respond to the interactive prompts displayed by <code>dpnnetutil</code>.</td>
</tr>
<tr>
<td><code>nodedb</code></td>
<td><code>nodedb update if --addr=10.6.250.87 --new-nat=192.168.6.4=192.168.6.5</code></td>
</tr>
</tbody>
</table>

2. If the Avamar storage subsystem is currently stopped, restart it by typing `dpnctl start gsan`.

3. If the Avamar storage subsystem is currently running, reread the `probe.xml` file by typing the following command:

   `avmaint networkconfig /usr/local/avamar/var/probe.xml --avamaronly`
4. Register clients by using the `avregister` (UNIX) or `avregister.bat` (Windows) command, or by using Avamar Administrator.

To determine whether NAT is in use, the client and Avamar server must have a network connection. The following table provides solutions for common NAT connection and configuration problems.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Avamar server terminates with a FATAL ERROR message.</td>
<td>Ensure that the <code>probe.xml</code> file:</td>
</tr>
<tr>
<td></td>
<td>• Exists in the <code>/usr/local/avamar/var/</code> directory.</td>
</tr>
<tr>
<td></td>
<td>• Is a valid XML file and adheres to the node resource database format.</td>
</tr>
<tr>
<td></td>
<td>• Lists NAT IP addresses correctly.</td>
</tr>
<tr>
<td></td>
<td>Use the <code>nodedb print --say</code> command to view the contents of <code>probe.xml</code>. The <code>--say</code> option displays the path and name of the current node resource database.</td>
</tr>
<tr>
<td>The server/client connection fails.</td>
<td>Use network diagnostic tools such as <code>ping</code>, <code>traceroute</code>, <code>tracert</code>, or <code>iperf</code> to verify network connectivity.</td>
</tr>
</tbody>
</table>

**Editing network settings for a single-node server**

The *Changing the Name and IP Addressing of Avamar Systems Technical Note*, which is available on EMC Online Support at [https://support.EMC.com](https://support.EMC.com), provides instructions on how to edit the network settings for a single-node server.

**Adding a custom security notification for web browser logins**

You can include a custom security notification on the login page of Avamar Enterprise Manager and Avamar Web Restore. This notification typically explains that only authorized users are permitted access. It can also list the penalties for unauthorized access.

**Procedure**

1. In a text editor, create a file with one of the following file names:

<table>
<thead>
<tr>
<th>Component</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Enterprise Manager</td>
<td><code>disclaimer_EM.txt</code></td>
</tr>
<tr>
<td>Avamar Web Restore</td>
<td><code>disclaimer_Web_Restore.txt</code></td>
</tr>
</tbody>
</table>

2. Add the notification content to the file.

   You can use some basic HTML tags and CSS inline styles in the notification content.

3. Copy the file to the following location on the utility node of a multi-node server or on a single-node server:

   `/usr/local/avamar/var/em/server_data/`
Viewing and editing server contact information

The Avamar server sends contact information for the Avamar server to EMC with every event it reports, including capacity reports that help prevent the system from exceeding critical thresholds. Keep this information current.

A server rollback applies the contact information that existed at the time of the checkpoint. When the rollback completes, you can view or edit the contact information to ensure that the information is current.

Procedure

1. In Avamar Administrator, select Help > View/Edit Contact Information.

The View/Edit Contact Information dialog box appears. The fields in the following table are read-only on the dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC site ID</td>
<td>Unique customer site identifier, specified during initial server installation. This field is read-only.</td>
</tr>
<tr>
<td>System ID</td>
<td>Unique Avamar server identifier, created during initial server installation. This field is read-only.</td>
</tr>
<tr>
<td>AVE</td>
<td>Yes (Y) if this server is an Avamar Virtual Edition (AVE) server; no (N) otherwise. This field is read-only.</td>
</tr>
</tbody>
</table>

2. Edit the contact information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Domain S/N</td>
<td>Serial number of any Data Domain systems that have been added to this server; not applicable (N/A) otherwise.</td>
</tr>
<tr>
<td>Server location</td>
<td>Physical location of the Avamar server at the customer site.</td>
</tr>
<tr>
<td>Company Information</td>
<td>Name and address of the company that owns this Avamar server.</td>
</tr>
<tr>
<td>Contact Information</td>
<td>Name, telephone number, and email address of the primary contact for this Avamar server.</td>
</tr>
</tbody>
</table>

3. Click OK.
CHAPTER 8

Server Monitoring

This chapter includes the following topics:

- Recommended daily server monitoring
- Monitoring activities
- Monitoring server status and statistics
- Event monitoring
- Server monitoring with syslog
- Server monitoring with SNMP
- Viewing Avamar server log files
- Audit logging
- Automatic notifications to EMC Customer Support
- Verifying system integrity
Recommended daily server monitoring

To ensure that the Avamar server is working properly, EMC recommends that you perform the system monitoring tasks listed in the following table on a daily basis.

Table 35 System monitoring tools and tasks

<table>
<thead>
<tr>
<th>Monitoring tool</th>
<th>Monitoring task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Monitor</td>
<td>Investigate any abnormal client activity, such as backups that complete with exceptions.</td>
</tr>
<tr>
<td>Server Monitor</td>
<td>Confirm that the last checkpoint and validated checkpoint are recent. Ideally, they should have occurred within the past 24 hours.</td>
</tr>
<tr>
<td>Event Monitor</td>
<td>Investigate any system errors or warnings.</td>
</tr>
<tr>
<td>Unacknowledged Events list</td>
<td>Investigate and clear (acknowledge) any unacknowledged events.</td>
</tr>
</tbody>
</table>

**NOTICE**

EMC recommends that you enable the Email Home feature and the ConnectEMC feature, which automatically email EMC Customer Service with the status of the daily data integrity check and other important server messages.

Monitoring activities

**Procedure**

1. In Avamar Administrator, click the **Activity** launcher button.
   
   The **Activity** window appears.

2. Click the **Activity Monitor** tab.

   *Activity Monitor details on page 168* provides details on the information available in the Activity Monitor.

3. (Optional) Filter the information in the Activity Monitor to display only activities with a specific state, type, group, client, or plug-in:

   a. Select **Actions > Filter**.
      
      The **Filter Activity** dialog box appears.

   b. Define the filtering criteria and click **OK**.

**Activity Monitor details**

By default, the Activity Monitor tab displays the most recent 5,000 client activities during the past 72 hours. You can increase or reduce the amount of information in the Activity Monitor by editing the `com.avamar.mc.wo completed_job_retention_hours` preference in the `/usr/local/avamar/var/mc/server_data/prefs/mcservice.xml` file, and then restarting the MCS.

The following table provides details on the information that is available in the Activity Monitor.
### Table 36 Activity Monitor details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Session</strong></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Status of the backup, restore, or validation activity. The <em>Avamar Administrator Online Help</em> provides details on each status.</td>
</tr>
<tr>
<td>Error Code</td>
<td>If the activity did not successfully complete, a numeric error code appears. Double-click the error code to view a detailed explanation.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time that this activity was initiated, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.</td>
</tr>
<tr>
<td>Elapsed Time</td>
<td>Elapsed time for this activity.</td>
</tr>
<tr>
<td>End Time</td>
<td>Date and time that this activity completed, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of activity. The <em>Avamar Administrator Online Help</em> provides details on each type.</td>
</tr>
<tr>
<td>Server</td>
<td>Server on which the activity occurred, either the Avamar server or a Data Domain system.</td>
</tr>
<tr>
<td>Progress Bytes</td>
<td>Total number of bytes examined during this activity.</td>
</tr>
<tr>
<td>New Bytes</td>
<td>Percentage of new bytes backed up to either the Avamar server or a Data Domain system. Low numbers indicate high levels of data deduplication.</td>
</tr>
<tr>
<td><strong>Client</strong></td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>Avamar client name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Full location of the client in the Avamar server.</td>
</tr>
<tr>
<td>OS</td>
<td>Client operating system.</td>
</tr>
<tr>
<td>Client Release</td>
<td>Avamar client software version. If this activity is a VMware image backup or restore, then this value is the Avamar client software version running on the image proxy client.</td>
</tr>
<tr>
<td>Proxy</td>
<td>If this activity is a VMware image backup or restore, then this value is the name of the proxy client performing the backup or restore on behalf of the virtual machine. Blank for all other activities.</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Sched. Start</td>
<td>Date and time that this activity was scheduled to begin.</td>
</tr>
<tr>
<td>Sched. End Time</td>
<td>Date and time that this activity was scheduled to end.</td>
</tr>
<tr>
<td>Elapsed Wait</td>
<td>Total amount of time that this activity spent in the activity queue. That is, the scheduled start time minus the actual start time.</td>
</tr>
<tr>
<td>Group</td>
<td>Group that initiated this activity. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• If the activity was a scheduled backup, this is the group that this client was a member of when this scheduled activity was initiated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On-demand</strong> is shown for other backup, restore and validation activities.</td>
</tr>
</tbody>
</table>
### Table 36 Activity Monitor details (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Column      | If the activity was a scheduled replication, then this value is the replication group.  
|             | • **Admin On-Demand Group** is shown for demand replication activities.  
| Plug-in     | Plug-in used for this activity.                                                                                                               |
| Retention   | Retention types assigned to this backup. One or more of the following values:  
|             | • **D**—Daily  
|             | • **W**—Weekly  
|             | • **M**—Monthly  
|             | • **Y**—Yearly  
|             | • **N**—No specific retention type                                                                                                           |
| Schedule    | If the activity was a scheduled backup, this is the schedule that initiated this activity. On-Demand or End User Request is shown for all other activities initiated from Avamar Administrator or the client, respectively. |
| Dataset     | Name of the dataset used to take the backup. If the activity is a replication job, this column lists the source system name on the destination system, and the destination name on the source system. |
| WID         | Work order ID. Unique identifier for this activity.                                                                                           |

### Monitoring server status and statistics

The **Server** window in Avamar Administrator enables you to monitor status and statistics for the Avamar server as a whole, for individual nodes on the Avamar server, and for any configured Data Domain systems.

The following tabs appear on the **Server** window:

- **The Server Monitor** tab presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server. A separate subtab provides the same information for any configured Data Domain systems.
- **The Server Management** tab shows a detailed view of the server hardware resources for the Avamar server and any configured Data Domain systems.
- **The Session Monitor** tab shows a list of active client backup and restore sessions.
- **The Checkpoint Management** tab shows detailed information for all system checkpoints performed for this Avamar server.
- **The Data Domain NFS Datastores** tab lists the temporary NFS share for VMware instant access on any configured Data Domain systems. The *EMC Avamar for VMware User Guide* provides more information on instant access.
Server Monitor tab

The **Server Monitor** tab on the **Server** window in Avamar Administrator includes separate tabs for the Avamar server and any configured Data Domain systems.

### Avamar tab

The **Avamar** tab in the Server Monitor presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server.

The following table describes the information available on the **Avamar** tab.

**Table 37 Avamar tab details in the Server Monitor**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td></td>
</tr>
<tr>
<td>Status indicators</td>
<td>Status of the node. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Online (green)—The node is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• Read-Only (blue)—This status occurs normally as background operations</td>
</tr>
<tr>
<td></td>
<td>are performed and when backups have been suspended.</td>
</tr>
<tr>
<td></td>
<td>• Time-Out (gray)—MCS could not communicate with this node.</td>
</tr>
<tr>
<td></td>
<td>• Unknown (yellow)—Node status cannot be determined.</td>
</tr>
<tr>
<td></td>
<td>• Offline (red)—The node has experienced a problem. If ConnectEMC has</td>
</tr>
<tr>
<td></td>
<td>been enabled, a Service Request (SR) is logged. Go to EMC Online Support</td>
</tr>
<tr>
<td></td>
<td>to view existing SRs. Search the knowledgebase for Avamar Data Node</td>
</tr>
<tr>
<td></td>
<td>offline solution esg112792.</td>
</tr>
<tr>
<td>ID</td>
<td>Each node in the Avamar server has a unique logical identifier. This node</td>
</tr>
<tr>
<td></td>
<td>ID is expressed in the format <code>module.node</code>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Module and node numbering begins with zero. Therefore, the ID for the third</td>
</tr>
<tr>
<td></td>
<td>node in the first module is 0.2.</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td></td>
</tr>
<tr>
<td>Load</td>
<td>Average number of CPU threads over the past minute.</td>
</tr>
<tr>
<td>User</td>
<td>Percentage of CPU capacity consumed by executing server instructions</td>
</tr>
<tr>
<td></td>
<td>(anything other than operating system overhead).</td>
</tr>
<tr>
<td>Sys</td>
<td>Percentage of CPU capacity consumed by operating system overhead.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>Time in seconds that this node took to respond to a ping request.</td>
</tr>
<tr>
<td>In</td>
<td>Received packet throughput reported in KB per second.</td>
</tr>
<tr>
<td>Out</td>
<td>Sent packet throughput reported in KB per second.</td>
</tr>
<tr>
<td><strong>Disk</strong></td>
<td></td>
</tr>
<tr>
<td>Reads</td>
<td>Average number of hard drive reads per second as reported by the operating</td>
</tr>
<tr>
<td></td>
<td>system.</td>
</tr>
</tbody>
</table>
Table 37 Avamar tab details in the Server Monitor (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writes</td>
<td>Average number of hard drive writes per second as reported by the operating system.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Percentage of total available server storage capacity currently used.</td>
</tr>
</tbody>
</table>

Data Domain tab

The Data Domain tab in the Server Monitor provides CPU, disk activity, and network activity for each node on the Data Domain system.

The following table describes the information available on the Data Domain tab.

Table 38 Data Domain tab details in the Server Monitor

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Status indicators Status of the node. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• OK (green)—The Data Domain system is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• Warning (yellow)—There is a problem with the Data Domain system, but backups and restores can continue.</td>
</tr>
<tr>
<td></td>
<td>• Error (red)—There is a problem with the Data Domain system, and backups and restores will not occur until the problem is resolved.</td>
</tr>
<tr>
<td></td>
<td>If the status is yellow or red, you can view additional status information to determine and resolve the problem. The EMC Avamar and EMC Data Domain System Integration Guide provides details.</td>
</tr>
<tr>
<td>Name</td>
<td>Hostname of the Data Domain system as defined in corporate DNS.</td>
</tr>
<tr>
<td>CPU</td>
<td>Busy Avg. Average CPU usage as a percentage of total possible CPU usage.</td>
</tr>
<tr>
<td></td>
<td>Max Maximum CPU usage that has occurred as a percentage of total possible CPU usage.</td>
</tr>
<tr>
<td>Disk (KB/S)</td>
<td>Read Disk read throughput in kilobytes per second.</td>
</tr>
<tr>
<td></td>
<td>Write Disk write throughput in kilobytes per second.</td>
</tr>
<tr>
<td></td>
<td>Busy Disk I/O usage as a percentage of total possible disk I/O usage.</td>
</tr>
<tr>
<td>Network (KB/S)</td>
<td>Eth#1 Desc—Description of the network interface.</td>
</tr>
<tr>
<td></td>
<td>In/Out—Network bandwidth usage in kilobytes per second on network interface 1.</td>
</tr>
<tr>
<td></td>
<td>Eth#2 Desc—Description of the network interface.</td>
</tr>
<tr>
<td></td>
<td>In/Out—Network bandwidth usage in kilobytes per second on network interface 2.</td>
</tr>
</tbody>
</table>
Table 38 Data Domain tab details in the Server Monitor (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth#3</td>
<td>Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 3.</td>
</tr>
</tbody>
</table>

Note
The number of Eth# columns depends on the maximum number of network interfaces that the configured Data Domain systems support.

Server Management tab

The Server Management tab on the Server window in Avamar Administrator shows a detailed view of the server hardware resources, including both the Avamar server and any configured Data Domain systems.

Avamar server information is listed under the Avamar folder in the tree, and configured Data Domain systems are listed under the Data Domain folder in the tree.

The information in the right pane of the window changes when you select different items in the tree.

Table 39 Data display based on selections on the Server Management tab

<table>
<thead>
<tr>
<th>Selected item</th>
<th>Information in the right pane of the Server Management tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers node</td>
<td>Summary of bytes protected</td>
</tr>
<tr>
<td>Avamar or Data Domain nodes</td>
<td>Blank</td>
</tr>
<tr>
<td>Avamar server name</td>
<td>Detailed information for the Avamar server</td>
</tr>
<tr>
<td>Module</td>
<td>Detailed information for that module</td>
</tr>
<tr>
<td>Node</td>
<td>Detailed information for that node</td>
</tr>
<tr>
<td>Partition</td>
<td>Detailed information for that logical hard drive partition</td>
</tr>
<tr>
<td>Data Domain system</td>
<td>Detailed information for that Data Domain system</td>
</tr>
</tbody>
</table>

NOTICE
Avamar is licensed in decimal units. Therefore, Total capacity and Capacity used are displayed in decimal units on the Server Management tab. All other parts of the product that output capacity are displayed in binary units.
Bytes Protected Summary

The following table provides details on the **Bytes Protected Summary** properties on the **Server Management** tab.

**Table 40** Bytes Protected Summary properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Name of the Avamar server and configured Data Domain systems.</td>
</tr>
<tr>
<td>Values</td>
<td>Number of bytes of protected data on the server or Data Domain system.</td>
</tr>
</tbody>
</table>

Server information

The following table provides details on the **Server** properties on the **Server Management** tab.

**Table 41** Server properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server details</strong></td>
<td></td>
</tr>
<tr>
<td>Active sessions</td>
<td>Current number of active client sessions. Click the <strong>Session Monitor</strong> tab</td>
</tr>
<tr>
<td></td>
<td>for additional information.</td>
</tr>
<tr>
<td>Total capacity</td>
<td>Total amount of server storage capacity.</td>
</tr>
<tr>
<td>Server utilization</td>
<td>Percentage of total available server storage capacity currently used. This</td>
</tr>
<tr>
<td></td>
<td>value is derived from the largest <strong>Disk Utilization</strong> value on the <strong>Avamar</strong></td>
</tr>
<tr>
<td></td>
<td>tab in the Server Monitor, and therefore represents the absolute maximum</td>
</tr>
<tr>
<td></td>
<td>Avamar server storage utilization. Actual utilization across all modules,</td>
</tr>
<tr>
<td></td>
<td>nodes and drives might be slightly lower.</td>
</tr>
<tr>
<td>Bytes protected</td>
<td>Total amount of client data in bytes that has been backed up (protected) on</td>
</tr>
<tr>
<td></td>
<td>this server.</td>
</tr>
<tr>
<td>Bytes protected quota</td>
<td>Maximum amount of client data in bytes that is licensed for protection on</td>
</tr>
<tr>
<td></td>
<td>this server.</td>
</tr>
<tr>
<td>License expiration</td>
<td>Calendar date on which this server's licensing expires, or never if licensing</td>
</tr>
<tr>
<td></td>
<td>is perpetual.</td>
</tr>
<tr>
<td>Time since Server initialization</td>
<td>Number of hours, days, and minutes that have elapsed since this Avamar</td>
</tr>
<tr>
<td></td>
<td>server was initialized.</td>
</tr>
<tr>
<td>Last checkpoint</td>
<td>Date and time that the last server checkpoint was performed. Checkpoints</td>
</tr>
<tr>
<td></td>
<td>are typically performed twice daily.</td>
</tr>
<tr>
<td>Last validated checkpoint</td>
<td>Date and time that the server checkpoint was last validated. Checkpoint</td>
</tr>
<tr>
<td></td>
<td>validation normally occurs once per day. Therefore, the <strong>Last validated</strong></td>
</tr>
<tr>
<td></td>
<td><strong>checkpoint</strong> time and <strong>Last checkpoint time</strong> might be different</td>
</tr>
<tr>
<td></td>
<td>depending on the time of day that you view this information.</td>
</tr>
</tbody>
</table>
**Table 41**  Server properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>If the Last validated checkpoint and Last checkpoint times are more than 36 hours apart, this indicates that checkpoint validation is not occurring. This is a problem.</td>
</tr>
<tr>
<td>System Name</td>
<td>User-assigned name of this Avamar server.</td>
</tr>
<tr>
<td>System ID</td>
<td>Unique identifier for this Avamar server.</td>
</tr>
<tr>
<td>HFSAddr</td>
<td>Hash File System (HFS) address (Addr). This is the hostname or IP address that backup clients use to connect to this Avamar server.</td>
</tr>
<tr>
<td>HFSPort</td>
<td>HFS data port. This is the data port that backup clients use to connect to this Avamar server. The default is port 27000.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of this Avamar server. If the HFSAddr is an IP address, this value is the same as the HFSAddr.</td>
</tr>
</tbody>
</table>

**Maintenance activities details**

<table>
<thead>
<tr>
<th>Suspended</th>
<th>One of the following values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No</td>
<td>Server maintenance activities are not currently suspended (that is, server maintenance activities will run normally during the next maintenance window).</td>
</tr>
<tr>
<td>• Yes</td>
<td>Server maintenance activities are currently suspended.</td>
</tr>
</tbody>
</table>

**Garbage collection details**

<table>
<thead>
<tr>
<th>Status</th>
<th>One of the following values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Idle</td>
<td>Garbage collection is not currently taking place.</td>
</tr>
<tr>
<td>• Processing</td>
<td>Garbage collection is currently taking place.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>One of the following values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• OK</td>
<td>Last garbage collection activity successfully completed.</td>
</tr>
<tr>
<td>• Error code</td>
<td>Last garbage collection activity did not successfully complete.</td>
</tr>
</tbody>
</table>

| Start time       | Date and time that the last garbage collection activity began.                                 |
| End time         | Date and time that the last garbage collection activity ended.                                 |
| Passes           | Total number of passes during the last garbage collection activity.                             |
| Bytes recovered  | Total amount of storage space in bytes that was recovered during the last garbage collection activity. |
| Chunks deleted   | Total number of data chunks that were deleted during the last garbage collection activity.       |
| Index stripes    | Total number of index stripes.                                                                 |
| Index stripes processed | Total number of index stripes that were processed during the last garbage collection activity. |
Module information

The following table provides details on the Module properties on the Server Management tab.

Table 42 Module properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total capacity</td>
<td>Total amount of server storage capacity.</td>
</tr>
<tr>
<td>Server utilization</td>
<td>Percentage of total available server storage capacity currently used. This value is derived from the largest Disk Utilization value shown on the Avamar tab in the Server Monitor, and therefore represents the absolute maximum Avamar server storage utilization. Actual utilization across all modules, nodes and drives might be slightly lower.</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>Total number of nodes in this module.</td>
</tr>
<tr>
<td>IP address</td>
<td>Base IP address of this module.</td>
</tr>
</tbody>
</table>

Node information

The following table provides details on the Node properties on the Server Management tab.

Table 43 Node properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status indicators</td>
<td>One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Online (green) — Node is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• Read-Only (blue) — This occurs normally as background operations are performed and when backups have been suspended.</td>
</tr>
<tr>
<td></td>
<td>• Time-Out (gray) — MCS could not communicate with this node.</td>
</tr>
<tr>
<td></td>
<td>• Unknown (yellow) — Node status cannot be determined.</td>
</tr>
<tr>
<td></td>
<td>• Offline (red) — Node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.</td>
</tr>
<tr>
<td>State</td>
<td>Current operational state of the server. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• ONLINE — Node is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• DEGRADED — One or more disk errors have been detected.</td>
</tr>
<tr>
<td></td>
<td>• OFFLINE — Node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.</td>
</tr>
<tr>
<td></td>
<td>• READONLY — This occurs normally as background operations are performed and when backups have been suspended.</td>
</tr>
</tbody>
</table>
Table 43 Node properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avamar server details</strong></td>
<td></td>
</tr>
<tr>
<td>Runlevel</td>
<td>Current operational state of the server. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• fullaccess — This Avamar server is fully operational.</td>
</tr>
<tr>
<td></td>
<td>• admin — Avamar server is fully operational but only the administrator root account can access the server.</td>
</tr>
<tr>
<td></td>
<td>• adminonly — Avamar server is fully operational but only the administrator root account can access the server.</td>
</tr>
<tr>
<td></td>
<td>• adminreadonly — Avamar server is in a read-only condition and only the administrator root account can access the server.</td>
</tr>
<tr>
<td></td>
<td>• readonly — Avamar server is in a read-only condition. Restores are allowed but no new backups can be taken.</td>
</tr>
<tr>
<td></td>
<td>• suspended — Scheduled backups are disabled and will not occur until you reenable the scheduler.</td>
</tr>
<tr>
<td></td>
<td>• synchronizing — Avamar server is priming or synchronizing stripes. This is a temporary condition. Some operations might be delayed.</td>
</tr>
<tr>
<td><strong>Server details</strong></td>
<td></td>
</tr>
<tr>
<td>Accessmode</td>
<td>Current access level of the server.</td>
</tr>
<tr>
<td></td>
<td>The full server access mode is typically represented as three four-bit fields. For example: mhpu+mhpu+0000</td>
</tr>
<tr>
<td></td>
<td>The most significant bits show server privileges, the middle bits show root user privileges, and the least significant bits show privileges for all other users.</td>
</tr>
<tr>
<td></td>
<td>Individual bits in these fields convey the following information:</td>
</tr>
<tr>
<td></td>
<td>• m — Migrate allowed.</td>
</tr>
<tr>
<td></td>
<td>• h — Hash File System (HFS) is writable.</td>
</tr>
<tr>
<td></td>
<td>• p — Persistent store is writable.</td>
</tr>
<tr>
<td></td>
<td>• u — User accounting is writable.</td>
</tr>
<tr>
<td>Port</td>
<td>Data port used for intra-node communication.</td>
</tr>
<tr>
<td>Dispatcher</td>
<td>Data port used by various utilities to communicate with this node.</td>
</tr>
<tr>
<td>Server uptime</td>
<td>Number of hours, days and minutes that have elapsed since this Avamar server was initialized.</td>
</tr>
<tr>
<td>Total capacity</td>
<td>Total amount of server storage capacity.</td>
</tr>
<tr>
<td>Capacity used</td>
<td>Total amount of server storage capacity that has been used for any reason.</td>
</tr>
<tr>
<td>Server utilization</td>
<td>Percentage of total available node storage capacity currently used.</td>
</tr>
<tr>
<td>Number of stripes</td>
<td>Total number of stripes on this node.</td>
</tr>
<tr>
<td>Server version</td>
<td>Version of Avamar software running on this node.</td>
</tr>
<tr>
<td><strong>OS details</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 43 Node properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Current operating system version running on this node.</td>
</tr>
<tr>
<td>Node uptime</td>
<td>Number of hours, days and minutes that have elapsed since this node was</td>
</tr>
<tr>
<td></td>
<td>last booted.</td>
</tr>
<tr>
<td>Load average</td>
<td>The average number of CPU threads over the past minute.</td>
</tr>
<tr>
<td>CPU %</td>
<td>Percentage of this node's CPU currently being used.</td>
</tr>
<tr>
<td>Ping time (sec)</td>
<td>Time in seconds this node took to respond to a ping request.</td>
</tr>
<tr>
<td>Disk reads</td>
<td>Number of hard drive read operations per second.</td>
</tr>
<tr>
<td>Disk writes</td>
<td>Number of hard drive write operations per second.</td>
</tr>
<tr>
<td>Network reads</td>
<td>Number of kilobytes per second read by way of this node's network</td>
</tr>
<tr>
<td></td>
<td>connection.</td>
</tr>
<tr>
<td>Network writes</td>
<td>Number of kilobytes per second written by way of this node's network</td>
</tr>
<tr>
<td></td>
<td>connection.</td>
</tr>
</tbody>
</table>

Table 44 Partition properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status indicators</td>
<td>One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Online (green) — The partition is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• Offline (yellow) — The partition has one or more offline stripes. If</td>
</tr>
<tr>
<td></td>
<td>ConnectEMC has been enabled, a Service Request (SR) should have</td>
</tr>
<tr>
<td></td>
<td>been logged. Go to EMC Online Support website to view existing SRs.</td>
</tr>
<tr>
<td></td>
<td>• Read-Only (blue) — The partition is read-only.</td>
</tr>
<tr>
<td></td>
<td>• Nonfunctional (red) — The partition is not functioning. Search the</td>
</tr>
<tr>
<td></td>
<td>knowledgebase on EMC Online Support website for solution esg108474.</td>
</tr>
</tbody>
</table>

Partition information

The following table provides details on Partition properties on the Server Management tab.

Table 44 Partition properties on the Server Management tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total capacity</td>
<td>Total amount of server storage capacity.</td>
</tr>
<tr>
<td>Server utilization</td>
<td>Percentage of total available partition storage capacity that is currently used.</td>
</tr>
<tr>
<td>State</td>
<td>Current operational state of this partition. One of the following values:</td>
</tr>
</tbody>
</table>
Table 44 Partition properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ONLINE — The partition is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• MIGRATING — Transitional state that might or might not be due to normal</td>
</tr>
<tr>
<td></td>
<td>operation.</td>
</tr>
<tr>
<td></td>
<td>• OFFLINE — Transitional state that might or might not be due to normal</td>
</tr>
<tr>
<td></td>
<td>operation.</td>
</tr>
<tr>
<td></td>
<td>• READY — Transitional state that might or might not be due to normal</td>
</tr>
<tr>
<td></td>
<td>operation.</td>
</tr>
<tr>
<td></td>
<td>• RESTARTING — Transitional state that might or might not be due to normal</td>
</tr>
<tr>
<td></td>
<td>operation.</td>
</tr>
<tr>
<td>Number of offline stripes</td>
<td>Total number of stripes on this partition that are offline due to media errors.</td>
</tr>
<tr>
<td>Number of transitioning</td>
<td>Total number of stripes on this partition that are in a transitional state</td>
</tr>
<tr>
<td>stripes</td>
<td>that might or might not be due to normal operation.</td>
</tr>
<tr>
<td>Properties</td>
<td>Various operating system properties (if known).</td>
</tr>
<tr>
<td>Values</td>
<td>Settings for operating system properties (if known).</td>
</tr>
</tbody>
</table>

Data Domain system information

The following table provides details on the Data Domain system properties on the Server Management tab.

Table 45 Data Domain system properties on the Server Management tab

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status indicators</td>
</tr>
<tr>
<td>One of the following values:</td>
</tr>
<tr>
<td>• Online (green)—The Data Domain system</td>
</tr>
<tr>
<td>is functioning properly.</td>
</tr>
<tr>
<td>• Offline (yellow)—The Data Domain</td>
</tr>
<tr>
<td>system is offline.</td>
</tr>
<tr>
<td>The Data Domain Offline Diagnostics</td>
</tr>
<tr>
<td>Suite User Guide, which is available</td>
</tr>
<tr>
<td>on EMC Online Support, provides more</td>
</tr>
<tr>
<td>information.</td>
</tr>
<tr>
<td>• Read-Only (blue)—The Data Domain</td>
</tr>
<tr>
<td>system is read-only.</td>
</tr>
<tr>
<td>• Nonfunctional (red)—The Data Domain</td>
</tr>
<tr>
<td>system is not functioning. The Data</td>
</tr>
<tr>
<td>Domain Offline Diagnostics Suite User</td>
</tr>
<tr>
<td>Guide provides more information.</td>
</tr>
<tr>
<td>Hostname</td>
</tr>
<tr>
<td>The network hostname of the Data Domain</td>
</tr>
<tr>
<td>system as defined in DNS.</td>
</tr>
<tr>
<td>Total Capacity (post-comp size)</td>
</tr>
<tr>
<td>The total capacity for compressed data</td>
</tr>
<tr>
<td>on the Data Domain system.</td>
</tr>
<tr>
<td>Server Utilization (post-comp use%)</td>
</tr>
<tr>
<td>The percentage of capacity used on the</td>
</tr>
<tr>
<td>Data Domain system for any reason</td>
</tr>
<tr>
<td>after compression of the data.</td>
</tr>
</tbody>
</table>
### Table 45 Data Domain system properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Protected</td>
<td>The total number of bytes of data that are protected, or backed up, on the Data Domain system. This value is the number of bytes before the data is compressed.</td>
</tr>
<tr>
<td>File System Available (post-comp avail)</td>
<td>The total amount of disk space available for compressed data in the DDFS.</td>
</tr>
<tr>
<td>File System Used (post-comp used)</td>
<td>The total amount of disk space used in the DDFS for compressed data.</td>
</tr>
<tr>
<td>User Name</td>
<td>The username of the Data Domain OpenStorage (OST) account that Avamar should use to access the Data Domain system for backups, restores, and replication, if applicable. This username is specified when you add the Data Domain system to the Avamar configuration.</td>
</tr>
<tr>
<td>Default Replication Storage System</td>
<td>Whether the Data Domain system is configured as default replication storage. This option is selected or cleared when you add the Data Domain system to the Avamar configuration.</td>
</tr>
<tr>
<td>Maximum Streams</td>
<td>The maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores. This number is configured for the Data Domain system when you add the system to the Avamar configuration.</td>
</tr>
<tr>
<td>DDOS Version</td>
<td>Version number of the Data Domain Operating System (DD OS) on the Data Domain system.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The manufacturer’s serial number for the disk in the Data Domain system.</td>
</tr>
<tr>
<td>Model number</td>
<td>Model number of the Data Domain system.</td>
</tr>
<tr>
<td>Monitoring Status</td>
<td>Monitoring status of the Data Domain system. The <em>EMC Avamar and EMC Data Domain System Integration Guide</em> provides details on the available values.</td>
</tr>
<tr>
<td>Monitoring status details</td>
<td>When the monitoring status is a value other than OK, then additional information appears in a list below the Monitoring Status row. The following rows describe the available values.</td>
</tr>
<tr>
<td>DD Boost licensing status, either:</td>
<td>The <em>EMC Avamar and EMC Data Domain System Integration Guide</em> provides details on how to troubleshoot error conditions that result from each of these values.</td>
</tr>
<tr>
<td>• DDBOost Licensed</td>
<td></td>
</tr>
<tr>
<td>• DDBOost not Licensed</td>
<td></td>
</tr>
<tr>
<td>DD Boost status, either:</td>
<td></td>
</tr>
<tr>
<td>• DDBOost Enabled</td>
<td></td>
</tr>
<tr>
<td>• DDBOost Disabled</td>
<td></td>
</tr>
<tr>
<td>Whether the DD Boost user is enabled or disabled, either:</td>
<td></td>
</tr>
<tr>
<td>• DDBOost User Enabled</td>
<td></td>
</tr>
<tr>
<td>• DDBOost User Disabled</td>
<td></td>
</tr>
</tbody>
</table>
### Table 45 Data Domain system properties on the Server Management tab (continued)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DD Boost user status, either:</strong></td>
</tr>
<tr>
<td>• DDBoost User Valid</td>
</tr>
<tr>
<td>• DDBoost User Changed</td>
</tr>
<tr>
<td><strong>DD Boost option status, either:</strong></td>
</tr>
<tr>
<td>• DDBoost Option Enabled</td>
</tr>
<tr>
<td>• DDBoost Option Disabled</td>
</tr>
<tr>
<td>• DDBoost Option not Available</td>
</tr>
<tr>
<td><strong>Status of the non-OST user, if configured, either:</strong></td>
</tr>
<tr>
<td>• Non-ost user state is Unknown</td>
</tr>
<tr>
<td>• Non-ost user Invalid</td>
</tr>
<tr>
<td>• Non-ost user disabled</td>
</tr>
<tr>
<td>• Non-ost user is not an admin user</td>
</tr>
</tbody>
</table>

**Note**

This row does not appear if the non-OST user has not been configured.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP status, either:</strong></td>
</tr>
<tr>
<td>• SNMP Enabled</td>
</tr>
<tr>
<td>• SNMP Disabled</td>
</tr>
<tr>
<td><strong>Status of the Data Domain file system, either:</strong></td>
</tr>
<tr>
<td>• File System Running</td>
</tr>
<tr>
<td>• File System Enabled</td>
</tr>
<tr>
<td>• File System Disabled</td>
</tr>
<tr>
<td>• File System Unknown</td>
</tr>
<tr>
<td>• File system status unknown since SNMP is disabled</td>
</tr>
<tr>
<td><strong>Whether synchronization of maintenance operations, such as checkpoints, HFS checks, and Garbage Collection, between the Avamar server and the Data Domain system can occur, either:</strong></td>
</tr>
<tr>
<td>• Synchronization of maintenance operations is off.</td>
</tr>
<tr>
<td>• Synchronization of maintenance operations is on.</td>
</tr>
</tbody>
</table>

### Event monitoring

All Avamar system activity and operational status is reported as events to the MCS. Examples of Avamar events include client registration and activation, successful and failed backups, and hard disk status.

Each event contains the information in the following table.
### Table 46 Event information

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event code</td>
<td>Unique identifier</td>
</tr>
<tr>
<td>Date and time</td>
<td>Date and time the event was reported</td>
</tr>
<tr>
<td>Category</td>
<td>Category of event:</td>
</tr>
<tr>
<td></td>
<td>• SYSTEM</td>
</tr>
<tr>
<td></td>
<td>• APPLICATION</td>
</tr>
<tr>
<td></td>
<td>• USER</td>
</tr>
<tr>
<td></td>
<td>• SECURITY</td>
</tr>
<tr>
<td>Type</td>
<td>Type of event:</td>
</tr>
<tr>
<td></td>
<td>• INTERNAL</td>
</tr>
<tr>
<td></td>
<td>• ERROR</td>
</tr>
<tr>
<td></td>
<td>• WARNING</td>
</tr>
<tr>
<td></td>
<td>• INFORMATION</td>
</tr>
<tr>
<td></td>
<td>• DEBUG</td>
</tr>
<tr>
<td>Summary</td>
<td>A one-line summary description of the event</td>
</tr>
<tr>
<td>Hardware source</td>
<td>System node that reported the event</td>
</tr>
<tr>
<td>Software source</td>
<td>System or application module that reported the event</td>
</tr>
</tbody>
</table>

### Event notifications

The following features generate notifications when specific events occur.

**Pop-up alerts**
You can configure individual events to generate a graphical pop-up alert each time the event occurs. Avamar Administrator must be running for the pop-up alerts to appear.

**Acknowledgement required list**
You can specify that when a certain event type occurs, the Avamar system administrator must acknowledge the event.

**Email messages**
You can specify that when a certain event type occurs, an email message is sent to a designated list of recipients. Email notifications can be sent immediately or in batches at scheduled times.

A typical batch email notification message looks like this:

MCS: avamar-1.example.com

MCS Version: 7.1.0-nnn
Avamar Server: avamar-1.example.com
Avamar Server Version: 7.1.0-nnn

Event profile: My Custom Profile
Count of events: 3

Summary of events:

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Count</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION</td>
<td>22207</td>
<td>1</td>
<td>New group created</td>
</tr>
<tr>
<td>INFORMATION</td>
<td>22208</td>
<td>1</td>
<td>Group modified</td>
</tr>
<tr>
<td>INFORMATION</td>
<td>22209</td>
<td>1</td>
<td>Group deleted</td>
</tr>
</tbody>
</table>

Event Code = 22207
Event Date/Time = 5/10/14 09:58:20 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = New group created
Software Source = MCS:CR

Event Code = 22209
Event Date/Time = 5/10/14 09:58:25 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group deleted
Software Source = MCS:CR

Event Code = 22208
Event Date/Time = 5/10/14 10:55:28 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group modified
Software Source = MCS:CR

Syslog support
You can specify that when an event type occurs, Avamar logs information to local or remote syslog files based on filtering rules configured for the syslog daemon that receives the events. Third-party monitoring tools and utilities capable of examining log entries can access the syslog files and process them to integrate Avamar event information into larger site activity and status reports.

SNMP support
The Avamar SNMP implementation provides two ways to access Avamar server events and activity completion status:

- SNMP requests provide a mechanism for SNMP management applications to “pull” information from a remote SNMP-enabled client (in this case, the Avamar server).
- SNMP traps provide a mechanism for the Avamar server to “push” information to SNMP management applications whenever designated Avamar events occur. You can configure an event type to output SNMP traps.
Event profiles

Profiles are a notification management feature that are used to logically group certain event codes together and specify which notifications to generate when the events occur.

There are two basic types of event profiles:

- **System profile** — There is only one system event profile. It contains all possible system event codes.
- **Custom profiles** — Custom profiles are used to send various notifications when certain system events occur. You can create as many custom profiles as you need to organize system events and generate notifications when any of those events occur.

Profile catalog

The Avamar system includes a set of preconfigured event profiles by default.

**System profile**
There is only one system event profile. It contains all possible system event codes.

**Evaluation profile**
The evaluation profile is primarily intended to be used to support system evaluations. If enabled, this profile generates an email notification and attaches two weeks' worth of Activities - DPN Summary report information to the email message. The *EMC Avamar Reports Guide* provides more information about the Activities - DPN Summary report.

**High Priority Events profile**
The High Priority Events profile is enabled by default. This special event profile automatically emails the following information to EMC Customer Support (emailhome@avamar.com) twice daily:

- Status of the daily data integrity check
- Selected Avamar server warnings and information messages
- Any Avamar server errors

The only change you can make to the High Priority Events profile is to add email addresses to the Recipient Email List. If you require custom High Priority Events profile settings, copy the profile and then edit the copy.

**Local SNMP Trap profile**
The Local SNMP Trap profile is read-only and is intended to be used for test purposes only. The profile enables you to verify that traps are successfully generated and received by the local `snmptrapd` process, which then writes the trap information to a syslog file.

**Local Syslog profile**
If enabled, the Local Syslog profile reports status by way of the local `syslogd` process on the Avamar server.

Editing the system event profile

The system event profile contains all possible system event codes. You can edit the system event profile to control whether an event generates a pop-up alert in Avamar Administrator, an entry in the common unacknowledged events list, or neither.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
The Manage All Profiles window appears.
2. Select **System Profile** in the left pane and click **Edit**.
   The **Edit Profile** dialog box appears with a list of event codes.

3. To show a graphical pop-up alert in Avamar Administrator each time an event occurs,
   select the **GUI Alert** checkbox next to the event.

4. To add an entry to the common unacknowledged events list each time an event
   occurs, select the **Acknowledgement Required** checkbox.

5. Click **OK**.

Creating a custom event profile

Custom event profiles enable you to send notifications when specific system events
occur.

You cannot view system events and profiles outside the domain that you are logged in to.
This affects the profiles that you can edit and the events that you can add to a profile.

Procedure

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   The **Manage All Profiles** window appears.

2. In the left pane, select the domain for the custom event profile, and click **New**.
   The **New Profile** wizard appears.

3. In the **Profile Name** box, type a name for the event profile.

4. Choose whether to enable or disable the profile by selecting or clearing the **Profile
   Enabled** checkbox.

5. Choose whether to enable email notifications for the profile by selecting or clearing
   the **Email Enabled** checkbox.

6. If you enabled email notifications, then specify whether to send email notifications as
   soon as events occur or on a scheduled basis:
   - To send email notifications as soon as events occur, select **Send data as events
     occur**.
   - To send email notifications on a scheduled basis, select **Send data on a schedule**,
     and then select the schedule from the list.

7. Choose whether to enable or disable syslog notification for the profile by selecting or
   clearing the **Syslog Notification – Enabled** checkbox.

8. Choose whether to enable or disable SNMP notification for the profile by selecting or
   clearing the **SNMP Trap Notification – Enabled** checkbox.

9. Click **Next**.
   The **Event Codes** page appears.

10. Click the **All Codes** tab, and then select the **Notify** checkbox next to the errors that
    should trigger notifications.

    **NOTICE**

    An asterisk (*) next to an event indicates an event of such severity that a notification
    is sent when that event occurs, even if other event notifications are sent on a
    schedule.

11. Click the **Audit Codes** tab, and then select the **Notify** checkbox next to the audit
    events that should trigger notifications.
NOTICE

An asterisk (*) next to an event code indicates an event of such severity that a notification is sent when that event occurs, even if other event notifications are sent on a schedule.

12. If you are adding this custom event profile at the top-level (that is, not to a domain or subdomain), specify the parameters to control capacity forecast alerts:

   a. Click the Parameters tab.

   b. Select the checkbox next to the parameter, and then type a new value for the parameter.

   c. Repeat the previous step as necessary for each parameter.

13. Click Next.

   The Attachments page appears.

14. (Optional) If the profile includes email notification messages, select the Attach Server status in email (XML) checkbox to include a report of overall Avamar server status in XML format in the messages.

15. (Optional) To include Avamar server logs in email notification messages, select the Attach Server logs in email checkbox and then type the full path to the location of Avamar server logs in the Directory box. The default location is /usr/local/avamar/var/cron/.

16. Specify the reports to include in email notification messages:

   a. Select the Attach checkbox next to the report to include.

   b. Select the checkbox next to the report for the file formats in which to send the report. You can select XML, CSV, or TXT.

   c. Specify the number of historical reports of this type to send with each notification message using the Since Count and Since Unit fields. For example, send the past two months of these reports.

   The following values are available from the Since Count list:

   • day(s) ago
   • week(s) ago
   • month(s) ago
   • since last modified

17. Click Next.

   The Email Notification page appears.

18. If the profile includes email notification messages, then specify the recipients and options for the email notification messages:

   a. In the Email Subject Header box, type an email subject line for the notification message.

   b. Add an email recipient to the list by typing a valid email address in the Enter Recipient box and then clicking +.

   c. (Optional) To remove a recipient from the Recipient Email List, select the recipient and click -.

   d. To insert all attachments into the body of the email notification message, select the Inline attachments checkbox.
When you insert the attachments, the email message may be very long.

e. To immediately send a test email message, click Send Email.

   If the test email message is sent successfully, an email accepted by transport layer confirmation message appears.

19. Click Next.

   The Syslog Notification page appears.

20. If the profile includes syslog notification messages, then specify the syslog notification parameters:

   a. In the Address (IP or hostname) box, type the IP address or hostname of the Avamar server node running the syslogd process.

   b. In the Port Number box, type the port number used for syslog communication.

   c. Choose whether to include extended event code information in the syslog message by selecting or clearing the Include extended event data checkbox.

      The extended information is delimited by using the following tags:

      <Code>
      <Type>
      <Severity>
      <Category>
      <HwSource>
      <Summary>
      <active>
      <lastEmailSendDate>
      <domain>
      <scheduleID>
      <num_prefs>
      <name>
      <isSystem>

   d. From the Facility list, select one of the following: user, local0, local1, local2, local3, local4, local5, local6, or local7.

   e. To test the syslog notification parameters, click Send Test Syslog Entry.

21. Click Next.

   The SNMP Trap Notification page appears.

22. If the profile includes SNMP notification messages, then specify SNMP notification parameters:

   a. In the SNMP Trap address (IP or hostname) box, type the IP address or hostname of the computer running an application that is capable of receiving and processing an SNMP trap.

   b. In the Port Number box, type the port number on the host machine that is listening for SNMP traps. The default data port is 162.

   c. In the SNMP Community box, type the name of the SNMP community that the SNMP trap listener is configured to use.

      The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application.
d. To test the SNMP notification parameters, click **Send Test SNMP Trap**.

23. Click **Finish**.

**Editing a custom event profile**

After you create a custom event profile for notifications of specific system events, you can edit any of the properties of the profile.

You cannot view system events and profiles outside the domain that you are logged in to. This affects the profiles that you can edit and the events that you can add to a profile.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
   The **Manage All Profiles** window appears.

2. In the left pane, select the custom event profile and click **Edit**.
   
   The **Edit Profile** dialog box appears.

3. Edit the custom event profile. The properties are the same as when you create the profile.

4. Click **OK**.

**Copying a custom event profile**

You can create a custom event profile with the same properties as a profile that you already created by copying the profile. You can copy the profile to the same domain or to a different domain.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
   The **Manage All Profiles** window appears.

2. In the left pane, select the profile and click **Copy**.
   
   The **Save As** dialog box appears.

3. Type a name for the new custom event profile in the **Save As** box.

4. (Optional) To copy the new custom event profile to a different domain, click the **...** button, browse to the new domain, and then click **OK**.

5. Click **OK**.

**Testing custom event profile notifications**

You can test custom event profile notification mechanisms by sending a short email message or writing a short message to the syslog file.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
   The **Manage All Profiles** window appears.

2. In the left pane, select the custom event profile and click **Edit**.
   
   The **Edit Profile** dialog box appears.

3. Test the custom event profile:
   
   - To send a test email message, select the **Email Notification** tab and click **Send Email**.
   
   - To write a test message to the syslog file, select the **Syslog Notification** tab and click **Send Test Syslog Entry**.
To send a test SNMP trap message, select the **SNMP Trap Notification** tab and click **Send Test SNMP Trap**.

If the test message is successfully sent, a confirmation message appears.

4. Click **OK**.
5. Click **OK** to close the **Edit Profile** dialog box.

### Enabling and disabling a custom event profile

When you disable an event profile, no email notifications are sent until you reenable the profile. You can disable any profile except the system events profile.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
   The **Manage All Profiles** window appears.
2. In the left pane, select the event profile.
3. Click **Disable** to disable the event profile, or **Enable** to enable the event profile.

### Deleting a custom event profile

You can permanently delete any custom event profile except the system events profile.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.
   
   The **Manage All Profiles** window appears.
2. Select the event profile and click **Delete**.
   
   A confirmation message appears.
3. Click **Yes**.

### Viewing events in the Event Monitor

**Procedure**

1. In Avamar Administrator, click the **Administration** launcher button.
   
   The **Administration** window appears.
2. Click the **Event Management** tab.
3. Click the **Event Monitor** tab near the bottom of the window.
   
   The **Avamar Administrator Online Help** provides details on each of the columns in the Event Monitor.
4. Select the display mode for the Event Monitor:
   
   - Select **Query** to display the most recent 5,000 system events for a defined range of dates.
   - Select **Monitor** to display the most recent 5,000 system events during the past 24 hours.
5. (Optional) Filter the events that appear in the Event Monitor:
   
   a. Open the **Actions** menu and select **Event Management > Filter**.
      
      The **Filter** dialog box appears.
   
   b. If you selected the **Query** display mode for the Event Monitor, select the range of dates for the events to display by using the **From Date** and **To Date** fields.
c. From the **Category** list, select the category of events to display.

d. From the **Type** list, select the type of events to display.

e. From the **Severity** list, select the severity of the events to display.

f. To view events for all domains, select **All Domains**. Or, to view events for a specific domain, select **Domain** and then browse to or type the domain name.

g. To display only events that contain certain case-sensitive keywords in the event code data XML element, type the keyword in the **Data** box.

   This criterion promotes easy filtering on important keywords across event attributes. For example, filtering the Event Monitor on `error` returns all events that contain the word `error` in any XML attribute (for example, category, type, or severity).

h. Choose whether to display events from all sources, from only the Avamar server, from all Data Domain systems, or from a single Data Domain system:

   - To view events from all sources, leave the default selection of **All Sources** in the **Source** list.
   - To view events from only the Avamar server, select **Avamar** from the **Source** list.
   - To view events from all Data Domain systems, select **Data Domain Systems** from the **Source** list and leave the default selection of **All Systems**.
   - To view events from a single Data Domain system, select **Data Domain Systems** from the **Source** list, select the **System** option, and then either type or browse to the Data Domain system.

i. Click **More** to view additional filtering criteria.

j. To limit the Event Monitor to events with a certain event code, select **Only include codes** and then add and remove codes from the list. Or, to exclude events with a certain event code from the Event Monitor, select **Exclude codes** and then add and remove codes from the list.

k. Click **OK**.

**Viewing the event catalog**

A sequential listing of all event codes and summary information is available in `/usr/local/avamar/doc/event_catalog.txt` on the Avamar server. You can also view `event_catalog.txt` by using a web browser.

**Procedure**

1. Open a web browser and type the following URL:

   http://Avamar_server

   where `Avamar_server` is the DNS name or IP address of the Avamar server.

   The **EMC Avamar Web Restore** page appears.

2. Click **Documentation**.

   The **Avamar Documentation** page appears.

3. Click the plus icon next to **Avamar Event Codes**.

4. Click **event_catalog.txt**.

   The file opens in the web browser.
Acknowledging system events

System events that are configured to require acknowledgment each time they occur, remain in the unacknowledged events list until they are explicitly cleared, or acknowledged, by an Avamar server administrator.

Procedure
1. In Avamar Administrator, click the Administration launcher button. The Administration window appears.
2. Click the Event Management tab.
3. Click the Unacknowledged Events tab near the bottom of the window.
4. Acknowledge the events:
   - To acknowledge one or more events, select the event entries and select Actions > Event Management > Acknowledge Unacknowledged Events.
   - To acknowledge all events in the list, select Actions > Event Management > Clear All Alerts.

Customizing error events

By default, Avamar software continually monitors /var/log/messages for any occurrence of the case-insensitive search string error. Any occurrences of error create an event code of the type ERROR. You can customize this default behavior.

Procedure
1. Define additional case-insensitive search strings that also create Avamar ERROR events.
2. Add the search strings to /usr/local/avamar/var/mc/server_data/adminlogpattern.xml.

Server monitoring with syslog

The syslog system logging feature on UNIX and Linux systems collects system log messages and writes them to a designated log file. You can configure the Avamar server to send event information in syslog format.

The Avamar server supports both syslog and syslog-ng implementations.

Note
Persons configuring syslog monitoring of an Avamar server should be familiar with basic syslog concepts. A complete discussion of basic syslog concepts and implementation is beyond the scope of this guide. The www.syslog.org website provides additional information.

At the operating system level, system monitoring and logging relies on the syslogd process to collect system log messages and write them to a designated log file. The syslogd process runs locally on every Avamar server node.

However, without additional configuration, each node's syslogd only collects system information for that node, and writes it to a local log file on that node. From a syslog perspective, each Avamar server node is unaware that any other server nodes exist. Also, the utility node syslogd process is not aware that the Avamar Management Console Server (MCS) is collecting and logging Avamar event information.
You can configure an Avamar event profile to format Avamar server event messages in syslog format and send this data to the `syslogd` process running on the Avamar server utility node.

The following table describes how an event profile maps Avamar server event data to syslog fields.

<table>
<thead>
<tr>
<th>Field in syslog</th>
<th>Avamar event data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>Either <code>User</code> or <code>Local#</code>, where # is a number from 0 to 7.</td>
</tr>
</tbody>
</table>
| Priority        | One of the following values, based on the Avamar event type:  
|                 | - `debug`, if the Avamar event type is DEBUG  
|                 | - `err`, if the Avamar event type is ERROR  
|                 | - `info`, if the Avamar event type is INFO  
|                 | - `none`, if the Avamar event type is INTERNAL  
|                 | - `warning`, if the Avamar event type is WARNING |
| Date            | Avamar event date. |
| Time            | Avamar event time. |
| Hardware source | Avamar event hardware source. |
| Software source | Avamar event software source. |
| Message         | The following fields from the Avamar event code:  
|                 | - event code  
|                 | - category  
|                 | - summary  
|                 | - event data |

### Configuring local syslog

The most basic way to implement Avamar server syslog monitoring is to configure the MCS to output Avamar event information to the local `syslogd` process running on the utility node. The local `syslogd` service merges the Avamar event information with the operating system messages in a single local log file.

**Procedure**

1. Enable the Local Syslog event profile on the Avamar server:
   a. In Avamar Administrator, select `Tools` > `Manage Profiles`.
   b. Select the `Local Syslog` event profile in the left pane and click `Enable`.
2. On single-node servers and utility nodes with SLES 11 or later, configure the local utility node syslogd process to listen for MCS event messages on UDP data port 514:
   a. Open a command shell and log in as admin on the single-node server or the utility node of a multi-node server.
   b. Switch user to root by typing `su -`. 
c. Open `/etc/syslog-ng/syslog-ng.conf` in a text editor.

d. Locate the following entry:

```plaintext
# uncomment to process log messages from network:
#
udp(ip("0.0.0.0") port(514));
```

e. Add the following entry, including the comment:

```plaintext
# uncomment to process log messages from MCS:
#
udp(ip("0.0.0.0") port(514));
```

f. Save and close the file.

g. Restart the syslog process by typing the following command:

```
service syslog restart
```

h. Verify that syslog is listening on port 514 by typing the following command:

```
netstat -nap | grep 514
```

The following output appears in the command shell:

```
udp 0 0 127.0.0.1:514 127.0.0.1:* 8043/syslog-ng
```

**Configuring remote syslog**

Remote syslog monitoring involves configuring each server node to send syslog data to a remote logging host, and creating a custom syslog event profile that sends Avamar server event messages in syslog format to the remote logging host.

EMC expects that sites implementing remote syslog monitoring of an Avamar server will in most cases already have a remote logging host configured and deployed.

Many different syslog monitoring tools are available. Any syslog monitoring tool will generally work with Avamar as long as it is configured to listen for remote syslog messages over a LAN connection on UDP data port 514.

---

**NOTICE**

For maximum security, EMC recommends implementing remote syslog monitoring.

---

**Procedure**

1. Create a custom syslog event profile that sends Avamar server event messages in syslog format to the remote logging host.
2. Configure all server nodes to send syslog messages to the remote logging host.
3. Configure the remote logging host to listen for syslog messages over a LAN connection on UDP data port 514.
4. If a firewall is enabled on the remote logging host, configure the firewall to allow UDP traffic on port 514 for a defined IP range.

**Creating a custom syslog event profile**

**Procedure**

1. In Avamar Administrator, select **Tools > Manage Profiles**.

   The **Manage All Profiles** window appears.
2. Select the **Local Syslog** event profile in the left pane and click **Copy**.
   The **Save As** dialog box appears.
3. Type a name for the new custom event profile in the **Save As** field.
4. Leave the domain set to root (/). Custom syslog profiles must reside in the root domain.
5. Click **OK**.
6. In the **Manage All Profiles** dialog box, select the custom syslog event profile that you created and click **Edit**.
   The **Edit Profile** dialog box appears.
7. Select the **Syslog Notification** tab and specify syslog notification parameters:
   a. In the **Address (IP or hostname)** field, type the IP address or hostname of the remote logging host.
   b. In the **Port Number** field, leave the port number set to **514**.
   c. Select the **Include extended event data** option to include extended event code information in the syslog message.
      The extended information is delimited by using the following tags:
      
      <Code>
      <Type>
      <Severity>
      <Category>
      <HwSource>
      <Summary>
      <active>
      <lastEmailSendDate>
      <domain>
      <scheduleID>
      <num_prefs>
      <name>
      <isSystem>
   d. From the **Facility** list, select one of the following values: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.
8. (Optional) To test the syslog notification parameters, click **Send Test Syslog Entry**.
9. Click **OK**.

**Configuring server nodes to send syslog messages to the remote logging server**

As part of the process to configure remote syslog, you must configure all Avamar server nodes to send syslog messages to a remote logging server over a LAN connection on UDP data port 514.

**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Open `/etc/syslog-ng/syslog-ng.conf` in a text editor.
3. Add the following entry:
destination logserver {udp("ip_address" port(514)); }
log { source(src); destination(logserver); }

where \textit{ip_address} is the IP address of the remote logging host.

4. Save and close the file.
5. Restart the syslog process by typing the following command:

\begin{verbatim}
  service syslog restart
\end{verbatim}

6. On multi-node servers, repeat the previous steps for each node.

Configuring RHEL remote logging hosts running syslog

\textbf{Procedure}

1. Open a command shell and log in to the remote logging host as root.
2. Open /etc/sysconfig/syslog in a text editor.
3. Locate the following entry:

\begin{verbatim}
SYSLOGD_OPTIONS="-m 0"
\end{verbatim}

4. Add the \texttt{-r} parameter to the entry:

\begin{verbatim}
SYSLOGD_OPTIONS="-r -m 0"
\end{verbatim}

5. Save and close the file.
6. Restart the syslogd process by typing the following command:

\begin{verbatim}
  service syslog restart
\end{verbatim}

Configuring SLES remote logging hosts running syslog-ng

\textbf{Procedure}

1. Open a command shell and log in to the remote logging host as root.
2. Open /etc/syslog-ng/syslog-ng.conf in a text editor.
3. Locate the following entry:

\begin{verbatim}
# uncomment to process log messages from network:
# udp(ip("0.0.0.0") port(514));
\end{verbatim}

4. Uncomment the entry:

\begin{verbatim}
# uncomment to process log messages from network:
# udp(ip("0.0.0.0") port(514));
\end{verbatim}

5. Save and close the file.
6. Restart the syslog process by typing the following command:

\begin{verbatim}
  service syslog restart
\end{verbatim}

7. Verify that syslog is listening on port 514 by typing the following command:

\begin{verbatim}
  netstat -nap | grep 514
\end{verbatim}

The following output appears in the command shell:

\begin{verbatim}
  udp 0 0 0.0.0.0:514 0.0.0.0:* 8043/syslog-ng
\end{verbatim}
Configuring the firewall on the remote logging host

If a firewall is enabled on the remote logging host, configure the firewall to allow UDP traffic on port 514 for a defined IP range.

Procedure

1. Restrict the source IP addresses of the remote log messages in iptables or another firewall to avoid Denial Of Service (DOS) attacks on the remote logging host.

   The following example rule for iptables would allow client system logs for an IP address range of Avamar server nodes:

   ```
   # Rules to allow remote logging for syslog(-ng) on the log HOST system
   iptables -A INPUT -p udp -s 192.168.1.0/24 --dport 514 -j ACCEPT
   
   where 192.168.1.0/24 is in the IP address range of the Avamar server nodes.
   
   The following example rule for iptables specifies the IP address for each Avamar server node on a single line and includes the Mac address of the Network Interface Card (NIC) for the node:
   ```
   ```
   iptables -A INPUT -p udp -s 192.168.1.15 -m mac --mac-source 00:50:8D:FD:E6:35 --dport 514 -j ACCEPT
   ```
   ...

   No rules are necessary for the outgoing syslog traffic on the client side.

2. Restart the firewall service on the remote logging host for the changes to take effect.

3. Restart the `syslog-ng` service on all server nodes and the remote logging host for the changes to take effect:

   ```
   service syslog restart
   ```

Server monitoring with SNMP

Simple Network Management Protocol (SNMP) is a protocol for communicating and monitoring event notification information between an application, hardware device, or software application and any number of monitoring applications or devices. The Avamar server supports SNMP versions v1, v2c, and v3.

Note

Persons configuring an Avamar server to send event information over SNMP should be familiar with basic SNMP concepts. A complete discussion of basic SNMP concepts and implementation is beyond the scope of this guide. The [www.net-snmp.org](http://www.net-snmp.org) website provides additional information.

The Avamar SNMP implementation provides SNMP requests and SNMP traps to access Avamar server events and activity status.
SNMP requests
SNMP requests provide a mechanism for SNMP management applications to “pull” information from a remote SNMP-enabled application or device (in this case, the Avamar server). The SNMP management application sends a request to an SNMP master agent running on the Avamar server. The SNMP master agent then communicates with the Avamar SNMP sub-agent, which passes the request to the MCS. The MCS retrieves the data and sends it back to the Avamar SNMP sub-agent, which passes it back to the management application by way of the SNMP master agent. Data port 161 is the default data port for SNMP requests.

Avamar servers purchased directly from EMC use the Net-SNMP master agent. Avamar servers built with other industry standard hardware likely use an SNMP master agent provided by the hardware manufacturer.

SNMP traps
SNMP traps provide a mechanism for the Avamar server to “push” information to SNMP management applications when designated Avamar events occur. Data port 162 is the default data port for SNMP traps. Typically, the SNMP management application listens for any SNMP traps generated by designated remote hosts.

Configuring server monitoring with SNMP

Procedure
1. To enable an SNMP management application to monitor an Avamar server, load the Avamar Management Information Base (MIB) definition file (AVAMAR-MCS-MIB.txt) into the master MIB used by the SNMP management application. The MIB contains definitions of the information that can be monitored or which traps are sent for each SNMP application or device.

The following table provides the locations for the Avamar MIB definition file.

<table>
<thead>
<tr>
<th>Computer type</th>
<th>MIB location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-node server</td>
<td>/usr/local/avamar/doc</td>
</tr>
<tr>
<td>Multi-node server</td>
<td>/usr/local/avamar/doc on the utility node</td>
</tr>
<tr>
<td>Computer with Avamar Administrator</td>
<td>install_dir/doc</td>
</tr>
<tr>
<td></td>
<td>where install_dir is typically:</td>
</tr>
<tr>
<td></td>
<td>• C:\Program Files\avs\administrator on Microsoft Windows computers</td>
</tr>
<tr>
<td></td>
<td>• /usr/local/avamar on Linux computers</td>
</tr>
<tr>
<td></td>
<td>• /opt/AVMRcons1 on Solaris computers</td>
</tr>
</tbody>
</table>

A copy of the Avamar MIB definition file also resides in the /usr/share/snmp/mibs directory on single-node servers and utility nodes. This copy is used by the Avamar SNMP sub-agent and should not be moved or distributed.

2. Install and configure an AgentX compliant master agent:
   - If the Avamar server was purchased directly from EMC, the Net-SNMP master agent is already installed. However, you must configure the Net-SNMP agent. Configuring the Net-SNMP agent on page 198 provides instructions.
   - If the Avamar server is built with other industry standard hardware, you must install and configure the AgentX compliant master agent provided by the hardware vendor.
3. Configure a custom event profile to output designated Avamar server events to an SNMP trap. Creating a custom event profile for an SNMP trap on page 199 provides instructions.

Configuring the Net-SNMP agent

The `avsetup_snmp` command line utility configures the Net-SNMP agent to communicate with the Avamar server by using the Avamar SNMP sub-agent.

Procedure

1. Type the following commands to launch the utility:
   ```
   cd /root
   avsetup_snmp
   ```
   The output prompts you to specify the port on which to listen for SNMP requests.

2. Specify the SNMP request data port:
   - To use port 161, the default SNMP request data port, press Enter.
   - To use a different SNMP request data port, type the data port number and press Enter.

   If `avsetup_snmp` was not able to detect any SNMP communities, the output prompts you to specify whether to allow SNMPv3 read-write user based access.

3. Type `n` and press Enter.

4. Type `n` and press Enter.

5. Type `n` and press Enter.

6. Press Enter to accept the default value of `y`.

7. Type the SNMP community name and press Enter.

8. Press Enter to accept the community name from all hostnames or network addresses.

9. Press Enter to specify no restriction.

10. Type `n` and press Enter.

   The output indicates that `/etc/snmp/snmpd.conf` was created and run to configure the system_setup group. Then the output prompts you to specify the location of the system.
11. Type the physical location of the Avamar server and press Enter.
   The output prompts you to specify contact information.

12. Type contact information (for example, email address, telephone extension, and so forth) and press Enter.
   The output prompts you to specify whether to properly set the value of the sysServices.0 OID.

13. Type n and press Enter.
   The output indicates that /etc/snmp/snmpd.conf was installed and that snmpd was enabled.

Creating a custom event profile for an SNMP trap

As part of the process of configuring server monitoring with SNMP, you must create a custom event profile to output designated Avamar server events to an SNMP trap.

The default Avamar configuration includes a Local SNMP Trap profile that outputs Avamar server event messages to the local Net-SNMP trap listener (snmptrapd process). However, you cannot edit the Local SNMP Trap profile, and the profile is intended to be used for test purposes only, to verify that traps are successfully generated and received by the local snmptrapd process, which then writes the trap information to a syslog file. In most cases, you must configure another custom profile to send Avamar SNMP traps to a remote Net-SNMP trap listener.

Procedure
1. Create a custom event profile by using the steps in Creating a custom event profile on page 185.
   On the first page of the New Profile wizard, select the option to enable SNMP trap notification.

2. Continue through the wizard until the SNMP Trap Notification page appears.

3. In the SNMP Trap Address (IP or hostname) box, type the IP address or hostname of a computer with an application capable of receiving and processing an SNMP trap.

4. In the Port Number box, type the port number on the host machine that listens for SNMP traps.

5. In the SNMP Community box, type the name of the SNMP community that the SNMP trap listener is configured to use.

6. (Optional) To test the SNMP notification parameters, click Send Test SNMP Trap.

7. Click Finish.

Viewing Avamar server log files

By default, the Avamar storage process log file (gsan.log) is limited to 25 MB in size and always contains the most recent information. Additional historic log files (for example, gsan.log.1, gsan.log.2, and so forth) might also exist. You can collect and view these log files by using command line operations.

Procedure
1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
a. Log in to the utility node as admin.

b. Load the admin OpenSSH key by typing:

```
ssh-agent bash
ssh-add ~admin/.ssh/admin_key
```

c. When prompted, type the admin_key passphrase and press Enter.

2. Create a new user-defined temporary directory and change directory to it by typing the following commands:

```
mkdir directory
cd directory
```

where `directory` is the directory name.

3. Retrieve copies of the storage node log files by typing the following command:

```
gaetlogs
```

The `getlogs` command gathers the important log files from a particular node, compresses them into a single tar file, `nodelogs.tgz`, then copies these files to numbered subdirectories in the current working directory.

4. Examine the `nodelogs.tgz` files for any entry that contains the string `ERROR`. To accomplish this, run the following shell commands, which write any `nodelogs.tgz` entries that contain the string `ERROR` to a user-defined temporary file:

```
for p in [01][!sm]*/nodelogs.tgz; do
tar xzf $p
grep ERROR: cur/gsan.log*
rm -rf cur/*
done
```

5. Remove the user-defined temporary directory by typing the following commands:

```
rm -rf directory
```

---

**Audit logging**

The audit log keeps a permanent log of system actions initiated by users. The data in this log enables enterprises that deploy Avamar to enforce security policies, detect security breaches or deviation from policies, and hold users accountable for those actions.

Only actions that are initiated by users are logged. Actions initiated by the system without a user account, such as scheduled backups, maintenance activities, and so forth, are not logged.

System events with a category of `SECURITY` and type of `AUDIT` are used to implement the Avamar audit logging feature. Because the underlying data for audit log entries are system events, this information is available in two places:

- Event Monitor, which also contains all other system events
- Audit Log, which only contains events that are also audit log entries

By default, audit log information is retained for one year.

You can increase or reduce the audit log retention period by editing the value of `clean_db_audits_days` in `/usr/local/avamar/var/mc/server_data/prefs/mcsserver.xml`, and restarting the MCS.
Viewing the Audit Log

Procedure

1. In Avamar Administrator, click the Administration launcher button.

   The Administration window appears.

2. Click the Event Management tab.

3. Click the Audit Log tab near the bottom of the window.

   The Avamar Administrator Online Help provides details on each of the columns in the Audit Log.

4. Select the display mode for the Audit Log:
   
   - Select Query to display the most recent 5,000 audit log entries for a defined range of dates.
   - Select Monitor to display the most recent 5,000 audit log entries during the past 24 hours.

5. (Optional) Filter the entries that appear in the Audit Log:
   
   a. Open the Actions menu and select Event Management > Filter.

      The Filter dialog box appears.

   b. If you selected the Query display mode for the Audit Log, select the range of dates for the entries to display by using the From Date and To Date fields.

   c. From the Severity list, select the severity of the log entries to display.

   d. To view log entries for all domains, select All Domains. Or, to view entries for a specific domain, select Domain and then browse to or type the domain name.

   e. To display only log entries that contain certain case-sensitive keywords in the audit log entry data XML element, type the keyword in the Data box.

      This criterion promotes easy filtering on important keywords across log entry attributes. For example, filtering the log on error returns all log entries that contain the word error in any XML attribute (for example, category, type, or severity).

   f. Click More to view additional filtering criteria.

   g. To limit the Audit Log to events with a certain event code, select Only include codes and then add and remove codes from the list. Or, to exclude events with a certain event code from the Audit Log, select Exclude codes and then add and remove codes from the list.

   h. Click OK.
Automatic notifications to EMC Customer Support

The Email Home and ConnectEMC features automatically send notifications to EMC Customer Support. These notifications include alerts for high priority events and daily reports to facilitate monitoring the Avamar server.

Email Home

The Avamar Email Home feature automatically emails configuration, capacity, and general system information to EMC Customer Support once daily, and provides critical alerts in near-real time as needed.

By default, notification schedule email messages are sent at 6 a.m. and 3 p.m. each day. The Notification Schedule controls the timing of these messages. Schedules on page 91 provides more information on editing schedules.

Editing Email Home mail settings

Email Home is configured and enabled during Avamar server installation. You can edit the mail settings for Email Home after the installation.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```
     c. When prompted, type the admin_key passphrase and press Enter.

2. Change directories by typing the following command:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

3. Open mcserver.xml in a UNIX text editor.

4. Find the com.avamar.asn.module.mail node.

   The com.avamar.asn.module.mail node contains the smtpHost and admin_mail_sender_address entries.

5. Verify that the value for the smtpHost entry is the DNS name of the outgoing SMTP mail server that is used to send Email Home messages, such as smtp.example.com.

   If the value for the entry is incorrect, edit the value.

   **NOTICE**

   The Avamar 6.0 and later server installation or upgrade automatically completes the value for the smtpHost entry. In most cases, some arrangement must be made to enable emails originating from the Avamar server to be forwarded through the outgoing SMTP mail server to EMC Customer Support over the Internet.
6. Specify a valid email address with access to a corporate outgoing SMTP mail server as the value for the `admin_mail_sender_address` entry.

**NOTICE**

If you do not configure the Email Home feature to send messages from a valid email address, messages generated by the Email Home feature are rejected by the EMC incoming email server. EMC Customer Support is completely unaware that these programmatical generated messages were rejected. In addition, because a valid sending email account is not known, programmatical-generated warnings to the sender that these messages could not be sent are never viewed by anyone who can correct the problem.

7. Save the changes and close the file.

8. Restart the MCS by typing the following commands:

```
  dpnctl stop mcs
  dpnctl start
```

9. Close the command shell.

**ConnectEMC**

ConnectEMC is a program that runs on the Avamar server and sends information to EMC Customer Support. ConnectEMC is typically configured to send alerts for high priority events as they occur, as well as reports once daily.

ConnectEMC is integrated with EMC Secure Remote Support (ESRS), provided that it is installed, operational, and network accessible by the Avamar server. Contact your EMC Sales Representative for additional information about implementing ESRS.

Although ConnectEMC is initially configured during Avamar server software installation, Avamar Administrator enables you to manage ConnectEMC settings, in the form of three user-configurable transports, after the server is operational:

- **Primary transport**
- **Failover transport**
- **Notification transport**

The primary and failover transports send alerts for high priority events as they occur. The primary transport is used unless it fails, at which time the failover transport is used.

The notification transport sends email notifications messages to one or more customer email addresses under certain conditions.

You also can control whether the MCS generates and sends ConnectEMC messages by enabling, disabling, stopping, and starting ConnectEMC.

**Enabling and disabling ConnectEMC**

Disabling ConnectEMC causes the MCS to stop generating ConnectEMC messages until ConnectEMC is reenabled. To allow the MCS to continue generating ConnectEMC messages but to queue the messages, stop ConnectEMC.

**Procedure**

1. In Avamar Administrator, select **Tools > Manage ConnectEMC**.

   The **Manage ConnectEMC** window appears.

2. Specify whether the MCS generates and sends ConnectEMC messages:
To stop the MCS from generating messages, click Disable.
To restart the generation of messages, click Enable.
To continue generating messages but queue the messages, click Stop.
To start sending the messages, click Start.
If you disable ConnectEMC, you are prompted to type a password.

3. Type a valid password and click OK.

Editing the primary and failover transports

Procedure
1. In Avamar Administrator, select Tools > Manage ConnectEMC.
   The Manage ConnectEMC window appears.
2. Select either Primary Transport or Failover Transport in the left pane, and click Edit.
   The Edit Primary/Secondary Transport dialog box appears.
3. Select the transport type from the Transport Type list:
   - Email
   - FTP
   - HTTPS

Note
An operational ESRS gateway is required to use the FTP or HTTPS transport types.

4. Specify the transport type settings.

<table>
<thead>
<tr>
<th>Transport type</th>
<th>Settings</th>
</tr>
</thead>
</table>
| Email          | a. In the SMTP Host (Email Server) field, specify the mail server hostname or IPv4 address.  
b. In the Email Address field, specify one or more recipients of these emails. Separate multiple email addresses with commas.  
c. In the Email Sender Address field, specify the email address from which to send the message.  
d. (Optional) To configure advanced settings, click Advanced, and then specify the following settings in the Edit Advanced Email Settings dialog box:  
Retries – The number of retries to attempt before reporting a failure. The default setting is 5 retries.  
Timeout – The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds).  
Description – A description of this transport that appears in the Manage ConnectEMC window. The default description is Email Transport.  
Email Subject – The subject line in the email. The default subject line is Avamar ConnectEMC Notification Email. |
<table>
<thead>
<tr>
<th>Transport type</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Do not change the email subject unless instructed to do so by EMC Customer Support. Email messages with other subject lines might be rejected by EMC spam filters.</td>
</tr>
<tr>
<td>e. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

**FTP**

| a. | In the **IP Address** field, specify an IPv4 address. |
| b. | In the **Username** field, specify an FTP username. The setting depends on the FTP server software. |
| c. | In the **Password** field, specify the password for the username. |
| d. (Optional) | To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced FTP Settings** dialog box: |
| **Retries** | The number of retries to attempt before reporting a failure. The default setting is 5 retries. |
| **Timeout** | The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds). |
| **Description** | A description of this transport that appears in the **Manage ConnectEMC** window. The default description is **FTP Transport**. |
| **FEP Folder** | A unique customer UNIX path in the ConnectEMC Front End Processor (FEP). Use the folder location supplied by EMC Customer Support. |
| **FTP Port** | An IP port. The default setting is port 21. |
| **Mode** | Either Active or Passive. The default setting is Active. |
| **Note** | Do not change the email subject unless instructed to do so by EMC Customer Support. Email messages with other subject lines might be rejected by EMC spam filters. |
| e. Click OK. | |

**HTTPS**

| a. | Type a valid ESRS Home page Universal Resource Locator (URL) in the **URL** field. Valid ESRS Home page URLs use the following format: |
| | `https://home_name[:port]/target_directory` |
| | where `home_name`, `port`, and `target_directory` are the home name, data port, and target directory, respectively. |
| | Use the ESRS Home page URL provided by EMC Customer Support. |
| b. (Optional) | To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced HTTPS Settings** dialog box: |
| **Retries** | The number of retries to attempt before reporting a failure. The default setting is 5 retries. |
| **Timeout** | The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds). |
### Transport Type Settings

<table>
<thead>
<tr>
<th>Transport Type</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Private Key Pass Phrase</strong> – The passphrase associated with the private key file.</td>
</tr>
<tr>
<td></td>
<td><strong>Private Key File</strong> – The filename of the private key file.</td>
</tr>
<tr>
<td></td>
<td><strong>Client Certificate</strong> – The client certificate to use. The default setting is “Default,” which uses the certificate that the MCS uses. Otherwise, type the filename of the client certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Server CA Bundle</strong> – File containing a list of root certificates.</td>
</tr>
<tr>
<td></td>
<td><strong>Verify Server Name</strong> – Whether to verify the server name. Either Yes or No. The default setting is No.</td>
</tr>
<tr>
<td></td>
<td><strong>c. Click OK.</strong></td>
</tr>
</tbody>
</table>

**Note**

Sample key files are provided in `/opt/connectemc/certs/` and `https-privatekey.pem`. Sample client certificates are provided in `/opt/connectemc/certs/` and `https-cert.pem`. Sample root certificate bundles are provided in `/opt/connectemc/certs/` and `https-ca-cert.pem`.

5. Click **OK** on the **Edit Primary/Secondary Transport** dialog box.

### Editing the notification transport

**Procedure**

1. In Avamar Administrator, select **Tools > Manage ConnectEMC**.

   The **Manage ConnectEMC** window appears.

2. Select **Notification Transport** and click **Edit**.

   The **Edit Notification Transport** dialog box appears.

3. From the **Notification Type** list, select one of the following types:

   - **On Success** — Notify recipients when an event file is successfully transferred to EMC.
   - **On Failure** — Notify recipients when an event file is not successfully transferred to EMC.
   - **On Success or Failure** — Notify recipients when an attempt is made to transfer an event file to EMC, regardless of the outcome.
   - **On All Failure** — Notify recipients when all attempts to transfer an event file to EMC have failed.

4. In the **SMTP Host (Email Server)** box, type the mail server hostname or IPv4 address.

5. In the **Email Address** box, type one or more recipients of these emails. Separate multiple email addresses with commas.

6. In the **Email Sender Address** box, type the email address from which the notification is sent.

7. (Optional) To specify advanced settings, click **Advanced** and then specify the settings in the **Edit Advanced Email Settings** dialog box:
a. In the **Retries** box, specify the number of retries to attempt before reporting a failure. The default setting is 5 retries.

b. In the **Timeout** box, specify the number of seconds to wait before reporting that the operation timed out. The default setting is 300 seconds (5 minutes).

c. In the **Description** box, specify the description of this transport that appears in the **Manage ConnectEMC** window. The default description is **Email Transport**.

d. In the **Email Subject** box, specify the subject line for the email. The default subject line is **Avamar ConnectEMC Notification Email**.

**NOTICE**

Do not change the email subject unless instructed to do so by EMC Customer Support. Email messages with other subject lines might be rejected by EMC spam filters.

e. From the **Email Format** list, select the format of the email, either ASCII or HTML. The default setting is ASCII.

f. Choose whether to include attachments sent to ConnectEMC in the notification email message by selecting or clearing the **Include CallHome Data** checkbox.

g. Click **OK**.

8. On the **Edit Notification Transport** dialog box, click **OK**.

Testing transports

**Procedure**

1. In Avamar Administrator, select **Tools > Manage ConnectEMC**.

   The **Manage ConnectEMC** window appears.

2. Click **Test**.

Verifying system integrity

To verify Avamar server integrity, you must first ensure that a validated server checkpoint exists.

You might also want to collect and examine the server log files to ensure that no errors have occurred since that checkpoint was performed. **Viewing Avamar server log files on page 199** provides instructions.

**Procedure**

1. In Avamar Administrator, click the **Server** launcher button.

   The **Server** window appears.

2. Click the **Server Management** tab.

3. Select the Avamar server name in the left pane.

4. Verify that the **Last validated checkpoint** field shows a recent calendar date.
CHAPTER 9

Capacity Management

This chapter includes the following topics:

- Viewing capacity utilization ................................................................. 210
- Capacity limits and thresholds ................................................................. 210
- Capacity forecasting ................................................................................ 211
- Viewing a graph of capacity utilization and forecasting .............................. 211
- Average daily change rates ...................................................................... 212
- Customizing capacity limits and behavior ................................................. 213
Viewing capacity utilization

You can view real-time capacity utilization information for a single server in Avamar Administrator or for multiple servers in Avamar Enterprise Manager.

Procedure

- In Avamar Administrator, capacity utilization information for a single Avamar server is available on the Capacity panel of the Avamar Administrator dashboard and on the Server Management tab in the Server window.
- In Avamar Enterprise Manager, consolidated capacity utilization information for all servers being monitored appears in the Dashboard. Capacity utilization information is also available on the information page for each server.

Capacity limits and thresholds

This following table describes how an Avamar server behaves as it crosses various consumed storage thresholds.

**Table 48 Capacity limits and thresholds**

<table>
<thead>
<tr>
<th>Storage utilization</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 75%</td>
<td>✔️</td>
<td>The system is considered to have adequate capacity to store future backups.</td>
</tr>
<tr>
<td>75%</td>
<td>!</td>
<td>You should study server storage utilization to determine if the server has adequate capacity to store future backups.</td>
</tr>
<tr>
<td>80%</td>
<td>!</td>
<td>A pop-up notification warns you that the server has consumed 80% of its available storage capacity. You should study server storage utilization to determine if the server has adequate capacity to store future backups.</td>
</tr>
<tr>
<td>90%</td>
<td>❌</td>
<td>You should study server storage utilization to determine if the server has adequate capacity to store future backups.</td>
</tr>
<tr>
<td>95%</td>
<td>❌</td>
<td>The server has reached the default health check limit, which is the amount of storage capacity that can be utilized and still have a “healthy” server. Backups that are in progress are allowed to complete, but all new backup activity is suspended by the dispatcher. A notification is sent in the form of a pop-up alert when you log in to Avamar Administrator. You must acknowledge that system event before any future backup activity can resume. You can customize the health check limit, but setting the limit higher than 95% is not recommended. <a href="#">Customizing capacity limits and behavior on page 213</a> provides instructions.</td>
</tr>
<tr>
<td>100%</td>
<td>❌</td>
<td>The server has reached the read-only limit and automatically becomes read-only to protect the integrity of the data already stored on the server.</td>
</tr>
</tbody>
</table>
Table 48 Capacity limits and thresholds (continued)

<table>
<thead>
<tr>
<th>Storage utilization</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>If ConnectEMC has been enabled, a Service Request (SR) is logged. Go to EMC Online Support to view existing SRs for the system. Search the knowledgebase for <em>Avamar User and OS Capacity Management solution esg118578</em>.</td>
</tr>
</tbody>
</table>

Capacity forecasting

To help you understand how quickly storage capacity is consumed, each server continuously tracks and analyzes the rate at which storage capacity is consumed, and projects how long you can continue to consume storage capacity at that rate. This forecasting occurs continuously in the background.

Capacity forecasting results for Avamar servers and configured Data Domain systems are available in Avamar Enterprise Manager on the **Dashboard** in the **Forecast** column for each system.

The following table describes the status icons that may appear in the **Forecast** column.

Table 49 Capacity forecast icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Capacity forecast for the Avamar server or Data Domain system</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>90 days or more storage capacity</td>
</tr>
<tr>
<td>❗</td>
<td>Less than 90 days of storage capacity</td>
</tr>
<tr>
<td>❌</td>
<td>Less than 30 days of storage capacity</td>
</tr>
</tbody>
</table>

**Note**

When an Avamar system rollback occurs, the historical capacity graph and report do not have any data from the date of the rollback to the checkpoint date. As a result, the graph shows a flat line and the capacity forecasting information and graph are skewed. In some cases, there is insufficient data to provide any information or graph at all. Forecasting information and graph become more accurate 30 days after the date of the rollback.

Viewing a graph of capacity utilization and forecasting

Avamar Enterprise Manager enables you to view a graph that provides both capacity utilization (that is, server storage capacity that has already been consumed) and capacity forecasting (that is, server storage capacity that is projected to be used in the future).

**Procedure**

1. In Avamar Enterprise Manager, place the mouse cursor over the **System** menu until a sub-menu appears, and then select **Capacity**.

   The **Capacity Utilization and Forecast** page appears.
2. From the **Systems** list, select the Avamar server for which to view capacity information.

3. To view capacity utilization and forecast data for one or more configured Data Domain systems, select the checkbox next to the Data Domain system name. Additional color-coded lines for each Data Domain system appear in the graph. The key below the graph provides details on the color coding.

4. (Optional) Customize the amount of capacity utilization data that appears:
   - To view data for a certain time period, select **Period** and then select the time period from the **Utilization for the** list.
   - To view data for a certain date range, select **Date Range** and then select the start and end dates from the **From Date** and **To Date** fields, respectively.

5. (Optional) Customize the amount of forecast data that appears by selecting a time period from the **Forecast out** list.

6. Click **Run**.

### Average daily change rates

When managing server capacity, it is useful to know the average daily change rate for both the server and for individual clients.

For example, the server average daily change rate can spike upward for a few days after you add several new clients, particularly database clients. This is to be expected. After a few days, data deduplication optimizes server storage efficiency, and the server daily change rate typically returns to normal.

However, if the server average daily change rate remains high for an extended period of time, it might be necessary to determine if this is due to one or more individual clients that might be experiencing less than expected data deduplication efficiencies.

### Viewing the average daily change rate for an Avamar server

**Procedure**

1. In Avamar Enterprise Manager, place the mouse cursor over the **System** menu until a sub-menu appears, and then select **Average Daily Change Rate > For Server**. The **Average Daily Change Rate For Server** page appears.

2. From the **Systems** list, select the Avamar server for which to view the average daily change rate.

3. (Optional) Customize the amount of data that appears:
   - To view data for a certain time period, select **Period** and then select the time period from the **Daily Average Change Rate for the** list.
   - To view data for a certain date range, select **Date Range** and then select the start and end dates from the **From Date** and **To Date** fields, respectively.

4. Click **Run**.

### Viewing the average daily change rate for clients

**Procedure**

1. In Avamar Enterprise Manager, place the mouse cursor over the **System** menu until a sub-menu appears, and then select **Average Daily Change Rate > For Clients with Maximum/Minimum rate/bytes**.
The Average Daily Change Rate For Client with maximum/minimum rate/bytes page appears.

2. From the Systems list, select the Avamar server for the clients.

3. From the Number of Clients list, select the number of clients for which to view daily change rate data.

4. Select Minimum or Maximum to specify whether to view clients with the lowest or highest daily change rate, respectively.

5. Select Rate to customize the display based on the percentage of new data, or New Bytes to customize the display based on the absolute capacity used.

6. (Optional) Customize the amount of data that appears:
   - To view data for a certain time period, select Period and then select the time period from the Daily Average Change Rate/New Bytes for the list.
   - To view data for a certain date range, select Date Range and then select the start and end dates from the From Date and To Date fields, respectively.

7. Click Run.
   The list of clients updates to match the selections.

8. Click a client name to display an average daily change rate graph for that client.

Customizing capacity limits and behavior

Edit the Avamar Administrator and Avamar Enterprise Manager preferences files to customize the settings that control capacity limits and system behavior.

Editing capacity settings for Avamar Administrator

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key

     c. When prompted, type the admin_key passphrase and press Enter.

2. Shut down the Management Console Server (MCS) by typing the following command:

    dpnctl stop mcs

3. Change directory by typing the following command:

    cd /usr/local/avamar/var/mc/server_data/prefs

4. Open mcservlet.xml in a text editor.

5. Find the com.avamar.mc.mcsm section of the preferences file.

6. Edit one or more of the following settings.
### Editing capacity settings for Avamar Enterprise Manager

**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

     ```bash
     ssh-agent bash
     ssh-add ~admin/.ssh/admin_key
     ```

2. Save the changes and close the file.

3. Start the MCS and the scheduler by typing:

   ```bash
   dpnctl start mcs
   dpnctl start sched
   ```
c. When prompted, type the `admin_key` passphrase and press Enter.

2. Shut down the Avamar Enterprise Manager Server (EMS) by typing the following command:
   ```bash
dpnctl stop ems
   ```

3. Change directory by typing the following command:
   ```bash
cd /usr/local/avamar/var/em/server_data/prefs
   ```

4. Open `emserver.xml` in a text editor.

5. Find the `com.avamar.mc.dashboard` section of the preferences file.

6. Edit one or more of the following settings.

<table>
<thead>
<tr>
<th>Preference</th>
<th>Description</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>capWarnPercent</td>
<td>When capacity usage reaches this percentage, the capacity state icon is yellow.</td>
<td>80%</td>
</tr>
<tr>
<td>capErrPercent</td>
<td>When capacity usage reaches this percentage, the capacity state icon is red.</td>
<td>95%</td>
</tr>
<tr>
<td>capForecastWarnDays</td>
<td>When forecasted capacity falls below this number of days, the capacity forecast icon is yellow.</td>
<td>90 days</td>
</tr>
<tr>
<td>capForecastErrDays</td>
<td>When forecasted capacity falls below this number of days, the capacity forecast icon is red.</td>
<td>30 days</td>
</tr>
</tbody>
</table>

7. Save the changes and close the file.

8. Restart the EMS by typing the following command:
   ```bash
dpnctl start ems
   ```
CHAPTER 10

Replication

This chapter includes the following topics:

- Overview of Avamar replication ................................................................. 218
- Configuring policy-based replication .......................................................... 222
- Configuring cron-based replication ............................................................ 229
- Performing on-demand replication ............................................................. 232
- Performing command line replication ......................................................... 233
- Monitoring replication ............................................................................... 244
- Canceling a replication activity ................................................................. 245
- Restoring replicated backup data ............................................................... 246
Overview of Avamar replication

The Avamar replication process copies client backups from a source Avamar server to a destination Avamar server. Replication enables you to avoid data loss if the source Avamar server fails because copies of the backups are available on the destination Avamar server.

Types of replication

Avamar supports both cron-based replication and policy-based replication. You can also log in to the Avamar server utility node and use the `avrepl` command line interface (CLI) to replicate data.

Policy-based replication

Policy-based replication provides granular control of the replication process. With policy-based replication, you create replication groups in Avamar Administrator to define the following replication settings:

- The members of the replication group, which are either entire domains or individual clients
- The priority for the order in which backup data replicates
- The types of backups to replicate based on the retention setting for the backup or the date on which the backup occurred
- The maximum number of backups to replicate for each client
- The destination server for the replicated backups
- The schedule for replication
- How long replicated backups are retained on the destination server

Cron-based replication

Cron-based replication was the only replication type until policy-based replication was introduced in Avamar 7.0. Cron-based replication has been deprecated in favor of policy-based replication, which is enabled by default on all new Avamar servers. Existing servers can continue to use the cron-based replication mechanism concurrently with or instead of policy-based replication.

With cron-based replication, you replicate backup data for all clients on the Avamar server. In Avamar Administrator, you can only limit cron-based replication to backups with a certain retention type. Cron-based replication occurs on daily at the time you specify when you configure replication.

Command line replication

The `avrepl` CLI enables you to perform on-demand replication from the command line. Command line replication also provides granular control of the replication process. Options for the `avrepl` command enable you to specify:

- The domains or clients to replicate
- The types of backups to replicate based on:
  - The plug-in used for the backup
  - The retention setting for the backup
  - The date on which the backup occurred
- The maximum number of backups to replicate for each client
The destination server for the replicated backups
How long replicated backups are retained on the destination server

Replication scheduling

You define the schedule for policy-based replication process by defining the same type of schedule that you use for scheduled backups. For cron-based replication, you define the daily start time and the maximum duration for replication. Command line replication occurs on-demand when you issue the `avrepl` command on the utility node of the Avamar server.

Defining a schedule for policy-based replication
Select Tools > Manage Schedules to open the Manage All Schedules window and configure schedules for policy-based replication. The schedules can automatically initiate replication on a daily, weekly, or monthly interval. You can also create an on-demand schedule that does not run automatically.

When you create a schedule, you define the start time and end time to control the duration during which replication can occur.

Defining a schedule for cron-based replication
When you configure cron-based replication, you define the daily start time and the timeout value, which controls the maximum duration for replication.

If you specify a timeout value when you first configure cron-based replication, recent backups might not replicate before the replication process times out. The timeout occurs because the cron-based replication process always replicates backups alphabetically by client name, and earliest backups before later backups. The default cron-based timeout setting is 72,000 seconds, or 20 hours.

You should regularly examine a sampling of recently replicated backups on the destination server to ensure that all backups are replicating. It is often necessary to increase the optional timeout value during the first few weeks of replication. As more data replicates to the destination server, greater levels of data deduplication and decreased transfer times occur. At that time, you can decrease the timeout value.

Do not perform normal source server background maintenance tasks such as checkpoint validation and garbage collection while replication is in progress.

Time zone considerations
When you schedule replication activities in Avamar Administrator or Avamar Enterprise Manager, the start time that appears is in the local time zone, not the time zone for the source or destination server.

For example, if you use Avamar Administrator in the Pacific time zone to configure replication to start at 8 p.m., and the replication source server is in the Eastern time zone, then the source server compensates for the three-hour difference between time zones and starts replication at 11 p.m.

Best practices for replication scheduling
Because only completed client backups are replicated, schedule replication during periods of low backup activity. This ensures that the greatest number of client backups replicate during each replication session.

In addition, optimize the size of each replication group for policy-based replication so that all clients replicate successfully during each scheduled replication operation. If a group grows to be too large, either edit the schedule to enable more time, or split the group into two smaller groups and schedule them to run separately.
Replication authentication

You must specify valid credentials for an account on the destination Avamar server when you configure either cron-based or policy-based replication. For command line replication, you must specify valid credentials for both the source and destination Avamar servers on the command line.

For policy-based replication, you specify the credentials when you add a replication destination on the Destinations tab in the Replication window.

For cron-based replication, you specify the credentials in the Destination User ID and Destination User Password boxes in the Replication cron job dialog box in Avamar Administrator or on the Replicator Setup page in Avamar Enterprise Manager.

For command line replication, specify the user account and password for the destination server by using the --[replscript]dstid and --dstpassword options. Use the --[avtar]id and --password options to specify the user account and password for the source server.

The repluser account is the default account on the source server for replication. When you use the repluser account for command line replication, omit the --[avtar]id option from the command and specify the password for the repluser account with the --password option. The EMC Avamar Product Security Guide provides a complete list of default accounts and passwords on the Avamar server.

Location of replicated backups on the destination server

On the destination server, replicated backups are available in the REPLICATE domain. This domain contains a mirrored representation of the source server client tree on the destination server.

In the following example figure, the avamar-1.example.com destination server contains both local clients and replicated backups from the avamar-2.example.com source server.

Figure 13 Example replication domain structure

All data in the REPLICATE domain is read-only. You can perform only the following operations on backups in the REPLICATE domain:

- Change the expiration date for a backup
- View backup statistics
- Delete a backup
Retention of replicated backups

When you replicate backups, the retention setting for the backup on the source server automatically applies to the replicated backup on the destination server. However, you can change the retention setting for the replicated backup.

For policy-based replication, you can specify a different retention setting for replicated backups on the Expiration page when you configure the replication group.

For command line replication, use the --avtar.expires option to specify a different retention setting for replicated backups.

You can also log in to the destination server in Avamar Administrator and manually change the expiration date after replication occurs. Changing the expiration date for a backup on page 112 provides instructions. Manually changing the expiration date after replication is the only way to edit retention for backups that replicate through cron-based replication.

Replication with Data Domain systems

The Avamar replication feature transfers data from a source Avamar server to a destination Avamar server. When you store Avamar backups on a Data Domain system, the replication process transfers Avamar data from the source Data Domain system to a destination Data Domain system.

Supported replication configurations

If the source Avamar server uses more than one Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. Also, if the source Avamar server uses a single Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. All of the data is replicated through DD Boost.

In a configuration with multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system by mapping a domain on the source Avamar server to a destination Data Domain system. You can also specify which Data Domain system is the default destination. The default destination is the Data Domain system to which Avamar replicates data when a destination Data Domain system is not identified on the Storage Mapping tab of the Replication window in Avamar Administrator. The EMC Avamar and EMC Data Domain System Integration Guide provides instructions on storage mapping and specifying the default destination Data Domain system.

Replication control

Avamar replicates Avamar data from the source Data Domain system to the destination Data Domain system by using DD Boost. The Data Domain replication feature is not used. You must have a Data Domain replication license to copy data from one system to another.

You configure and monitor replication on the Avamar server. There is no way to track replication by using Data Domain administration tools.

Avamar replicates the data directly from one Data Domain system to another. In other words, Avamar does not stage the data on the Avamar server before replicating the data to the destination Data Domain system.

Replication schedule

The replication of Avamar data on a Data Domain system occurs on the Avamar replication schedule. You cannot schedule replication of data on the Data Domain system separately from the replication of data on the Avamar server.
Restore of replicated backups

If the source Avamar server fails, you can restore replicated data from clients in the REPLICATE domain on the destination server to clients in other domains.

Restore of replicated backups on page 222 provides instructions.

Configuring policy-based replication

Procedure

1. Log in to the source server in Avamar Administrator.
2. Add a replication destination for each Avamar server to which you plan to replicate data.
3. Create a daily, weekly, or monthly schedule for when replication should occur. The process to create a replication schedule is the same process to create a backup schedule.
4. Create one or more replication groups to define the policy settings for replication.

When you create a replication group, you specify:
- The domains and clients that are members of the replication group
- The backup types and the number of backups to replicate
- The destination server to which the data replicates
- The schedule on which replication occurs for the replication group
- The amount of time that the backup data remains on the destination server before it is automatically deleted

Replication destinations

To enable policy-based replication, you must configure the replication destination on the source Avamar server. You specify the DNS name or IP address of the destination Avamar server, a common name (alias) for the server, the data port for communication with the server, and the username and password for authentication with the server.

Replication between servers of different versions is supported. However, for best results, ensure that the Avamar server software on the destination server is the same version or a newer version than the source Avamar server.

Adding a replication destination

Procedure

1. In Avamar Administrator, click the Replication launcher button.
   The Replication window appears.
2. Select the Destinations tab.
3. Select Actions > New Destination.
   The New Replication Destination dialog box appears.
4. In the Name box, type a short common name for the destination server.
5. In the Host/IP box, type the DNS name or IP address of the destination server.
6. From the Encryption list, select the encryption method for replication data transfers to the destination server.

7. In the Base Port box, specify the data port for communication with the destination server.

   The default port is 27000. Leave the default value unless you changed the Avamar client-server communication port setting on the destination server.

   If you selected High or Medium from the Encryption list, then an offset is applied to this base data port to facilitate connections through firewalls. The default offset is +2000. However, you can edit the offset by manually editing the secured_port_offset preference in mcserver.xml, and then restarting the MCS.

8. In the Username box, type repluser.

   Note
   The repluser account is the only user account that is known to work reliably on all destination servers.

9. In Password, type the password for the repluser account.

10. Click Verify Authentication to verify that the source Avamar server can authenticate with the destination server by using the specified settings.

   A results message appears.

11. Click OK.

12. If the verification succeeded, then click Save. Otherwise, edit the settings on the New Replication Destination dialog box and repeat the verification.

### Editing a replication destination

**Procedure**

1. In Avamar Administrator, click the Replication launcher button.

   The Replication window appears.

2. Click the Destinations tab.

3. Select the replication destination to edit.

4. Select Actions > Edit Destination.

   The Replication Destination dialog box appears.

5. Edit the settings for the replication destination.

   The settings are the same settings that you specified when you added the destination.

6. Click Save.

### Deleting a replication destination

When you delete a replication destination from the configuration on the source Avamar server, any data that you already replicated to the destination server remains on the destination server until the replicated backups expire or you delete the backups.

**Procedure**

1. In Avamar Administrator, click the Replication launcher button.

   The Replication window appears.

2. Click the Destinations tab.
3. Select the replication destination to delete.

4. Select **Actions** > **Delete Destination**.

   A confirmation message appears.

5. Click **Yes**.

### Replication groups

Replication groups enable you to define the settings for policy-based replication, including the domain and client members of the replication group, the backup types to replicate, the number of backups to replicate, the destination server, the replication schedule, and how long replicated backups are retained on the destination server.

You also specify the priority for which backup data replicates first. When you define the members of the replication group, the order in which members are listed in the **Member(s)** list controls the order in which backup data is replicated.

Backup data for a client replicates only once, even if a client is listed individually and is also a member of a domain in the **Member(s)** list.

In addition, if an individual client is a higher priority in the **Member(s)** list than the domain to which it belongs, then the backup data for the individual client replicates before the backup data for any other clients in the domain.

### Creating a replication group

**Before you begin**

- Add a destination Avamar server to the configuration on the source Avamar server.
- (Optional) Create a schedule for when replication for the group should occur. Creating a schedule on page 93 provides instructions.

**Procedure**

1. In Avamar Administrator, click the **Replication** launcher button. The **Replication** window appears.

2. Select the **Groups** tab.

3. Select **Actions** > **New Replication Group**.

   The **New Replication Group** wizard opens, starting with the **General** page.

4. Type a name for the replication group in the **Replication group name** box.

5. Choose whether to enable or disable replication for the replication group:

   - Select the **Disabled** checkbox to disable replication for the replication group.
   - Leave the checkbox clear to enable replication for the replication group.

6. From the **Encryption method** list, select the encryption setting for data transfers between the source and destination servers.

   The encryption technology and bit strength used for a connection depends on several factors, including the server platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

7. Click **Next**.

   The **Source** page appears.

8. Select the domains and clients that should be members of the replication group.
### Replication groups

<table>
<thead>
<tr>
<th>Replication group members</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>All clients</td>
<td>Select Replicate all client backups.</td>
</tr>
</tbody>
</table>
| Specific domains or clients | a. Select Choose specific client(s) and/or domain(s) to replicate.  
b. Click Choose Membership.  
The Replication Group Membership dialog box appears.  
c. Select the checkboxes next to the domains or clients to add to the replication group.  
Selected members appear in the Member(s) list.  
d. Set replication priority for the replication group members by controlling the order in which domains and clients appear in the Member(s) list.  
Select members in the list and use the up and down arrow buttons to change the order of the list.  
e. To remove a member from the replication group, select the member in the Member(s) list and click X.  
f. Click Finish. |

9. Select the backups to replicate as part of the replication group.

<table>
<thead>
<tr>
<th>Backups to replicate</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>All backups from all members of the replication group</td>
<td>Select Replicate all backups.</td>
</tr>
</tbody>
</table>
| Specific backups     | a. Select Include/exclude backups by type, date, and more.  
b. Click Change Filter.  
The Replication Filter Options dialog box appears.  
c. Select the type of backups to replicate: Daily, Weekly, Monthly, Yearly, or Not tagged.  
You must select at least one backup type.  
d. Specify the maximum number of backups to replicate for each client that is a member of the replication group.  
To replicate all backups (no maximum), select No limit.  
To replicate a certain number of the most recent backups for each member client, select backup(s) and then specify the maximum number in the list.  
e. Specify date restrictions for the backups to replicate for each client that is a member of the replication group.  
To replicate all backups regardless of when the backups occurred, select No Date Restrictions. |
<table>
<thead>
<tr>
<th>Backups to replicate</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To replicate only backups that occurred within a recent time period, select Last and then specify the number of past Day(s), Weeks(s), Month(s), or Year(s) to include.</td>
</tr>
<tr>
<td></td>
<td>To replicate only backups that occurred during a range of dates, select Range and then specify the start date and time in the From fields, the end date and time in the To fields, or both.</td>
</tr>
<tr>
<td></td>
<td>f. Click OK.</td>
</tr>
</tbody>
</table>

10. Click Next.

The Destination page appears.

11. Select the destination server from the Where would you like to replicate backups to? list.

You can also add a new destination server by selecting New Destination from the list, or edit the settings for a destination server by selecting the server from the list and then clicking Modify.

12. Click Next.

The Expiration page appears.

13. Specify when the replicated backups should expire on the destination server:
   - To expire the replicated backups at the current expiration setting, select Keep current backup expiration.
   - To expire the replicated backups at a different time than the current expiration setting, select Set expiration by backup type and then specify the number of days, weeks, months or years to retain each backup type.

   If a backup is of multiple types, then the expiration for the replicated backup is set to the specified value for the longest duration backup type. For example, if a backup is both a daily and a monthly backup, then the expiration for the replicated backup is set to the value that you specify for monthly backups.

14. Click Next.

The Schedule page appears.

15. Select the replication schedule from the How often would you like this replication to run? list.

You can also create a schedule by selecting New Schedule from the list, or edit the settings for a schedule by selecting the schedule from the list and then clicking Modify.

16. Click Next.

The Overview page appears.

17. Review the settings for the replication group.

18. (Optional) Specify plug-in options for the replication group:
   a. Click More Options.
   b. To replicate only backups from specific plug-ins, specify the numeric plug-in descriptor in the Include plug-in specific backups box.
Separate multiple entries with a comma, or leave the box empty to replicate all backups. Numeric plug-in descriptors on page 240 provides a list of numeric plug-in descriptors.

c. To exclude backups from specific plug-ins from replication, specify the numeric plug-in descriptor in the **Exclude plug-in specific backups** box. Separate multiple entries with a comma, or leave the box empty to replicate all backups.

d. From the **Informational message level** list, select the amount of informational messages to include in replication log files:

- Select **No informationals** to suppress all informational messages but include errors and warnings in the log files.
- Select **Some informationals** to provide some information messages in the log files in addition to errors and warnings.
- Select **Many informationals** to provide additional status information in the log files in addition to errors and warnings.
- Select **All informationals** to provide maximum information in the log files, including all informational messages, errors, and warnings.

e. Specify whether to include advanced timing and deduplication statistics in the replication log files by selecting or clearing the **Report advanced statistics** checkbox.

f. From the **Maximum concurrent processes** list, select the maximum number of clients to replicate simultaneously.

g. Select the **Show Advanced Options** checkbox to specify advanced options. The advanced options appear in red on the **More Options** dialog box.

h. To replicate only a specific backup, specify the backup sequence number in the **Backup sequence number** box or the backup label in the **Backup label** box. You must specify the complete backup sequence number or label.

i. To replicate backups that have a label that matches a specific pattern, specify the pattern in the **Backup label pattern** box.

j. From the **List contents being replicated** list, specify how much information about the replicated backups to include in the replication log files:

- **No file listing**
- **List file names**
- **List files and dates**

Use caution when including file information in the replication log files. Replication performance decreases, and the size of the log files can be very large.

k. To write maximum information to log files for debugging purposes, select the **Enable debugging messages** checkbox. The replication process generates very large log files.

l. To reduce network usage to a specified rate in megabits per second, specify the number of megabits in the **Network usage throttle** box.

Specify 0 (zero) for unrestricted network usage. Specify 0.772 to use 50 percent of a T1.

m. Click **OK**.
19. Click Finish.

Enabling and disabling a replication group

You can disable a replication group to prevent scheduled replications from occurring for that group. This is typically done to place the system in a state that supports maintenance activities. If you disable a replication group, you must re-enable the group to resume scheduled replications.

Procedure
1. In Avamar Administrator, click the Replication launcher button. The Replication window appears.
2. Select the Groups tab.
3. Select the replication group.
4. Select Actions > Disable Replication Group.
   If the group is enabled, then a check mark appears next to Disable Replication Group to indicate that the group has been disabled. If the group is disabled, then the check mark clears to indicate that the group has been disabled.
5. Click Yes on the confirmation message.

Editing a replication group

Procedure
1. In Avamar Administrator, click the Replication launcher button. The Replication window appears.
2. Select the Groups tab.
3. Select the replication group to edit.
   The Edit Replication Group wizard appears.
5. Edit the settings for the replication group.
   The settings are the same settings that you specified when you created the group.
6. Click OK.

Deleting a replication group

When you delete a replication group from the configuration on the source Avamar server, any data that you already replicated to the destination server for the group remains on the destination server until the replicated backups expire or you delete the backups.

Procedure
1. In Avamar Administrator, click the Replication launcher button. The Replication window appears.
2. Select the Groups tab.
3. Select the replication group to delete.
4. Select Actions > Delete Replication Group.
   A confirmation message appears.
5. Click Yes.
Configuring cron-based replication

You can configure cron-based replication in either Avamar Administrator or Avamar Enterprise Manager. Use Avamar Administrator to configure cron-based replication for a single Avamar server. Use Avamar Enterprise Manager to configure cron-based replication for multiple Avamar servers in an enterprise.

Cron-based replication was deprecated starting in Avamar 7.0 in favor of policy-based replication. Policy-based replication provides more granular control of the replication process. Avamar servers that were using cron-based replication before Avamar 7.0 can continue to use that replication method concurrently with or instead of policy-based replication.

Configuring cron-based replication with Avamar Administrator

Procedure

1. In Avamar Administrator, click the Administration launcher button. The Administration window appears.
2. Click the Services Administration tab.
3. Double-click the Replication cron job entry in the properties table.

The Replication cron job dialog box appears. The following read-only fields appear on the Replication cron job dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Current replication status. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Running — Scheduled replication operations are occurring normally.</td>
</tr>
<tr>
<td></td>
<td>• Not Running — Scheduled replication operations are not occurring normally.</td>
</tr>
<tr>
<td></td>
<td>• Not Running, Suspended — Scheduled replication operations are not occurring normally, and replication operations will not occur until replication resumes on this Avamar server.</td>
</tr>
<tr>
<td></td>
<td>• Running, Suspended — Replication operations were suspended while a replication job was running. When operations are resumed, this job will also resume from where it left off.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Indicates whether scheduled replication operations have been started (No) or stopped (Yes).</td>
</tr>
<tr>
<td>Configuration File</td>
<td>Location of the repl_cron.cfg configuration file, which stores replication settings for this Avamar system.</td>
</tr>
<tr>
<td>Configured</td>
<td>Indicates whether scheduled replication is configured on this source Avamar server.</td>
</tr>
<tr>
<td>Last started</td>
<td>Start time of the last replication operation.</td>
</tr>
<tr>
<td>Last completed</td>
<td>Elapsed time since last replication operation completed.</td>
</tr>
<tr>
<td>Last Status</td>
<td>Status of the last completed replication operation. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• None — Status for last replication operation is not available.</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Last replication operation successfully completed.</td>
</tr>
<tr>
<td>Failed</td>
<td>One or more errors were encountered during the last replication operation.</td>
</tr>
</tbody>
</table>

4. In the **Destination** box, specify the DNS name of the destination Avamar server.

Replication between servers of different versions is supported. However, for best results, ensure that the Avamar server software on the destination server is the same version or a newer version than the source Avamar server.

5. In the **Destination Directory: /REPLICATE/** box, specify the destination directory on the destination Avamar server for the replicated data.

   The default location is `/REPLICATE/source`, where `source` is the hostname of the source Avamar server. You can edit the destination directory. However, the destination must always exist under the `/REPLICATE` domain.

6. In the **Destination User ID** box, specify the Avamar administrative user account ID (`repluser`) that is used to log in to the destination Avamar server.

7. In the **Destination User Password** box, specify the password for the Avamar administrative user account ID (`repluser`).

   **NOTICE**

   If you change the password for the `replonly` account on the target server, then remember to update the **Destination User Password** value in the replication configuration on the source server.

8. In the **Timeout (seconds)** box, specify the maximum length of time that each replication operation should run.

9. In the **Bandwidth (Mbps)** box, specify the network utilization throttling setting that specifies the maximum average network utilization allowed in megabits per second (Mbps).

   If the replication operation exceeds this setting, it is “throttled back” by introducing delays until the average network utilization falls below the specified threshold.

10. In the **Work directory** box, specify the full path to the temporary folder or directory for replication log files.

11. To limit the replication operation to only backups that have been assigned a specific retention type, select the checkbox next to the retention type in the **Include backups with the following retention** section.

12. From the **Schedule** list, select the time of day at which to initiate replication, or select **Don't Run** to temporarily suspend replication.

13. Click **OK**.

### Configuring cron-based replication with Avamar Enterprise Manager

#### Before you begin

Add both the source and destination servers in Avamar Enterprise Manager. **Adding an Avamar system in Avamar Enterprise Manager on page 271** provides instructions.
Procedure

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Select Replicator > Setup.
   
   The Replicator Setup page appears.
3. Click the link for the source Avamar server in the Source column.
   
   A list of replication configuration fields appears below the table.
4. From the Destination list, select the destination Avamar server.
   
   Replication between servers of different versions is supported. However, for best results, ensure that the Avamar server software on the destination server is the same version or a newer version than the source Avamar server.
5. In the Destination Directory: /REPLICATE/ box, specify the destination directory on the destination Avamar server for the replicated data.
   
   The default location is /REPLICATE/source, where source is the hostname of the source Avamar server. You can edit the destination directory. However, the destination must always exist under the /REPLICATE domain.
6. In the Destination User ID box, specify the Avamar administrative user account ID (repluser) that is used to log in to the destination Avamar server.
7. In the Destination User Password box, specify the password for the Avamar administrative user account ID (repluser).

   NOTICE

   If you change the password for the replonly account on the target server, then remember to update the Destination User Password value in the replication configuration on the source server.
8. From the Schedule list, select the time of day at which to initiate replication, or select Don't Run to temporarily suspend replication.
9. From the Timeout list, select the maximum length of time that each replication operation should run.
10. In the Work directory box, specify the full path to the temporary folder or directory for replication log files.
11. In the Bandwidth (Mbps) box, specify the network utilization throttling setting that specifies the maximum average network utilization allowed in megabits per second (Mbps).

   If the replication operation exceeds this setting, it is “throttled back” by introducing delays until the average network utilization falls below the specified threshold.
12. In the Include backups with the following retention section, select the checkbox next to the retention types of the backups to replicate.
13. Specify the clients for which to replicate data.

<table>
<thead>
<tr>
<th>Clients</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>All clients</td>
<td>In the Replication type section, select Full.</td>
</tr>
<tr>
<td>Select clients</td>
<td>a. In the Replication type section, select Selective.</td>
</tr>
<tr>
<td></td>
<td>b. Choose whether to Exclude or Include certain clients in the replication process.</td>
</tr>
</tbody>
</table>
Performing on-demand replication

You can perform on-demand replication of a replication group when you use policy-based replication. An on-demand replication is a one-time replication of data for the replication group. You may want to perform an on-demand replication for the first replication of the replication group after you configure policy-based replication. You should also perform on-demand replication before system maintenance, software installations, or software upgrades.

You can initiate on-demand replication from either the Replication window or the Policy window.

Performing on-demand replication from the Replication window

Procedure
1. In Avamar Administrator, click the Replication launcher button.
   The Replication window appears.
2. Select the Groups tab.
3. Select the replication group.
4. Select Actions > Replicate Now.
   An On-Demand Replication Request dialog box indicates that the replication request was submitted.
5. Click Close.

Performing on-demand replication from the Policy window

Procedure
1. In Avamar Administrator, click the Policy launcher button.
   The Policy window appears.
2. Click the Policy Management tab.
3. Click the Groups tab.
4. Select the replication group from the list.
   Replication groups appear with a value of Replication in the Type column for the group.
5. Click Run.
   A confirmation message appears.
6. Click Close.
Performing command line replication

The avrepl command line interface (CLI) enables you to replicate data from a source Avamar server to a destination Avamar server.

The avrepl binary is located in the \usr\local\avamar\bin directory on the server utility node. You must log in as admin or root and run the command from that location.

Command reference

The following topics provide a reference for the operations and options that the avrepl command supports.

Synopsis

    avrepl --operation=replicate [options] [target]

Operations

The only supported operation for avrepl is --operation=replicate, which replicates data from the source Avamar server to a destination Avamar server.

Options

The options that you specify with the avrepl command enable you to control replication behavior.

Account options

Account options for the avrepl command enable you to specify credentials to connect to the destination Avamar server for replication.

The following account options are available for the avrepl command.

Table 50 Account options for the avrepl command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--account=location</td>
<td>Specifies a hierarchical location on the destination Avamar server. This option is relative to the current home location, unless you use a slash (/) as a prefix to the path designation, in which case an absolute path is assumed. The default account is REPLICATE.</td>
</tr>
<tr>
<td>--acnt=location</td>
<td></td>
</tr>
<tr>
<td>--path=location</td>
<td></td>
</tr>
<tr>
<td>--[replscript]dstaddr=destination_server</td>
<td>Specifies the DNS name or IP address of the destination Avamar server. Replication between servers of different versions is supported. However, for best results, ensure that the Avamar server software on the destination server is the same version or a newer version than the source Avamar server.</td>
</tr>
<tr>
<td>--[replscript]dstid=repluser</td>
<td>Specifies the Avamar user ID and domain to use for authentication on the destination Avamar server.</td>
</tr>
</tbody>
</table>

Note

The repluser account is the only user account that is known to work reliably on all destination servers.
### Table 50 Account options for the avrepl command (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--dstpassword=password</code></td>
<td>Specifies the password for repluser account on the destination Avamar server.</td>
</tr>
<tr>
<td><code>--dstap=password</code></td>
<td></td>
</tr>
<tr>
<td><code>--dstpswd=password</code></td>
<td></td>
</tr>
<tr>
<td><code>--[replscript]dstpath=domain</code></td>
<td>Specifies a location (domain) on the destination Avamar server to store replicated source data. The default value is the top-level directory (/), which stores the replicated data in a new domain named for the source Avamar server. You must use this option with the <code>--[replscript]srcpath</code> option. You cannot use this option with the <code>--[replscript]dpnname</code> option.</td>
</tr>
<tr>
<td><code>--[replscript]dstport=port</code></td>
<td>Specifies the data port to use when connecting to the destination Avamar server. The default value is 27000.</td>
</tr>
<tr>
<td><code>--hfsadd=Avamar_server</code></td>
<td></td>
</tr>
<tr>
<td><code>--server=Avamar_server</code></td>
<td></td>
</tr>
<tr>
<td><code>--[avtar]id=user@auth</code></td>
<td>Specifies the Avamar user ID and authentication system to use for authentication on the source Avamar server. The default value is repluser, which is the default replication user account on the Avamar server. To authenticate with the Avamar authentication system, specify avamar for auth. For example: <code>--[avtar]id=jdoe@avamar</code>.</td>
</tr>
<tr>
<td><code>--password=password</code></td>
<td></td>
</tr>
<tr>
<td><code>--ap=password</code></td>
<td></td>
</tr>
<tr>
<td><code>--pswd=password</code></td>
<td></td>
</tr>
</tbody>
</table>

### Logging options

Logging options for the avrepl command enable you to specify the path and file name for the avrepl log file, and to control how much information the plug-in writes to the log file.

The following logging options are available for the avrepl command.

### Table 51 Logging options for the avrepl command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--[avtar]informationals=n</code></td>
<td>Sets the information level for status messages, where n is a number such as 0, 1, 2, and so on.</td>
</tr>
<tr>
<td>`--[avtar]noinformationals=True</td>
<td>Specify true to disable all status messages.</td>
</tr>
<tr>
<td>`--[avtar]statistics=True</td>
<td>Specify true to include advanced timing and deduplication statistics in the replication log files.</td>
</tr>
</tbody>
</table>
**Table 51 Logging options for the avrepl command (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--log=file</td>
<td>Specifies the full path and file name of the avrepl plug-in log file.</td>
</tr>
<tr>
<td>--logfile=file</td>
<td></td>
</tr>
<tr>
<td>--nostream={true</td>
<td>false}</td>
</tr>
<tr>
<td>--nowarnings={true</td>
<td>false}</td>
</tr>
<tr>
<td>--quiet={true</td>
<td>false}</td>
</tr>
<tr>
<td>--verbose</td>
<td>Specify either --verbose or --v to enable all messages, including status and warning messages. Specify --verbose=n to control the level of verbosity. The default value is --verbose=6.</td>
</tr>
<tr>
<td>--v</td>
<td></td>
</tr>
</tbody>
</table>

**Replication options**

Replication options for the avrepl command enable you to control replication functionality, such as which backups should replicate and how long to retain replicated backups on the destination server.

The following replication options are available for the avrepl command.

**Table 52 Replication options for the avrepl command**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--[avtar]after=timestamp</td>
<td>Specifies that only backups matching timestamp and later should be replicated. For timestamp, use 24 hour local timezone values that conform to the syntax yyyy-mm-dd hh:mm:ss. You can use partial timestamp values. The resolution is truncated to the last supplied value. For example, 2014-02 is equivalent to 2014-02-01 00:00:00. You can also use this option with --[avtar]before=timestamp to define a range of effective dates. Only backups that occurred within the date range are replicated.</td>
</tr>
<tr>
<td>--[avtar]allsnapups={true</td>
<td>false}</td>
</tr>
<tr>
<td>--[avtar]before=timestamp</td>
<td>Specifies that only backups that occurred before timestamp should be replicated. For timestamp, use 24 hour local timezone values that conform to the syntax yyyy-mm-dd hh:mm:ss.</td>
</tr>
</tbody>
</table>
### Table 52 Replication options for the `avrepl` command (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can use partial <code>timestamp</code> values. The resolution is truncated to the last supplied value. For example, 2014-02 is equivalent to 2012-02-01 00:00:00. You can also use this option with <code>--[avtar]after=timestamp</code> to define a range of effective dates. Only backups that occurred within the date range are replicated.</td>
<td></td>
</tr>
<tr>
<td><code>--[avtar]count=n</code></td>
<td>Limits replicated backups to this maximum number (<code>n</code>) of most recent backups for each client.</td>
</tr>
<tr>
<td><code>--[avtar]exclude-pluginid-list=list</code></td>
<td>Excludes backups performed with the specified plug-in, where <code>list</code> is a comma-separated list of plug-in IDs.</td>
</tr>
<tr>
<td>`--[avtar]expires=(n</td>
<td>period</td>
</tr>
<tr>
<td>- A number of days (<code>n</code>).</td>
<td></td>
</tr>
<tr>
<td>- An expiration <code>period</code> as a specific number of days, weeks, months, or years.</td>
<td></td>
</tr>
<tr>
<td>To specify a period, use one of the following values:</td>
<td></td>
</tr>
<tr>
<td><code>days=n</code></td>
<td></td>
</tr>
<tr>
<td><code>weeks=n</code></td>
<td></td>
</tr>
<tr>
<td><code>months=n</code></td>
<td></td>
</tr>
<tr>
<td><code>years=n</code></td>
<td></td>
</tr>
<tr>
<td>where <code>n</code> is a positive integer. For example, supply <code>--[avtar]expires=years=2</code> to retain replicated backups for two years on the destination server. Also, <code>--[avtar]expires=30</code> and <code>--[avtar]expires=days=30</code> are equivalent.</td>
<td></td>
</tr>
<tr>
<td>- A <code>timestamp</code> for the date and time at which the replicated backup expires. Use 24 hour local timezone values that conform to the syntax <code>yyyy-mm-dd hh:mm:ss</code>. You can use partial <code>timestamp</code> values. The resolution is truncated to the last supplied value. For example, 2014-02 is equivalent to 2014-02-01 00:00:00.</td>
<td></td>
</tr>
<tr>
<td><code>--[avtar]pluginid-list=list</code></td>
<td>Replicates only backups performed with the specified plug-ins, where <code>list</code> is a comma-separated list of plug-in IDs.</td>
</tr>
<tr>
<td>`--[avtar]retention-type={daily</td>
<td>weekly</td>
</tr>
<tr>
<td>- daily</td>
<td></td>
</tr>
<tr>
<td>- weekly</td>
<td></td>
</tr>
<tr>
<td>- monthly</td>
<td></td>
</tr>
<tr>
<td>- yearly</td>
<td></td>
</tr>
<tr>
<td>- none</td>
<td></td>
</tr>
<tr>
<td>If you supply <code>none</code>, then only backups without a specific retention type are replicated.</td>
<td></td>
</tr>
</tbody>
</table>
Table 52 Replication options for the `avrepl` command (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--replscript dpnname=source_server</code></td>
<td>Specifies a name to use to represent the source Avamar server (<code>source_server</code>) as part of the path for the replicated files in the <code>REPLICATE</code> domain on the destination server. Specify the fully qualified domain name of the source server. You cannot use this option with the <code>--replscript dstpath</code> or <code>--replscript srcpath</code> options.</td>
</tr>
<tr>
<td>`--replscript dstencrypt={ssl</td>
<td>tls}`</td>
</tr>
<tr>
<td><code>--replscript srcpath=domain</code></td>
<td>Specifies a location (<code>domain</code>) on the source Avamar server from which to begin replication. Only data within this location is replicated. The default setting is the top-level domain (<code>/</code>), which replicates the entire server. You must use this option with the <code>--replscript dstpath</code> option. You cannot use this option with the <code>--replscript dpnname</code> option.</td>
</tr>
</tbody>
</table>
| `--backup-type=type` | Replicates only the specified type of backup, where `type` is one of the following values:  
  - differential  
  - differential_full  
  - incremental  
  - incremental_full  
  - level0_full  
  - synthetic_full |
| `--within={days | weeks | months | years}=n` | Replicates backups that occurred within this most recent `days`, `weeks`, `months`, or `years`, where `n` is a positive integer. For example, supply `--within=months=3` to replicate three months' worth of backups for each client. |

Avamar-only options

Avamar-only options access advanced functionality that is normally reserved for use by EMC personnel only. Misuse of these advanced options can cause loss of data. If you are unsure about any aspect of these options, contact EMC Customer Support for additional information before using them.

The following Avamar-only options are available for the `avrepl` command.

Table 53 Avamar-only advanced options for the `avrepl` command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--bindir=path</code></td>
<td>Specifies the directory that contains Avamar binary files. The default value is <code>/usr/local/avamar/bin</code>.</td>
</tr>
<tr>
<td>`--[avtar] exp-delta={days</td>
<td>weeks</td>
</tr>
</tbody>
</table>
### Table 53 Avamar-only advanced options for the `avrepl` command (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `--[avtar]expiration-policy=type=period`    | Replicates backups of a specific retention `type` within the specified `period`, where `type` is one of the following values:  
  - dailies  
  - weeklies  
  - monthlies  
  - yearlies  
  and `period` is one of the following values:  
  - days=`n`  
  - weeks=`n`  
  - months=`n`  
  - years=`n`  
  and `n` is a positive integer.  
  For example, supply `--[avtar]expiration-policy=dailies=years=2` to replicate two years’ worth of daily backups for each client.  
  The `--[avtar]expiration-policy` option takes precedence over `--[avtar]expires`. |
| `--[avtar]label=name`                       | Specifies the labels of the backups to replicate. Separate multiple values with a comma.                                                                                                                     |
| `--[avtar]label-pattern=pattern`           | Replicates backups with a label that matches the specified `pattern`. Common glob operators (wildcards) such as asterisk (*) and question mark (?) are allowed.  
  Separate multiple patterns by commas, such as `--[avtar]label-pattern=temp,tmp`. You can also specify the `--[avtar]label-pattern` option multiple times in a single command. |
| `--[avtar]sequencenumber=n`                 | Specifies the sequence number of the backup to replicate. Separate multiple entries with a comma.                                                                                                         |
| `--[avtar]labelnumber=n`                    |                                                                                                                                                                                                             |
| `--[avtar]throttle=n`                       | Controls the rate at which the underlying `avtar` process sends data to the server. If you specify this option, `avtar` pauses as long as necessary after sending each packet to ensure that network usage does not exceed the specified maximum bandwidth in megabits per second (Mbps).  
  For example, `--[avtar]throttle=5` uses half of a 10 Mbps connection, and `--[avtar]throttle=0.772` restricts usage to half of a T1 link. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--[replscript]exclude=pattern</code></td>
<td>Excludes domains or clients that contain <code>pattern</code> from replication, where <code>pattern</code> is a matching pattern in the domain or client name. Common glob operators (wildcards) such as asterisk (*) and question mark (?) are allowed. For example, specify <code>--[replscript]exclude=spot</code> to exclude any domain or client with a name that contains the pattern <code>spot</code>. Specify <code>--[replscript]exclude=/clients/</code> to exclude all clients in the <code>/clients</code> domain. Separate multiple patterns by commas, such as <code>--[replscript]exclude=spot,/clients/</code>. You can also specify the <code>--[replscript]exclude</code> option multiple times in a single command to specify more than one pattern.</td>
</tr>
<tr>
<td>`--[replscript]forcecreate={true</td>
<td>false}`</td>
</tr>
<tr>
<td>`--[replscript]force-move={1</td>
<td>0}`</td>
</tr>
<tr>
<td>`--[replscript]fullcopy={true</td>
<td>false}`</td>
</tr>
<tr>
<td>`--[replscript]globalcid={true</td>
<td>false}`</td>
</tr>
<tr>
<td>`--[replscript]reportonly={true</td>
<td>false}`</td>
</tr>
<tr>
<td>`--[replscript]restore={true</td>
<td>false}`</td>
</tr>
<tr>
<td><code>--[replscript]small-client-mb=n</code></td>
<td>Threshold in MB before which the new data for a client is considered “small.” The default setting is 128 MB of new data. Specify <code>0</code> to disable this optimization.</td>
</tr>
</tbody>
</table>
| `--rechunk={disable | enable | default}` | Controls whether replicated data should be rechunked to maximize data deduplication on the destination server. Use one of the following values:  
  - **disable** — Do not rechunk data before storing on the destination server.  
  - **enable** — Rechunk data before storing on the destination server to maximize data deduplication. |
Table 53 Avamar-only advanced options for the `avrepl` command (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• default — Automatically rechunk data when source and destination server chunking parameters are different.</td>
<td></td>
</tr>
</tbody>
</table>

Help option

The `--help` option displays a list of available options for the `avrepl` command:

`avrepl --help`

Version option

The `--version` option displays the software version of the `avrepl` command:

`avrepl --version`

Target list

To replicate specific clients or Avamar domains, include a list of the clients and domains at the end of the `avrepl` command. Separate multiple entries with a space.

If you do not supply a list, then the replication includes all client backups on the source Avamar server.

Numeric plug-in descriptors

Some command options require one or more numeric plug-in descriptors as values. Valid numeric plug-in descriptors are listed in the following table.

Table 54 Numeric plug-in descriptors

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Plug-in name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Linux <em>avagent</em></td>
</tr>
<tr>
<td>1001</td>
<td>Linux <em>avtar</em></td>
</tr>
<tr>
<td>1002</td>
<td>Linux Oracle RMAN</td>
</tr>
<tr>
<td>1003</td>
<td>Linux NDMP</td>
</tr>
<tr>
<td>1009</td>
<td>Linux DB2</td>
</tr>
<tr>
<td>1014</td>
<td>Linux Lotus</td>
</tr>
<tr>
<td>1016</td>
<td>Linux VMware image</td>
</tr>
<tr>
<td>1019</td>
<td>Linux VMware File Level Restore (FLR)</td>
</tr>
<tr>
<td>1024</td>
<td>Linux extended retention</td>
</tr>
<tr>
<td>1025</td>
<td>Linux extended retention restore</td>
</tr>
<tr>
<td>1029</td>
<td>Linux Sybase</td>
</tr>
<tr>
<td>1030</td>
<td>Linux SAP</td>
</tr>
<tr>
<td>1034</td>
<td>Linux extended retention import</td>
</tr>
</tbody>
</table>
Table 54 Numeric plug-in descriptors (continued)

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Plug-in name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1035</td>
<td>Linux VDR Migration</td>
</tr>
<tr>
<td>1038</td>
<td>Linux VMware image restore</td>
</tr>
<tr>
<td>1039</td>
<td>Linux vApp image</td>
</tr>
<tr>
<td>2000</td>
<td>Oracle Solaris avagent</td>
</tr>
<tr>
<td>2001</td>
<td>Oracle Solaris avtar</td>
</tr>
<tr>
<td>2002</td>
<td>Oracle Solaris RMAN</td>
</tr>
<tr>
<td>2009</td>
<td>Oracle Solaris DB2</td>
</tr>
<tr>
<td>2014</td>
<td>Oracle Solaris Lotus</td>
</tr>
<tr>
<td>2029</td>
<td>Oracle Solaris Sybase</td>
</tr>
<tr>
<td>2030</td>
<td>Oracle Solaris SAP</td>
</tr>
<tr>
<td>3000</td>
<td>Windows avagent</td>
</tr>
<tr>
<td>3001</td>
<td>Windows avtar</td>
</tr>
<tr>
<td>3002</td>
<td>Windows Oracle RMAN</td>
</tr>
<tr>
<td>3004</td>
<td>Windows Exchange message</td>
</tr>
<tr>
<td>3005</td>
<td>Windows Exchange database</td>
</tr>
<tr>
<td>3006</td>
<td>Windows SQL</td>
</tr>
<tr>
<td>3009</td>
<td>Windows DB2</td>
</tr>
<tr>
<td>3011</td>
<td>Windows Exchange 2007 database</td>
</tr>
<tr>
<td>3012</td>
<td>Windows Exchange 2007 web</td>
</tr>
<tr>
<td>3014</td>
<td>Windows Lotus</td>
</tr>
<tr>
<td>3015</td>
<td>Windows VSS</td>
</tr>
<tr>
<td>3016</td>
<td>Windows VMware image</td>
</tr>
<tr>
<td>3017</td>
<td>Windows MOSS</td>
</tr>
<tr>
<td>3018</td>
<td>Windows Exchange VSS</td>
</tr>
<tr>
<td>3019</td>
<td>Windows VMware File Level Restore (FLR)</td>
</tr>
<tr>
<td>3026</td>
<td>Windows MOSS VSS</td>
</tr>
<tr>
<td>3027</td>
<td>Windows Exchange Granular Level Restore (GLR)</td>
</tr>
<tr>
<td>3028</td>
<td>Windows MOSS Granular Level Restore (GLR)</td>
</tr>
<tr>
<td>3029</td>
<td>Windows Sybase</td>
</tr>
<tr>
<td>3030</td>
<td>Windows SAP</td>
</tr>
<tr>
<td>3032</td>
<td>Windows Hyper-V VSS</td>
</tr>
<tr>
<td>3033</td>
<td>Windows Hyper-V Granular Level Restore (GLR)</td>
</tr>
<tr>
<td>3036</td>
<td>Windows cluster file system</td>
</tr>
</tbody>
</table>
Table 54 Numeric plug-in descriptors (continued)

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Plug-in name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3041</td>
<td>Windows VMware Granular Level Restore (GLR)</td>
</tr>
<tr>
<td>4000</td>
<td>HP-UX avagent</td>
</tr>
<tr>
<td>4001</td>
<td>HP-UX avtar</td>
</tr>
<tr>
<td>4002</td>
<td>HP-UX Oracle RMAN</td>
</tr>
<tr>
<td>4009</td>
<td>HP-UX DB2</td>
</tr>
<tr>
<td>4029</td>
<td>HP-UX Sybase</td>
</tr>
<tr>
<td>4030</td>
<td>HP-UX SAP</td>
</tr>
<tr>
<td>5000</td>
<td>IBM AIX avagent</td>
</tr>
<tr>
<td>5001</td>
<td>IBM AIX avtar</td>
</tr>
<tr>
<td>5002</td>
<td>IBM AIX Oracle RMAN</td>
</tr>
<tr>
<td>5009</td>
<td>IBM AIX DB2</td>
</tr>
<tr>
<td>5014</td>
<td>IBM AIX Lotus</td>
</tr>
<tr>
<td>5029</td>
<td>IBM AIX Sybase</td>
</tr>
<tr>
<td>5030</td>
<td>IBM AIX SAP</td>
</tr>
<tr>
<td>6000</td>
<td>Mac OSX avagent</td>
</tr>
<tr>
<td>6001</td>
<td>Mac OSX avtar</td>
</tr>
<tr>
<td>7003</td>
<td>NetApp NDMP</td>
</tr>
<tr>
<td>8003</td>
<td>EMC Celerra NDMP</td>
</tr>
<tr>
<td>10000</td>
<td>Novell NetWare avagent</td>
</tr>
<tr>
<td>10001</td>
<td>Novell NetWare avtar</td>
</tr>
<tr>
<td>10003</td>
<td>Novell NetWare NDMP</td>
</tr>
<tr>
<td>11000</td>
<td>FreeBSD avagent</td>
</tr>
<tr>
<td>11001</td>
<td>FreeBSD avtar</td>
</tr>
<tr>
<td>12000</td>
<td>SCO OpenServer avagent</td>
</tr>
<tr>
<td>12001</td>
<td>SCO OpenServer avtar</td>
</tr>
<tr>
<td>13000</td>
<td>SCO UnixWare avagent</td>
</tr>
<tr>
<td>13001</td>
<td>SCO UnixWare avtar</td>
</tr>
<tr>
<td>14003</td>
<td>EMC Isilon NDMP</td>
</tr>
</tbody>
</table>
CLI examples

Review the avrepl command examples for details on how to use options to control replication behavior.

You must specify the following options with the avrepl command:

Table 55 Required options for the avrepl command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--operation=replicate</td>
<td>Command operation for avrepl.</td>
</tr>
<tr>
<td>--[replscript]dpnname=source_server</td>
<td>Fully qualified domain name of the source Avamar server.</td>
</tr>
<tr>
<td>--[avtar]id=user@auth</td>
<td>User account for the source Avamar server. The default value is repluser. To use the repluser account, you can omit --[avtar]id and specify only the password for the repluser account with the --password option.</td>
</tr>
<tr>
<td>--password=password</td>
<td>Password for the user account on the source Avamar server.</td>
</tr>
<tr>
<td>--[replscript]dstaddr=destination_server</td>
<td>Destination Avamar server.</td>
</tr>
<tr>
<td>--[replscript]dstid=repluser</td>
<td>Specifies the Avamar user ID and domain to use for authentication on the destination Avamar server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The repluser account is the only user account that is known to work reliably on all destination servers.</td>
</tr>
<tr>
<td>--dstpassword=password</td>
<td>Specifies the password for repluser account on the destination Avamar server.</td>
</tr>
<tr>
<td>--dstap=password</td>
<td></td>
</tr>
<tr>
<td>--dstpswd=password</td>
<td></td>
</tr>
</tbody>
</table>

If the firewall is installed and enabled on the destination server, then you must also specify the --[replscript]dstencrypt option with the correct encryption method, which is either ssl or tls.

Replicating all client backups

The following command replicates all client backups from the avamar-1.example.com source server to the replication-server-1.example.com destination server. The user account on the source server is jdoe@avamar (the jdoe user account with the Avamar internal authentication system), and the password is password. The user account on the destination server is repluser, and the password is password.

```
avrepl --operation=replicate -- [replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --dstpassword=password --dstap=password --dstpswd=password
```
Replicating backups for specific clients or domains
The following command replicates all backups for the client1 and client2 clients, as well as for all clients in the domain3 domain.

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
password=password --[replscript]dstaddr=replication-server-1.example.com --
dstid=repluser --dstpassword=password --[replscript]dstencrypt=ssl client1 client2
```

Replicating specific types of backups
The following command replicates all full (level 0) backups that occurred after February 1, 2014 for the client1 and client2 clients.

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
ap=password --[replscript]dstaddr=replication-server-1.example.com --
[replscript]dstid=repluser --dstpassword=password --
[replscript]dstencrypt=ssl --[avtar]after=2014-02-01 --backup-type=level0_full client1 client2
```

Monitoring replication

You can monitor replication to ensure that replication is completing successfully and to troubleshoot issues.

The Activity Monitor in Avamar Administrator enables you to view status information for both on-demand and scheduled replication activity, including both policy-based and cron-based replication.

The Replicator Status page in Avamar Enterprise Manager enables you to view status information for cron-based replication only.

Monitoring replication in Avamar Administrator

**Procedure**
1. In Avamar Administrator, click the Activity launcher button. The Activity window appears.
2. Click the Activity Monitor tab. A list of all activities appears.
3. To filter the results to display only replication activity, select Actions > Filter. The Filter Activity dialog box appears.
4. Select All Replication Source & Destination from the Type list.
5. Click OK.
6. To view statistics for a replication activity, select the activity and then select Actions > View Statistics. The Replicate Statistics dialog box appears. The Details tab provides detailed information from the v_repl_activities database view. The Backups tab
provides a list of backups that were included in the replication operation. The Errors tab shows any errors that occurred during the replication operation.

7. Click Close.

Monitoring cron-based replication in Avamar Enterprise Manager

Procedure

1. Open a web browser and log in to Avamar Enterprise Manager.

2. Select Replicator > Status.

The Replicator Status page appears. The following table lists the information that appears on the Replicator Status page for each Avamar system.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>DNS name of the source Avamar server.</td>
</tr>
</tbody>
</table>
| Status     | Current replication status. One of the following values:  
  - Running — Scheduled replication operations are occurring normally.  
  - Not Running — Scheduled replication operations are not occurring normally.  
  - Not Running and Suspended — Scheduled replication operations are occurring normally, and no future replication operations will occur until replication resumes on this Avamar server. |
| Suspended  | Whether scheduled replication operations have been started (No) or stopped (Yes). |
| Destination| DNS name of the destination Avamar server. |
| Schedule   | Hour of the day that replication is scheduled to occur, or Don’t Run if replication is temporarily suspended. |
| Last Completed | Elapsed time since the last replication operation completed. |
| Last Status | Status of the last completed replication operation. One of the following values:  
  - None — Status for the last replication operation is not available.  
  - Success — The last replication operation successfully completed.  
  - Failed — One or more errors were encountered during the last replication operation. |

Canceling a replication activity

You can cancel a policy-based or cron-based replication activity in the Activity Monitor any time before it completes. The cancellation might take five minutes or longer. The replication may complete before the cancellation finishes.

You can also cancel a cron-based replication activity on the Replicator Status page in Avamar Enterprise Manager by selecting the checkbox next to the source server and then clicking Stop Replication. The process cancels any replication operation that is currently in progress if that replication operation was initiated using Avamar Enterprise Manager. However, if the replication operation was initiated by way of a cron mechanism and you stop replication on that server, then the replication operation runs to completion.
Procedure
1. In Avamar Administrator, click the Activity launcher button.
   The Activity window appears.
2. Click the Activity Monitor tab.
   A list of all activities appears.
3. Select the replication activity from the list.
4. Select Actions > Cancel Activity.
   A confirmation message appears.
5. Click Yes.

Restoring replicated backup data
If the source Avamar server fails, you can restore replicated data from a client in the REPLICATE domain on the destination server to a client in another domain.

Procedure
1. Register the client with the destination Avamar server that manages the replicated data to restore:
   a. On a Windows client, right-click the Avamar system tray icon and select Manage > Activate Client.
      The Activate Client Setup dialog box appears.
   b. Type the hostname of the destination Avamar server in the Administrator Server Address box.
   c. Type 28001 in the Administrator Server Port box.
   d. Type the Avamar domain for the client in the Client Domain box.
   e. Click Activate.
      Client registration on page 52 provides instructions for other registration methods.
      You can also use Avamar Client Manager to activate clients with the destination server.
      Moving a client to a new server on page 313 provides instructions.
2. In Avamar Administrator, click the Backup & Restore launcher button.
   The Backup, Restore and Manage window appears.
3. Click the Restore tab.
   The upper left pane contains a list of domains.
4. Select the REPLICATE domain, and then select the hostname of the source Avamar server.
5. Select the domain that contains the client.
6. Select the client from the list.
7. Click the By Date tab or the By File/Folder tab and select the data to restore.

Note
Restoring data from a backup on page 118 provides alternate methods to find a backup and perform a restore.
8. Select **Actions** \(\rightarrow\) **Restore Now**.

   The **Restore Options** dialog box appears.

9. Click **Browse** next to the **Restore Destination Client** box, and then browse to and select the destination client.

   Do not select a client in the **REPLICATE** domain. The client must be listed in either the **clients** domain or another domain on the Avamar server.

10. Select the plug-in to use for the restore from the **Restore Plug-in** list.

11. From the **Avamar encryption method** list, select an encryption method for client/server data transfer during the restore.

   **Note**

   The encryption technology and bit strength for a client/server connection depend on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

12. Select either **Restore everything to a different location** or **Restore everything to multiple locations**.

13. Click **Set Destination** below the **Items Marked for Restore** list, and then select the destination path(s) for the data to restore.

14. To include plug-in options with this restore, click **More Options**, and then configure the settings.

15. Click **OK** on the **Restore Options** dialog box.

   The **Restore Request** dialog box indicates that the restore was initiated.

16. Click **Close**.

17. (Optional) Re-register the client with the source Avamar server.
Replication
CHAPTER 11
Server Updates and Hotfixes

This chapter includes the following topics:

- Overview of the Avamar server software update process........................................250
- Installing and configuring the Avamar Downloader Service.....................................252
- Downloading new packages from the EMC repository........................................256
- Managing the Avamar Downloader Service............................................................257
- Troubleshooting Avamar Downloader Service issues..............................................259
- Downloading and installing packages on the Avamar server..................................260
- Viewing a list of installation packages on the Avamar server.................................261
- Deleting packages from the Avamar server............................................................262
- Viewing the history of installations.......................................................................263
Overview of the Avamar server software update process

EMC periodically provides updates and hotfixes for the Avamar server software. EMC stores these update and hotfix packages in the EMC repository. The Avamar Downloader Service enables you to download the installation packages to a local Windows server and then push the packages to an Avamar server. Then you can use the System Maintenance feature in Avamar Enterprise Manager or Avamar Installation Manager to install the packages on the Avamar server.

This process minimizes network bandwidth usage by enabling you to download files from the EMC repository one time (to the Avamar Downloader Service computer) and then distribute the files to each Avamar server on demand (by using Avamar Enterprise Manager or Avamar Installation Manager).

You can remove old installation packages from the local repository on the Avamar server and then download them from the Avamar Downloader Service computer again, if necessary.

If a customer site prohibits access to the Internet, you can manually copy packages to the `/data01/avamar/repo/packages` directory on the utility node or single-node server instead of using the Avamar Downloader Service. Then you can use the System Maintenance feature in Avamar Enterprise Manager or Avamar Installation Manager to install the packages on the Avamar server.

Avamar Downloader Service

The Avamar Downloader Service downloads server update, hotfix, and workflow packages from the EMC repository to a single local computer. You can then distribute the packages to all Avamar servers in the environment.

EMC Customer Support typically installs the Avamar Downloader Service software during the installation or upgrade of an Avamar server. You can also download the Avamar Downloader Service from the Avamar server and install the software yourself.

The Avamar Downloader Service computer is a standalone Microsoft Windows server that allows network access to both EMC sites on the Internet and all internal Avamar servers. If the Avamar Downloader Service computer is on a private network with restrictions on access to the EMC repository server, then you can set up a proxy server for communication between the Avamar Downloader Service computer and the EMC repository server.

The Avamar Downloader Service runs as a Windows service to monitor the EMC repository. A desktop shortcut, task tray icon, and Windows Start menu items provide access to the Avamar Downloader Service user interface, which enables you to configure the Avamar Downloader Service and check the EMC repository for installation packages. The Avamar Downloader Service monitor contains status messages for the service.

Local repository

The `C:\Program Files\EMC\Avamar Downloader Service\repository` directory on the Avamar Downloader Service computer serves as the local repository for downloaded installation packages.

Note

Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.
The manifest.xml file in the local repository contains a list of all server, client, and workflow packages that are currently available for download from the EMC repository.

**Security**
The Avamar Downloader Service encrypts outgoing communication to the EMC repository by using SSL (Secure Socket Layers) over an HTTP connection. Then the Avamar Downloader Service validates each package it downloads to ensure the package has been properly signed and transmitted.

In addition, the Avamar Downloader Service accepts incoming requests for installation packages only from Avamar systems that are on a known systems list.

**AvInstaller and Avamar Installation Manager**
The AvInstaller process controls the download and installation process for installation packages on the Avamar server.

**Installation**
EMC Customer Support installs AvInstaller during the installation or upgrade of an Avamar server. AvInstaller is installed on the utility node in a multi-node environment or the server in a single-node environment.

**Local repository**
The /data01/avamar/repo/packages directory on the Avamar utility node or single-node server serves as the local repository for downloaded installation packages.

A manifest file in the local repository contains a list of all server, client, and workflow packages that are currently available for download from the EMC repository. The Avamar Downloader Service automatically downloads the manifest file from the EMC repository once a day and determines if new download packages are available.

Then the Avamar Downloader Service sends the updated manifest file to the local repository for each known Avamar system.

AvInstaller also manages a temporary directory that is used to extract the packages during installation.

**User interfaces**
The following user interfaces are available for managing AvInstaller:

- The System Maintenance feature in Avamar Enterprise Manager
- Avamar Installation Manager

Avamar Installation Manager is installed automatically with AvInstaller and is available only for EMC Customer Support use.

**System Maintenance in Avamar Enterprise Manager**
The System Maintenance feature in Avamar Enterprise Manager enables you to download installation packages from the Avamar Downloader Service computer to an Avamar server and install the packages on the Avamar server.

You can also view a list of installation packages in the local repository on the Avamar server, delete old installation packages from the Avamar server to reclaim storage, and view the history of installations on the Avamar server.

Avamar Enterprise Manager is a web-based user interface that enables you to monitor and manage multiple Avamar servers and Data Domain systems in an environment.
Installing and configuring the Avamar Downloader Service

The following topics explain how to prepare for, install, and configure the Avamar Downloader Service software on a Microsoft Windows system, as well as how to update and uninstall the software.

Avamar Downloader Service installation requirements

The Avamar Downloader Service is available as either a 32-bit or 64-bit application. You install the Avamar Downloader Service on a Microsoft Windows server that has network access to the Avamar server. This system can be a desktop or laptop system.

The following table provides the installation requirements for the computer on which you install the Avamar Downloader Service.

<table>
<thead>
<tr>
<th>Software/hardware</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Operating system  | • Microsoft Windows Server 2012 (64-bit only)  
|                   | • Microsoft Windows Server 2008  
|                   | • Microsoft Windows 8  
|                   | • Microsoft Windows 7  
|                   | • Microsoft Windows Vista |
| File system       | Any file system |
| Hard drive space  | Minimum of 12 MB |
| RAM               | Minimum of 20 MB |

Downloading the Avamar Downloader Service software

Download the Avamar Downloader Service software from the EMC Avamar Web Restore page on the Avamar server.

Procedure

1. Log in to the Windows host system as an administrator.
2. Type the URL of the Avamar server into the web browser:
   http://Avamar_server
   where Avamar_server is the Avamar system network hostname (as defined in DNS) or IP address.
   The EMC Avamar Web Restore page appears.
3. Click Downloads.
   The Downloads list appears.
4. Click + next to the platform heading for the Windows computer.
5. Click + next to the operating system heading for the Windows computer.
6. Click the link for AvamarDownloaderService-windows-platform-version.exe.
   where:
• *platform* is the type of Windows platform (32-bit or 64-bit).

• *version* is the version of the Avamar server software.

A dialog box prompts you to either run the file or save it.

7. Save the installation file to a temporary directory.

### Installing the Avamar Downloader Service software

**Procedure**

1. Log in to the Windows host computer as an administrator.

2. Navigate to the directory that contains `AvamarDownloaderService-windows-platform-version.exe`, and then double-click the file to start the installation.

   The setup wizard opens, starting with the welcome page.

3. Click Next.

   The *Destination Folder* page appears.

4. Specify the folder for the Avamar Downloader Service installation:
   - To accept the default folder, `C:\Program Files\EMC\Avamar Downloader Service`, click Next.
   - To specify a different folder, click Change and then browse to the folder. Then click Next.

   The *Ready to install Avamar Downloader Service* page appears.

5. Click Install.

   The *Installing Avamar Downloader Service* page appears and displays the progress of the installation. After the installation completes, the **Completed the Avamar Downloader Service Setup Wizard** page appears.

6. Click Finish.

   The installation adds an Avamar Downloader Service icon to the Control Panel and the system tray. The installation also adds the `AvamarDownloaderService` to Windows Services.

### Defining an outbound rule for Microsoft Windows 7 hosts

When Microsoft Windows 7 security rules block port 22, the Avamar Downloader Service cannot request files from `ftp.avamar.com`. To address this issue, define a custom outbound rule in the Windows Firewall with Advanced Security interface. Define an outbound rule for Microsoft Windows 7 64-bit and 32-bit host systems.

If you cannot unblock port 22 on the Avamar Downloader Service host, then unblock port 21 and configure the Avamar Downloader Service to use the FTP protocol, which uses port 21. The Avamar Downloader Service uses the Secure File Transfer Protocol (SFTP) and port 22 by default. To use the FTP protocol, right-click the Avamar Downloader Service task tray icon and select Show Advanced Settings. Select the FTP checkbox on the Repository Credentials page, and then click Apply. Note that use of SFTP and port 22 will be required in a future release.

**Procedure**

1. Select **Control Panel** > **Windows Firewall** > **Advanced settings**.

   The Windows Firewall with Advanced Security console appears.
2. In the navigation pane, click **Outbound Rules**.
3. In the **Actions** pane, click **New Rule**.
   The **New Outbound Rule Wizard** appears.
4. Select **Custom**, and then click **Next**.
   The **Program** page appears.
5. Select **This program path** and type the path in the text box:

<table>
<thead>
<tr>
<th>Windows 7 version</th>
<th>Program path</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>C:\Program Files\EMC\Avamar Downloader Service Setup x64\avamardownloaderService.exe</td>
</tr>
<tr>
<td>32-bit</td>
<td>C:\Program Files\EMC\Avamar Downloader Service \avamardownloaderService.exe</td>
</tr>
</tbody>
</table>
6. Click **Next**.
   The **Protocol and Ports** page appears.
7. Click **Next**.
   The **Scope** page appears.
8. Click **Next**.
   The **Action** page appears.
9. Select **Allow the connection**, and then click **Next**.
   The **Profile** page appears.
10. Select the **Domain**, **Private**, and **Public** checkboxes, and then click **Next**.
   The **Name** page appears.
11. Type a name and description for the rule:
    - In the **Name** box, type **Avamar Downloader Service Program from EMC**.
    - In the **Description (optional)** box, type **C:\Program Files\EMC\Avamar Downloader Service**.
12. Click **Finish**.
13. In the **Windows Firewall with Advanced Security** console, verify that the **Outbound Rules** list contains the **Avamar Downloader Service Program from EMC** entry.

**Configuring the Avamar Downloader Service**

Before you can use the Avamar Downloader Service to download packages from the EMC repository server, you must configure the system. Configuration tasks include verifying the connection between the Windows server and the EMC repository server, and building a known systems list of Avamar servers that can use the Avamar Downloader Service on the computer. You can also specify proxy server settings.

**Procedure**

1. Right-click the Avamar Downloader Service task tray icon and select **Configure Service**.
   The Avamar Downloader Service configuration wizard opens, starting with the welcome page.
2. (Optional) To use the local version of the `manifest.xml` file, select **Disable Internet access. Use only local files.** This option is for customers who do not have Internet connectivity to the EMC repository.

3. (Optional) To use the local version of the `manifest.xml` file, select **Disable Internet access. Use only local files.**
   This option is for customers who do not have Internet connectivity to the EMC repository.

4. Click **Check For Network Connectivity.**
   - If the Avamar Downloader Service has not been configured yet, then a notification message appears. Click **OK** to continue.
   - If the Avamar Downloader Service has already been configured, then the **Run Diagnosis** page appears and displays the status of the network connectivity verification process. You can let the process run while you configure the Avamar Downloader Service.

5. On the welcome page of the configuration wizard, click **Next.**
   The **Proxy Configuration** page appears.

6. (Optional) To use a proxy server as an intermediary for requests from the Avamar Downloader Service computer to the EMC repository server, specify the hostname or IP address and the port number for the proxy server.
   - You may need to use a proxy server if the Avamar Downloader Service computer is on a private network. In this type of environment, access to the EMC repository server may be restricted and the file download process may be blocked.

7. Click **Next.**
   The **Avamar Systems** page appears.

8. Click **Add.**
   The **Avamar Downloader Service - Add Known System** dialog box appears.

9. Specify the hostname, username, and password for an Avamar server that can use the Avamar Downloader Service:
   - In the **Hostname** box, type the IP address or hostname for the Avamar server.
   - In the **Username** box, type **root** to specify the Linux operating system root user.
   - In the **Password** and **Confirm Password** boxes, type the password for the root user.

10. Click **OK.**
    - If the configuration process cannot resolve the hostname, an informational message appears. Click **Yes** to add the system or **No** to cancel the add operation. You can add systems with unresolvable hostnames, such as offline systems, to the known systems list.

11. Repeat the previous steps to add all remaining Avamar servers.

12. When you finish adding systems to the known systems list, click **Next.**
    The **Review Configuration** page appears.

13. Review the configuration details, and then click **Finish.**
    The task tray icon changes to the following icon to reflect that the Avamar Downloader Service is configured.
After you finish
Rerun the configuration wizard to edit the hostname, IP address, or port number for a proxy server, or to edit the known systems list to add and remove Avamar servers.

Updating the Avamar Downloader Service software

You can use the Avamar Downloader Service to check for updates to the Avamar Downloader Service software itself, and then download and install the updates.

Procedure
1. Right-click Avamar Downloader Service task tray icon and select Check for Updates.
   The Avamar Downloader Service Updater dialog box appears. If an update is available, the message Update is ready to install appears. If no updates are available, then the message Your software is up to date appears.
2. If an update is available, click Install.
   The Welcome to the Avamar Downloader Service Setup Wizard appears.
3. Follow the prompts to proceed through the wizard and install the new software build.

Uninstalling the Avamar Downloader Service

Exit any running applications and then use the Windows Programs and Features console from the Control Panel to uninstall the Avamar Downloader Service. The uninstall process removes all files, including file cache contents, configuration items, and Windows registry entries for the Avamar Downloader Service.

Downloading new packages from the EMC repository

You can check the EMC repository for new server, client, and workflow packages, and then download the packages to install them.

Before you begin
Ensure that the status of the Avamar Downloader Service is either OK or Waiting for configuration. Otherwise, you cannot check for new packages.

Procedure
1. Right-click the Avamar Downloader Service task tray icon and select Check for New Packages.
   The Check for New Packages dialog box appears and provides status messages while the Avamar Downloader Service downloads the manifest file from the EMC repository server to the local repository on the Windows server and to Avamar servers on the known systems list.
   A check mark next to a status message indicates that the process was successful. An X next to a status message indicates that the process failed.
2. To view details about failed processes, double-click the X next to the status message.
3. Click Close on the Check for New Packages dialog box.
Managing the Avamar Downloader Service

The following topics describe how to manage the Avamar Downloader Service.

Viewing a list of packages available for download

The manifest.xml file in the repository folder on the Avamar Downloader Service host computer contains a list of server, client, and workflow packages that are currently available for download from the EMC repository.

Procedure

1. Right-click the Avamar Downloader Service task tray icon and select Open Repository. Windows Explorer opens and displays the C:\Program Files\EMC\Avamar Downloader Service\repository folder, which contains the manifest.xml file.

2. Open the manifest.xml to view the package information.

   Package names use the .avp file extension and appear in <filename> </filename> tags.

Verifying connectivity with the EMC repository

When you edit repository connection settings or experience failures downloading installation packages, you can verify that the Avamar Downloader Service computer can connect to the EMC repository server to download packages.

Procedure

1. Right-click the Avamar Downloader Service task tray icon and select Run Diagnosis. The Run Diagnosis dialog box appears, and the process to check network connectivity starts automatically.

   The status of the process appears in the Run Diagnosis dialog box. An X next to a status message indicates a problem with the network connection. Click the X next to failures to view more information about the error in the Error Information dialog box.

2. To stop the verification process before it completes, click Stop System Check.

3. When the verification completes, click Close.

Monitoring Avamar Downloader Service status

The Avamar Downloader Service monitor automatically starts when you log in to the Windows server that runs the Avamar Downloader Service.

Procedure

- To view the status from the monitor, move the mouse over the task tray icon.

  A popup window with a status message appears.

  The following table lists Avamar Downloader Service monitor status messages.
Table 57 Avamar Downloader Service monitor status messages

<table>
<thead>
<tr>
<th>Status message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Downloader Service</td>
<td>Default status message.</td>
</tr>
<tr>
<td>Authentication Failure with the EMC Repository</td>
<td>HTTP basic authentication failure.</td>
</tr>
<tr>
<td>Authentication Failure with one or more “Known Systems.”</td>
<td>HTTP basic authentication failure including:</td>
</tr>
<tr>
<td></td>
<td>- Failed communication with the EMC repository.</td>
</tr>
<tr>
<td></td>
<td>- SSL (Secure Socket Layers) handshake failed.</td>
</tr>
<tr>
<td></td>
<td>- HTTP dropped connection.</td>
</tr>
<tr>
<td></td>
<td>- HTTP NAK (negatively acknowledged message).</td>
</tr>
<tr>
<td>Failed communication with one or more “Known Systems.”</td>
<td>SSL handshake failed.</td>
</tr>
<tr>
<td></td>
<td>- HTTP dropped connection.</td>
</tr>
<tr>
<td></td>
<td>- HTTP NAK.</td>
</tr>
<tr>
<td>Failed file download from the EMC repository</td>
<td>File transfer was aborted.</td>
</tr>
<tr>
<td>Failed file transfer to one or more known systems.</td>
<td>File transfer was aborted.</td>
</tr>
<tr>
<td>Network Error</td>
<td>Windows 7 firewall settings prevent the Avamar Downloader Service from requesting files from the Avamar FTP site.</td>
</tr>
<tr>
<td>Out of space.</td>
<td>The Avamar Downloader Service file cache is full.</td>
</tr>
<tr>
<td></td>
<td>To free up disk space, remove files from the local repository.</td>
</tr>
<tr>
<td>Running.</td>
<td>The service is running and communicating with all known systems as well as the EMC repository.</td>
</tr>
<tr>
<td>Socket failure on host computer.</td>
<td>Either the Microsoft Windows machine is out of socket resources or there is a binding problem with the NIC.</td>
</tr>
<tr>
<td></td>
<td>- Deadlock condition within Winsock.</td>
</tr>
<tr>
<td>Waiting for configuration.</td>
<td>The Avamar Downloader Service was installed, but not configured.</td>
</tr>
</tbody>
</table>
Stopping and restarting the Avamar Downloader Service monitor

The Avamar Downloader Service monitor starts automatically when you log in to the Windows server on which the Avamar Downloader Service is installed. You can stop and restart the monitor.

Procedure

- To stop the monitor, right-click the Avamar Downloader Service task tray icon and select Exit.
- To restart the monitor, open the Windows Start menu and select All Programs > EMC Avamar Downloader Service version > Avamar Downloader Service Monitor.

Troubleshooting Avamar Downloader Service issues

This topic describes how to resolve common issues with the Avamar Downloader Service.

Error messages when checking for new packages

After you click Check for New Packages, the Avamar Downloader Service writes the following error messages to AvamarDownloaderService.log, which is located in the EMC\Avamar Downloader Service\var\log directory by default:

6/1/2014 13:36:38 PM [380] SendManifest failed

Microsoft Windows 7 security rules block port 22, which prevents the Avamar Downloader Service from requesting files from the Avamar FTP site (ftp.avamar.com).

To resolve this issue, define an outbound rule in the Windows Firewall with Advanced Security console. Defining an outbound rule for Microsoft Windows 7 hosts on page 253 provides instructions.

Package download fails

If the utility node or the single-node server cannot access the Windows host computer, a message similar to the following might appear when you try to download a package:

The selected package cannot be downloaded.

To correct this problem, add a new line to the /etc/hosts file on the utility node and enter the IP address, fully qualified domain name, and short name of the Windows computer with the Avamar Downloader Service. See the following sample entry:

10.6.172.50 avamar-1.example.com avamar-1

Temporary IPv6 addresses cause package download to fail

The Avamar Downloader Service fails to download a package when temporary IPv6 addresses are in use on all operating systems. The download process fails with connection refused errors.

The connection refused errors are due to the use of temporary IPv6 addresses. Windows Vista, Windows 2008 Server, or later versions of Windows use temporary IPv6 addresses by default.

To work around this issue, block temporary IPv6 addresses on the system that runs the Avamar Downloader Service. Type each of the following netsh commands in the command prompt window on a single line:

```
netsh interface ipv6 set privacy state=disabled store=active
netsh interface ipv6 set privacy state=disabled store=persistent
netsh interface ipv6 set global randomizeidentifiers=disabled
```
store=active
netsh interface ipv6 set global randomizeidentifiers=disabled
store=persistent

Downloading and installing packages on the Avamar server

You can download and install workflow packages, patches, and hotfixes from the System Maintenance page in Avamar Enterprise Manager.

Before you begin

If you access Avamar Enterprise Manager by using Microsoft Internet Explorer or Mozilla Firefox on a Microsoft Windows computer, ensure that the computer has a minimum of 2 GB of RAM.

Procedure

1. Open a web browser and log in to Avamar Enterprise Manager:
   a. In the web browser, type the following URL:
      
      http://Avamar-server/em
      
      where Avamar-server is the hostname of the Avamar server.
      
      The EMC Avamar Enterprise Manager login page appears.
   b. Type the Avamar administrator user account in the User Name field and the password in the Password field.
   c. Click Log On.
      
      The Avamar Enterprise Manager dashboard appears.

2. Click System Maintenance.
   
   The System Maintenance page appears.

3. Select whether to install workflow packages or patches and hotfixes:
   
   a. To install workflow packages, click the Maintenance tab. The Maintenance tab appears only when workflow packages are available for installation.
   b. To install patches or hotfixes, click the SW Updates tab.

4. From the Systems list, select the Avamar server on which to download and install the packages.

   The following table lists the information that appears in the Systems list for each Avamar server.

<table>
<thead>
<tr>
<th>Systems list column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>A yellow icon indicates that one or more packages are available to download and install on the Avamar server.</td>
</tr>
<tr>
<td>Status</td>
<td>One of the following icons:</td>
</tr>
<tr>
<td></td>
<td>- A green checkmark indicates that Avamar Installation Manager is running on the Avamar server.</td>
</tr>
<tr>
<td></td>
<td>- A yellow exclamation point indicates that either the Avamar server is running a version of the Avamar server software earlier than 6.0 or that the installation process has encountered an issue and requires attention.</td>
</tr>
<tr>
<td>Systems list column heading</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|                           | • A purple progress icon indicates that an Avamar package installation is in progress.  
• A red icon indicates that the AvInstaller process is not running. |
| System                    | The fully qualified domain name for the Avamar server. |
| Version                   | The version of the Avamar server software. |

Packages that are available for the selected system appear in the **Package List**.

5. If a **Download** button appears for the package, click the button to download the package to the local repository.

   After the download completes, the **Download** button is replaced with an **Install** button and a **Delete** button.

6. To start the installation, click **Install**.

   The background color for the package changes to yellow and the initialization begins. When the initialization process completes, the **Installation Setup** page appears.

7. Provide installation setup information.

   Some packages do not require setup information.

8. To provide advanced settings, select **Show advanced settings**.

9. Click **Continue**.

   The **Installation Progress** page displays the status of the installation.

   **NOTICE**

   If you accidently close the browser during the installation of a package, the installation pauses but does not stop. To resume the installation, open a new browser window and log in to Avamar Enterprise Manager. The installation continues from the point when the browser window closed.

10. Respond to all installation prompts.

    After the installation completes, the **Install** button becomes a **Run** button for workflow packages. The **Run** button enables you to run the workflow package again.

---

**Viewing a list of installation packages on the Avamar server**

You can view a list of installation packages in the repository on an Avamar server on the **Repository** tab of the **System Maintenance** page in Avamar Enterprise Manager.

**Procedure**

1. Open a web browser and log in to Avamar Enterprise Manager.

2. Click **System Maintenance**.

   The **System Maintenance** page appears.

3. Click **Repository**.

   The **Repository** tab appears.
4. From the **Systems** list, select the Avamar server.

The packages in the repository on the Avamar server appear on the **Repository** page. The most recently installed package appears at the bottom of the list.

The following table lists the information that appears for each package.

<table>
<thead>
<tr>
<th>Repository page column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>The name of the package.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The checksum of the package the AvInstaller service calculated during download. Compare this data with the checksum in the manifest file.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the package:</td>
</tr>
<tr>
<td></td>
<td>• Waiting — The AvInstaller service is copying the package to the EMC repository.</td>
</tr>
<tr>
<td></td>
<td>• Checksum — The AvInstaller service is calculating the package checksum.</td>
</tr>
<tr>
<td></td>
<td>• Unsigning — The AvInstaller service is verifying the package signature.</td>
</tr>
<tr>
<td></td>
<td>• Extracting — The AvInstaller service is extracting the package from the tarball.</td>
</tr>
<tr>
<td></td>
<td>• Accepted — The package is fully downloaded to the EMC repository and is ready to be installed.</td>
</tr>
<tr>
<td></td>
<td>• Rejected — The package was rejected due to a problem in transit.</td>
</tr>
<tr>
<td>Note</td>
<td>A brief description of the status.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time of the last status update.</td>
</tr>
</tbody>
</table>

5. To toggle the sort order of the packages in the list, click the heading in any column.

**Deleting packages from the Avamar server**

After you successfully install a workflow, patch, or hotfix package, the AvInstaller service automatically deletes the package from the repository on the Avamar system. You can delete packages that you choose not to install.

Only EMC Customer Support can delete restricted packages.

**Procedure**

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Click **System Maintenance**.
   
   The **System Maintenance** page appears.
3. Select whether to delete workflow packages or patch and hotfix packages:
   
   • To delete a workflow package, click the **Maintenance** tab.
   
   • To delete a patch or hotfix package, click the **SW Updates** tab.
4. From the **Systems** list, select the Avamar server from which to delete the package.
5. Click the **Delete** button next to the package in the **Package List**.
   
   A confirmation message appears.
6. Click **Yes**.
Viewing the history of installations

You can view a history of the software installations, updates, and hotfixes for an Avamar server on the History tab on the System Maintenance page in Avamar Enterprise Manager.

Procedure

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Click System Maintenance.
   The System Maintenance page appears.
3. Click History.
   The History tab appears.
4. From the Systems list, select the Avamar server.
   All installed packages for the selected Avamar server appear in the History table. The most recently installed packages appear at the bottom of the list.

The following table lists the information that appears for each package.

<table>
<thead>
<tr>
<th>History table column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the package.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of Avamar server software.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the package.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the package:</td>
</tr>
<tr>
<td></td>
<td>- Available — The package is in the manifest and is available to download.</td>
</tr>
<tr>
<td></td>
<td>- Completed — The package installation completed.</td>
</tr>
<tr>
<td></td>
<td>- Processing — A package installation is in progress.</td>
</tr>
<tr>
<td></td>
<td>- Ready — The package is ready to install.</td>
</tr>
<tr>
<td></td>
<td>- Removed — The package has been deleted from the Avamar grid.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time of the last status update for the package.</td>
</tr>
</tbody>
</table>

5. To toggle the sort order of the packages in the list, click the heading in any column.
6. To filter the list of packages, select a filter value from the Show list.
7. To view details about a package in the list, select the row for the package.

The details in the following table appear in the Details table in the lower right pane of the History page.

<table>
<thead>
<tr>
<th>Details table column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status details for a package:</td>
</tr>
<tr>
<td></td>
<td>- Available — The package is in the manifest and is available to download.</td>
</tr>
<tr>
<td>Details table column heading</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>• Ready — The package is ready to install.</td>
</tr>
<tr>
<td></td>
<td>• Deployed — The start of the installation initialization.</td>
</tr>
<tr>
<td></td>
<td>• Deploying — The start of the package deployment.</td>
</tr>
<tr>
<td></td>
<td>• Processing — The start of the package installation.</td>
</tr>
<tr>
<td></td>
<td>• Completed — The completion of the package installation.</td>
</tr>
<tr>
<td></td>
<td>• Removed — The removal of the package.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Updated</th>
<th>The corresponding date and time of the package status message.</th>
</tr>
</thead>
</table>

| Logs | Displays a Logs button for packages with a processing status. Click Logs to open a window that provides details about the tasks performed to install the package. |

8. To view the log file for packages with a processing status, click Logs in the Details table.

   You can export the log information to a Microsoft Excel or PDF file by clicking Export.
CHAPTER 12
Avamar Enterprise Manager

This chapter includes the following topics:

- Overview of Avamar Enterprise Manager .............................................................. 266
- Logging in to Avamar Enterprise Manager ............................................................ 267
- Avamar Enterprise Manager dashboard .............................................................. 267
- Adding an Avamar system in Avamar Enterprise Manager ................................. 271
- Viewing system status ......................................................................................... 272
- Viewing capacity information .............................................................................. 280
- Viewing policy information .................................................................................. 280
- Running reports ................................................................................................... 281
- Managing cron-based replication ........................................................................ 281
- Managing server updates and hotfixes ............................................................... 282
- Starting Avamar Client Manager.......................................................................... 282
Overview of Avamar Enterprise Manager

Avamar Enterprise Manager is a web-based multi-system management console application that provides centralized Avamar system administration capabilities for larger businesses and enterprises. With Avamar Enterprise Manager, you can monitor all Avamar 6.x and 7.x systems in the enterprise from a single web browser session.

An integrated dashboard provides an “at-a-glance” view that enables you to assess the operational status and capacity utilization of each Avamar system, and to determine if backups are completing successfully.

The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar system information, and provides a mechanism to manage Avamar systems using a standard web browser. The EMS also communicates directly with Management Console Servers (MCSs), which are an integral part of all Avamar systems in an enterprise. Therefore, it is important to understand that only one operational EMS is required for an enterprise; you do not need to run EMS on every Avamar system, nor is it recommended to do so.

Use the default installation and configuration options, which configure the EMS to use the local MCS (the MCS running on the same Avamar host) to authenticate Avamar Enterprise Manager logins. There is usually no reason to authenticate Avamar Enterprise Manager logins by using a remote MCS running on another Avamar host.

Comparison of Avamar Enterprise Manager with other Avamar user interfaces

Avamar Enterprise Manager provides similar functionality to other Avamar user interfaces, including Avamar Administrator and Backup & Recovery Manager. However, there are several key differences.

Avamar Administrator is a graphical management console software application that also enables you to remotely monitor and administer an Avamar system from a supported Windows client computer. However, Avamar Enterprise Manager enables you to administer multiple Avamar systems from a single application, while Avamar Administrator enables you to manage a single Avamar system at a time.

Like Avamar Enterprise Manager, Backup & Recovery Manager manages all Avamar systems in the enterprise. However, Backup & Recovery Manager additionally has an integrated user interface to manage the enterprise’s NetWorker servers and Data Domain backup targets. User interfaces on page 24 provides more detailed comparison between Avamar Enterprise Manager and Backup & Recovery Manager.

Web browser security

Certain web browser security settings (for example, the Internet Explorer High security setting) are known to interfere with logins to Avamar Enterprise Manager. You may need to respond to security prompts to access the system.

Session time-outs

The default session time-out setting for most Avamar Enterprise Manager features and functions is 72 hours. However, the dashboard page and the replicator page automatically refresh every minute.

Effectively, this means that if you leave the web browser pointed to the dashboard or replicator pages, the Avamar Enterprise Manager session continues indefinitely.
However, if you leave the web browser pointed to any other page, the Avamar Enterprise Manager session automatically times out after 72 hours of inactivity.

You can edit the default session time-out setting by changing the session-timeout preference in /usr/local/avamar-tomcat/webapps/cas/WEB-INF/web.xml.

Logging in to Avamar Enterprise Manager

Procedure
1. Open a web browser and type the following URL:
   \[http://Avamar_server/em\]
   where \textit{Avamar_server} is the DNS name or IP address of the Avamar server that hosts the EMS.
   The login page appears.
2. Select \textit{Enterprise Manager}.
3. In \textit{User Name}, type the username of an account with the Avamar role of administrator.
4. In \textit{Password}, type the password for the user account.
5. Click \textit{Log On}.
6. If a security warning appears, click \textbf{Yes} to proceed with the login.
   Avamar Enterprise Manager opens to the \textbf{Dashboard} page.

After you finish
To log out of Avamar Enterprise Manager when you finish, click the door icon in the upper right corner of the window.

Avamar Enterprise Manager dashboard

The Avamar Enterprise Manager dashboard provides an “at-a-glance” view that enables you to assess the operational status and capacity utilization of each Avamar system, and to determine if backups are completing successfully.

\textbf{Figure 14} Avamar Enterprise Manager dashboard

The dashboard appears when you log in to Avamar Enterprise Manager and when you select \textit{Dashboard} from any other page.
To select an effective period of time for the backup information that appears for each Avamar system, select a value from the **Backup period** list above the table on the Dashboard page.

General system information, capacity information, the total amount of protected data, and backup information appears for each system in the list.

**General system information**

The General information appears for each Avamar server on the Avamar Enterprise Manager dashboard. The information includes the server name, the elapsed time since Avamar Enterprise Manager last contacted the Avamar server, the overall status of the Avamar server and any configured Data Domain systems, and the version of the Avamar server software running on the Avamar server.

**Server**

The **Server** column in the dashboard lists the DNS name of each Avamar server that you are monitoring in Avamar Enterprise Manager. Click the server name to view detailed system information for the server.

**Last Contacted**

The **Last Contacted** information is the elapsed time since Avamar Enterprise Manager last contacted the Avamar server and collected data.

The following table lists the status icons that may appear and details about the conditions that the icons indicate.

**Table 58 Status icons for the Last Contacted column in Avamar Enterprise Manager**

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Avamar Enterprise Manager is operating normally and is able to communicate and collect data at the specified refresh/polling interval from this Avamar server. The elapsed time since the last communication appears next to the status icon.</td>
</tr>
<tr>
<td>❗</td>
<td>The last attempt by Avamar Enterprise Manager failed to communicate or collect data from this Avamar server. Avamar Enterprise Manager waits one minute and retries as many as three times before considering the refresh/polling cycle a failure. The specific reason for this condition appears next to the status icon. This condition can happen intermittently if network access to the Avamar server is slow or unreliable. It can also occur if the Avamar server is not running or has encountered an error or warning condition.</td>
</tr>
</tbody>
</table>
|❌           | One of the following conditions occurred:  
  - Avamar Enterprise Manager failed to communicate and or collect data from the Avamar server for a specified number of refresh/polling cycles.  
  - The Avamar server hostname could not be resolved. Search the knowledgebase on EMC Online Support for solution esg114453.  
  - The Avamar server login credentials (username or password) were refused.  
  The default polling setting is three cycles (30 minutes total elapsed time based on a 10-minute refresh/polling cycle). The specific reason for this condition appears next to the status icon. |
Table 58 Status icons for the Last Contacted column in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Investigate and remedy any red status condition immediately to ensure that system operation is not adversely affected.</td>
</tr>
</tbody>
</table>

NOTICE

If the last updated indicator shows a status other than a green check mark, then all other information for the system should be considered stale and might not reflect Avamar system status.

Status

The Status column provides the overall status of the Avamar server and any configured Data Domain systems.

The following table lists the status icons that may appear and details about the conditions that the icons indicate.

Table 59 Status icons for the Status column in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Check" /></td>
<td>The Avamar server and all configured Data Domain systems are fully operational.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>There is an issue with either the Avamar server, a configured Data Domain system, or both that requires attention. However, backups and restores can continue.</td>
</tr>
<tr>
<td><img src="image" alt="Error" /></td>
<td>There is a problem with either the Avamar server, a configured Data Domain system, or both that requires immediate attention. Backups and restores will not occur until the problem is resolved.</td>
</tr>
</tbody>
</table>

Click the status icon to view the System Information page, which contains detailed information about the server.

Version

The Version column in the Avamar Enterprise Manager dashboard lists the version of the Avamar server software running on the server.

Capacity information

The Capacity section of the Avamar Enterprise Manager dashboard displays the percentage of used capacity on the Avamar server and any configured Data Domain systems, as well as the forecast number of days of additional storage capacity. For the Avamar server, the used capacity information includes the amount of storage capacity consumed in bytes and the amount of free storage capacity available as a percentage of total available storage capacity.

Used capacity

The following table lists the status icons that may appear for used capacity, as well as details about the conditions that the icons indicate.
Table 60 Status icons for used capacity in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>The Avamar server or configured Data Domain systems have used less than 80% of total storage capacity.</td>
</tr>
<tr>
<td>!</td>
<td>The Avamar server or configured Data Domain systems have used more than 80 percent but less than 95 percent of total storage capacity. Consider adding capacity or deleting old backups.</td>
</tr>
<tr>
<td>❌</td>
<td>The Avamar server or configured Data Domain systems have used more than 95 percent of total storage capacity. No new backups occur until you add capacity or delete old backups. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.</td>
</tr>
</tbody>
</table>

Forecast capacity
The following table lists the status icons that may appear for forecast capacity, as well as details about the conditions that the icons indicate.

Table 61 Status icons for forecast capacity in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>The Avamar server or configured Data Domain systems are forecast to have 90 days or more storage capacity.</td>
</tr>
<tr>
<td>!</td>
<td>The Avamar server or configured Data Domain systems are forecast to have less than 90 days of storage capacity.</td>
</tr>
<tr>
<td>❌</td>
<td>The Avamar server or configured Data Domain systems are forecast to have less than 30 days of storage capacity.</td>
</tr>
</tbody>
</table>

Click a used capacity or forecast capacity status icon to view the Capacity Utilization and Forecast.

Data protected information
The Data Protected column on the Avamar Enterprise Manager dashboard shows how much data is currently being protected on each Avamar server.

Backup information
Backup status information appears on the Avamar Enterprise Manager dashboard.

Status
The Status column in the Backups section of the dashboard provides a quick overview of scheduled backup status for the Avamar server. The following table lists the status icons that may appear and details about the conditions that the icons indicate.
Table 62 Backup status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>All scheduled backups successfully completed within the allotted period of time.</td>
</tr>
<tr>
<td>⬤</td>
<td>One or more scheduled backups successfully completed with exceptions.</td>
</tr>
<tr>
<td>⬠</td>
<td>One or more scheduled backups did not successfully complete within the allowed period of time.</td>
</tr>
</tbody>
</table>

Click a backup status icon to view the Reports page for more information.

Fail
The Fail column lists the number of failed backups.

Exceptions
The Exceptions column lists the number of backups that successfully completed with exceptions.

Success
The Success column lists the number of backups that completed successfully.

Adding an Avamar system in Avamar Enterprise Manager

Avamar Enterprise Manager enables you to monitor the Avamar system on which the Avamar Enterprise Manager Server (EMS) is running by default. To monitor other Avamar systems in an enterprise, add them in Avamar Enterprise Manager.

The release number of the server software on the Avamar server that you add in Avamar Enterprise Manager must be the same or earlier than the release number of the server software on the Avamar server that hosts EMS. You cannot monitor an Avamar server with a newer release than the Avamar server with EMS.

Procedure
1. Select Configure on the menu bar.
2. Click Add.
   Additional fields appear on the Configure page.
3. In the System name or IP box, type the DNS name or IP address of the Avamar server.
4. In the Port box, type the port number to use for communication with the MCS on the Avamar server.
5. Choose whether to enable or disable monitoring of the Avamar server with Avamar Enterprise Manager by selecting or clearing the Monitor checkbox.

   Note
   You can suspend and resume system monitoring after you add the Avamar system in Avamar Enterprise Manager by selecting the Avamar system name on the Configure page and then selecting or clearing the Monitor checkbox.
6. Specify the security protocol to use for connections to the Avamar server:
   - To use a secure HTTPS connection, select the Secure Protocol checkbox.
   - To use an unsecure HTTP connection, leave the checkbox clear.
7. In the **Password** box, type the Avamar administrative user account password.
8. In the **Note** box, type an optional note or comment about the Avamar system.
9. Click **Save**.

**After you finish**

To edit the settings for an Avamar system, select the link for the system on the **Configure** page. You can edit the following settings:

- Port number
- Whether the system is monitored in Avamar Enterprise Manager
- Whether to use the HTTPS or HTTP protocol for connections
- The password for the Avamar administrative user account
- Notes or comments about the Avamar system

To remove an Avamar system from the list on the **Configure** page, select the checkbox next to the system and then click **Remove**.

### Viewing system status

You can view detailed server status and activity information for a specific Avamar server or for all Avamar servers at the same time on the system status page in Avamar Enterprise Manager.

**Procedure**

- To view system status for a specific Avamar server, use one of the following methods:
  - Click the name of the server on the **Dashboard** page.
  - Select **System > Status** in the menu bar, and then select the Avamar server from the **Systems** list.
- To view a consolidated page with system information for all Avamar servers, select **System > Status** in the menu bar.

### Last Contacted

The **Last Contacted** information is the elapsed time since Avamar Enterprise Manager last contacted the Avamar server and collected data.

The following table lists the status icons that may appear and details about the conditions that the icons indicate.

**Table 63** Status icons for the Last Contacted column in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![checkmark] (✓)</td>
<td>Avamar Enterprise Manager is operating normally and is able to communicate and collect data at the specified refresh/polling interval from this Avamar server. The elapsed time since the last communication appears next to the status icon.</td>
</tr>
<tr>
<td>![exclamation] (‼️)</td>
<td>The last attempt by Avamar Enterprise Manager failed to communicate or collect data from this Avamar server. Avamar Enterprise Manager waits one minute and retries as many as three times before considering the refresh/polling cycle a failure. The specific reason for this condition appears next to the status icon.</td>
</tr>
</tbody>
</table>
Table 63 Status icons for the Last Contacted column in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![X]</td>
<td>One of the following conditions occurred:</td>
</tr>
<tr>
<td>![X]</td>
<td>• Avamar Enterprise Manager failed to communicate and or collect data from the Avamar server for a specified number of refresh/polling cycles.</td>
</tr>
<tr>
<td>![X]</td>
<td>• The Avamar server hostname could not be resolved. Search the knowledgebase on EMC Online Support for solution esg114453.</td>
</tr>
<tr>
<td>![X]</td>
<td>• The Avamar server login credentials (username or password) were refused.</td>
</tr>
<tr>
<td>![X]</td>
<td>The default polling setting is three cycles (30 minutes total elapsed time based on a 10-minute refresh/polling cycle). The specific reason for this condition appears next to the status icon.</td>
</tr>
<tr>
<td>![X]</td>
<td>Investigate and remedy any red status condition immediately to ensure that system operation is not adversely affected.</td>
</tr>
</tbody>
</table>

**NOTICE**

If the last updated indicator shows a status other than a green check mark, then all other information for the system should be considered stale and might not reflect Avamar system status.

**General server status information**

General server status information for each Avamar server and Data Domain system appears on the system status page in Avamar Enterprise Manager. Details include the operational run level for the Avamar server, the system ID, capacity information, and unacknowledged event information.

**Avamar Server**

The **Avamar Server** field on the system status page in Avamar Enterprise Manager provides the operational run level for the Avamar server.

The following table lists the status icons that may appear and details about the conditions that the icons indicate.

Table 64 Status icons for the Avamar Server field in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![✓]</td>
<td>A status of Full access appears, which indicates that the Avamar server is fully operational.</td>
</tr>
<tr>
<td>![⚠️]</td>
<td>This Avamar server is less than fully operational due to one of the following conditions:</td>
</tr>
<tr>
<td>![⚠️]</td>
<td>• Admin — The Avamar server is fully operational, but only the administrator root account can access the server.</td>
</tr>
</tbody>
</table>
Table 64 Status icons for the Avamar Server field in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Only</td>
<td>The Avamar server is fully operational, but only the administrator root account can access the server.</td>
</tr>
<tr>
<td>Admin Read Only</td>
<td>The Avamar server is in a read-only condition, and only the administrator root account can access the server.</td>
</tr>
<tr>
<td>Read Only</td>
<td>The Avamar server is in a read-only condition. Restores can take place, but no new backups can occur.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Scheduled backups are disabled and will not occur until you re-enable the scheduler.</td>
</tr>
<tr>
<td>Synchronizing</td>
<td>The Avamar server is priming or synchronizing stripes. This is a temporary condition. Some operations might be delayed.</td>
</tr>
</tbody>
</table>

The Avamar server is experiencing one of the following conditions that requires immediate attention:

- Inactive – One or more storage nodes are unresponsive to communication requests from the local MCS (that is, nodes are functioning but frequently timing out on communication requests).
- Node Offline – One or more storage nodes has experienced a problem.
- Not available – Avamar Enterprise Manager cannot obtain any information from this Avamar server. This might indicate communication problems or errors in retrieving data. Ensure that the Last updated status indicator is green.
- Unknown State – The Avamar server is in an unknown state. It is either not running or does not respond to communication requests.

Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. If the status is Node Offline, then search the knowledgebase on EMC Online Support for Avamar Data Node offline solution esg112792.

System ID

The System ID field on the system status page in Avamar Enterprise Manager lists a system identification number for the Avamar server.

Capacity Forecast

The Capacity Forecast field on the system status page in Avamar Enterprise Manager provides a projection of how long you can continue to consume storage capacity on the Avamar server at the current rate.

The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.
Table 65 Capacity forecast status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>90 days or more storage capacity</td>
</tr>
<tr>
<td>⚠</td>
<td>Less than 90 days of storage capacity</td>
</tr>
<tr>
<td>✗</td>
<td>Less than 30 days of storage capacity</td>
</tr>
</tbody>
</table>

Capacity Usage

The **Capacity Usage** field on the system status page in Avamar Enterprise Manager lists how much storage capacity is in use on the Avamar server. Detailed information includes the total capacity, used capacity, and the total number of protected bytes.

The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.

Table 66 Capacity usage status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Less than 80% of total storage capacity.</td>
</tr>
<tr>
<td>⚠</td>
<td>More than 80% but less than 95% of total storage capacity. Consider adding capacity or deleting old backups.</td>
</tr>
<tr>
<td>✗</td>
<td>More than 95% of total storage capacity. No new backups are performed until you add capacity or delete old backups. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.</td>
</tr>
</tbody>
</table>

All Unack. Events

The **All Unack. Events** field on the system status page in Avamar Enterprise Manager shows whether there are any unacknowledged events on the Avamar server.

The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.

Table 67 All Unack. Events status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>No warning or error events have occurred on this Avamar server that have not been explicitly acknowledged by an Avamar server administrator.</td>
</tr>
<tr>
<td>⚠</td>
<td>One or more warning events have been encountered on this Avamar server, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect server operation.</td>
</tr>
</tbody>
</table>
Table 67 All Unack. Events status icons in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![x]</td>
<td>One or more serious error events have been encountered on this Avamar server, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.</td>
</tr>
</tbody>
</table>

### Unack. Hardware Events

The **Unack. Hardware Events** field on the system status page in Avamar Enterprise Manager shows whether there are any unacknowledged hardware events on the Avamar server.

The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.

Table 68 Unacknowledged hardware event status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![check]</td>
<td>No hardware warning or error events have occurred on this Avamar server that have not been explicitly acknowledged by an Avamar server administrator.</td>
</tr>
<tr>
<td>![warning]</td>
<td>One or more hardware warning events have been encountered on this Avamar server, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect server operation.</td>
</tr>
<tr>
<td>![x]</td>
<td>One or more serious hardware error events have been encountered on this Avamar server, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. An automatic Service Request may already have been opened by the ConnectEMC program.</td>
</tr>
</tbody>
</table>

### Data Domain system information

If one or more Data Domain systems are configured on the Avamar server, then status information for each Data Domain system appears on the system status page in Avamar Enterprise Manager.

The **Data Domain Server** field lists the fully qualified domain name of the Data Domain system. The **Capacity Forecast**, **Capacity Usage**, **All Unack. Events**, and **Unack. Hardware Events** fields lists the same status indicators and information for the Data Domain system as they do for the Avamar server.

The **Status** field lists the overall status of the Data Domain system. The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.

Table 69 Data Domain system status icon in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![check]</td>
<td>The Data Domain system is fully operational.</td>
</tr>
</tbody>
</table>
Table 69 Data Domain system status icon in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>The Data Domain system is experiencing problems. However, backups to and restores from the Data Domain system can continue.</td>
</tr>
<tr>
<td>⚠️</td>
<td>The Data Domain system is experiencing problems, and backups and restores will not occur until the problem is resolved.</td>
</tr>
</tbody>
</table>

The *EMC Avamar and EMC Data Domain System Integration Guide* provides a complete list of the available status messages.

**Garbage collection information**

The GC row on the system status page in Avamar Enterprise Manager shows whether garbage collection (GC) is running or has successfully freed additional storage space on this Avamar server.

Detailed information includes:

- Amount of time since the last successful garbage collection
- Current status of the garbage collection process
- Result of the most recent garbage collection
- Date and time that the most recent garbage collection started and ended
- Number of passes that occurred during the most recent garbage collection
- Number of bytes recovered during the most recent garbage collection
- Number of chunks deleted during the most recent garbage collection
- Number of index stripes affected during the most recent garbage collection
- Total number of index stripes scanned during the most recent garbage collection

The following table lists the status icons that may appear and provides details on the conditions that the icons indicate.

Table 70 Garbage collection status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Garbage collection successfully completed on this Avamar server within the past 30 hours.</td>
</tr>
</tbody>
</table>
| 🚨           | Garbage collection has not successfully completed on this Avamar server within the past 30 hours, possibly due to one of the following conditions:  
  - In progress — Garbage collection is currently running.  
  - None — Garbage collection has never successfully completed on this Avamar server. |
| ⚠️           | Garbage collection encountered an error the last time it was run. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. |
Table 70 Garbage collection status icons in Avamar Enterprise Manager (continued)

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to EMC Online Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.</td>
</tr>
</tbody>
</table>

**Last Checkpoint**

The **Last Checkpoint** row on the system status page in Avamar Enterprise Manager shows whether regularly scheduled checkpoints are successfully completing.

The elapsed time since last successful checkpoint and the checkpoint time stamp are shown if at least one successful checkpoint has completed on this Avamar server. Otherwise, one of the following status messages appears:

- **None** indicates that no checkpoints are stored on this Avamar server.
- **Init** indicates that this is a new Avamar server and that the initial checkpoint has not yet completed.

The following table lists the available status icons and provides details on the condition that the icon indicates.

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>A checkpoint successfully completed on this Avamar server within the past 24 hours.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>More than 24 hours but less than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>More than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.</td>
</tr>
</tbody>
</table>

**Last Validated Checkpoint**

The **Last Validated Checkpoint** row on the system status page in Avamar Enterprise Manager shows whether regularly scheduled checkpoint validations are successfully completing on this Avamar server.

The age, date, and time of the most recently validated checkpoint appears. Otherwise, one of the following status messages appears:

- **None** indicates that no checkpoints have ever successfully been validated on this Avamar server.
- **Errors** indicates that the last checkpoint validation operation failed.
- **Not configured** indicates that checkpoint validation is not enabled on this server.

The following table lists the status icons that may appear and provides details on the condition that the icon indicates.
Table 72 Status icons for last validated checkpoint in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Checkpoint validation successfully completed on this Avamar server within the past 48 hours.</td>
</tr>
<tr>
<td>!</td>
<td>More than 48 hours but less than 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server.</td>
</tr>
<tr>
<td>✗</td>
<td>More than 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server.</td>
</tr>
</tbody>
</table>

The Validation type field describes the extent of checking performed during the checkpoint. One of the following values appears:

- **Full** — A full checkpoint (all checks) was performed.
- **Rolling** — A rolling checkpoint (all new and modified stripes fully validated and a subset of unmodified stripes were validated).

**Replication**

The Replication row on the system status page in Avamar Enterprise Manager shows whether regularly scheduled replication is successfully completing on each Avamar server.

The date and time of the most recently completed replication appears. Otherwise, one of the following status messages appears:

- **Failed** indicates that the last replication operation failed.
- **Disabled** indicates that the Avamar data replication feature is not enabled on this server.

The following table lists the status icons that may appear and provides details on the condition that the icon indicates.

Table 73 Replication status icons in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Replication successfully completed on this Avamar server within the past 48 hours, or the Avamar data replication feature is not enabled on this server.</td>
</tr>
<tr>
<td>!</td>
<td>More than 48 hours but less than 72 hours have elapsed since replication successfully completed on this Avamar server.</td>
</tr>
<tr>
<td>✗</td>
<td>More than 72 hours have elapsed since replication successfully completed on this Avamar server, or the last replication operation failed. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.</td>
</tr>
</tbody>
</table>

**System Activity**

The System Activity table on the system status page Avamar Enterprise Manager provides information on system activity that is currently in progress on the Avamar server.

**Scheduler**

The Scheduler column shows whether regularly scheduled server activities (for example, backups, maintenance activities) are enabled for this Avamar server. The following table
lists the status icons that may appear and provides details on the condition that the icon indicates.

Table 74 Scheduler status icon in Avamar Enterprise Manager

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Regularly scheduled activities are enabled (resumed) on this Avamar server.</td>
</tr>
<tr>
<td>🟡</td>
<td>Regularly scheduled activities are suspended on this Avamar server.</td>
</tr>
</tbody>
</table>

**Waiting**

The **Waiting** column shows the number of jobs in the server wait queue.

**Running**

The **Running** column shows the number of server jobs that are currently running.

**Sessions**

The **Sessions** column shows the number of active client sessions.

### Viewing capacity information

Avamar Enterprise Manager provides a number of ways to view detailed and summary capacity utilization and forecasting information for the Avamar system.

*Capacity Management on page 209* provides details on the capacity features in Avamar Enterprise Manager.

**Procedure**

1. To view consolidated capacity utilization information for all servers that you are monitoring in Avamar Enterprise Manager, open the **Dashboard** or the system status page.
2. To view a graph that provides both capacity utilization and forecasting, select **System** ➔ **Capacity**, and then select the Avamar server from the list.
3. To view the average daily change rate for an Avamar server or for clients, select **System** ➔ **Average Daily Change Rate** ➔ **For Server or System** ➔ **Average Daily Change Rate** ➔ **For Clients with Maximum/Minimum rate/bytes**.

### Viewing policy information

The **Policy** page in Avamar Enterprise Manager enables you to view details on the groups, clients, datasets, schedules, and retention policies configured on an Avamar server.

**Procedure**

1. Select **Policy** on the menu bar.
2. From the **Systems** list, select the Avamar server.
3. Select whether to view policy information for a single domain or all domains on the Avamar server:
   1. To view policy information for all domains, select **All Domains**.
   2. To view policy information for a single domain, select **Single Domain** and then browse to and select the domain from the tree.
4. Select the type of policy information to view:
   - Groups
   - Clients
   - Datasets
   - Schedules
   - Retention Policies

   The policy information appears in a table on the Policy page. You cannot edit the policy settings. To edit the settings, use Avamar Administrator.

Running reports

The Reports page in Avamar Enterprise Manager enables you to run preconfigured reports on completed activities, licensing, capacity usage, and capacity forecasting.

The EMC Avamar Reports Guide provides details on the information available in each of the reports.

Procedure
1. Select Reports from the menu bar.
2. Select the Avamar server from the Systems list.
3. Select the report type from the Reports list.
4. Filter the range of data that appears in the report.
   - To limit the data in the report to a specific time period, select Time Period and then select a value from the Since list.
   - To limit the data in the report to a date and time range, select Date/Time Range, and then select the start and end dates and times in the From and To fields, respectively.
5. Click Run.

   The report appears in a table on the Reports page.
6. To export the report to a comma-separated values (.csv) file, click Export this report, and then browse to the location for the file.

Managing cron-based replication

Avamar Enterprise Manager enables you to configure cron-based replication and view status information for cron-based replication for multiple Avamar servers.

Cron-based replication was deprecated starting in Avamar 7.0 in favor of policy-based replication. Policy-based replication provides more granular control of the replication process. Avamar servers that were using cron-based replication before Avamar 7.0 can continue to use that replication method concurrently with or instead of policy-based replication.

Procedure
- To configure replication:
  a. Add both the source and destination servers to Avamar Enterprise Manager.
  b. Select Replicator > Setup.

    The Replicator Setup page appears.
c. Click the link for the source Avamar server in the **Source** column.

d. Configure the replication settings. *Configuring cron-based replication with Avamar Enterprise Manager on page 230* provides details on each of the settings.

- To view replication status information, select **Replicator > Status**.
  
  The **Replicator Status** page displays the source system, destination system, current status, suspension status, scheduled time, time the last replication completed, and status of the last replication for each Avamar server that you are monitoring.

- To start or stop replication:
  
  a. Select **Replicator > Status**.
  
  The **Replicator Status** page appears.

  b. Select the checkbox next to the source server.

  c. Click **Start Replication** or **Stop Replication**.

  When you stop replication, the process cancels any replication operation that is currently in progress if that replication operation was initiated by using Avamar Enterprise Manager. However, if the replication was initiated by a cron mechanism and you stop replication on that server, then the replication runs to completion.

### Managing server updates and hotfixes

The System Maintenance feature in Avamar Enterprise Manager enables you to download installation packages from the Avamar Downloader Service computer to an Avamar server and install the packages on the Avamar server. You can also view a list of installation packages in the local repository on the Avamar server, delete old installation packages from the Avamar server to reclaim storage, and view the history of installations on the Avamar server.

**Procedure**

1. Click **System Maintenance** on the menu bar.

2. Manage server updates and hotfixes:

   - To download and install server patches or hotfixes, click the **SW Updates** tab, select the Avamar server from the **Systems** list, and then click **Download** or **Install** next to the package.

   - To download and install workflow packages, click the **Maintenance** tab, select the Avamar server from the **Systems** list, and then click **Download** or **Install** next to the package.

   - To view a list of installation packages in the repository on the Avamar server, click the **Repository** tab and then select the Avamar server from the **Systems** list.

   - To delete old installation packages, click either the **SW Updates** or **Maintenance** tab, select the Avamar server from the **Systems** list, and then click **Delete** next to the package.

   - To view the history of installations on an Avamar server, click the **History** tab and then select the Avamar server from the **Systems** list.

### Starting Avamar Client Manager

You can open the Avamar Client Manager user interface from Avamar Enterprise Manager.

Avamar Client Manager is a web-based management application that provides centralized Avamar client administration capabilities for larger businesses and
enterprises. Avamar Client Manager facilitates the management of large numbers of Avamar clients.

To start Avamar Client Manager, select Client Manager from the menu bar. Avamar Client Manager on page 285 provides details on the functionality available in Avamar Client Manager.
CHAPTER 13

Avamar Client Manager

This chapter includes the following topics:

- Overview of Avamar Client Manager ................................................................. 286
- Starting Avamar Client Manager ....................................................................... 289
- Global tools ..................................................................................................... 289
- Overview .......................................................................................................... 297
- Clients .............................................................................................................. 301
- Policies ............................................................................................................ 318
- Queues ............................................................................................................ 320
- Logs ................................................................................................................... 321
Overview of Avamar Client Manager

Avamar Client Manager is a web-based management application that provides centralized Avamar client administration capabilities for larger businesses and enterprises. Avamar Client Manager facilitates the management of large numbers of Avamar clients.

Avamar Client Manager works with Avamar clients on a supported native operating system and Avamar clients on a supported operating system running in a VMware virtual machine. Avamar Client Manager cannot work with Avamar clients through virtual center, virtual machine, or virtual proxy configurations. The Avamar Client Manager UI displays supported Avamar clients and hides all unsupported clients.

Connection security

To secure data transmissions between a computer and the Avamar server, a secure connection is created using HTTPS.

This form of the HTTP protocol encrypts messages before they are sent and decrypts them when they are received. HTTPS is used for all login transmissions and for all transmission of data during registration and activation operations.

All attempts to access the Avamar server through the UI over standard HTTP protocol are redirected to HTTPS to prevent plain text transmissions.

Apache web server authentication

The Avamar Client Manager UI uses only secure web pages, and an authentication warning appears in web browsers that access those pages unless you install a trusted public key certificate on the Apache web server that is provided with Avamar.

The *EMC Avamar Product Security Guide* describes how to obtain and install a trusted public key certificate for the Apache web server.

Editing the session time-out period

When a session has been running for 72 hours or more without any interaction between the web browser and the Avamar Client Manager server, Avamar Client Manager ends the session. The automatic session time-out protects the security of the assets accessible through Avamar Client Manager. You can increase or decrease the time-out period.

When Avamar Client Manager ends a session, close the web browser window or tab in which the session was running, and restart Avamar Client Manager. Avamar Client Manager does not end a session while a commit task is in progress.

**Procedure**

1. Stop the Apache Tomcat server by typing the following command:

   `/usr/local/avamar/bin/emwebapp.sh --stop`

2. Open the following file in a text editor:

   `/usr/local/avamar-tomcat/webapps/aam/WEB-INF/web.xml`

3. Change the value of the `session-timeout` tag to a new value in minutes.

   The following example illustrates the `session-timeout` tag with the default value of 4320 minutes (72 hours):
<session-config>
    <session-timeout>4320</session-timeout>
</session-config>

4. Save and close the file.
5. Restart the Apache Tomcat server by typing the following command:
   /usr/local/avamar/bin/emwebapp.sh --start

Increasing the JavaScript time-out period

The Avamar Client Manager UI uses JavaScript to perform many of its tasks. Sometimes an Avamar Client Manager UI script requires more time to finish than is permitted by a web browser's default script time-out value.

When this happens, a message appears and the script is stopped. You can click continue to allow the script to finish its work.

To avoid seeing this message, increase the script time-out period. The steps depend on the web browser.

Increasing the JavaScript time-out period in Internet Explorer on Windows

Procedure
1. Open a registry editor, such as Regedt32.exe.
2. Open the following registry key:
   HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Styles
   If the key does not exist, create it.
3. Create a DWORD value called MaxScriptStatements under the key.
4. Set the value of the DWORD to 20,000,000.
   This number represents the number of script statements.
5. Restart the web browser.

Increasing the JavaScript time-out period in Firefox

Procedure
1. In the browser address bar, type about:config.
   A warning message appears.
2. Click I'll be careful, I promise!.
   The preferences window opens.
3. In Filter, type dom.max_script_run_time.
   The script runtime preference appears.
4. Double-click the preference.
   The Enter integer value dialog box appears.
5. Type 30 and click OK.
6. Restart the browser.
Avamar Client Manager configuration properties

Avamar Client Manager normally does not require any changes to its default configuration. However, some properties can be adjusted to suit a particular deployment requirement.

Avamar Client Manager properties are in the `/usr/local/avamar/etc/` `acm.properties` file.

The following table provides information about the properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>activation.retry.attempts</code></td>
<td>The number of client activation attempts made before activation fails.</td>
<td>24</td>
</tr>
<tr>
<td><code>activation.retry.frequency.minutes</code></td>
<td>The number of minutes between client activation attempts.</td>
<td>120</td>
</tr>
<tr>
<td><code>move.getactivities.retry.attempts</code></td>
<td>The number of checks to determine whether a client is inactive (so that it can be moved).</td>
<td>7</td>
</tr>
<tr>
<td><code>move.getactivities.frequency.seconds</code></td>
<td>The number of seconds between checks to determine whether a client is inactive (so that it can be moved).</td>
<td>5</td>
</tr>
<tr>
<td><code>move.queue.error.codes</code></td>
<td>Sets a comma-separated list of error codes that determine whether a move task failure is added to the queue. A move is only added to the queue if its failure generates one of these error codes. Use the value <code>none</code> to prevent all failed move tasks from being added to the queue. Use the value <code>empty</code> to add all failed move tasks to the queue.</td>
<td>22271, 22280, 22282, 22295, 30006, 30012, 30016, 30017, 30019</td>
</tr>
<tr>
<td><code>move.retry.attempts</code></td>
<td>Sets the number of times a failed move task will be retried.</td>
<td>24</td>
</tr>
<tr>
<td><code>move.retry.frequency.minutes</code></td>
<td>Sets the span of time in minutes between retry attempts.</td>
<td>120</td>
</tr>
<tr>
<td><code>toolbar.displaytime.client</code></td>
<td>Determines whether time displayed within Avamar Client Manager uses the time zone of the web browser’s host</td>
<td>true</td>
</tr>
</tbody>
</table>
Table 75 Avamar Client Manager configuration properties (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer or time zone of the Avamar server. The default value uses the time zone of the web browser's host computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>orgu.name.append.domain</td>
<td>Determines whether clients displayed in the Client Information area of the UI are listed using the client hostname or FQDN. The default value displays the FQDN for each client.</td>
<td>true</td>
</tr>
</tbody>
</table>

Changing an Avamar Client Manager configuration property

Procedure
1. Change the current working directory by typing the following command:
   `cd /usr/local/avamar/etc`
2. Open the Avamar Client Manager properties file, `acm.properties`, in a text editor.
3. Edit the value of the property.
4. Save and close the file.
5. Restart the Avamar Enterprise Manager service:
   `dpnctl stop ems`
   `dpnctl start ems`

Starting Avamar Client Manager

Start Avamar Client Manager either from Backup & Recovery Manager or Avamar Enterprise Manager.

Procedure
- To start Avamar Client Manager from Backup & Recovery Manager, log in to Backup & Recovery Manager and select Client Manager from the Launch menu.
- To start Avamar Client Manager from Avamar Enterprise Manager, log in to Avamar Enterprise Manager and click Client Manager on the menu bar.

Results
Avamar Client Manager appears in a new tab or window and opens the Overview page.

Global tools

Avamar Client Manager provides several tools that you can use with more than one page. Use these tools to help with the following tasks:
Selecting a server

Use the server selection field to display, and work with, information for a specific server.

Before you begin

Expand the Navigation panel on the left side of the UI so that the server selection field is visible at the top of the panel. Navigate to a page that displays the server selection field in an active, selectable, state.

Procedure

1. On the server selection field, click the arrow icon.

   When the server selection field is not visible, expand the Navigation panel on the left side of the UI. When the server selection field is not relevant to the current page view it appears in a dimmed state, that is, it is not active and selectable.

2. From the list of servers, select a server.

   The page view refreshes. Information about the server and its tasks appears.

Filters

Avamar Client Manager offers you a wide range of filters.

Use a filter to determine which objects appear in the list on the current page. Filters work with a variety of objects. The type of object and the available filters depend on the page’s context. In Avamar Client Manager you can filter the following types of objects:

- Servers
- Clients
- Policies
- Groups
- Tasks
- Log entries

Filters that apply to the current context appear on the Filters bar at the top of the page.

Searching by name

To find objects by comparing a search string to object names, use the search field.

Before you begin

Navigate to a view that has one of the following search-enabled fields on the Filters bar:

- User name
- Client name
- Group name
- Domain name

Use search to limit the list to objects with the same and similar names.
Procedure
1. Click the arrow next to the search-enabled field.
   A text entry box appears.
2. In the text entry box, type a search string.
   Avamar Client Manager compares the search string you type to the names of objects and includes matching objects on the list. Objects match when a portion of the name contains the search string.
3. Click  .

Results
Avamar Client Manager refreshes the list. The results include only matching objects.

Example 1  Searching by username
To include all clients that have a user with the characters "eng" in their username, type *eng* in the text entry field.

After you finish
(Optional) To remove the search string and to display all objects, click X next to the text entry field.

Search string rules
A search string is one or more characters that you type into a name search field. Avamar Client Manager compares the search string with all object names. When the search string matches all or part of an object's name, Avamar Client Manager adds the object's name to the results.

The following rules apply to a search string:
- No more than 24 characters
- Can use an asterisk (*) character to represent zero or more characters
- Cannot start with a period character
- Cannot include any of the characters listed in the Character column of the following table:

Table 76 Characters not allowed in search strings

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Unicode</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>Solidus</td>
<td>002F</td>
</tr>
<tr>
<td>:</td>
<td>Colon</td>
<td>003A</td>
</tr>
<tr>
<td>;</td>
<td>Semicolon</td>
<td>003B</td>
</tr>
<tr>
<td>?</td>
<td>Question Mark</td>
<td>003F</td>
</tr>
<tr>
<td>*</td>
<td>Quotation Mark</td>
<td>0022</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less-than Sign</td>
<td>003C</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater-than Sign</td>
<td>003E</td>
</tr>
<tr>
<td>\</td>
<td>Reverse Solidus</td>
<td>005C</td>
</tr>
<tr>
<td>,</td>
<td>Comma</td>
<td>002c</td>
</tr>
</tbody>
</table>
### Table 76 Characters not allowed in search strings (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Name</th>
<th>Unicode</th>
</tr>
</thead>
<tbody>
<tr>
<td>~</td>
<td>Tilde</td>
<td>007E</td>
</tr>
<tr>
<td>!</td>
<td>Exclamation Mark</td>
<td>0021</td>
</tr>
<tr>
<td>@</td>
<td>Commercial At</td>
<td>0040</td>
</tr>
<tr>
<td>#</td>
<td>Number Sign</td>
<td>0023</td>
</tr>
<tr>
<td>$</td>
<td>Dollar Sign</td>
<td>0024</td>
</tr>
<tr>
<td>%</td>
<td>Percent Sign</td>
<td>0025</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex Accent</td>
<td>005E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vertical Line</td>
</tr>
<tr>
<td>&amp;</td>
<td>Ampersand</td>
<td>0026</td>
</tr>
<tr>
<td>'</td>
<td>Apostrophe</td>
<td>0027</td>
</tr>
<tr>
<td>`</td>
<td>Grave Accent</td>
<td>0060</td>
</tr>
<tr>
<td>(</td>
<td>Left Parenthesis</td>
<td>0028</td>
</tr>
<tr>
<td>)</td>
<td>Right Parenthesis</td>
<td>0029</td>
</tr>
<tr>
<td>{</td>
<td>Left Curly Bracket</td>
<td>007B</td>
</tr>
<tr>
<td>}</td>
<td>Right Curly Bracket</td>
<td>007D</td>
</tr>
<tr>
<td>[</td>
<td>Left Square Bracket</td>
<td>005B</td>
</tr>
<tr>
<td>]</td>
<td>Right Square Bracket</td>
<td>005D</td>
</tr>
<tr>
<td>_</td>
<td>Low Line</td>
<td>005F</td>
</tr>
</tbody>
</table>

> a. An exception to this exclusion permits the solidus character in the Domain Name filter on the Policies page.

### Using the activity type filter

Use the activity type filter to limit a list to one type of activity.

**Before you begin**

Navigate to a view that includes Activity Type on the Filters bar.

**Procedure**

1. On the Filters bar, click the arrow next to Activity Type.
   
   A selection list appears, with the values: Backup and Restore.

2. Select a value.

   Select Backup to include only backup tasks in the list. Select Restore to only include restore tasks in the list.

   For example, in the Idle Clients section of the Clients page, select Backup on the Activity Type filter. Avamar Client Manager limits the list to clients without any backup activity during the defined period.

**Results**

Avamar Client Manager filters the results using the activity type you selected.
Using the client status filter

Use the client status filter to add clients with the specified client status to the list.

**Before you begin**

Navigate to a view that includes **Client Status** on the **Filters** bar.

**Procedure**

1. On the **Filters** bar, click the arrow next to **Client Status**.
   
   A selection list of the client statuses for all clients in that context appears.

2. Select a status.

   For example, in the **Add Clients** section of the **Clients** page, select **Activation Failure** on the **Client Status** filter. Avamar Client Manager limits the list to registered computers with at least one unsuccessful activation attempt. Avamar Client Manager refreshes the list. Only entries with the selected client status appear on the list.

3. Optional: Repeat the steps to select additional statuses.

**Results**

Avamar Client Manager refreshes the list. Only entries with the selected client statuses appear on the list.

Using the failure criteria filter

Use the failure criteria filter to define which clients Avamar Client Manager includes in a list of failed clients.

**Before you begin**

Navigate to a view that includes **Failure Criteria** on the **Filters** bar.

**Procedure**

1. On the **Filters** bar, click the arrow next to **Failure Criteria**.

   A selection list appears, with the values: **At least one activity failed**, **All activities failed**, and **Last activity failed**.

2. Select a value.

   The value you select determines which clients Avamar Client Manager includes in the list of failed clients. Avamar Client Manager includes only clients that match the selected activity status.

   For example, select **Last activity failed**. Avamar Client Manager refreshes the list and includes clients only when their most recent activity failed. The failed activity can be either a backup or a restore.

**Results**

Avamar Client Manager refreshes the list. Only clients with an activity status that matches the selected value appear on the list.

Using the OS filter

Use the OS filter to limit a list to clients with specific operating systems.

**Before you begin**

Navigate to a view that includes **OS** on the **Filters** bar.
Procedure
1. On the Filters bar, click the arrow next to OS.
   A list of the OS versions of all clients in that context appears.
2. Select an OS version.
   Avamar Client Manager refreshes the list. Only clients with the selected OS version appear on the list.
3. Optional: Repeat the steps to select additional OS versions.

Results
Avamar Client Manager refreshes the list. Only clients with the selected OS versions appear on the list.

Using the period filter
Use the period filter to define the calendar date boundaries of the displayed results.

Before you begin
Navigate to a view that includes Period on the Filters bar.

Procedure
1. On the Filters bar, click the arrow next to Period.
   A selection list appears, with the values: Before, After, and On.
2. Select a value.
3. Click the arrow next to the selected value.
   A date entry field and a small calendar icon appear.
4. Click the calendar icon, navigate to a specific date, and then click the date.
   Alternatively, in the date entry field, type a date using the format m/d/yy, and click.
   Avamar Client Manager refreshes the list. Only entries within the specified period appear on the list.
5. Optional: Further refine the results by repeating these steps using the other values.

Results
Avamar Client Manager refreshes the list. Only entries within the specified period appear on the list.

Using the status filter
Use the status filter to limit a list to entries with specific statuses.

Before you begin
Navigate to a view that includes Status on the Filters bar.

Procedure
1. On the Filters bar, click the arrow next to Status.
   A selection list of all statuses for all entries in that context appears.
2. Select a status.
   Avamar Client Manager refreshes the list. Only entries with the selected status appear on the list.
3. Optional: Repeat the steps to select additional statuses.

**Results**
Avamar Client Manager refreshes the list. Only entries with the selected statuses appear on the list.

**Using the status code filter**
Use the status code filter to limit a list to entries with specific status codes.

**Before you begin**
Navigate to a view that includes **Status Code** on the **Filters** bar.

**Procedure**
1. On the **Filters** bar, click the arrow next to **Status Code**.
   A selection list of the status codes for all entries in that context appears.
2. Select a status code.
   Avamar Client Manager refreshes the list. Only entries with the selected status code appear on the list.
3. Optional: Repeat the steps to select additional status codes.

**Results**
Avamar Client Manager refreshes the list. Only entries with the selected status codes appear on the list.

**Using the success criteria filter**
Use the success criteria filter to define which clients Avamar Client Manager includes in a list of successful clients.

**Before you begin**
Navigate to a view that includes **Success Criteria** on the **Filters** bar.

**Procedure**
1. On the **Filters** bar, click the arrow next to **Success Criteria**.
   A selection list appears, with the values: At least one activity successful, All activities successful, and Last activity successful.
2. Select a value.
   The value you select determines which clients Avamar Client Manager includes in the list of successful clients. Avamar Client Manager only includes clients that match the selected activity status.
   For example, select Last activity successful. Avamar Client Manager refreshes the list and only includes the clients with a successful backup or restore.

**Results**
Avamar Client Manager refreshes the list. Only clients with an activity status that matches the selected value appear on the list.

**Using the version filter**
Use the version filter to limit a list to clients with specific versions of the Avamar client software.

**Before you begin**
Navigate to a view that includes **Version** on the **Filters** bar.
Procedure
1. On the **Filters** bar, click the arrow next to **Version**. A selection list of the Avamar client software versions for all clients in that context appears.
2. Select a version. Avamar Client Manager refreshes the list. Only clients with the selected software version appear on the list.
3. Optional: Repeat the steps to select additional software versions.

**Results**
Avamar Client Manager refreshes the list. Only clients with the selected software versions appear on the list.

Viewing details
Use the Details panel to view context relevant details.

**Before you begin**
Navigate to a view that includes the Details panel or Details bar on the right-side.

**Procedure**
1. On the right-side of the page, click the Details bar. The Details panel expands.
2. In **Summary**, select an object. The page context determines the object type. An object can be a client or a group. You can select more than one object.

   Detailed information for the selected object appears in the Details panel.
3. (Optional) When you select more than one object, use the paging controls at the bottom of the Details panel to view information for each selected object.

Exporting data
Use export to download the selected summary as an Excel spreadsheet.

**Before you begin**
Navigate to a page view that includes **Export** on the page bar.

**Procedure**
1. On the page bar, click **Export**. Avamar Client Manager includes all information from the summary in the exported data.

   The web server pushes an Excel file containing the summary information to the browser.
2. Save the file to your computer.
3. Use an application that can read the Excel-formatted spreadsheets to open the file.

Setting the entries per page limit
Increase the limit on the number of entries displayed in summary lists.

By default, Avamar Client Manager limits its summary lists to 25 entries per page. When there are more entries than the current entries per page limit, the entries appear on 2 or
more pages. You can increase the entries per page limit to make it easier to work with many entries.

**Procedure**
1. On the status bar at the bottom of Avamar Client Manager, click **Entries Per Page**. The list of choices appears.
2. Click a number on the list.

**Results**
Avamar Client Manager sets the selected number as the new limit and refreshes the page.

**Viewing tool tips**

Enable and display tool tips to view concise help messages for various elements of the UI.

**Procedure**
1. On the status bar at the bottom of Avamar Client Manager, select **Show Tooltips**.
2. Hover the pointer over a user interface element that has a tool tip.

The following elements may have tool tips:
- Dashboard chart sections
- Controls
- Column headings

**Overview**

The Overview page provides access to high level information about the management of an enterprise’s Avamar clients.

From the left-side menu of the Overview page, select:
- **Server Summary** for information about a selected Avamar server.
- **Dashboard** for information about client backups.

**Server Summary**

The Server Summary page provides columns of information about the Avamar servers that you have registered with Enterprise Manager.

Filter this information by using the filters available on the Filters bar. Change the sorting method used for the list by clicking on a column heading.

In each of the following columns, nonzero values are hyperlinked to a more detailed report about that column’s information:
- Active Clients
- Idle Clients
- Successful Clients
- Failed Clients

**Server Summary columns**
The following table describes the columns on the Server Summary page.
### Table 77: Columns on the Server Summary page

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Hostname or IP address of the Avamar server. Only servers registered in Enterprise Manager are visible in Avamar Client Manager.</td>
</tr>
<tr>
<td>Total Clients</td>
<td>Total number of clients registered with the Avamar server. Does not include retired clients.</td>
</tr>
<tr>
<td>Active Clients</td>
<td>Total number of clients with activity (backup or restore) during the specified period.</td>
</tr>
<tr>
<td>Idle Clients</td>
<td>Total number of clients with no backup activity during the specified period.</td>
</tr>
<tr>
<td>Successful Clients</td>
<td>Total number of clients with a backup status that matches the value set in the Successful Backups filter. Also includes the average amount of time for those backups.</td>
</tr>
<tr>
<td>Failed clients</td>
<td>Total number of clients with failed backups during the specified period.</td>
</tr>
<tr>
<td>Clients with Restore</td>
<td>Total number of clients with restore activity (successful or unsuccessful) during the specified period.</td>
</tr>
</tbody>
</table>

### Dashboard

The Dashboard page provides a graphical snapshot view of a selected server. The dashboard provides information in panels that you can expand, collapse, or delete to create the view you need.

**Usage tips:**
- Collapse or expand a panel by clicking the arrow icon in the panel's title bar.
- Delete a panel by clicking the X in the panel's title bar.
- Return the dashboard to its default view by reloading the page in your web browser.

### Setting a panel's period

Set a panel's period to define the number of days of data in the display.

**Before you begin**

Navigate to the Dashboard page with any of the following panels displayed: Analyze, Backup Report, and Backup Trend.

**Procedure**

1. On a panel, in the period field, click the arrow icon.
   - The period field is available on the following panels:
     - Analyze
     - Backup Report
     - Backup Trend
   - The period list appears.
2. Select a period.
   - The available choices are:
     - Last 24 hours
• Last 7 days
• Last 30 days
Avamar Client Manager refreshes the panel with data for the selected period.

Client panel

The Client panel uses a pie chart to represent the total number of potential clients for the selected server. Colors represent the percentage of the total for:
• Activated
  Green represents the percentage of clients that the selected server has activated.
• Not activated
  Red represents the percentage of clients that the selected server has registered, but not activated.
• Free
  Gray represents the percentage of unused client connections available on the selected server.

Server panel

The Server panel provides a grid view of information about the selected server.

Table 78 Server information on the Server panel

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies the server’s node type: Single or Multi.</td>
</tr>
<tr>
<td>Active Backup</td>
<td>Number of running backups.</td>
</tr>
<tr>
<td>Backup in Queue</td>
<td>Number of backups in the server’s queue waiting to run.</td>
</tr>
<tr>
<td>Replication</td>
<td>Current state of the replication cron job:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Not running</td>
</tr>
<tr>
<td>Status</td>
<td>Current state of the server’s Management Console Server (MCS) system:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
</tbody>
</table>

Backup Trend panel

The Backup Trend panel is a line chart that shows the size of data backed up at specific points in time over a defined period. The x-axis represents points in time over the selected period. The y-axis represents the size of data in the backup at each point in time.

The line drawn between the plotted points represents the backup trend, which is the change in backed up data over time.

Client Type panel

The Client Type panel uses a bar chart to represent the number of activated clients of each category that a server has:
• Regular
  All activated clients that do not fit into one of the other three categories.
vMachine
Guest clients; the virtual computers backed up through Avamar client software running on the host computer.

Proxy
Proxy virtual machine clients; clients that use Avamar for VMware image backup and restore.

vCenter
Avamar clients that protect vCenter management infrastructure by backing up vCenter hosts.

Analyze panel
The Analyze panel uses a bar chart to represent the number of clients that are in each of the following states during the selected period:

- **Successful**
  Clients with at least one successful backup.

- **Failed**
  Clients with backup activity but no successful backups.

- **Idle**
  Clients with no backup activity.

Backup Report panel
For backups attempted during the selected period, the Backup Report panel uses a bar chart to represent the number of each of the following results:

- **Successful**
  Successfully completed backups; with or without errors.

- **Failed**
  Backups that failed to complete.

- **Canceled**
  Backups canceled before completion.

Client Queues panel
The Client Queues panel uses a bar chart to display the number of clients in each of the following queues:

- **Upgrade**
- **Move to server**
- **Activation**

Storage Capacity panel
The Storage Capacity panel uses a pie chart to represent the total storage capacity of the selected server. Colored slices represent the following:

- **Used**
  Red represents the portion of storage that contains data.

- **Free Capacity**
  Green represents the portion of storage that is unused and available.
Backup Health panel

The Backup Health panel uses a bar chart to represent the number of clients that have retained backup data for specific periods of time. The panel uses the periods: 1 day, 30 days, 60 days, and 90 days.

On the bar chart, the x-axis represents the period that Avamar has retained the data and the y-axis represents the number of clients.

Clients

The Clients page provides information and tools for working with Avamar clients.

From this page you can:
- Select the computers in your enterprise's domain and add them as Avamar clients
- View detailed information about individual clients
- Move, retire, and delete clients
- Change a client's group associations
- Upgrade the Avamar software on the client

To navigate between the sections of the Clients page, select from the choices in the left-side menu.

Client and server tools

Avamar Client Manager provides several tools to help manage Avamar clients and Avamar servers.

A tool only appears when it is relevant to the context. Changes made by the tool apply to the selected client and the selected server. Launch a tool by clicking its command button.

Creating an Avamar domain

Create an Avamar domain to add a new branch to an Avamar server's administrative hierarchy.

Before you begin

Navigate to a view that includes Create Domain: either the Add New Clients dialog box or the Client Move dialog box.

Procedure

1. In the Domain Selection pane, select the location for the new domain.
   
   To locate the new domain directly beneath the root domain, select the server icon. To locate the new domain beneath another domain, select that domain.

2. Click Create Domain.
   
   The New domain dialog box appears.

3. In New Domain Name, type a name for the domain.

   Avamar does not allow the following characters in a domain name: =~!@#$%^ () {} [] ;/ :*<>"&+

4. Optional: Type information in the Contact, Phone, Email, and Location fields.

5. Click OK.
Results
Avamar Client Manager adds the new domain to the selected server and the new domain appears on the Domain Selection pane.

Viewing a client’s group associations
To determine the policies that apply to a client, view the client’s group associations.

Before you begin
Navigate to a view that includes Group Associations on the Actions bar.
A client’s group associations determine the client’s backup dataset, the client’s backup schedule, and the client’s backup retention period.

Procedure
1. Select a client.
2. Click Group Associations.

Results
The Groups for Client dialog box appears and lists the client’s groups.

Adding group associations to a client
To apply the policies of a group to a client, add the group association to the client.

Before you begin
Navigate to a view that includes Group Associations on the Actions bar.
This task results in an association between a client and a group. The Avamar server applies the group’s policies to the client.

Procedure
1. Select a client.
2. Click Group Associations.
3. On the Groups for Client dialog box, click Add Groups.
   The Add Groups for Client dialog box appears.
4. Select a group.
   You can select more than one group.
5. Click Add.

Results
Avamar Client Manager adds the group associations to the client.

Creating a group
To make a new set of policies available for assignment to clients, create a group with the policies. The Create Group command is available when adding a client to a group, and when moving a client to a new domain or to a new server.

Before you begin
Navigate to a view that includes Create Group: either the Add Groups dialog box or the Client Move dialog box.
Procedure
1. Click **Create Group**.
   
   On the **Client Move** dialog box selecting a domain enables the button.
   
   The **Create Group in Domain** dialog box appears.
2. In **Group Name**, type a name for the new group.
   
   Avamar does not allow any of the following characters in a group's name: 

   "\~!@$^%(){}[]\|,`;#\/:*?<>'"&+

3. (Optional) Select **Enable** to enable scheduled backups of clients that you assign to the group.
   
   Clear this checkbox to disable scheduled backups of clients that you assign to the group.
4. In **Dataset**, select a dataset for the group.
5. In **Schedule**, select a schedule for the group.
6. In **Retention Policy**, select a retention policy for the group.
7. Click **OK**.

Results
Avamar Client Manager creates the new group in the selected domain.

Removing group associations from a client

To stop applying a group's policies to a client, remove the group association from the client.

**Before you begin**

Navigate to a view that includes **Group Associations** on the Actions bar.

This task removes the association between a client and a group. When you complete the task the group's policies no longer apply to the client.

**Procedure**

1. Select a client.
2. Click **Group Associations**.
3. On the **Groups for Client** dialog box, select a group.
   
   You can select more than one group.
4. Click **Remove**.

**Results**

Avamar Client Manager removes the association between the client and the selected groups.

Overriding group policy settings for a client

To modify policies applied to a client, override the policies of its group.

**Before you begin**

Navigate to a view where **View/Edit Details** appears on the Actions bar and the client appears in the clients list.
Procedure
1. Select a client.
2. On the Actions bar, click View/Edit Details.
   The Client Details dialog box appears.
3. Select the Advanced tab.
   The policy override settings appear with the client's current state shown.
4. Make changes to the client's current state by selecting or clearing settings.
5. Click OK.

Results
Avamar Client Manager changes the group policy settings for the client.

Group policy override settings
To modify a policy applied to a client, use one of the policy override settings.
The following table describes the policy override settings on the Advanced tab of the Client Details dialog box.

Table 79 Settings on the Advanced tab of Client Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override group retention</td>
<td>Permits you to assign to a client a retention setting that is different from the group setting. After selecting this option, assign a retention setting by selecting it from the Select an existing retention policy list.</td>
</tr>
<tr>
<td>Select an existing retention policy</td>
<td>List of available retention settings that you can assign to a client. To use this list, first select Override group retention.</td>
</tr>
<tr>
<td>Disable all backups</td>
<td>Disables all backups of the client. Users can still restore data.</td>
</tr>
<tr>
<td>Activated</td>
<td>Places a registered client in an activated state. When you clear this setting, users cannot perform backups or restores.</td>
</tr>
<tr>
<td>Allow client-initiated backups</td>
<td>Permits users to begin backups from the client.</td>
</tr>
<tr>
<td>Allow file selection for client-initiated backups</td>
<td>Permits users to select files to include in backups started from the client. The Exclude list for the group's dataset does not apply.</td>
</tr>
<tr>
<td>Allow client to add to dataset</td>
<td>Permits users to add folders to the datasets of the client's groups. The following rules apply to this setting:</td>
</tr>
<tr>
<td></td>
<td>• The Avamar server filters the added data with the group's Exclude list and Include list.</td>
</tr>
<tr>
<td></td>
<td>• The added data is in every scheduled and on-demand backup for each group assigned to the client.</td>
</tr>
<tr>
<td></td>
<td>• User must have access to the Avamar client web UI to add folders or remove folders.</td>
</tr>
<tr>
<td>Allow client to override daily group schedules</td>
<td>Permits users to select a start time for scheduled backups that is different from the start time assigned by the group. Prerequisites:</td>
</tr>
<tr>
<td></td>
<td>• Add time entries to the Avamar server's Override schedule.</td>
</tr>
</tbody>
</table>
### Viewing summary information about a client

Use Client Details to see information about a client and its users.

**Before you begin**

Navigate to a view where View/Edit Details appears on the Actions bar and the client appears in the clients list.

**Procedure**

1. Select a client.
2. On the Actions bar, click View/Edit Details.
   
   The Client Details dialog box appears.
3. Select the Summary tab.

**Results**

Information about the client appears. Also, a list of users associated with the client appears.

### Changing a client's name on the server

When you change a computer’s name, you must also change its client name on the Avamar server.

**Before you begin**

Change the client’s name on the client, and in DNS, before performing this task. Navigate to a view where View/Edit Details appears on the Actions bar and the client appears in the clients list.

**Procedure**

1. Select a client.
2. On the Actions bar, click View/Edit Details.
   
   The Client Details dialog box appears.
3. Select the Summary tab.
4. In Client name, type the new name for the client.
5. Click OK.

---

**Table 79** Settings on the Advanced tab of Client Details (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a daily schedule to the client’s group.</td>
<td>• Assign a daily schedule to the client’s group.</td>
</tr>
<tr>
<td>Provide users access to the Avamar client web UI to</td>
<td>• Provide users access to the Avamar client web UI to allow them to select a new schedule.</td>
</tr>
<tr>
<td>allow them to select a new schedule.</td>
<td></td>
</tr>
<tr>
<td>Allow client to override retention policy on client-</td>
<td>Assigns the retention policy specified in Select an existing retention policy to client-initiated backups. Prerequisites:</td>
</tr>
<tr>
<td>initiated backups</td>
<td>• Enable Override group retention.</td>
</tr>
<tr>
<td></td>
<td>• Enable Allow client-initiated backups.</td>
</tr>
</tbody>
</table>
Results
Avamar Client Manager changes all references on the server to the new client name.

Viewing a client's backup history
To determine whether an Avamar server has backed up a client as expected, view the client’s backup history.

Before you begin
Navigate to a view where View/Edit Details appears on the Actions bar and the client appears in the clients list.

Procedure
1. Select a client.
2. On the Actions bar, click View/Edit Details.
   The Client Details dialog box appears.
3. Select the Backups tab.
4. In From, select the earliest date of the period to view.
5. In To, select the latest date of the period to view.
6. (Optional) Select On-demand backups.
   Select this choice to include user-initiated backups in the results. Clear this choice to exclude those backups.
7. (Optional) Select Scheduled backups.
   Select this choice to include backups initiated by a group schedule in the results. Clear this choice to exclude those backups.

Results
A list of the client's backups that match the filter settings appears.

Viewing a client's installed plug-ins
View the Avamar plug-ins installed on an Avamar client to help determine the types of data in its backups.

Before you begin
Navigate to a view where View/Edit Details appears on the Actions bar and the client appears in the clients list.

Procedure
1. Select a client.
2. On the Actions bar, click View/Edit Details.
   The Client Details dialog box appears.
3. Select the Plug-ins tab.

Results
The plug-ins installed on the client appear.
Deleting a client from a server

To remove a client's records and backups from an Avamar server, delete the client from the server.

**Before you begin**

Navigate to a view where the client appears in the client list and **Delete** appears on the Actions bar.

When Avamar Client Manager deletes a client from an Avamar server it stops all activity with that client, deletes the client's backups, and removes all record of the client from the server's database.

**Procedure**

1. Select a client.
2. On the Actions, bar, click **Delete**.
3. On the **Confirm** dialog box, type your password.
   - Use the password of the account logged into Avamar Client Manager.
4. Click **OK**.
   - The **Alert** dialog box appears.
5. Click **OK**.

**Results**

Avamar Client Manager runs a background process that removes all the client's information and data from the server.

**Add Clients**

The Add Clients section provides information and tools to register and activate your enterprise computers as Avamar clients.

Use the Add Clients section to import information about the computers in your enterprise. You can import the information from your LDAP v.3-compliant naming system or from a CSV file.

After import, you can filter the information by client status and client name to help in the selection of prospective Avamar clients.

You can use Avamar Client Manager to register and activate the selected computers to an Avamar server. Completion of the activation process requires installation of the Avamar client software on the computers and access to that software from the server. The normal workflow is to install the client software on a computer before you select it for activation.

**Directory service information**

You can use your enterprise's directory service to provide Avamar Client Manager with information about the computers that are potential Avamar clients.

Any LDAP v.3-compliant directory service can be used, such as Microsoft Active Directory.

When you use this method, Avamar Client Manager queries your enterprise's directory service to obtain information about clients and, if available, directory service organizational units, such as directory domains, and directory groups.

Before using the directory service method, complete LDAP server configuration for Avamar Enterprise Manager as described in the administration guide.

This method also requires the following:
TCP/IP access to your enterprise’s LDAP v.3-compliant directory service from the server that is running Avamar Enterprise Manager.

- Account information for a user account with read access to the directory service.
- The name of the directory service domain for the computers that you want to import.

Importing information from a directory service

To prepare to add computers as Avamar clients, import information about the computers from the directory service.

Before you begin

Do the following:

- Ensure access to your enterprise's LDAP v.3-compliant directory service from the server that is running Avamar Enterprise Manager.
- Obtain a username, and its associated domain and password for an account with read access to the directory service.
- Have available the name of the directory service domain of the computers.

Procedure

1. In the left-side menu, click Clients > Add Clients.
2. On the Actions bar, click New Clients.
   
   The Client Information Source dialog box appears.
4. In User Domain, select the domain of the account you are using to access the directory service.
   
   To add directory service domains to this list, refer to the administration guide.
5. In User Name, type the name of the account.
6. In Password, type the password of the account.
7. In Directory Domain, select the name of the directory service domain for the computer information you are importing.
8. Click OK.

Results

Avamar Client Manager imports the information from the directory service.

After you finish

Using the imported computer information, select and activate computers as clients of an Avamar server.

CSV file information

You can use a comma-separated values (CSV) file to provide Avamar Client Manager with information about the computers that are potential Avamar clients.

You can create the CSV file manually or you can create it by using the output of a Systems management tool such as the Microsoft System Center Configuration Manager or the Microsoft Systems Management Server.

When a Systems management tool creates the CSV file after an installation of the Avamar client software, only those clients that have the software successfully installed appear in Avamar Client Manager.
During the upload of a CSV file, Avamar Client Manager checks the file for correct formatting, and cancels the upload when it finds a problem.

**CSV file format**

A correctly formatted CSV file complies with the following rules:

- At least two rows.
- Values separated by a comma only.
- The first row of the file must consist of the literal names for each type of value. The name for the first value is **Hostname**. The name for the second value is **Group**.
- The second row, and all subsequent rows, must have at least one value and no more than two values.
- The formatting rules require a first value that is a valid hostname for a computer and a trailing comma.
- The second value is optional, but when you include it, it must be the directory service logical group name for the computer. When you do not provide the second value for a computer, Avamar Client Manager lists the computer at the root level in the hierarchical display.
- In the second value, use a forward slash (/) to separate the hierarchical levels of the directory service logical group name.

If you use spreadsheet software to create or edit the client list, do not add a comma with the value to try to create comma separated values. This can result in an incorrectly formatted file. When you save the client list in the editor as a CSV file type, the editor adds the comma separators as part of the file conversion process. To check the formatting, open the client list in a plain text editor.

**Example of a correctly formatted client list file**

In a plain text editor, a correctly formatted client list file looks like the following example.

<table>
<thead>
<tr>
<th>Hostname, Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1-desktop.Acme.corp.com,acme.corp/USA/MA</td>
</tr>
<tr>
<td>User1-laptop.Acme.corp.com,acme.corp/USA/CA/SFO</td>
</tr>
<tr>
<td>User2-desktop.Acme.corp.com,acme.corp/Engineering</td>
</tr>
<tr>
<td>User3-desktop.Acme.corp.com,</td>
</tr>
<tr>
<td>User4-desktop.Acme.corp.com,</td>
</tr>
</tbody>
</table>

The first line lists the literal names of each type of value.

The second line contains the hostname **User1-desktop.Acme.corp.com**, the separating comma, and the group **acme.corp/USA/MA**.

The third line contains the hostname **User1-laptop.Acme.corp.com**, the separating comma, and the group **acme.corp/USA/CA/SFO**.

The fourth line contains the hostname **User2-desktop.Acme.corp.com**, the separating comma, and the group **acme.corp/Engineering**.

The fifth and sixth lines contain only the hostnames **User3-desktop.Acme.corp.com** and **User4-desktop.Acme.corp.com**, each followed by a comma. The formatting rules require a comma, even without a group. The lines do not list groups, so both hostnames appear at the root level of the hierarchical display.
Uploading information in a CSV file

To prepare to add computers as Avamar clients, upload information about the computers in a comma-separated values (CSV) file.

Before you begin
Generate or create a correctly formatted CSV file and have a copy available on the web browsing computer.

Procedure
1. In the left-side menu, click Clients > Add Clients.
2. On the Actions bar, click New Clients.
   The Client Information Source dialog box appears.
3. Select CSV File.
4. Click Browse.
   The Choose File to Upload dialog box appears.
5. Navigate to your CSV file, select it, and click Open.
6. On the Client Information Source dialog box, click OK.

Results
Avamar Client Manager uploads the information from the CSV file.

After you finish
Using the uploaded computer information, select and activate computers as clients of an Avamar server.

Activation

Activation consists of changing the relationship between a computer and an Avamar server to enable the server to manage backups of the computer.

The relationship moves through three states:

- No relationship
  The computer is unknown to the server. Computers in this state appear in Add Clients, when you first add the computer information to Avamar Client Manager.

- Registered
  Avamar Client Manager entered the information about the computer into the Avamar server's database. Computers in this state appear in Registered Clients after Avamar
Client Manager starts the activation process and completes registration with the Avamar server. The changed state of these computers also appears in **Add Clients**.

- **Activated**
The computer has Avamar client software installed and running. The client software and the server are in communication and have exchanged an encrypted key to verify their identities. Computers in this state appear in **Activated Clients** after activation is complete. The changed state of these computers also appears in **Add Clients** and **Registered Clients**.

A computer that is in the activation process appears on the *Queues* page, in **Activation**. Avamar Client Manager attempts to activate a computer every 2 hours until it succeeds or until it reaches the limit of 24 attempts. When the process completes, Avamar Client Manager removes the computer from this view and adds an entry on the *Logs* page, in **Activation**.

**Activating your computers**
To enable backup management of a client, activate it with an Avamar server.

**Before you begin**
Install Avamar client software on the computers being activated and import information about the computers from either your directory service or a CSV file.

**Procedure**
1. On the left-side menu, click **Clients > Add Clients**.
   A hierarchical view of the computers in your enterprise appears. Avamar Client Manager generates this view from the information that you imported.
2. Browse or search the hierarchy to find the computers to activate.
3. Select each computer to activate.
   To select all computers in a folder, expand the folder to show the computers, then select the folder.
4. Click **Activate**.
   The *Server - Domain Selection* dialog box appears.
5. Expand the listing for a server, and select an Avamar domain.
   Avamar Client Manager assigns the computers to the selected server and domain during activation.
6. Click **Next**.
   The *Server - Group Selection* dialog box appears.
7. Select a group or multiple groups.
   Avamar Client Manager assigns the computers to the selected group or groups during activation.
8. Click **Finish**.

**Results**
Avamar Client Manager sends the activation task to the queue.

**After you finish**
Check the **Activation** section of the *Queues* page to determine the status of the activation process. After the process completes, check the **Activation** section of the *Logs* page to determine its final status.
Registered Clients

Clients that an Avamar server has registered but not activated appear in the Registered Clients section.

Use this section to select clients and perform the following client-related tasks:

- Activate
- Delete
- Associate with groups
- View and edit details
- Add and remove group override settings

Activating a registered client

To enable backup management of a registered client that failed to activate when registered, activate it from the Registered Clients section.

Before you begin

Install Avamar client software on the computers you want to activate.

When activation of a computer as a client of an Avamar server fails, Avamar Client Manager still registers the computer with the server. You can correct any problems that prevented the activation and retry it.

Procedure

1. On the left-side menu, click Clients > Registered Clients.
2. Select each client to activate.
3. Click Activate.

Results

Avamar Client Manager sends the activation task to the queue.

After you finish

Check the Activation section of the Queues page to determine the status of the activation process. After the process completes, check the Activation section of the Logs page to determine its final status.

Activated Clients

Activated clients of the selected Avamar server appear in the Activated Clients section.

Use the Activated Clients section to perform the following tasks:

- Move client to a different server
- Move client to a different Avamar domain
- Retire a client
- Delete a client
- Manage a client’s group associations
- View and edit a client’s details
- Add and remove group override settings
Moving a client to a new server

To use a new Avamar server to manage an Avamar client, move the client's registration, activation, and backups to the new server.

Before you begin
Do the following:

- Select a client activated to a server with Avamar server software version 5.0.1.31 or newer.
- For a client activated with an Avamar server older than version 6.x, fully initialize the MCS process on that server.

Procedure

1. On the left-side menu, click Clients > Activated Clients.
2. Select a client.
   - Do not select an NDMP client. Do not select a client that has backups on a Data Domain server.
3. On the Actions bar, click Move.
   - The Domain Selection pane of the Client Move dialog box appears.
4. At the top of the Domain Selection pane, from the server selection list, select the Avamar server that is the target of the move.
   - The target server's domains appear in the Domain Selection pane.
5. In the Domain Selection pane, select the target domain.
6. Click Next.
   - The Group Selection pane of the Client Move dialog box appears.
7. Select a target group.
   - You can optionally select more than one target group. Avamar Client Manager adds the client to all selected groups.
8. In Replicate Existing Backups at the bottom of the Group Selection pane, select a value.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Replicate all of the client's backups to the target server.</td>
</tr>
<tr>
<td>Last</td>
<td>Replicate only the last backup.</td>
</tr>
<tr>
<td>None</td>
<td>Replicate none of the backups.</td>
</tr>
</tbody>
</table>

Replication makes the backups available from the target server.

9. Optional: In Delete From Source:
   - Select to remove all the client’s backups from the source server.
   - Clear to move the source server's registration of the client to the source server's MC_RETIRED domain and retain copies of the client's backups on the source server.

10. Click Finish.

   The Confirm Replication Authentication dialog box appears.
11. In **Source Server**, type the password for the repluser account on the source server.
12. In **Target Server**, type the password for the repluser account on the target server.
13. Click **OK**.

**Results**
In a background process, Avamar Client Manager moves the client to the selected target.

### Moving a client to a different Avamar domain

To change the administrative relationship between an Avamar client and an Avamar server you can move the client to a different Avamar domain.

**Before you begin**
Select a client activated to a server with Avamar server software version 6.x or newer.

**Procedure**
1. On the left-side menu, click **Clients > Activated Clients**.
2. Select a client.
3. On the **Actions** bar, click **Move**.
   - The **Client Move** dialog box appears.
4. In the **Domain Selection** pane of the **Client Move** dialog box, select the target domain.
5. Click **Next**.
   - The **Group Selection** pane appears on the **Client Move** dialog box.
6. Select a target group.
   - You can optionally select more than one target group. Avamar Client Manager adds the client to all the selected groups.
7. Click **Finish**.
   - An alert box appears.
8. Click **OK**.

**Results**
In a background process, Avamar Client Manager moves the client to the selected target.

### Retiring a client

When you no longer need to run backups of a client, retire it. Avamar Client Manager retains backups that exist at the time of retirement so that you can restore data when necessary.

**Procedure**
1. On the left-side menu, click **Clients > Activated Clients**.
2. Select a client.
   - You can select more than one client. The retention policy setting you select applies to all selected clients.
3. On the **Actions** bar, click **Retire**.
   - The **Retire Client** dialog box appears.
4. In **Select Retention Policy**, select one of the options.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retire client and retain backups with existing expiration date</td>
<td>The Avamar server retains the backups for the existing retention period</td>
</tr>
<tr>
<td>Retire client and retain all backups indefinitely</td>
<td>The Avamar server retains the backups until you manually delete them</td>
</tr>
<tr>
<td>Retire client and reset backup expiration date</td>
<td>The Avamar server retains the backups until the date set in New Expiration Date</td>
</tr>
</tbody>
</table>

5. If you select **Retire client and reset backup expiration date** in the previous step then, in **New Expiration Date**, select a date.
   
The Confirm dialog box appears.

6. Click **Yes**.
   
The Alert dialog box appears.

7. Click **OK**.

**Results**

In a background process, Avamar Client Manager retires the selected client.

## Failed Clients

Clients that have unsuccessful backup or restore activity appear in the Failed Clients section.

Use the Failed Clients section to perform the following tasks:

- Delete a client
- Manage a client's group associations
- View and edit a client's details
- Add and remove group override settings

When working with failed clients, use the filters described in the following table.

**Table 80 Failed client filters**

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Specifies the period that Avamar Client Manager examines.</td>
</tr>
<tr>
<td>Activity Type</td>
<td>Specifies the type of activity that Avamar Client Manager examines.</td>
</tr>
<tr>
<td>Failure Criteria</td>
<td>Defines the failure threshold used by Avamar Client Manager.</td>
</tr>
</tbody>
</table>

## Idle Clients

Clients activated with an Avamar server that do not have activity during a specified period appear in the Idle Clients section.

When working with idle clients, use the **Period** filter to specify the period that Avamar Client Manager examines for activity, and the **Activity Type** filter to specify the type of activity.

Use the Idle Clients section to perform the following tasks:

- Delete a client
• Manage a client's group associations
• View and edit a client's details
• Add and remove group override settings

Upgrade Clients

The Upgrade Clients section provides information and tools you can use to apply upgrades and hot fixes to Avamar clients.

Use the Upgrade Clients section to perform the following tasks:
• Download an upgrade package to a server
• Select an upgrade package
• Apply the package to selected clients
• Remove an upgrade package from a server

Upgrade Clients section requirements

Before using the Avamar Client Manager Upgrade Clients section, do the following:
• For each client or plug-in, install the minimum client version listed in the EMC Avamar Push Client upgrade compatibility table of the EMC Avamar Compatibility and Interoperability Matrix. Obtain the latest version of this document from EMC Online Support (https://support.emc.com).

Note
Use of the Upgrade Clients feature to upgrade Avamar client software on Windows cluster nodes is not supported. The EMC Avamar for Windows Server User Guide describes how to upgrade Avamar client software on Windows cluster nodes.

• Install Avamar server version 6.0 and newer on the Avamar servers associated with the clients and plug-ins selected for upgrade.
• Install, configure, and run the Avamar Downloader Service. The Avamar Downloader Service obtains the client packages and plug-in packages required by the upgrade feature. This service pulls the packages from EMC and pushes them onto the Avamar data server subsystem (GSAN). After the packages are updated in GSAN, the packages appear in the Avamar Client Manager Select Package window, and upgrades can be performed.

Multiple system deployments

For Avamar deployments that involve more than one Avamar system, Avamar Client Manager running on one of the Avamar systems (managing system) can be used to manage clients associated with other Avamar systems (managed systems).

The managed systems must meet the following requirements:
• Managed system is added to Enterprise Manager on the managing system. Adding managed systems to Enterprise Manager on the managing system provides the managing system with the information it needs to support client upgrades on the managed systems.
• Managed system is running the same version of Avamar software as the managing system.

The same version requirement ensures that all packages required by clients on the managed systems are available for deployment through the managing system.
To provide full client upgrade support for clients associated with Avamar systems that do not meet the same version requirement, run Avamar Client Manager on those systems.

Downloading upgrade and hotfix packages
Use Avamar Client Manager to download upgrade and hotfix packages to an Avamar server.

Before you begin
Do the following:
- Install and configure the Avamar Downloader Service and the AvInstaller service. Refer to the administration guide for information about these tasks.
- Select an Avamar server.

Before applying an upgrade or hotfix package to an Avamar client, download the package to the Avamar server associated with the Avamar client.

Procedure
1. On the left-side menu, click Clients > Upgrade Clients.
2. On the Actions bar, click Select Package.
   The Upgrade Client dialog box appears.
3. In the Status column for the package, click Download.
   The status of the package must be Available.

Results
Avamar Client Manager begins the download. A progress bar appears. After the download finishes, Avamar Client Manager updates the package status, in sequence, to each of the following values: Waiting, Processing, and Ready.

Selecting an upgrade package
Select an upgrade package or hotfix package to apply to Avamar clients.

Before you begin
Do the following:
- Install and configure the Avamar Downloader Service and the AvInstaller service. Refer to the administration guide for information about these tasks.
- Select an Avamar server.
- Download the upgrade or hotfix package to the selected Avamar server.

Procedure
1. On the left-side menu, click Clients > Upgrade Clients.
2. On the Actions bar, click Select Package.
   The Upgrade Client dialog box appears.
3. Select a package.
   Before you can select a package, the package must have a Ready status.
4. Click Select.
   The Upgrade Client dialog box closes.

Results
The Avamar clients that are eligible for the upgrade or the hotfix appear.
After you finish
Select clients and apply the upgrade or hotfix package to them.

Applying the upgrade package
Select Avamar clients and apply the upgrade package or hotfix package.

Before you begin
Select an upgrade package or hotfix package. View the list of Avamar clients that are eligible for the selected package.

Procedure
1. From the list of Avamar clients that are eligible for the upgrade or the hotfix, select a client.
   You can select more than one client.
2. On the Actions bar, click Upgrade.

Results
Avamar Client Manager starts upgrading the selected clients. The upgrade runs in the background.

After you finish
Track the progress of the upgrade in the Upgrade section of the Queues page. View the final status of the upgrade in the Upgrade section of the Logs page.

Deleting upgrade and hotfix packages
Use Avamar Client Manager to delete upgrade and hotfix packages from an Avamar server.

Before you begin
Select an Avamar server that has an unneeded upgrade or hotfix package.

Procedure
1. On the left-side menu, click Clients > Upgrade Clients.
2. On the Actions bar, click Select Package.
   The Upgrade Client dialog box appears.
3. Select a package.
   You can only delete packages that have a Ready status.
4. Click Delete.

Results
Avamar Client Manager removes the selected package from the Avamar server.

Policies

The Policies page provides access to group policies and to group members.
The Policies page includes a summary view of the policies for the groups on the selected Avamar server.
Use the Policies page to perform the following tasks:
- Add clients to a group
Adding clients to a group

To apply the policies of a group to clients, add the clients to the group. This task results in an association between a client and a group. The Avamar server applies the group's policies to the client.

Procedure
1. Click Policies > Groups.
2. Select a group.
3. Click Edit Group Members. The Edit Group Members dialog box appears.
4. Click Add.
   The Add Clients to Group dialog box appears.
5. Select a client.
   You can select more than one client.
6. Click Add.

Results
Avamar Client Manager adds the clients to the group.

Removing clients from a group

To remove the policies of a group from clients, remove the clients from the group. This task removes the association between a client and a group. When you complete the task the group's policies no longer apply to the client.

Procedure
1. Click Policies > Groups.
2. Select a group.
3. Click Edit Group Members. The Edit Group Members dialog box appears.
4. Select a client.
   You can select more than one client.
5. Click Remove.

Results
Avamar Client Manager removes the clients from the group.

Viewing a group's dataset policy

Use a group's entry on the Policies page to view details of the group's dataset policy.

Procedure
1. Click Policies > Groups. A summary view of the groups on the selected server appears.
2. On a group’s entry, in the Dataset column, click the name of the dataset policy.

Results
The selected group's dataset policy details appear in a dialog box.

Viewing a group's retention policy

Use a group's entry on the Policies page to view details of the group's retention policy.

Procedure
1. Click Policies > Groups.
   A summary view of the groups on the selected server appears.
2. On a group’s entry, in the Retention column, click the name of the retention policy.

Results
The selected group's retention policy details appear in a dialog box.

Viewing a group's schedule policy

Use a group's entry on the Policies page to view details of the group's schedule policy.

Procedure
1. Click Policies > Groups.
   A summary view of the groups on the selected server appears.
2. On a group’s entry, in the Schedule column, click the name of the schedule policy.

Results
The selected group's schedule policy details appear in a dialog box.

Queues

The Queues page provides access to the Avamar Client Manager activity queues.

The Queues page provides a summary view of active and pending Avamar Client Manager tasks for the selected Avamar server. Tasks appear in separate sections based on the type of task, as follows:

- Activation
  Click Queues > Activation to view active and pending tasks related to client activation.

- Delete
  Click Queues > Delete to view active and pending tasks related to the removal of clients from Avamar servers.

- Move
  Click Queues > Move to view active and pending tasks related to moving clients from one Avamar server to another.

- Retire
  Click Queues > Retire to view active and pending tasks related to retiring Avamar clients.

- Upgrade
  Click Queues > Upgrade to view active and pending tasks related to upgrading the software on Avamar clients.

Use the Queues page to perform the following tasks:
View the details of active and pending tasks

Cancel tasks

## Canceling a task

Cancel a pending task to prevent it from running.

You can stop a task from running by canceling it while it is in the pending state.

### Procedure

1. On the left-side menu, click Queues > task_queue, where task_queue is the Queues page section for the type of task you are canceling.
   
   For example to cancel a client activation, click Queues > Activation.
2. Select a task.
3. Click Cancel.
   
   A confirmation dialog box appears.
4. Click OK.

### Results

Avamar Client Manager removes the task from the queue, cancels the task, and adds an entry to the log.

## Logs

The Logs page provides access to the Avamar Client Manager logs.

The Logs page provides a summary view of Avamar Client Manager logs. Log entries appear in separate sections based on the type of task that generated the entry, as follows:

- **Activation**
  
  Click Links > Activation to view log entries related to client activation.

- **Delete**
  
  Click Links > Delete to view log entries related to the removal of clients from Avamar servers.

- **Move**
  
  Click Links > Move to view log entries related to moving clients from one Avamar server to another.

- **Retire**
  
  Click Links > Retire to view log entries related to retiring Avamar clients.

- **Upgrade**

  Click Links > Upgrade to view log entries related to upgrading the software on Avamar clients.

Use the Logs page to perform the following tasks:

- View log entries
- View the client log for upgrades
- Clear all log entries in a section
Viewing the client log after upgrading an Avamar client

View the Avamar client's local log after a completed upgrade attempt.

Before you begin
Use Avamar Client Manager to apply an upgrade package or hotfix to an Avamar client.
Viewing the Avamar client's local log can provide details about the reasons for an unsuccessful client upgrade.

Procedure
1. On the left-side menu, click Logs > Upgrade.
2. On the right-side of the page, click the Details bar.
   The Details panel expands.
3. In Summary, select a client upgrade log entry.
   Detailed information for the selected log entry appears in the Details panel.
4. On the Details panel, in Log, click View Log.

Results
The Upgrade Log window opens and the client's local log appears in the window.

After you finish
(Optional) Select and copy information from the client's local log. Paste the copied information into a text editor.

Clearing all log entries in a section

Avamar Client Manager provides a method for you to remove all log entries from a task section of Logs.

Before you begin
Complete at least one task that results in a log entry in one of the task sections of the Logs page.

Procedure
1. On the left-side menu, click Logs > task_log, where task_log is a Logs page section.
   For example, to clear all upgrade entries, click Logs > Upgrade.
2. Click Clear All.
   The Alert dialog box appears.
3. Click Yes.

Results
Avamar Client Manager removes all log entries for the selected section.
CHAPTER 14
Avamar Desktop/Laptop

This chapter includes the following topics:

- Overview of Avamar Desktop/Laptop ................................................................. 324
- Requirements for Avamar Desktop/Laptop .......................................................... 325
- Avamar client software installation .................................................................... 327
- Avamar Desktop/Laptop user authentication ...................................................... 331
- Avamar Desktop/Laptop user interfaces ............................................................. 335
- Backup with Avamar Desktop/Laptop ............................................................... 341
- Restore with Avamar Desktop/Laptop ............................................................... 345
- Client backup and restore activity history ......................................................... 349
- Editing the Avamar Desktop/Laptop properties file ........................................... 349
- Client log locations ............................................................................................ 351
Overview of Avamar Desktop/Laptop

Avamar Desktop/Laptop is a version of the Avamar client software for Windows and Macintosh that adds enhanced features for enterprise desktop and laptop computers. Many Avamar Desktop/Laptop features are also available on supported Linux computers.

Client installation and management
In a corporate environment, you can push install Avamar Desktop/Laptop on Windows and Macintosh desktop and laptop computers by using systems management tools such as Microsoft Systems Management Server 2003 (SMS).

You can also install the Avamar Desktop/Laptop software locally by launching an installation wizard.

After client installation, you can activate, upgrade, analyze, and manage clients by using the Avamar Client Manager web browser UI.

User authentication
Avamar Client Manager users authenticate through the enterprise Active Directory or OpenLDAP-compliant directory service, with or without Kerberos encryption. Users can also authenticate by using built-in Avamar authentication, or a combination of Avamar authentication and LDAP authentication. NIS authentication is also supported.

Pass-through authentication enables users to access the web UI without using the login screen. A secure message mechanism authenticates users based on information from the client computer. Pass-through authentication also enables administrators to allow non-domain users to restore files to their local account on the computer.

User interfaces
Avamar Desktop/Laptop functionality is available through two user interfaces:

- The client local user interface (client UI) is installed on the client computer when you install either the Avamar Client for Windows or the Avamar Client for Mac OS X. With the client UI, an Avamar icon appears in the notification area (“system tray”) on Windows computers or on the menu bar on Mac computers. Right-click the icon on Windows or click the icon on Mac to open the client menu, which provides access to backup, restore, program settings, and logs.

- Use the web browser user interface (web UI) to start an on-demand backup or restore, view backup and restore activity for a client computer, or configure other backup settings for a client computer.

Backup
Users can start an on-demand backup with a single click on the client menu, or open the web UI for an interactive on-demand backup. Options to customize on-demand backup behavior include:

- Allowing users to create on-demand backup sets.
- Limiting the total number of backups that can occur each day for each client computer.
- Changing the retention policy for on-demand backups.
- Disabling on-demand backups.

You should perform scheduled backups of all Avamar Desktop/Laptop clients. For daily scheduled backups, you can allow users to select a different start time for their backups from a list of available times that you create. The system runs the backup as soon as possible after the selected time.
You can also allow users to add folders to the source data defined by the groups to which a client belongs. The folders are included in both on-demand and scheduled backups for the client.

**Restore**

Users can search for or browse to folders, files, and file versions to either the original location or to a new location on the same computer. Users can restore data with the same name or a new name.

When users restore data to the original location with the same name, the restore process overwrites any current local file versions with the restored files. This type of restore is useful in situations where the current local versions contain errors or have data corruption issues.

To avoid overwriting the current local file versions, users can restore to a new location, restore with a new name, or both.

Domain users can restore files from any Windows or Mac computer on which they have a user profile to the Windows or Mac computer to which they are logged in.

If large restore tasks are impacting network performance, you can specify a limit for the amount of data that users are allowed to restore.

Users are allowed to initiate only one restore task at a time. Additional requests are blocked and a message appears to the user. You can change this behavior to allow users to start multiple restore tasks.

**Activity history**

The **History** page in the web UI provides a 14-day history of the status of restore and backup tasks for a client computer, as well as listings of the folders and files backed up during that period. If you are a domain user with a user profile on the source computer, then you can view the activity history for the source computer from a different computer.

**Requirements for Avamar Desktop/Laptop**

You should work with an EMC field sales representatives when deciding on the characteristics of the Avamar system deployment that work best to support desktop and laptop clients for an enterprise. The environment must meet the requirements in the following topics.

Due to the wide range of differences in desktop and laptop topology for each enterprise, a description of the requirements for an Avamar system to support desktops and laptops at any one enterprise is beyond the scope of this guide.

**Client computer requirements**

Avamar client computers with Avamar Desktop/Laptop must meet the minimum requirements in the following sections.

**Operating system requirements**

Avamar Desktop/Laptop client computers require a Windows, Mac, or Linux operating system that is supported for use with the Avamar client. The **EMC Avamar Compatibility and Interoperability Matrix** on EMC Online Support provides a complete and updated list.

Windows Server, Mac OS X Server, and Linux computers that meet the requirements specified in the **EMC Avamar Backup Clients User Guide** are supported as server-class clients. Generally, the Avamar Desktop/Laptop enhancements function the same for server-class computers as for desktop and laptop computers. Differences include:

- On a server-class computer, clicking **Back Up Now** on the **Client** menu or on the **Backup** reminder launches a backup of the dataset assigned individually to the
computer. You can view or edit the dataset assigned to a server-class computer in Avamar Administrator by overriding group policy settings for the client. Overriding group policy settings for a client on page 107 provides instructions.

- The Avamar Desktop/Laptop feature for disabling backups for computers running on battery power is not available for server-class computers. Backups are always enabled on these computers.
- You can disable locally initiated restores on both Windows and Macintosh server-class computers by editing the dtlt.properties file. When you disable server-class computer restores, you can only perform a restore by using Avamar Administrator. However, users with local administrative rights on the server-class computer can restore backups to a different computer.

**Hardware requirements**
The following table lists hardware requirements for Avamar Desktop/Laptop client computers.

**Table 81 Avamar Desktop/Laptop hardware requirements**

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>250 MB permanent hard drive space minimum for software installation.</td>
</tr>
<tr>
<td></td>
<td>Additional space may be required by snapshot technology and to back up system state.</td>
</tr>
<tr>
<td>Network interface</td>
<td>Either of the following:</td>
</tr>
<tr>
<td></td>
<td>• 10BaseT or higher, configured with the latest drivers for the platform</td>
</tr>
<tr>
<td></td>
<td>• IEEE 802.11a/b/g, configured with the latest drivers for the platform</td>
</tr>
</tbody>
</table>

**Supported Avamar plug-ins**
Avamar Desktop/Laptop supports backup and restore with the following Avamar file system plug-ins:

- Windows
- Mac
- Linux

Avamar Desktop/Laptop does not support application plug-ins or file system plug-ins for other operating systems.

**Port requirements**
The TCP data port must allow bidirectional communication with the Avamar server.

**Web browser requirements**
The web browser that you use for the Avamar Desktop/Laptop user interface must be JavaScript-enabled and meet other requirements.

The following table lists supported web browsers.
Table 82 Supported web browsers for Avamar Desktop/Laptop

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Supported web browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>• Windows Internet Explorer</td>
</tr>
<tr>
<td></td>
<td>• Mozilla Firefox</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome</td>
</tr>
<tr>
<td>Macintosh</td>
<td>Apple Safari</td>
</tr>
<tr>
<td>Linux</td>
<td>Mozilla Firefox</td>
</tr>
</tbody>
</table>

The browser must be configured to be launched by a call to one of the environment variables in the following table.

Table 83 Environment variables for launching a web browser in Avamar Desktop/Laptop

<table>
<thead>
<tr>
<th>Browser</th>
<th>Environment variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>KDE</td>
<td>kfmclient</td>
</tr>
<tr>
<td>GNOME</td>
<td>gnome-open</td>
</tr>
<tr>
<td>Others</td>
<td>BROWSER</td>
</tr>
</tbody>
</table>

Network requirements

The network in an Avamar Desktop/Laptop environment must meet the requirements in the following table.

Table 84 Avamar Desktop/Laptop network requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>TCP/IP.</td>
</tr>
<tr>
<td>Routers</td>
<td>Must permit TCP packet routing between the Avamar server and each client computer.</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Must allow bidirectional communication between the Avamar server and each client computer using TCP data port 28002.</td>
</tr>
<tr>
<td>Naming system</td>
<td>Must facilitate connections between each client and the Avamar server, including situations where IP address changes are caused by DHCP and VPN access.</td>
</tr>
</tbody>
</table>

Avamar client software installation

The recommended method to install the Avamar client software on large numbers of Windows or Mac computers is to use a systems management tool. A systems
A management tool can remotely push install the software on large numbers of computers in a short amount of time.

Also, a systems management tool can often generate a list of the computers where the software is successfully installed. You can use this list in Avamar Client Manager to register and activate computers.

You can install the Avamar Client for Windows by using several silent install options.

**NOTICE**

Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.

**Supported systems management tools**

Remote installation has been tested and approved using the following systems management tools:

- Microsoft Systems Management Server 2003 (SMS) on Windows computers
- SMS with Quest Software’s Quest Management Xtensions for SMS on Macintosh computers

You may also be able to use other systems management tools, such as the tools in the following list, to remotely push install the Avamar client software:

- Microsoft System Center Configuration Manager 2007
- IBM Tivoli Management Framework
- HP OpenView ServiceCenter
- Symantec Altiris
- Apple Remote Desktop

Systems management tools vary. The steps required to push software to a set of computers depend on the tool. Consult the documentation for the tool to determine the steps required to perform these tasks.

**Push installation on Windows computers**

**Procedure**

1. Copy the installer package for the Avamar Client for Windows to a location that is accessible to the systems management tool.
2. Configure the systems management tool to copy the correct installer package to each computer.
3. Designate the computers on which to install the software.
4. Provide an installation launch command that uses the following format:

   ```
   msiexec /qn /I "path_to_MSI_pkg" SERVER=server DOMAIN=domain
   GROUP="groups" UICOMPONENT={0|1} PROGRESSBAR={true|false}
   BALLOONMESSAGE={true|false} BACKUPREMINDER=days
   ```

   The following table provides details on the arguments for the installation launch command.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;path_to_MSI_pkg&quot;</td>
<td>Specifies the full path to the location of the installer package relative to the root of the computer file system.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SERVER=server</td>
<td>Specifies the IP address or FQDN of the Avamar server assigned to the client. When this argument is omitted or incorrect, the client is successfully installed but is not activated.</td>
</tr>
<tr>
<td>DOMAIN=domain</td>
<td>Specifies the Avamar domain for the client. The path must start with a slash path character (Unicode 002F: /). The default value is /clients.</td>
</tr>
<tr>
<td>GROUP=groups</td>
<td>Specifies a comma-separated list of Avamar backup groups for the client. Start the path for each group with a slash path character (Unicode 002F: /), and enclose the group path in quotation marks. For example: GROUP=&quot;/clients/text,/clients/admin&quot; The default value is &quot;/Default Group&quot;.</td>
</tr>
<tr>
<td>UICOMPONENT={0</td>
<td>1}</td>
</tr>
<tr>
<td>PROGRESSBAR={true</td>
<td>false}</td>
</tr>
<tr>
<td>BALLOONMESSAGE={true</td>
<td>false}</td>
</tr>
<tr>
<td>BACKUPREMINDER=days</td>
<td>Specifies the number of days after the last backup before a backup reminder appears. The possible values for days are numbers 1 through 7 and Never. The default value is 3.</td>
</tr>
</tbody>
</table>

Users can change the values set by the UICOMPONENT, PROGRESSBAR, BALLOONMESSAGE, and BACKUPREMINDER by using options on the client menu in the client UI. You can also change the values during an upgrade.

5. Launch the systems management tool installation process.

**Push installation on Macintosh computers**

**Procedure**

1. Copy the installer package for the Avamar Client for Mac OS X to a location that is accessible to the systems management tool.
2. Configure the systems management tool to copy the correct installer package to each computer.
3. Designate the computers on which to install the software.
4. Provide the installation launch command:

   ```bash
   /usr/sbin/installer -pkg "path_to_install_pkg" -target install_location
   ```

   where path_to_install_pkg is the full path to the location of the installer package relative to the root of the computer file system, and install_location is the location in which to install the software. Normally, install_location is the root (/), but any local volume is allowed.
5. Launch the systems management tool installation process.

**After you finish**

After installation of the Avamar Client for Mac OS X, a restart of some clients may be required. This is caused by a change to the process data size setting that is made on those computers. During installation, the installer determines if the process data size is less than 96 MB. A minimum process data size of 96 MB is required for optimal performance of the Avamar Client for Mac OS X.

If the process data size is less than 96 MB, then the installer changes it to 96 MB and displays a restart reminder. If you leave the message open for more than 30 seconds without clicking a button to restart immediately or at a later time, then the reminder is hidden and appears again in 2 hours.

If you choose to restart the computer but the restart process is interrupted, then the reminder does not appear again. You must remember to restart the computer to complete the process data size change.

**Local client installation**

You can install the Avamar Desktop/Laptop software locally by launching a graphical installation interface. After the installation, the computer is ready to register and activate with an Avamar server.

To perform a local installation, you can download the client installer by using the downloads link. If the downloads link is disabled, you must transfer the client installer to the computer by some other file transfer method.

The disadvantages of using local installation are:

- It is very time consuming when performed individually on thousands of computers.
- It does not provide a list that you can use to register and activate groups of computers in Avamar Client Manager.

The *EMC Avamar Backup Clients User Guide* provides more information on local installation, upgrade, and uninstall of Avamar Desktop/Laptop.

**Avamar client software uninstall**

When you uninstall Avamar client software from a client computer, scheduled backups no longer occur for the client. You cannot restore backups to the client after you uninstall the software.

When you uninstall the Avamar client software, you can keep or delete the backups for the client:

- To keep the backups for the client so that you can restore the backups to a different client, retire the client by using Avamar Administrator.
- To delete the backups for the client, delete the client by using Avamar Administrator.

Retire or delete the client either before or after you uninstall the Avamar client software.

**Uninstall on Windows**

**Procedure**

1. Open the Windows *Add or Remove Programs* or *Programs and Features* applet.
2. In the list of currently installed programs, select *EMC Avamar for Windows*.
3. Click *Remove*.

   A confirmation message appears.
4. Click Yes.

Uninstall on Macintosh

**Procedure**

1. Open a Terminal (shell) session.
2. Log in as an administrator.

   The uninstall command requires root (super-user) permissions. The `sudo` command is used to run the command with root permissions. An administrator account or another account listed in `sudoers` is required by `sudo`.

3. Run the uninstall script by typing the following command:
   
   ```bash
   sudo /usr/local/avamar/bin/avuninstall.sh
   ```

---

**Avamar Desktop/Laptop user authentication**

Avamar Desktop/Laptop protects backup data by authenticating users and enforcing access rights. Avamar Desktop/Laptop uses a separate server process running on the Avamar system to facilitate authentication through both internal and external methods. Every Avamar system installation includes the Avamar Desktop/Laptop server process.

**Pass-through authentication**

Pass-through authentication uses encrypted channels to access user credentials from a client computer and associate the credentials with file ownership properties. The client computer operating system obtains the user credentials during login to the computer or through common access card (CAC) technology.

Avamar Desktop/Laptop performs pass-through authentication transparently. Users can back up and restore files without viewing the Avamar Desktop/Laptop login screen.

Avamar Desktop/Laptop enables pass-through authentication by default. It is limited to users on Windows computers and Mac computers. Also, Windows users with local administrator privileges can restore files owned by anyone on the computer without additional login.

Pass-through authentication is supported with LDAP authentication, NIS authentication, and Avamar authentication. With Avamar authentication, Avamar Desktop/Laptop determines if the client computer is in one of the specified Avamar domains. It authenticates users of those computers through Avamar authentication. It authenticates other users through pass-through authentication.

**Enabling local user access for pass-through authentication**

You can configure Avamar Desktop/Laptop to allow local user access through pass-through authentication. A local user is a user that is authenticated through a local computer account instead of a domain account.

With local user access enabled, local users can access the Avamar client web UI to restore data they own on the authenticating computer.

Local user access requires pass-through authentication on a Windows computer or a Mac computer. By default local user access is disabled.
Note

Enabling local user access applies to all clients and backups associated with the server. Before you enable local user access, carefully consider its security implications within the context of the organization. Local user authentication is inherently less secure than domain authentication.

To enable local user access for pass-through authentication, uncomment the `allowLocalUsers` property in the `dtlt.properties` file on the Avamar server, and then set its value to `true` by changing `#allowLocalUsers=false` to `allowLocalUsers=true`.

Disabling pass-through authentication

You can disable pass-through authentication and require that all users log in through the Avamar Desktop/Laptop login screen. When pass-through authentication is disabled, configure one of other methods of authentication for Windows users and Mac users.

To disable pass-through authentication, set the value of the `userLoginRequired` property in the `dtlt.properties` file on the Avamar server to `true`.

LDAP authentication

You can configure Avamar Desktop/Laptop to use an LDAP v.3-compliant directory service such as Microsoft Active Directory or OpenLDAP to authenticate users with a directory service username and password.

The authentication process uses Kerberos in a Simple Authentication and Security Layer (SASL) Bind by default. You can also configure it to use plaintext in a Simple Bind. However, only SASL Bind is supported with pass-through authentication. Plaintext Simple Bind is not compatible with pass-through authentication.

With LDAP authentication, users log in to the client computer with a domain account authenticated through a domain directory service. To use a local account, enable local user access.

To increase the security of user data, Avamar Desktop/Laptop obtains the domain username of a Windows user or Mac user from the client computer and enters it in a read-only field on the Avamar Desktop/Laptop login screen.

Note

You cannot use the root account on a Mac to restore files from backups.

Configuring LDAP authentication for Avamar Desktop/Laptop

To configure Avamar Desktop/Laptop to authenticate users through an LDAP v.3-compliant directory service with either Kerberos in an SASL Bind or plaintext in a Simple Bind, edit the LDAP configuration file.

Before you begin

- Configure Avamar with information about the directory service. Adding directory service information on page 66 provides instructions.
- Ensure that the configuration of the Avamar Desktop/Laptop server correctly describes any domain components used to segregate authentication.
- If you are using Kerberos in an SASL Bind, then ensure that the Kerberos realm for LDAP user authentication from Macintosh computers is the default Kerberos realm.
Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the LDAP Management tab.
3. Click Edit LDAP file.
4. In the text area, edit or create the user-login-module key:
   - To specify Kerberos in an SASL Bind, set user-login-module=kerberos.
   - To specify plaintext in a Simple Bind, set user-login-module=ldap.

   Kerberos is the default value. Avamar Desktop/Laptop assumes this value when the key is missing.
5. Click Save.
6. Click Close.

Changing the Kerberos encryption type

If you use LDAP authentication with Kerberos, you may need to change the Kerberos encryption type.

Avamar Desktop/Laptop uses the MIT Kerberos encryption type “DES cbc mode with CRC-32” to communicate with LDAP servers by default. This encryption type may conflict with a key distribution center (KDC) in the Active Directory environment. If that occurs, the message KDC has no support for encryption type appears. To resolve this issue, remove the specified encryption type from the krb5.conf configuration file, which enables the KDC to select the encryption type.

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the LDAP Management tab.
3. Click Edit KRB5 file.
4. In the text area, find the following entries:

   [libdefaults]
   default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
   default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5

5. Comment out the entries:

   [libdefaults]
   #default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
   #default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5

6. Click Save.
7. Click Close.
NIS authentication

You can configure Avamar Desktop/Laptop to authenticate Linux users through the enterprise NIS.

When you use NIS authentication, client computers must all use the same static, resolvable, fully qualified NIS domain name. In addition, users must have properly configured user accounts in the NIS domain.

Adding directory service information on page 66 provides instructions on configuring NIS authentication.

Avamar authentication

You can configure Avamar Desktop/Laptop to authenticate users by using Avamar authentication, which uses internal Avamar domain information.

Avamar authentication works with users who authenticate at the Avamar root level, Avamar domain levels, or Avamar subdomain levels. The mechanism first checks at the subdomain level. If the username is found at that level, then authentication proceeds. If the username is not found, then the next level is checked. This continues until the username is found, or the Avamar root is reached without finding the username.

For example, if the login computer 123abc.example.com is activated with the /clients/mountain Avamar subdomain, then the mechanism checks the Avamar system in the following order until the username is found:

1. /clients/mountain (activation subdomain)
2. /clients (next level up)
3. / (root)

With Avamar authentication, client computers must have a static, resolvable, fully qualified domain name. In addition, users must have a local or domain login account for the client computer and an account on the Avamar domain associated with the client computer.

Avamar Desktop/Laptop applies the role assigned to the Avamar user account when it grants access to the account through Avamar authentication. Users can perform only those operations that are allowed by their role. The one exception is that users with the Restore only operator role can launch a backup from Avamar Desktop/Laptop.

Configuring Avamar authentication

Configure an Avamar system to use Avamar authentication through the LDAP Management tab of Avamar Administrator.

Before you begin

Add Avamar user records to domain-level lists. Adding a user to a client or domain on page 79 provides instructions.

Procedure

1. In Avamar Administrator, click the Administration launcher button.
   The Administration window appears.
2. Click the LDAP Management tab.
3. Click Edit LDAP file.
4. Edit or create the user-login-module key:
• To use Avamar authentication and all other configured and enabled authentication methods, set `user-login-module=mix`.
• To use Avamar authentication and all other configured and enabled authentication methods except LDAP, set `user-login-module=avamar`.

5. In the text area, type the following key/value pair:

```
avamar-authentication-domains=/domain1,/domain2,/domain3,...
```

where `domain1`, `domain2`, and `domain3` are Avamar domain names that are combined in a comma-separated list. Each domain name must begin with the root path designator: `/`.

For example, to use Avamar authentication for the following domains:

```
/clients/accounting
/clients/shipping
```

Type the following key/value pair:

```
avamar-authentication-domains=/,clients/accounting,clients/shipping
```

6. Click **Save**.
7. Click **Close**.

**Mixed authentication**

You can use multiple authentication methods in the same environment.

The authentication process occurs in the following order when you enable multiple authentication methods:

1. Users on a client in an Avamar domain are authenticated by using Avamar authentication.
2. Users who are not logged in to a client in an Avamar domain are authenticated by using pass-through authentication.
3. Linux users who are not logged in to a client in an Avamar domain are authenticated through NIS.
4. When mixed authentication is enabled and LDAP is configured, authenticates users, who are not logged in to a client assigned to a specified Avamar domain, through LDAP.

**Avamar Desktop/Laptop user interfaces**

Avamar Desktop/Laptop functionality is available through the client UI and the web UI.

**Client UI**

The client local user interface (client UI) is installed on the client computer when you install either the Avamar Client for Windows or the Avamar Client for Mac OS X. With the client UI, an Avamar icon appears in the notification area ("system tray") on Windows computers or on the menu bar on Mac computers. Right-click the icon on Windows or click the icon on Mac to open the client menu, which provides access to backup, restore, program settings, and logs.

The following table lists the functionality that is available in the client UI.
<table>
<thead>
<tr>
<th>Client menu item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Up Now</td>
<td>Launches a single-click on-demand backup.</td>
</tr>
<tr>
<td>Back Up...</td>
<td>Launches an interactive on-demand backup.</td>
</tr>
<tr>
<td>Restore...</td>
<td>Launches an interactive restore.</td>
</tr>
<tr>
<td>Settings &gt; Show Backup Reminder (days)</td>
<td>Controls when a backup reminder appears to remind you that the computer has not been backed up for a period of time between one and seven days. You can also disable the reminder by selecting Never.</td>
</tr>
<tr>
<td>Settings &gt; Show Progress Bar</td>
<td>Controls whether the Progress window appears during a backup. You can cancel, pause, or view logs for a backup from the Progress window.</td>
</tr>
<tr>
<td>Settings &gt; Show Balloon Messages</td>
<td>Controls whether system status balloon messages appear near the Avamar icon on supported Windows computers.</td>
</tr>
<tr>
<td>Settings &gt; Back Up On Battery Power</td>
<td>Controls whether scheduled or on-demand backups can occur for the computer when the computer is running on battery power.</td>
</tr>
<tr>
<td>Settings &gt; Back Up On Wireless</td>
<td>Controls whether scheduled or on-demand backups can occur for the computer when the computer is joined to the network solely by a wireless connection.</td>
</tr>
<tr>
<td>Languages</td>
<td>Enables you to select the language for the client UI.</td>
</tr>
<tr>
<td>Manage &gt; Activate Client</td>
<td>Activates the client, which provides a unique ID for the client and links the client to a specific Avamar server.</td>
</tr>
<tr>
<td>Manage &gt; View Console</td>
<td>Opens the client console, which provides access to local status records for tasks, the Agent Log, the Console Log, and the Work Order Log.</td>
</tr>
<tr>
<td>Manage &gt; Create ZIP File of Logs</td>
<td>Creates a ZIP file of logs required by administrators to diagnose backup and restore problems.</td>
</tr>
<tr>
<td>(Mac only) Client Agent Tasks</td>
<td>Stops or restarts the backup agent process.</td>
</tr>
<tr>
<td>(Mac only) Logs</td>
<td>Provides access to the Agent Log, Console Log, and functionality for creating a ZIP file of logs required by administrators to diagnose backup and restore problems.</td>
</tr>
<tr>
<td>About</td>
<td>Provides version, server, and copyright information for Avamar Desktop/Laptop.</td>
</tr>
<tr>
<td>Help</td>
<td>Launches online help for Avamar Desktop/Laptop when the client is activated to an Avamar server.</td>
</tr>
<tr>
<td>Exit</td>
<td>Shuts down the Avamar client.</td>
</tr>
</tbody>
</table>
Web UI

Use the web browser user interface (web UI) to start an on-demand backup or restore, view backup and restore activity for a client computer, or configure other backup settings for a client computer.

The following table describes the main elements of the web UI.

Table 86 Avamar Desktop/Laptop web UI functionality

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Avamar Desktop/Laptop logo</td>
<td>You can replace the EMC Avamar logo and the Desktop/Laptop logo in the top left corner of the web UI to rebrand the web UI.</td>
</tr>
<tr>
<td>Settings menu</td>
<td>The settings menu in the top right corner of the web UI enables you control web UI configuration settings, including:</td>
</tr>
<tr>
<td></td>
<td>• Whether to show tooltips</td>
</tr>
<tr>
<td></td>
<td>• The language for the web UI</td>
</tr>
<tr>
<td></td>
<td>• How many entries to show on the Search, Browse, or History pages</td>
</tr>
<tr>
<td></td>
<td>• The default page that appears when you perform a restore</td>
</tr>
<tr>
<td></td>
<td>• Whether the full web UI or the browse-only mode, which displays only the Search and History pages, is used</td>
</tr>
<tr>
<td>Refresh icon</td>
<td>Refreshes the web UI page.</td>
</tr>
<tr>
<td>Help menu</td>
<td>Provides access to the Avamar Desktop/Laptop online help and to software version information.</td>
</tr>
<tr>
<td>Search page</td>
<td>Enables you to search for files and folders on the client computer to restore.</td>
</tr>
<tr>
<td>Browse page</td>
<td>Enables you to browse to files and folders on the client computer to restore.</td>
</tr>
<tr>
<td>Backup page</td>
<td>Provides information about the backup groups to which the client is assigned, as well as the next scheduled backup.</td>
</tr>
<tr>
<td></td>
<td>Also enables you to perform an on-demand backup of the client by using the group policies for the groups to which the client is assigned.</td>
</tr>
<tr>
<td></td>
<td>When the Add Data button is enabled on the Backup page, users can add folders to the group datasets for scheduled and on-demand backups.</td>
</tr>
<tr>
<td>History page</td>
<td>Provides a 14-day record of backup and restore activity on the computer, including:</td>
</tr>
<tr>
<td></td>
<td>• Status of backups, and for each backup, a listing of the file data that was transferred</td>
</tr>
<tr>
<td></td>
<td>• Status of restores</td>
</tr>
<tr>
<td>Status bar</td>
<td>Displays the date and time of the last and next scheduled backup, as well as the outcome of the last backup.</td>
</tr>
<tr>
<td></td>
<td>The status bar displays information for the most recent 14 days. When the last backup was more than 14 days in the past, the status bar displays the message No backups found. However, you may still see files on the Browse and</td>
</tr>
</tbody>
</table>
Limited user interface

The Avamar server presents a limited version of the web UI to a client when the number of files and directories in a client backup exceeds about 4 million or when there is insufficient allocated memory for Avamar Desktop/Laptop.

**Large number of files and directories in a client backup**

The exact number of files and directories that causes these changes is based on the available memory on the Avamar server.

There is no upper limit to the number of files and directories that can be in a backup.

**Insufficient allocated memory**

The limited version of the web UI also appears for all clients accessing the Avamar server when the memory it requires to satisfy its current Avamar Desktop/Laptop requests exceeds the memory that it has allocated for Avamar Desktop/Laptop.

Encouraging users to log out of the web UI at the end of their session helps prevent this issue.

**Description of the limited web UI**

The limited version of the web UI has the following changes:

- The Search and History pages do not appear on the web UI.
- File versions are not available on the Browse page.
- Restore is only allowed for users with local administrator rights on the computer. Non-administrator users cannot restore any files, including those that they own locally on a server-class computer.
- Restore data size limits are not enforced.

Apache web server authentication

To protect user security, web browsers display an authentication warning when accessing a secure web page unless the web server provides a trusted public key certificate with the page. The Avamar Desktop/Laptop web UI uses only secure web pages, and this warning is seen in browsers that access those pages. To avoid the warning, install a trusted public key certificate on the Apache web server provided with Avamar.

The *EMC Avamar Product Security Guide* describes how to obtain and install a trusted public key certificate for the Apache web server.
Rebranding the web UI

You can rebrand the Avamar client web UI by replacing the two logo graphics in the top left corner of the UI.

**Procedure**

1. Create two replacement graphics named `ProductNameAvamar.png` and `ProductNameDTLT.png`.

   The replacement graphics must meet the following requirements:
   - The file format must be Portable Network Graphic (.png).
   - The background must be transparent so that the background gradient is visible behind the graphic text and images.
   - `ProductNameAvamar.png` must be 97 pixels wide and 18 pixels tall.
   - `ProductNameDTLT.png` must be 128 pixels wide and 18 pixels tall.

2. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.

3. Change the working directory by typing the following command:
   ```
   cd /usr/local/avamar-dtlt-tomcat/webapps/dtlt/images/banner
   ```

4. Make backup copies of the original graphics by typing the following commands:
   ```
   cp ProductNameAvamar.png ProductNameAvamar.png_orig
   cp ProductNameDTLT.png ProductNameDTLT.png_orig
   ```

5. Move the new logos to the current working directory as `ProductNameAvamar.png` and `ProductNameDTLT.png`.

6. If the new graphics do not appear, delete the cached copies of previously viewed files in the web browser, and then refresh the page.

Changing the web UI port

Access to the web UI involves HTTPS communication between the Avamar server and the client web browser. When a user requests a backup or restore by using the Avamar client menu, the default web browser on the client is instructed to contact the Avamar server on port 443, the standard HTTPS port. On the Avamar server, this initial request to port 443 is redirected to port 8443, the HTTPS port for the web UI. You can change the initial contact port by editing the `avscc.cfg` configuration file on the client and the Apache SSL configuration file on the server.
Procedure

1. Edit the avscc.cfg file on the client computer to use the new port number:
   a. Open avscc.cfg in a text editor.
      
      On Windows clients, the file is in the %SystemDrive%\Program Files\avs \var directory. On all other clients, the file is in the /usr/local/avamar/var directory.
      
      If avscc.cfg does not exist at this location, then create the file.
   b. Add the following line to the file:
      
      --port=n
      
      where n is the initial contact port number.
   c. Save and close avscc.cfg.
   d. Restart the client.

2. Edit the Apache SSL configuration file on the Avamar server:
   a. Open a command shell and log in as admin on a single-node server or on the utility node of a multi-node server.
   b. Open the Apache SSL configuration file in a text editor.
      
      On Red Hat Enterprise Linux, the file is /etc/httpd/conf.d/ssl.conf. On SuSE Linux Enterprise Server, the file is /etc/apache2/vhosts.d/vhost-ssl.conf.
   c. Find the HTTPS port listening directive and change Listen 443 to Listen n,
      
      where n is the initial contact port number.
   d. Save and close the file.
   e. Restart the Apache server process by typing apachectl restart.

Changing the secure token time-out value

Avamar Desktop/Laptop includes a temporary secure token as part of the URL it uses to begin a backup or restore session in a client web browser. The client web browser must establish an HTTPS connection with the Avamar server before the token expires or the session is rejected and the backup or restore cannot proceed. You can edit the default time-out value of 20 seconds.

Procedure

1. Open a command shell and log in by using one of the following methods:
   
   • For a single-node server, log in to the server as admin.
   • For a multi-node server, log in to the utility node as admin.

2. Stop the MCS by typing the following command:

   dpnctl stop mcs

3. Change the working directory by typing the following command:

   cd /usr/local/avamar/var/mc/server_data/prefs

4. Open mcserver.xml in a text editor.

5. In the <node name="dtlt"> section, edit the value of <entry key="expire_data_after_secs" value="20" /> from 20 to the new time-out value in seconds.
6. Save the change and close the file.
7. Start the MCS and the scheduler by typing:
   
   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Forcing clients to use the alternate file browsing method

The Avamar client web UI uses the OS-specific file browsing services on the client computer to provide a file manager interface for users to select local files and folders to back up or restore. However, if these services are not available because the client uses NAT or because port 28002 on the client is blocked by a firewall rule, then an alternate file browsing method is offered. You can require clients to use the alternate file browsing method.

One reason to make this change is to provide support for removable media. The default file browsing method does not support removable media, but the alternate method does.

The alternate method uses a Java applet to provide file browsing services. When the default services are unavailable, and the user elects to permit the alternate method, the Java applet is loaded. During loading of the applet, the user may see authentication warnings about the website certificate of the Avamar server and the digital signature of the Java applet. You must acknowledge these warnings or the applet does not load.

After the applet loads, the web page is automatically refreshed to allow the Avamar client web UI to use the applet. The user must restart the task after the page is refreshed.

To force clients to use the alternate file browsing method, add the `useAppletToBrowseLocalFile` property to the `dtlt.properties` file on the Avamar server, and set the value to `true`.

### Backup with Avamar Desktop/Laptop

The following topics provide details on performing backups and controlling backup-related settings in Avamar Desktop/Laptop.

#### On-demand backups

Authenticated users on an Avamar Desktop/Laptop client computer can perform an on-demand backup with a single click on the client menu or the client backup reminder, or open the web UI for an interactive on-demand backup.

#### Single-click backups

To start a single-click on-demand backup on an Avamar Desktop/Laptop client computer, click **Back Up Now** on the client menu or the client backup reminder.

The data that is included in a single-click backup depends on the operating system of the client computer.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Data included in the backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Dataset for each group that the client belongs to</td>
</tr>
<tr>
<td>Mac</td>
<td>Dataset assigned to the computer</td>
</tr>
<tr>
<td>Linux</td>
<td>Dataset assigned to the computer</td>
</tr>
</tbody>
</table>
Table 87 Datasets for single-click on-demand backups (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Data included in the backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server</td>
<td></td>
</tr>
<tr>
<td>Mac OS X Server</td>
<td></td>
</tr>
</tbody>
</table>

If you allow users to add data to backups by using the Add Data button in the web UI, then the data additions are also included in single-click backups.

Interactive backups

An interactive on-demand backup in the web UI enables you to select a backup group to which the client belongs, and then to back up the client by using the settings for the group.

To perform an interactive on-demand backup select Back Up... on the client menu, select the backup group on the Backup page in the web UI, and then click Back Up Now.

You can also allow users to create on-demand backup sets for interactive backups.

Allowing users to create on-demand backup sets

You can enable users on Windows, Mac, and Linux clients that use Avamar Desktop/Laptop to create sets of folders and files to back up through interactive on-demand backups. Users can create multiple backups sets and save the backup sets for reuse. Automatic backup of clients according to their group policies is not affected by on-demand backup sets.

Procedure

1. Enable the Allow file selection on client initiated backups setting in Avamar Administrator. Overriding group policy settings for a client on page 107 provides instructions.

2. Change the value of the allowUserInitiatedBackupsFileSelection key in the dtlt.properties file on the Avamar server to true.

3. Users create the on-demand backup sets:
   a. On the Avamar Desktop/Laptop client computer, right-click the Avamar icon and select Back Up....
      The web UI opens to the Backup page.
   b. In Select folders and files to backup, click Select Now.
      The On-Demand Backup Sets dialog box appears.
   c. Select the folders and files to back up, and then click OK.
   d. To save the backup set for reuse, type a name for the backup set in Save backup set as, and then click Save.
   e. To perform an on-demand backup of the backup set, click Start Backup.
   f. Click OK on the confirmation message.

4. Users perform on-demand backups of the backup sets:
   a. On the Avamar Desktop/Laptop client computer, right-click the Avamar icon and select Back Up....
      The web UI opens to the Backup page.
b. In Select folders and files to backup, click Select Now. The On-Demand Backup Sets dialog box appears.

c. In Load Backup Set, select the backup set, and then click Start Backup.

d. Click OK on the confirmation message.

Setting an on-demand backup limit

There is no limit on the number of on-demand backups that Avamar client users can perform for a client computer. However, only one backup from a client is allowed in the task queue at a time, and a backup cannot start while another backup for the client is in progress.

To limit the total number of backups that can occur each day for Avamar Desktop/Laptop client computers, set the restrictBackupsPerDay property in the dtlt.properties file on the Avamar server to one of the values in the following table.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>There is no limit on the number of on-demand backups that can successfully run in a day. This is the default setting.</td>
</tr>
<tr>
<td>0</td>
<td>On-demand backups cannot be run by any user.</td>
</tr>
<tr>
<td>n</td>
<td>No more than ( n ) on-demand backups can occur for each client in a day, where ( n ) is any positive integer less than or equal to 100, and a day is defined as midnight to midnight in the time zone for the Avamar server.</td>
</tr>
</tbody>
</table>

The limit applies to all clients activated on the Avamar server. You cannot apply the limit only to certain client computers. All successfully completed backups for all users on the computer count toward the total number of backups allowed each day.

Changing the retention policy for on-demand backups

The End User On Demand Retention policy controls the retention of data for on-demand backups. You can change the End User On Demand Retention policy on an Avamar server by using Avamar Administrator. The change applies to all on-demand backups initiated by a client activated with that server. However, the change only applies to on-demand backups that occur after the change.

Procedure

1. In Avamar Administrator, select Tools > Manage Retention Policies.

   The Manage All Retention Policies window appears.

2. Select End User On Demand Retention from the list and click Edit.

   The Edit Retention dialog box appears.

3. In Retention period, type a number and select a unit of time (days, weeks, months, or years).

4. Click OK.
Disabling on-demand backups

You can prevent one or more clients from performing either single-click or interactive on-demand backups in Avamar Desktop/Laptop.

Procedure
1. In Avamar Administrator, click the Policy launcher button.
The Policy window appears.
2. Click the Clients tab.
3. Disable on-demand backups for either a single client or multiple clients.

<table>
<thead>
<tr>
<th>Number of clients</th>
<th>Steps to disable on-demand backups</th>
</tr>
</thead>
</table>
| One               | a. Select the client and click Edit.  
b. In the Edit Client dialog box, clear Allow client initiated backups.  
c. Click OK. |
| Two or more       | a. Select the clients and click Edit.  
b. In the Edit Multiple Clients dialog box, change Allow client initiated backups to No.  
c. Click Apply Change.  
d. Click OK. |

Scheduled backups

You should perform scheduled backups of Avamar Desktop/Laptop client computers the same way that you back up other Avamar client computers in the environment. Create datasets, schedules, retention policies, and groups for the backups in Avamar Administrator.

The groups to which an Avamar Desktop/Laptop client belongs appear on the Backup page in the web UI. The next scheduled start time for a group backup also appears on the Backup page.

Users can perform an on-demand backup by using the settings for a backup group to which the client computer belongs.

You can also enable users to select a different start time for a scheduled backup.

Allowing users to select the start time for scheduled backups

You can allow users to select a start time for scheduled backups other than the start time assigned through group policy. Users select from a list of administrator-defined times on the Backup page in the web UI. The different start time applies to all subsequent scheduled backups for the client.

When you remove a client from a group, any record of a different start time for scheduled backups of that client is also removed.

Procedure
1. Ensure that the client belongs to a group that uses a daily schedule.
2. Add time entries to the Override Daily Schedule. Editing the start times for client overrides of group schedules on page 95 provides instructions.

When you edit the Override Daily Schedule, you select from times on the Avamar server. If the client is in a different time zone than the Avamar server, the available start times on the Backup page in the web UI are adjusted to the time zone for the client.

When you remove a time entry from the Override Daily Schedule after a user selects the entry, the client continues to use the time specified by that entry as its backup start time until the next time that the user logs in to the web UI. At that time, the system prompts the user to select a new time from the list.

3. Enable the Allow override of group's daily schedule setting for the client. Overriding group policy settings for a client on page 107 provides instructions.

Allowing users to add data to backups

You can enable users to specify folders to include in both scheduled and on-demand backups for the client computer. If a client belongs to multiple groups, then the additions apply to scheduled backups for all of the groups. Exclusions and inclusions that are defined in the datasets for the groups do apply to the folders that the user specifies.

Overriding group policy settings for a client on page 107 provides instructions on enabling this feature.

Then the user can add the folders by clicking the Add Data button on the Backup page of the web UI, and selecting the folders.

Restore with Avamar Desktop/Laptop

The following topics provide information on performing a restore and controlling restore-related settings in Avamar Desktop/Laptop.

Finding data to restore

Avamar Desktop/Laptop users can use the web UI to either browse to or search for folders, files, and file versions to restore.

**Browsing for data to restore**

From the left-side menu, select Browse to view the backups for a client computer in a tree view that you can browse to find folders and files to restore.

To browse a specific backup instead of all backups for the client, use Backup Date and Time to select the date and time of the backup.

**Searching for data to restore**

From the left-side menu in the web UI, select Search to search for specific folders and files to restore. To start a search, type a search string in the search field, and click Search. Results appear as they are gathered, and a progress indicator provides information about the length of the search.

The search string that you specify in the search field must be 255 characters or fewer and is not case sensitive. Supported wildcards in the search string include an asterisk (*) to represent zero or more characters and a question mark (?) to represent one character.

The string is compared to the names of all folders and files in the backups for the client computer. If all or part of a folder or file name matches the string, then the folder or file name appears in the search results.
Selecting a file version
The backups for a client computer contain more than one version of many of the files that are backed up. When a file is backed up and then subsequently edited, the next backup contains a new version of the file. Each version is kept for the retention period set by the Avamar administrator.

The number of versions of a file in the client backups depends on many factors, including:

- The length of time that backed up data is retained
- The frequency of backups
- How often the file is edited

When there are multiple versions of a file in the backups for a client, a version icon appears next to the file name when you browse or search for data to restore. To select a version of the file other than the most recent version, click the version icon and then select the version. Then choose whether to overwrite the existing file on the client computer or to restore the file version with a new name.

Restore types

Avamar Desktop/Laptop users can restore data to the original location or to a new location on the same computer. Users can restore data with the same name or a new name.

When users restore data to the original location with the same name, the restore process overwrites any current local file versions with the restored files. This type of restore is useful in situations where the current local versions contain errors or have data corruption issues.

To avoid overwriting the current local file versions, users can restore to a new location, restore with a new name, or both.

Domain users can restore files from any Windows or Mac computer on which they have a user profile to the Windows or Mac computer to which they are logged in. You can disable restore from a different computer by setting the value of the disableRestoreFromAlternateComputer property in the dtlt.properties file on the Avamar server to true. This is a global property that affects all clients.

Restore requirements
Review the permissions requirements and the requirements to restore from a different computer before you perform a restore.

Restore permissions
The data that users can browse to, search for, and restore depends on user login account permissions.

When users search or browse for data to restore, the results that appear are filtered based on the current login credentials and the data that has been backed up from the client computer. The following table provides details on the filtering.

Table 89 Avamar Desktop/Laptop data restore filtering

<table>
<thead>
<tr>
<th>Data type</th>
<th>Filtering on Windows</th>
<th>Filtering on Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folders</td>
<td>Displays all folders for which the logged in user is owner or is a member of a group with</td>
<td>Displays all folders for which the logged in user has Read permission</td>
</tr>
</tbody>
</table>
Table 89 Avamar Desktop/Laptop data restore filtering (continued)

<table>
<thead>
<tr>
<th>Data type</th>
<th>Filtering on Windows</th>
<th>Filtering on Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>ownership rights, and any folder that contains folders or files for which the user has rights.</td>
<td>either as owner or based on the folder’s group or other permissions.</td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td>Displays all files that the logged in user owns.</td>
<td>Displays all files that the logged in user owns.</td>
</tr>
</tbody>
</table>

When users browse for data to restore, a folder that a user does not have ownership rights for appears when it is on the file system path for a folder or file for which the user does have ownership rights. This helps to provide a more accurate representation of the file system on the computer. A dimmed checkbox appears next to the folders, and the folders are not restored when you restore a folder or file that includes them in its path.

Users can restore data only if their login credentials grant operating system Write permission for the restore location. Also, to restore data that has the same path and name as data on the client computer, the login credentials must authenticate the user as the owner of the existing data before and the restore proceeds.

To restore files on Windows, the login account must have the Restore files and directories user right in Local Security. This user right is assigned by default to accounts that are members of either the Administrators or Backup Operators groups. You must assign this right to an account that is not a member of either of these groups, or of another group that includes this user right, before a user can use the account to restore data.

Requirements to restore from a different computer

To restore from a different computer, the requirements in the following table must be met.

Table 90 Requirements to restore from a different computer with Avamar Desktop/Laptop

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Operating system  | • Windows operating system  
                    | • Mac operating system  |
|                   | **Note**    |
|                   | Restores between Windows and Mac computers are supported. |
| Account type      | Domain      |
| Profile           | Both source and target computers have a local profile for the user’s domain account.  
|                   | **Note**    |
|                   | A local profile for a domain account is created automatically at a user’s first login on the computer. |
| Avamar client     | Version 6.0 or later is installed on both source and target. |
Table 90 Requirements to restore from a different computer with Avamar Desktop/Laptop (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar server</td>
<td>Both source and target are activated with the same Avamar server and the server is running Avamar 6.0 or later.</td>
</tr>
<tr>
<td>Backup</td>
<td>There is at least one qualifying backup. A qualifying backup is one completed successfully after both:</td>
</tr>
<tr>
<td></td>
<td>• Avamar Desktop/Laptop 6.0 or later is installed on the source computer.</td>
</tr>
<tr>
<td></td>
<td>• A local profile for the user's domain account is created on the source computer.</td>
</tr>
</tbody>
</table>

By default, users with local administrator rights on a Windows source computer at the time of a backup can restore any file from that source computer to a target computer, regardless of file ownership. You can change this behavior to restrict their access to only files that they own. To restrict file access for Windows administrators, change the value of the `checkAlternateComputerOwnership` property in the `dtlt.properties` file on the Avamar server to `true`.

### Restore limits

You can limit the amount of data in a single restore task and the number of concurrent restore tasks for a client computer.

**Restore data size limit**

Avamar client users do not normally have a limit on the amount of data that is restored in a single task. This default setting enables a user to restore an entire backup in a single task. Very large restore tasks can sometimes cause undesirable load on the network. Set a restore data size limit to control the network load caused by these large restore tasks.

When you set a limit, individual users cannot restore more than the limit in any one restore task. Users must restore files that exceed the limit in multiple tasks that do not exceed the limit, or an administrator must perform the restore.

**NOTICE**

By design, the restore data size limit does not apply to server-class clients (those clients with a very large backup data set).

To specify a restore data size limit, uncomment the `limitRestoreSize` key in the `dtlt.properties` file on the Avamar server, and set the value to the data size limit in MB.

**Restore queue limit**

The Avamar client web UI minimizes network and server load by blocking restore requests for clients that already have a restore task in the queue. Users who attempt to start a new restore while one is pending receive a message, and the request is blocked. After the pending task is complete, users can initiate a new restore task. You can change this behavior to allow users to start multiple restore tasks. The change applies to all clients of the Avamar server.

To remove the restore queue limit, change the value of the `disallowMultipleRestores` property in the `dtlt.properties` file on the Avamar server to `false`. 
Restore of replicated backups

You can move an Avamar client to a new Avamar server by using either Avamar Client Manager or Avamar Enterprise Manager replication commands. When you move a client, the backups for the client are replicated on the new server. Avamar Desktop/Laptop must index replicated backups before they are available to browse or search in the web UI.

When a user logs in from the web UI on the client after the client has been moved, the **Replicated Backups Available** dialog box appears. The user can either initiate indexing of the replicated backups or close the dialog box without initiating indexing. When the user closes the dialog box without indexing, an alert icon appears on the web UI banner bar. The user can also initiate indexing from the alert icon.

Indexing is a one-time task for a computer that has been moved to a new server. It runs in the same session in which it is initiated. When it completes, Avamar Desktop/Laptop sends the web browser a refresh command, and the data from the replicated backups appears in the web UI.

Client backup and restore activity history

The **History** page in the Avamar Desktop/Laptop web UI provides a 14-day record of backup and restore activity on the client computer.

The **Activity History** section of the **History** page provides information about each backup and restore initiated during the past 14 days. It also provides links to more detailed information about the backups. Information includes the results of the activity, the start date and time, the duration of the activity, the amount of data, and the workorder ID. Click the activity label for a backup to view a list of files in the dataset for the backup.

To view the backup history for a different computer, select the computer from the list. The requirements in **Requirements to restore from a different computer on page 347** must be met before you can view the backup history for a different computer.

Editing the Avamar Desktop/Laptop properties file

The Avamar Desktop/Laptop properties file, `dtlt.properties`, enables you to change settings that affect functionality for all Avamar Desktop/Laptop that connect to the Avamar server. The file is available in the `/usr/local/avamar/etc` directory on the Avamar server.

**Procedure**

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Change directory to `/usr/local/avamar/etc` by typing the following command:
   ```
   cd /usr/local/avamar/etc
   ```
3. Open `dtlt.properties` in a text editor.
4. Create or edit the properties.
5. Save and close the file.

Avamar Desktop/Laptop properties

The following table lists the properties that are available in the `dtlt.properties` file.
Table 91 Avamar Desktop/Laptop property settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowLocalUsers</td>
<td>Enables and disables local user access for pass-through authentication. Uncomment the property by removing the <code>#</code> in front of the property, and then set the value to <code>true</code> to enable local user access for pass-through authentication. Use the default value of <code>false</code> to disable local user access for pass-through authentication.</td>
</tr>
<tr>
<td>userLoginRequired</td>
<td>Enables and disables pass-through authentication. Use the default value of <code>false</code> to enable pass-through authentication, or <code>true</code> to disable pass-through authentication.</td>
</tr>
<tr>
<td>useAppletToBrowseLocalFile</td>
<td>Controls whether users use the OS-specific file browsing services on the client computer or the alternate file browsing method. This property does not appear by default in the <code>dtlt.properties</code> file. You must create this property. Specify <code>false</code> to allow users to use the OS-specific file browsing services, or <code>true</code> to force users to use the alternate file browsing method.</td>
</tr>
<tr>
<td>restrictBackupsPerDay</td>
<td>Controls whether there is a limit to the number of on-demand backups that can be performed from the client computer in a single day, and if so, the maximum number. Use the default value of <code>false</code> if you do not want to limit the number of on-demand backups that can successfully run in a day. Specify 0 to disable on-demand backups on the client computer. To limit the number of on-demand backups that can successfully run in a day, specify the limit as a positive integer that is less than or equal to 100.</td>
</tr>
<tr>
<td>allowUserInititedBackupsFileSelection</td>
<td>Enables or disables the ability for users to create sets of folders and files to back up in on-demand backups. To enable selectable backup sets, enable the <strong>Allow file selection on client initiated backups</strong> setting for the client in Avamar Administrator, and then set the value of the <code>allowUserInitiatedBackupsFileSelection</code> property to <code>true</code>. Use the default value of <code>false</code> to disable selectable backup sets.</td>
</tr>
<tr>
<td>disableRestoreFromAlternateComputer</td>
<td>Enables or disables restore from a different computer. Specify <code>true</code> to disable restore from a different computer, or the default value of <code>false</code> to enable restore from a different computer.</td>
</tr>
<tr>
<td>checkAlternateComputerOwnership</td>
<td>Controls whether users with local administrator rights can restore any file from the source computer or only files that they own. Specify <code>true</code> to restrict local administrators to restore only files that they own, or the default value of <code>false</code> to allow local administrators restore any file from the source computer.</td>
</tr>
<tr>
<td>allowServerRestores</td>
<td>Enables or disables locally initiated restores on server class computers.</td>
</tr>
</tbody>
</table>
Table 91 Avamar Desktop/Laptop property settings (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limitRestoreSize</td>
<td>Controls whether to limit the amount of data that is restored in a single task. To specify a limit, uncomment the limitRestoreSize property and specify the data size limit in MB. The default limit is 500 MB.</td>
</tr>
<tr>
<td>disallowMultipleRestores</td>
<td>Controls whether users can start multiple restore tasks for a client computer at the same time. Specify false to allow multiple simultaneous restores, or use the default value of true to prevent multiple simultaneous restores.</td>
</tr>
</tbody>
</table>

Client log locations

Local logs on client computers provide information about backup and restore operations and UI functionality.

Available logs
The following table lists the available logs on client computers.

Table 92 Available client logs

<table>
<thead>
<tr>
<th>Log type</th>
<th>Log file name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workorder</td>
<td>workorder_name.log, where workorder_name is the full name of a task</td>
<td>Provide detailed information about a specific task.</td>
</tr>
<tr>
<td>Agent</td>
<td>avagent.log</td>
<td>Provides information about the status of all backup and restore activity on the computer.</td>
</tr>
<tr>
<td>Console</td>
<td>avscc.log</td>
<td>Provides information about the performance of the UI. A console log is created for each user on a computer.</td>
</tr>
</tbody>
</table>

While these logs are readily accessible through the client UI you can also access them directly.

Log locations on Windows computers
On Windows computers the logs are available through the paths in the following table.

Table 93 Paths to logs on Windows computers

<table>
<thead>
<tr>
<th>Log</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workorder</td>
<td>%SystemDrive%\Program Files\avs\var\clientlogs\</td>
</tr>
<tr>
<td>Agent</td>
<td>%SystemDrive%\Program Files\avs\var\</td>
</tr>
<tr>
<td>Console</td>
<td>%APPDATA%\Avamar\</td>
</tr>
</tbody>
</table>
Log locations on Linux and Mac computers
On Linux and Mac computers the logs are available through the paths in the following table.

Table 94 Paths to logs on Windows computers

<table>
<thead>
<tr>
<th>Log</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workorder</td>
<td>/usr/local/avamar/clientlogs</td>
</tr>
<tr>
<td>Agent</td>
<td>/var/avamar/</td>
</tr>
<tr>
<td>Console</td>
<td>$HOME/.avamardata/</td>
</tr>
</tbody>
</table>
CHAPTER 15
Data Domain System Integration

This chapter includes the following topics:

- Overview of Data Domain system integration ....................................................... 354
- Preparing to add a Data Domain system .............................................................. 359
- Adding a Data Domain system ......................................................................... 361
Overview of Data Domain system integration

You can store Avamar backups on one or more Data Domain systems, and then seamlessly restore data from the backups.

You can back up both file system and application data to a Data Domain system. Storage of Avamar backups on a Data Domain system is recommended in environments with databases that are large and have a high change rate. Store the following types of backups on the Avamar server instead:

- File system backups
- Virtual machine backups
- Remote office backups
- Desktop/laptop backups
- Backups of databases with low change rates

When you store VMware image backups on a Data Domain system, you can boot a lost or corrupted virtual machine almost instantly from the backup by using the instant access feature.

You also can store Avamar checkpoints for a single-node server or Avamar Virtual Edition (AVE) on a Data Domain system.

Architecture of Avamar with Data Domain

A Data Domain system performs deduplication through DD OS software. Avamar source-based deduplication to a Data Domain system is facilitated through the use of the Data Domain Boost (DD Boost) library.

Avamar uses the DD Boost library through API-based integration to access and manipulate directories, files, and other items on the Data Domain File System. The DD Boost API gives Avamar visibility into some of the properties and capabilities of the Data Domain system. This enables Avamar to control backup images stored on Data Domain systems. It also enables Avamar to manage maintenance activities and to control replication to remote Data Domain systems.

DD Boost is installed on the backup clients and on the Avamar utility node or an Avamar single node system. DD Boost is installed automatically when you install the Avamar client or server software.
You can specify whether specific backup datasets are stored on an Avamar server or a Data Domain system. When you select an Avamar server as the backup target, the Avamar client on each host performs deduplication segment processing. Data and metadata sent from the client are stored on the Avamar server. When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. The related metadata generated by the Avamar client software is simultaneously sent to the Avamar server for storage. The metadata enables the Avamar management system to perform restore operations directly from the Data Domain system without first going through the Avamar server.

The process of data recovery is transparent to the backup administrator. The backup administrator uses the same Avamar recovery processes that are native to current Avamar implementations.

**File system backups on a Data Domain system**

Avamar supports storage of file system backups on a Data Domain system for the following operating systems:

- Windows and Windows Server
- IBM AIX
- HP-UX (IA-64 only, requires ONCPlus Library revision 11.31.06 or later)
- Solaris (for Solaris 10 on SPARC, client side deduplication is disabled and deduplication is performed on the Data Domain system)
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)

Only 64-bit operating systems are supported. You cannot store file system backups of desktop/laptop computers on a Data Domain system. The *EMC Avamar Compatibility and*
Interoperability Matrix on EMC Online Support provides updated client compatibility information, including a complete list of supported operating system versions and service packs.

Application backups on a Data Domain system

You can store application data backups from the following Avamar plug-ins on a Data Domain system:

- Avamar Plug-in for DB2
- Avamar Plug-in for Exchange VSS
- Avamar Plug-in for Hyper-V VSS
- Avamar Plug-in for Lotus Domino
- Avamar Plug-in for Oracle
- Avamar Plug-in for SAP with Oracle
- Avamar Plug-in for SharePoint VSS
- Avamar Plug-in for Sybase ASE
- Avamar Plug-in for SQL Server

You can also store VMware image backups and backups with the Avamar NDMP Accelerator on a Data Domain system.

VMware instant access

When you store VMware image backups on a Data Domain system, you can boot a lost or corrupted virtual machine almost instantly from the backup by using the instant access feature.

With instant access, the virtual machine image backup is staged to a temporary NFS share on the Data Domain system. You can then use the vSphere Client to power on the virtual machine and initiate a vMotion of the virtual machine to a datastore within the vCenter. When the vMotion is complete, the restored virtual machine files no longer exist on the Data Domain system. Then you use Avamar Administrator to delete the NFS share on the Data Domain system.

**Note**

When you use instant access, do not leave the virtual machine running on the Data Domain system for extended periods. When the virtual machine runs on the Data Domain system, performance might degrade because of the workflow.

You can also restore a virtual machine to the production environment instead of using instant access. The Avamar software leverages Changed Block Tracking (CBT) to dramatically speed the recovery process.

The **EMC Avamar for VMware User Guide** provides details on instant access and restore of image backups.

Checkpoints on a Data Domain system

You can store Avamar checkpoints for a single-node server or Avamar Virtual Edition (AVE) on a Data Domain system that uses DD OS 5.3 or later. Checkpoints are system-wide backups of the Avamar server for disaster recovery purposes.

Storage of checkpoints on a Data Domain system is recommended in environments that do not include replication to a secondary Avamar server or in environments where most client backups are stored on a Data Domain system.
To configure storage of checkpoints on a Data Domain system, select the **Use as target for Avamar Checkpoint Backups** checkbox when you add or edit the Data Domain system in Avamar Administrator.

Contact EMC Professional Service representatives for assistance with rolling back the Avamar server to a checkpoint on a Data Domain system.

**Data Domain system streams**

Each Data Domain system has a soft limit to the maximum number of connection and data streams that can be sustained simultaneously while maintaining performance. The number of streams varies depending on the Data Domain system model.

You configure the maximum number of streams Avamar can use when you add a Data Domain system to the Avamar server. The Avamar server uses the backup stream value to limit the number of concurrent backup or restore jobs.

If the Data Domain system is fully dedicated to the Avamar server, the stream value entered in Avamar Administrator could potentially be the maximum number of streams supported by the Data Domain system model. In cases where the Data Domain system is shared with other third-party applications or another Avamar server, then a subset of the number of streams should be allocated.

Each Avamar backup client that supports multi-stream backups can be configured to use the appropriate number of streams (typically based on the number of databases) through multi-streaming configuration when the Avamar backup job is configured. The streams are released when the backup or restore operation completes. The number of streams allocated should depend on the number and type of Avamar clients that backs up data at about the same time.

**Replication with Data Domain systems**

The Avamar replication feature transfers data from a source Avamar server to a destination Avamar server. When you store Avamar backups on a Data Domain system, the replication process transfers Avamar data from the source Data Domain system to a destination Data Domain system.

**Supported replication configurations**

If the source Avamar server uses more than one Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. Also, if the source Avamar server uses a single Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. All of the data is replicated through DD Boost.

In a configuration with multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system by mapping a domain on the source Avamar server to a destination Data Domain system. You can also specify which Data Domain system is the default destination. The default destination is the Data Domain system to which Avamar replicates data when a destination Data Domain system is not identified on the **Storage Mapping** tab of the **Replication** window in Avamar Administrator. The *EMC Avamar and EMC Data Domain System Integration Guide* provides instructions on storage mapping and specifying the default destination Data Domain system.

**Replication control**

Avamar replicates Avamar data from the source Data Domain system to the destination Data Domain system by using DD Boost. The Data Domain replication feature is not used. You must have a Data Domain replication license to copy data from one system to another.
You configure and monitor replication on the Avamar server. There is no way to track replication by using Data Domain administration tools.

Avamar replicates the data directly from one Data Domain system to another. In other words, Avamar does not stage the data on the Avamar server before replicating the data to the destination Data Domain system.

**Replication schedule**

The replication of Avamar data on a Data Domain system occurs on the Avamar replication schedule. You cannot schedule replication of data on the Data Domain system separately from the replication of data on the Avamar server.

**Monitoring and reporting Data Domain system status**

Avamar can collect and display data for health monitoring, system alerts, and capacity reporting on a Data Domain system by using Simple Network Management Protocol (SNMP).

SNMP enables you to monitor Data Domain activities, events, capacity, and system status in the same way that you monitor activities, events, capacity, and system status for the Avamar server. You configure SNMP settings when you add a Data Domain system to the Avamar configuration.

You can also run reports to analyze the system. The *EMC Avamar Reports Guide* provides more information about creating reports.

The *EMC Avamar and EMC Data Domain System Integration Guide* provides more information on monitoring system status for a Data Domain system.

**Security with Data Domain system integration**

The following sections provide details on security in an Avamar environment with Data Domain for encryption and user access.

**Encryption**

The connection between the Avamar client and the Data Domain system is not encrypted. The DD Boost library does not support data encryption between the client and the Data Domain system. Backups from the Avamar client to the Avamar server are always compressed and encrypted.

**User access**

Use caution when granting users access to the Data Domain system. A user should not be able to directly access the Data Domain system and manually delete data.

**Data migration to a Data Domain system**

You cannot migrate backup data directly from the Avamar server to the Data Domain system.

To start using the Data Domain system as the backup target for an Avamar client instead of the Avamar server, edit the dataset to use the Data Domain system, and start performing backups to the Data Domain system. When you change the backup target to the Data Domain system, you must perform a full backup.

After you successfully perform a backup to the Data Domain system, you can delete the earlier backups from the Avamar server.
Preparing to add a Data Domain system

Before you add a Data Domain system to the Avamar configuration, install and configure both the Avamar server and the Data Domain system. You must also ensure that the environment meets the system requirements, and create a DD Boost user account on the Data Domain system.

System requirements for Data Domain system integration

Ensure that the environment meets the necessary system requirements before you add a Data Domain system to the Avamar configuration.

The following table lists the requirements for the Data Domain system.

**Table 95 Data Domain system requirements**

<table>
<thead>
<tr>
<th>Feature or specification</th>
<th>Requirement for use with Avamar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Domain Operating System (DD OS)</td>
<td>DD OS 5.3.x. or 5.4.x</td>
</tr>
<tr>
<td>DD Boost</td>
<td>DD Boost 2.6.x</td>
</tr>
</tbody>
</table>

**Note**

DD Boost software enables backup servers to communicate with storage systems without the need for Data Domain systems to emulate tape. There are two components to DD Boost: one component that runs on the backup server and another that runs on the Data Domain system. In the context of Avamar, the component that runs on the backup server (DD Boost libraries) is integrated into the Avamar client. DD Boost software is an optional product that requires a license to operate on the Data Domain system.

<table>
<thead>
<tr>
<th>Data Domain device type</th>
<th>Avamar supports any Data Domain system that supports the execution of the required DD OS version.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Domain File System</td>
<td>Enable Data Domain File System by using either the Data Domain System Manager or CLI.</td>
</tr>
<tr>
<td></td>
<td>After you enable file system operations, it may take as many as 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is using the DD Extended Retention option. Do not perform backups, restores, or system maintenance operations until the status appears correctly in Avamar Administrator. Otherwise, backups, restores, or system maintenance operations may fail.</td>
</tr>
<tr>
<td>DD Boost</td>
<td>Enable DD Boost on the Data Domain system.</td>
</tr>
<tr>
<td></td>
<td>When you enable DD Boost, DD Boost becomes the preferred method of connectivity for any clients that are enabled for DD Boost. While this method is acceptable for clients that can take advantage of DD Boost features, it can result in performance degradation for other clients. Proper due diligence and effective data gathering are keys to avoiding such interactions, especially during upgrades.</td>
</tr>
</tbody>
</table>
Table 95 Data Domain system requirements (continued)

<table>
<thead>
<tr>
<th>Feature or specification</th>
<th>Requirement for use with Avamar</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD Boost user account</td>
<td>The DD Boost library uses a unique login account name created on the Data Domain system; this account name is known as the DD Boost account. Only one DD Boost account exists per Data Domain system. If the account is renamed and/or the password is changed, these changes must be immediately updated on the Avamar system by editing the Data Domain configuration options. Failure to update the DD Boost account information could potentially yield integrity check errors or backup and restore problems. The DD Boost account must have administrator privileges.</td>
</tr>
</tbody>
</table>

Capacity requirements

Carefully assess backup storage needs when evaluating how much data to store on the Data Domain system and the Avamar server. Include estimates from data that is sent to the Data Domain system from any other servers.

When the Data Domain system reaches its maximum storage capacity, no further backups to the Data Domain system occur until additional capacity is added or old backups are deleted.

Requirements when using other backup products

Data Domain systems can use other third-party backup and archiving software. The Avamar server does not assume it has sole ownership of the Data Domain system. Ensure that proper sizing is evaluated if the system is shared with other software products.

The Avamar server makes no use of the native Data Domain system snapshot and replication features. Replication occurs through the DD Boost SDK library by using copying and cloning. However, other third party products may make use of the native Data Domain system snapshot and replication features. In this case, a snapshot of an entire Data Domain system or a replication of an entire Data Domain system includes the Avamar data.

Network requirements

The Avamar server and all Data Domain systems must be on the same local network. Do not connect the Avamar server and Data Domain systems over a Wide Area Network (WAN). Configurations that use a WAN are not supported.

You can use Avamar replication over a WAN to replicate data from source Avamar servers and Data Domain systems to target Avamar servers and Data Domain systems.

Before integrating a Data Domain system with an Avamar server, ensure that enough network bandwidth is available. To obtain the maximum throughput available on a Data Domain system (for restores, level zero backups, and subsequent incremental backups after a level-zero backup), verify that the network infrastructure provides more bandwidth than the bandwidth required by the maximum throughput of the Data Domain system.

The network configuration must also meet the following requirements:

- Assign a Fully Qualified Domain Name (FQDN) to each Data Domain system.
- Do not use IP addresses in place of hostnames when registering a Data Domain system. This can limit the ability to route optimized duplication traffic exclusively through a registered interface.
Ensure that DNS on the Data Domain system is properly configured.
Ensure that forward and reverse DNS lookups work between the Avamar server, the Data Domain system, and all backup and restore clients.
Use Hosts files to resolve hostnames to non-routable IP addresses.
Do not create secondary hostnames to associate with alternate or local IP interfaces.

NTP requirements
The Avamar server and the Data Domain system must use the same Network Time Protocol (NTP) server.

Port usage and firewall requirements
To enable communication between Avamar and the Data Domain systems, review and implement the port usage and firewall requirements in the following documents, which are available on EMC Online Support:
- EMC Avamar Product Security Guide
- Port Requirements for Allowing Access to Data Domain System Through a Firewall

Creating a DD Boost user account
Before you can add a Data Domain system to the Avamar configuration, prepare the Data Domain system by enabling DD Boost and creating a DD Boost user account for the Avamar server to use to access the Data Domain system for backups and restores (and replication, if applicable).
If you change the DD Boost account name or password after you create the account, remember to edit the Data Domain system configuration in Avamar Administrator. Otherwise all backups, restores and maintenance activities fail.

Procedure
1. Disable DD Boost on the Data Domain system by logging into the Data Domain CLI as an administrative user and typing the following command:
   
   `ddboost disable`

2. Create the DD Boost user account with administrator privileges by typing the following command:
   
   `user add username role admin`
   
   where `username` is the username for the new account.

3. Set the new account as the DD Boost user by typing the following command:
   
   `ddboost set user-name username`
   
   where `username` is the username for the account.

4. Enable DD Boost to allow the changes to take effect by typing the following command:
   
   `ddboost enable`

Adding a Data Domain system

Procedure
1. In Avamar Administrator, click the Server launcher button.
   
   The Server window appears.
2. Click the Server Management tab.

3. Select Actions > Add Data Domain System.

The Add Data Domain System dialog box appears.

4. On the System tab, specify Data Domain system information:
   a. In the Data Domain System Name box, type the fully qualified domain name of the Data Domain system to add.

   **Note**
   Do not use an IP address or a secondary hostname that associates with alternative or local IP interfaces. It may limit the ability of Avamar to route optimized deduplication traffic.

   b. In the DDBoost User Name box, type the username of the DD Boost account for Avamar to use to access the Data Domain system for backups, restores, and replication.

   c. In the Password box, type the password for the account that Avamar should use to access the Data Domain system for backups, restores, and replication.

   d. In the Verify Password box, type the password again to verify it.

   e. If you have more than one Data Domain system associated with Avamar, you can specify one Data Domain system to be the default replication storage. Select Use system as default replication storage if this system is the default replication storage.

   f. To store checkpoints for a single-node Avamar server or Avamar Virtual Edition (AVE) server on the Data Domain system instead of the Avamar server, select the Use as target for Avamar Checkpoint Backups checkbox.

   g. Click Get Stream Info to view the maximum number of streams that the Data Domain system supports.

   h. Specify the maximum number of streams that Avamar can use at any one time to perform backups and restores:
      - To specify a defined number of streams, type the number in the Max used by Avamar box.
      - To specify a maximum number of streams based on the percentage of the total number of supported streams, type the percentage in the Max used by Avamar box and then select the As percentage of the max limit checkbox.

   Consider both the maximum number of streams that the Data Domain system supports, as well as whether other applications are using streams to send data to and receive data from the Data Domain system.

   If the processes writing to and reading from the Data Domain system use all available streams, then Avamar queues backup or restore requests until one or more streams become available.

5. To configure SNMP, click the SNMP tab.

SNMP configuration enables Avamar to collect and display data for system health monitoring, system alerts, and capacity reporting.

6. Verify the SNMP configuration:
   - The Getter/Setter Port Number box lists the port on the Data Domain system from which to receive and on which to set SNMP objects. The default value is 161.
• The **SNMP Community String** box lists the community string Avamar uses for read-only access to the Data Domain system.

• The **Trap Port Number** box lists the trap port on the Avamar server. The default value is 163.

7. Click **OK**.

   A progress message appears.

8. When the operation completes, click **Close**.

**Results**

When you add a Data Domain system to the Avamar configuration, Avamar creates an MTree on the Data Domain system for the Avamar server. The MTree refers to the directory created within the DD Boost path. Data Domain systems support a maximum of 100 MTrees. If you reach the limit, then you cannot add the Data Domain system to the Avamar configuration.
APPENDIX A

Command Shell Server Logins

- User accounts ........................................................................................................................... 366
- Starting command shell sessions ............................................................................................... 366
- Switching user IDs ..................................................................................................................... 366
- Using sudo ................................................................................................................................. 367
User accounts

The following user accounts are commonly used for system administration and maintenance tasks:

- root
- admin
- dpn

The admin and dpn user accounts require authentication by way of Secure Shell (SSH).

Starting command shell sessions

Log in to an Avamar server or utility node through SSH as the admin user to perform configuration and maintenance tasks for the Avamar system.

Procedure

1. To start a command shell session on a single-node server, open a command shell and log in to the server as admin.
2. To start a command shell session on a multi-node server:
   a. Open a command shell and log in to the utility node as admin.
   b. Load the admin OpenSSH key by typing the following commands:

   ```
   ssh-agent bash
   ssh-add ~admin/.ssh/admin_key
   ```
   c. When prompted, type the admin_key passphrase and press Enter.

Switching user IDs

You can switch the user of a command shell session to root by typing `su`, and switch back to the previous login ID by typing `exit`. When you switch the user of a command shell session to dpn, you must also load the dpn OpenSSH key.

Procedure

1. Switch user to the dpn user account and login shell by typing `su - dpn`.
2. When prompted for a password, type the dpn password and press Enter.
3. Load the dpn OpenSSH key by typing:

   ```
   ssh-agent bash
   ssh-add ~dpn/.ssh/dpnid
   ```

Note

To determine the active user account (login ID) of a shell session, type `whoami`. 
Using sudo

On Gen4 and later Avamar Data Stores, the admin and dpn user accounts are automatically added to the `sudoers` file. This enables admin and dpn users to execute a limited set of commands that would otherwise require operating system root permission.

Prefixing commands with sudo

Instead of switching user to root with the `su` command, admin and dpn users can directly issue commands normally requiring root permissions by prefixing each command with `sudo`.

For example, the following command installs `MyPackage.rpm`:

```
sudo rpm -ivh MyPackage.rpm
```

If prompted for a password, type the password and press `Enter`.

You might be periodically prompted to retype the admin or dpn password when prefixing other commands with `sudo`. This is normal.

Spawning a sudo Bash subshell

If you need to execute several commands that normally require root permissions, you can spawn a persistent sudo Bash subshell by typing `sudo bash`. Using `sudo bash` enables you to directly type multiple commands with no additional changes to the command line syntax when the commands normally require root permissions.

For example:

```
sudo bash
rpm -ivh MyPackage1.rpm
rpm -ivh MyPackage2.rpm
rpm -ivh MyPackage3.rpm
exit
```
Command Shell Server Logins
APPENDIX B

Plug-in Options

- How to set plug-in options ................................................................. 370
- Backup options ................................................................................ 370
- Restore options ............................................................................... 372
How to set plug-in options

Plug-in options enable you to control specific actions for on-demand backups, restores, and scheduled backups. The plug-in options that are available depend on the operation type and plug-in type.

You specify plug-in options in Avamar Administrator for on-demand backup or restore operations, or when you create a dataset for a scheduled backup. You set plug-in options with the graphical user interface (GUI) controls (text boxes, checkboxes, radio buttons, and so forth). In addition to using the GUI controls for the options, you can type an option and its value in the Enter Attribute and Enter Attribute Value fields.

NOTICE

The Avamar software does not check or validate the information that you type in the Enter Attribute and Enter Attribute Value fields. In addition, the values in the Enter Attribute and Enter Attribute Value fields override settings that you specify with the GUI controls for the options.

Backup options

The backup options that appear depend on the type of plug-in.

The table in this topic lists the backup options for the following plug-ins:

- AIX file system
- FreeBSD file system
- HP-UX file system
- Linux file system
- Macintosh file system
- NetWare file system
- SCO OpenServer file system

Backup options for the Avamar Plug-in for Microsoft Windows are available in the *EMC Avamar for Windows Server User Guide*. Backup options for application plug-ins, such as SQL Server, SharePoint VSS, and so on, are available in the user guide for the plug-in.

The following options are available when you perform an on-demand backup or when you configure a dataset for scheduled backups for the file system plug-ins listed in this topic.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store backup on Data Domain system</td>
<td>(AIX, HP-UX, Linux, and Macintosh only) Stores the backup on a configured Data Domain system instead of on the Avamar server. To store the backup on a Data Domain system, select the checkbox and then select the Data Domain system from the list.</td>
</tr>
<tr>
<td>Encryption method to Data Domain system</td>
<td>(AIX, HP-UX, Linux, and Macintosh only) Specifies the encryption method for data transfer between the client and the Data Domain system.</td>
</tr>
<tr>
<td>Backup label</td>
<td>Assigns this descriptive label to the backup.</td>
</tr>
</tbody>
</table>
Table 96 Backup plug-in options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(NetWare only) SMS Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Server login ID</td>
<td>(NetWare only) Specifies the SMS login username. For example, CN=admin.O=HOSTNAME_CTX.</td>
</tr>
<tr>
<td>Server password</td>
<td>(NetWare only) Specifies the password for the SMS login username.</td>
</tr>
<tr>
<td>Snapshot stored-on pool</td>
<td>(NetWare only) Specifies the snapshot stored-on pool name.</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
</tr>
</tbody>
</table>
| List backup contents | Specifies how much information about the backup contents to include in the log files. One of the following:  
  - No file listing  
  - List file names  
  - List files and dates |
| Informational message level | Specifies how many informational messages to include in the log files. One of the following:  
  - No informationals—Suppresses all informational messages, but includes errors and warnings in the log files.  
  - Some informationals—Includes some informational messages in the log files.  
  - Many informationals—Includes additional status information in the log files.  
  - All informationals—Provides maximum information. Includes all informational messages, errors, and warnings in the log files. |
| Report advanced statistics | Specifies whether to write advanced timing and deduplication statistics to the log files. |
| Enable debugging messages | Specifies whether to write maximum information to log files, which creates very large log files. |
| **File System Traversal** | |
| Do not traverse any mounts | Specifies whether to traverse mount points during the backup. |
| Traverse fixed-disk mounts | Specifies whether to traverse only fixed-disk file system mount during the backup. |
| Traverse fixed-disk and remote network mounts | Specifies whether to traverse both fixed-disk and NFS network mount points during the backup. |
| Force traversal of specified file system type(s) | Accepts a comma-separated list of one or more file system types (for example, nfs, ext2, jfs, xfs) that should not be traversed during this backup. |
| **Pre-Script** | |
| Run user-defined script at beginning of backup | Runs a user-defined script at the beginning of the backup session. The script must be located in /usr/local/avamar/etc/scripts. |
### Table 96 Backup plug-in options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort backup if script fails</td>
<td>Specifies whether to stop the backup if the script returns a non-zero status code.</td>
</tr>
<tr>
<td><strong>Post-Script</strong></td>
<td></td>
</tr>
<tr>
<td>Run user-defined script at end of backup</td>
<td>Runs a user-defined script at the end of the backup session. The script must be located in /usr/local/avamar/etc/scripts.</td>
</tr>
<tr>
<td>Exit process with script failure exitcode</td>
<td>Specifies whether avtar should exit with the exit code of the script instead of a standard avtar exit code.</td>
</tr>
<tr>
<td><strong>Client Cache Options</strong></td>
<td></td>
</tr>
<tr>
<td>Check client-side caches and report</td>
<td>If selected, a backup does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server.</td>
</tr>
<tr>
<td>inconsistencies</td>
<td></td>
</tr>
<tr>
<td>Check and repair client-side caches</td>
<td>If selected, a backup does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server, and repairs inconsistencies.</td>
</tr>
<tr>
<td>Maximum client file cache size (MBs)</td>
<td>Specifies the maximum client file cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of physical RAM should be allocated to the client file cache.</td>
</tr>
<tr>
<td>Maximum client hash cache size (MBs)</td>
<td>Specifies the maximum client hash cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of physical RAM should be allocated to the client hash cache.</td>
</tr>
<tr>
<td><strong>Advanced Options</strong></td>
<td></td>
</tr>
<tr>
<td>Client-side flag file</td>
<td>Specifies the path to a flag file on the client that contains additional option settings.</td>
</tr>
<tr>
<td>Network usage throttle (Mbps)</td>
<td>Specifies a setting that reduces network usage to a specified rate, expressed as megabits/second. For example, 0 = unrestricted, 50% of a T1 = 0.72.</td>
</tr>
<tr>
<td>Directly connect to all server nodes</td>
<td>Specifies whether to establish multiple connections to the server. This can improve backup performance under certain circumstances.</td>
</tr>
</tbody>
</table>

### Restore options

The restore options that are available depend on the type of plug-in.
The table in this topic lists the backup options for the following plug-ins:

- AIX file system
- FreeBSD file system
- HP-UX file system
- Linux file system
• Macintosh file system
• NetWare file system
• SCO OpenServer file system

Restore options for the Avamar Plug-in for Microsoft Windows are available in the *EMC Avamar for Windows Server User Guide*. Restore options for application plug-ins, such as SQL Server, SharePoint VSS, and so on, are available in the user guide for the plug-in.

The following options are available when you perform a restore using the file system plug-ins listed in this topic.

**Table 97 Restore plug-in options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overwrite existing files</td>
<td>Controls behavior when the file to be restored already exists. One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Never</td>
</tr>
<tr>
<td></td>
<td>• Always</td>
</tr>
<tr>
<td></td>
<td>• Generate New Name</td>
</tr>
<tr>
<td></td>
<td>• If Modified</td>
</tr>
<tr>
<td></td>
<td>• If Newer</td>
</tr>
<tr>
<td>Encryption method from Data Domain system</td>
<td>If the backup was stored on a Data Domain system, select the encryption method to use for data transfer from the Data Domain system to the client.</td>
</tr>
</tbody>
</table>

**(NetWare only) SMS Authentication**

<table>
<thead>
<tr>
<th>Server login ID</th>
<th>(NetWare only) Specifies the SMS login username. For example, CN=admin.O=HOSTNAME_CTX.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server password</td>
<td>(NetWare only) Specifies the password for the SMS login username.</td>
</tr>
</tbody>
</table>

**Logging**

<table>
<thead>
<tr>
<th>List backup contents</th>
<th>Specifies how much information about the backup contents to include in the log files. One of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• No file listing</td>
</tr>
<tr>
<td></td>
<td>• List file names</td>
</tr>
<tr>
<td></td>
<td>• List files and dates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Informational message level</th>
<th>Specifies how many informational messages to include in the log files. One of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• No informationals—Suppresses all informational messages, but includes errors and warnings in the log files.</td>
</tr>
<tr>
<td></td>
<td>• Some informationals—Includes some informational messages in the log files.</td>
</tr>
<tr>
<td></td>
<td>• Many informationals—Includes additional status information in the log files.</td>
</tr>
<tr>
<td></td>
<td>• All informationals—Provides maximum information. Includes all informational messages, errors, and warnings in the log files.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Report advanced statistics</td>
<td>Specifies whether to write advanced timing and deduplication statistics to the log files.</td>
</tr>
<tr>
<td>Enable debugging messages</td>
<td>Specifies whether to write maximum information to log files, which creates very large log files.</td>
</tr>
<tr>
<td><strong>Pre-Script</strong></td>
<td></td>
</tr>
<tr>
<td>Run user-defined script at</td>
<td>Runs a user-defined script at the beginning of the restore session. The script must be located in <code>/usr/local/avamar/etc/scripts</code>.</td>
</tr>
<tr>
<td>beginning of restore</td>
<td></td>
</tr>
<tr>
<td>Abort restore if script fails</td>
<td>Specifies whether to stop the restore if the script returns a non-zero status code.</td>
</tr>
<tr>
<td><strong>Post-Script</strong></td>
<td></td>
</tr>
<tr>
<td>Run user-defined script at</td>
<td>Runs a user-defined script at the end of the restore session. The script must be located in <code>/usr/local/avamar/etc/scripts</code>.</td>
</tr>
<tr>
<td>end of restore</td>
<td></td>
</tr>
<tr>
<td>Exit process with script</td>
<td>Specifies whether <code>avtar</code> should exit with the exit code of the script instead of a standard <code>avtar</code> exit code.</td>
</tr>
<tr>
<td>failure exitcode</td>
<td></td>
</tr>
<tr>
<td><strong>Client Cache Options</strong></td>
<td></td>
</tr>
<tr>
<td>Check client-side caches and</td>
<td>If selected, a restore does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server.</td>
</tr>
<tr>
<td>report inconsistencies</td>
<td></td>
</tr>
<tr>
<td>Check and repair client-side</td>
<td>If selected, a restore does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server, and repairs inconsistencies.</td>
</tr>
<tr>
<td>caches</td>
<td></td>
</tr>
<tr>
<td>Rebuild client-side caches</td>
<td>Does not restore data. If selected, Avamar uses the contents of the last backup to re-create the client-side file cache.</td>
</tr>
<tr>
<td>from most recent backup</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Options</strong></td>
<td></td>
</tr>
<tr>
<td>Do not descend into</td>
<td>Specifies whether to restore only the specified top-level directory and not any subdirectories.</td>
</tr>
<tr>
<td>subdirectories</td>
<td></td>
</tr>
<tr>
<td>Recreate original path</td>
<td>Specifies whether to re-create the original path to files and directories beneath the specified target directory.</td>
</tr>
<tr>
<td>beneath target directory</td>
<td>For example, if you restore <code>/usr/MyDir/MyFile</code> to <code>/tmp</code> and you select this option, then the full path to the restored file is <code>/tmp/usr/MyDir/MyFile</code>.</td>
</tr>
<tr>
<td>Directly connect to all server</td>
<td>Specifies whether to establish multiple connections to the server. This can improve restore performance under certain circumstances.</td>
</tr>
<tr>
<td>nodes</td>
<td></td>
</tr>
</tbody>
</table>
GLOSSARY

A

accelerator The Avamar NDMP Accelerator (accelerator) is a specialized Avamar server node that, when used as part of an Avamar system, enables backup and restore of network addressed storage (NAS) systems by way of the network data management protocol (NDMP).

activation The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also client activation

authentication system A username and password system that is used to grant user access to the Avamar server. Avamar supports its own internal authentication system (avs), as well as several external authentication systems (OpenLDAP, Windows Active Directory, NIS, and SMB).

Avamar Administrator A graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.

Avamar client A computer or workstation that runs Avamar software and accesses the Avamar server over a network connection. Avamar client software comprises a client agent and one or more plug-ins.

Avamar Downloader Service A Windows-based file distribution system that delivers software installation packages to target Avamar systems.

Avamar Enterprise Manager Avamar Enterprise Manager is a multi-server management console application that provides centralized Avamar server administration capabilities for larger businesses and enterprises.

Avamar File System (AvFS) A browsable virtual file system view of the normally inaccessible Avamar HFS. The Avamar File System provides read-only accessibility to all backups stored on an Avamar server down to the individual file level. This allows an Avamar server to be used as an online long-term historical strategic enterprise information store in addition to a backup and restore repository.

Avamar Installation Manager A web interface that manages installation packages. A successful Avamar server software installation or upgrade embeds the Avamar Installation Manager functionality in the Avamar Enterprise Manager as the System Maintenance page.

Avamar server The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

Avamar Web Access A browser-based user interface that provides access to the Avamar server for the express purpose of restoring files to a client.

Avinstaller A backend service that executes and reports package installations.
B

backup A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

C

client activation The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also activation

client agent A platform-specific software process that runs on the client and communicates with the Management Console Server (MCS) and with any plug-ins installed on that client.

client registration The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during client activation.

See also registration

ConnectEMC A program that runs on the Avamar server and that sends information to EMC Technical Support. ConnectEMC is typically configured to send alerts for high priority events as they occur, as well as reports once daily.

D

dataset A policy that defines a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

DNS Domain Name Server. A dynamic and distributed directory service for assigning domain names to specific IP addresses.

domain A feature in Avamar Administrator that is used to organize large numbers of clients into named areas of control and management.

E

Email Home An optional feature that uses the High Priority Events profile and Notification schedule to regularly send server error and status messages to EMC Technical Support.

EMC repository A repository that contains server installation packages, client installation packages, and manifest files. The repository is located on the EMC network. Each EMC customer has a download center that contains files available to them. Outgoing communication from the Avamar Downloader Service to the EMC repository is encrypted with SSL over an HTTP connection.
**Enterprise Manager Server (EMS)**

The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar system information, and provides a mechanism for managing Avamar systems using a standard web browser. The EMS also communicates directly with MCS.

**ESRS**

EMC Secure Remote Support.

**full replication**

A full “root-to-root” replication creates a complete logical copy of an entire source system on the destination system. The replicated data is not copied to the REPLICATE domain. Instead, it is added to the root domain just as if source clients had registered with the destination system. Also, source server data replicated in this manner is fully modifiable on the destination system. This replication method is typically used for system migration (from a smaller Avamar configuration to a larger, possibly multi-node configuration) or system replacement (for instance, in a case of disaster recovery).

**group**

A level of organization in Avamar Administrator for one or more Avamar clients. All clients in an Avamar group use the same group policies, which include the dataset, schedule, and retention policy.

**group policy**

The dataset, schedule, and retention policy for all clients in an Avamar group.

**HFS**

Hash File System. The content addressed storage area inside the Avamar server used to store client backups.

**HFS check**

An Avamar Hash File System check (HFS check) is an internal operation that validates the integrity of a specific checkpoint. Once a checkpoint has passed an HFS check, it can be considered reliable enough to be used for a server rollback.

**JRE**

Java Runtime Environment.

**LAN**

Local Area Network.

**local repository**

The /data01/avamar/repo/packages directory on the utility node or single-node server. This directory contains the most current manifest file from the EMC repository. The Avamar Downloader Service pushes packages from the EMC repository to the local repository. If a customer site does not allow Internet access, you can manually copy packages into the local repository.

**LOFS**

Loopback File System
**MAC address**  Media Access Control Address. A unique hardware address, typically embedded at the lowest level in a hardware assembly, that uniquely identifies each device on a network.

**manifest file**  An XML file listing all the server, client, and workflow packages currently available for download from the EMC repository.

**MCS**  Management console server. The server subsystem that provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by *Avamar Administrator*.

**module**  Avamar 1.2.0 and earlier multi-node Avamar servers utilized a dual-module synchronous RAIN architecture in which nodes were equally distributed in two separate equipment cabinets on separate VLANs. The term “module” is a logical construct used to describe and support this architecture (older multi-node Avamar servers comprised a primary module and a secondary module). These legacy systems continue to be supported. However, newer multi-node Avamar servers use a single module architecture, and even though Avamar Administrator provides “module detail” information, a module is therefore logically equivalent to the entire server.

**N**

**NAT**  Network Address Translation.

**NDMP**  Network data management protocol. An open protocol that is used to move data from a NAS system to a backup server.

**NFS**  Network file system.

**NIS**  Network Information Service. An external authentication system that can be used to log in to an Avamar server.

**node**  A networked storage subsystem that consists of both processing power and hard drive storage, and runs Avamar software.

**NTP**  Network Time Protocol. Controls the time synchronization of a client or server computer to another reference time source.

**O**

**ODBC**  Open DataBase Connectivity. A standard database access method that makes it possible to access any data from any application, regardless of which database management system (DBMS) is handling the data.

**OpenLDAP**  Open Lightweight Directory Access Protocol. An external authentication system that can be used to log in to an Avamar server.
packages
Avamar software installation files, hotfix patches, and OS patches available from the EMC repository. Packages comprise three types:
- Client—A release of Avamar file system or application backup software.
- Server—A new release of Avamar server software, a service pack, or a patch for the operating system, MC, or GSAN.
- Workflow—A package that runs operations such as adding a node or replacing a node.
Package files use the .avp file extension.

PAM
Pluggable Authentication Module. A Linux library that enables a local system administrator to define how individual applications authenticate users.

plug-in
Avamar client software that recognizes a particular kind of data resident on that client.

plug-in options
Options that you specify during backup or restore to control backup or restore functionality.

policy
A set of rules for client backups that can be named and applied to multiple groups. Groups have dataset, schedule, and retention policies.

R
RAIN
Redundant Array of Independent Nodes. A flexible, fault-tolerant architecture that enables an Avamar server to maintain availability and preserve data storage if single nodes fail in an Avamar module.

RDMS
Relational Database Management System.

registration
The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during client activation.

See also client registration

replication
Replication is an optional feature that enables one Avamar server to store a read-only copy of its data on another Avamar server to support future disaster recovery of that server.

restore
An operation that retrieves one or more file systems, directories, files, or data objects from a backup and writes the data to a designated location.

retention
The time setting to automatically delete backups on an Avamar server. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

roles
A setting in Avamar Administrator that controls which operations each user can perform in the Avamar server. Roles are assigned on a user-by-user basis.
S

**schedule**  The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

**SSH**  Secure Shell. A remote login utility that authenticates by way of encrypted security keys instead of prompting for passwords. This prevents passwords from traveling across networks in an unprotected manner.

**storage node**  A node in the Avamar server that provides storage of data.

**system migration**  A planned operation that uses full “root-to-root” replication to copy all data residing on a source Avamar server to a new destination server. If global client IDs (global CIDs) are used, clients that formerly backed up to the source server can continue to operate transparently without reregistering with the new destination server.

T

**TFTP**  Trivial File Transfer Protocol. A version of the TCP/IP FTP protocol that has no directory or password capabilities.

U

**utility node**  In scalable multi-node Avamar servers, a single utility node provides essential internal services for the server. These services include MCS, cronjob, Domain Name Server (DNS), External authentication, Network Time Protocol (NTP), and Web access. Because utility nodes are dedicated to running these essential services, they cannot be used to store backups.

V

**VLAN**  Virtual Local Area Network.