

EMC ISILON CUSTOMER TROUBLESHOOTING GUIDE

TROUBLESHOOT YOUR LDAP AUTHENTICATION PROVIDER

Abstract

This guide will help you to troubleshoot the following scenarios:

- The user is unable to connect to the cluster by IP address.
- The user is unable to connect to the cluster by FQDN or SmartConnect zone.
- The user is unable to connect to some nodes.
- The LDAP authentication provider is reporting as offline.

August 1, 2016

Contents and overview

Note

Follow all of these steps, in order, until you reach a resolution.

1. Follow these steps.

2. Perform troubleshooting steps in order.

[Page 3](#) Before you begin

[Page 4](#) Start troubleshooting

[Page 5](#) LDAP configuration

[Page 6](#) Access zone configuration

[Page 8](#) Verify required user attributes

[Page 10](#) NTLM password hash

[Page 11](#) NT password attribute

[Page 12](#) Test authentication

[Page 16](#) LDAP is offline

[Page 18](#) Verify LDAP configuration

[Page 19](#) Test LDAP ports

[Page 22](#) Verify secure LDAP configuration - StartTLS

[Page 23](#) Verify secure LDAP configuration - SSL

[Page 29](#) Test LDAP

3. Appendixes

[Appendix A](#) If you need further assistance

[Appendix B](#) How to use this flowchart

[Appendix C](#) Example output `isi auth ldap view <provider>`

[Appendix D](#) Example output `isi auth users view <user> --provider=ldap`

[Appendix E](#) Example LDIF output

Before you begin



CAUTION!

If the node, subnet, or pool that you are working on goes down during the course of troubleshooting and you do not have any other way to connect to the cluster, you could experience data unavailability.

Therefore, make sure that you have more than one way to connect to the cluster before you start this troubleshooting process. The best method is to have a serial cable available. This way, if you are unable to connect through the network, you will still be able to connect to the cluster physically.

For specific requirements and instructions for making a physical connection to the cluster, see [article 16744](#) on the EMC Online Support site.

Before you begin troubleshooting, confirm that you can either connect through another subnet or pool, or that you have physical access to the cluster.

Configure logging through SSH

We recommend that you configure screen logging to log all session input and output during your troubleshooting session. This log file can be shared with EMC Isilon Technical Support if you require assistance at any point during troubleshooting.

Note: The screen session capability does not work in OneFS 7.1.0.6 and 7.1.1.2. If you are running either of these versions, configure logging by using your local SSH client's logging feature.

1. Open an SSH connection to the cluster and log in by using the root account.

Note: If the cluster is in compliance mode, use the compadmin account to log in. All compadmin commands must be preceded by the `sudo` prefix.

2. Change the directory to `/ifs/data/Isilon_Support` by running the following command:

```
cd /ifs/data/Isilon_Support
```

3. Run the following command to capture all input and output from the session:

```
screen -L
```

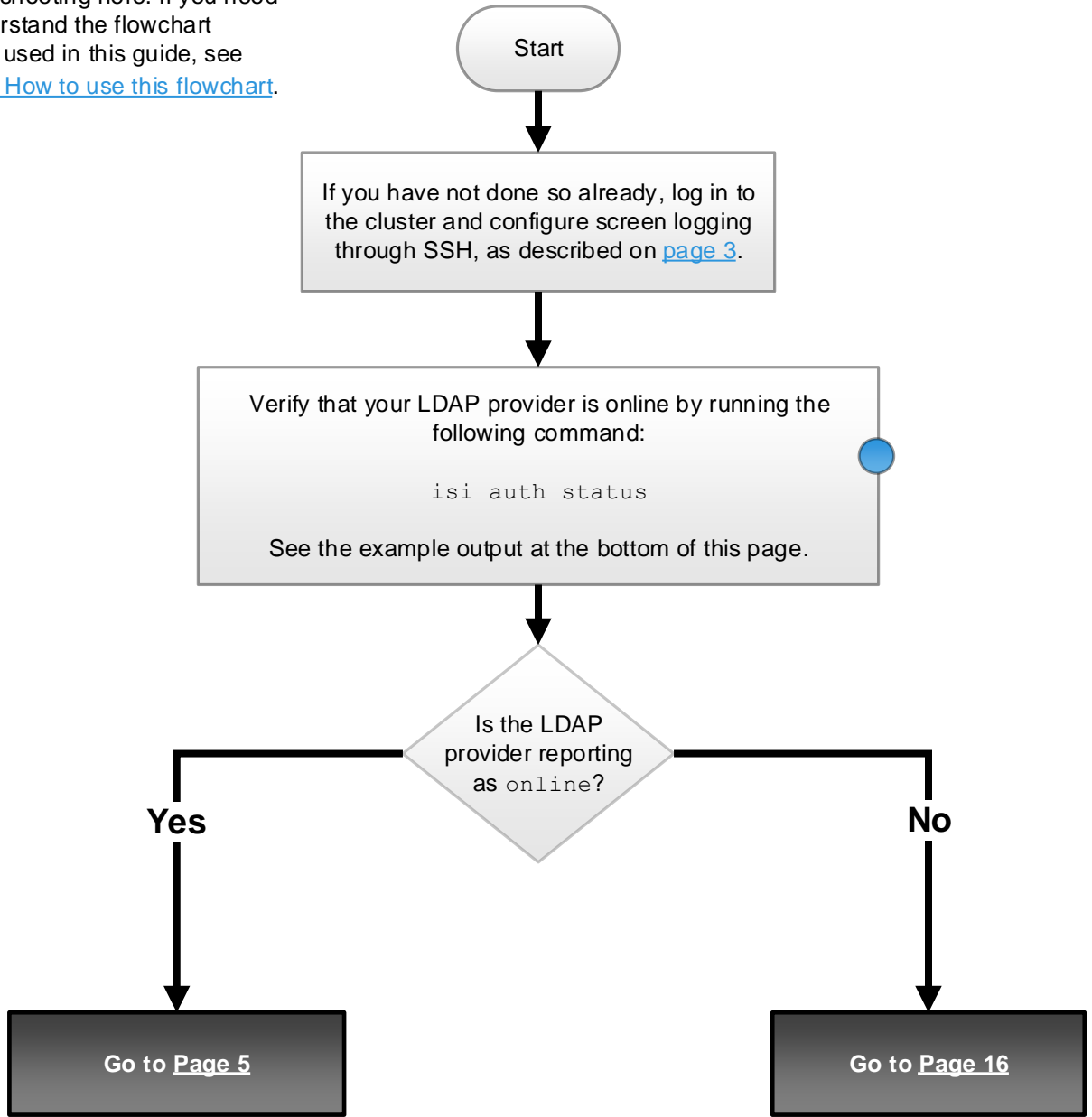
This will create a file named `screenlog.0` that will be appended to during your session.

4. Perform troubleshooting.

Start troubleshooting

Introduction

Start troubleshooting here. If you need help to understand the flowchart conventions used in this guide, see [Appendix B: How to use this flowchart](#).



Example `isi auth status` output

ID	Active Server	Status
lsa-activedirectory-provider:AD.JBLOGS.COM	ad-dc.jblogs.com	online
lsa-local-provider:System	-	active
lsa-file-provider:System	-	active
lsa-ldap-provider:ldap_example	ldap://192.168.100.50	online
lsa-nis-provider:nis_example	192.168.100.50	online

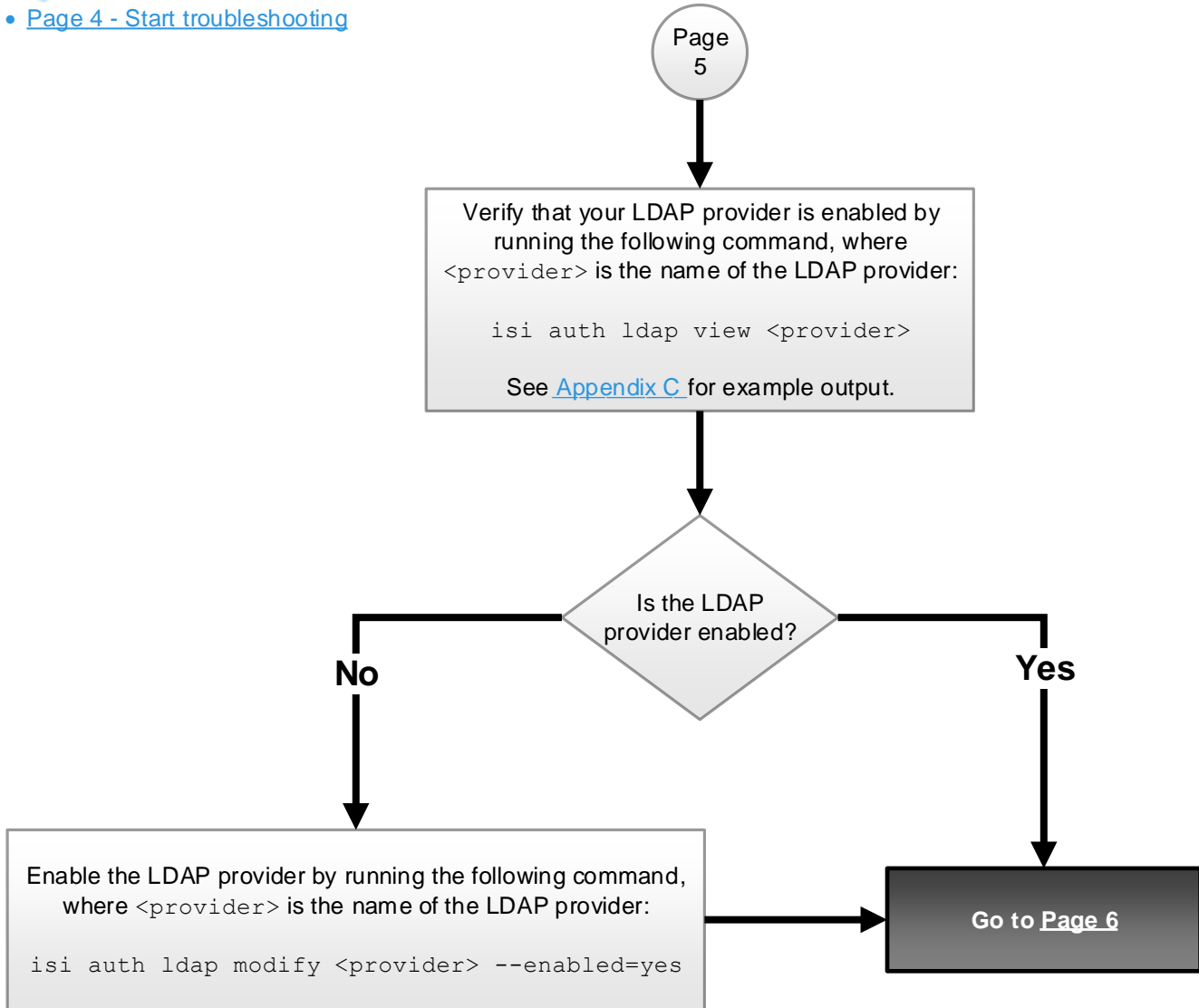


LDAP configuration



You could have arrived here from:

- [Page 4 - Start troubleshooting](#)



Access zone configuration



You could have arrived here from:

- [Page 5 - LDAP configuration](#)

Page
6

View the access zone configuration by running the following command:

```
isi zone zones list --verbose
```

See example output at the bottom of this page.

Go to [Page 7](#)

Example `isi zone zones list --verbose` output

```
Cluster1# isi zone zones list --verbose
Name: System
Cache Size: 4.77M
Map Untrusted:
SMB Shares: -
Auth Providers: lsa-local-provider:System, lsa-file-provider:System, lsa-ldap-provider:ldap_example, lsa-nis-
provider:nis_example
Local Provider: Yes
NetBIOS Name:
All SMB Shares: Yes
All Auth Providers: No
User Mapping Rules: -
Home Directory Umask: 0077
Skeleton Directory: /usr/share/skel
Audit Success: close, create, delete, get_security, logoff, logon, read, rename, set_security, tree_connect, write
Audit Failure: close, create, delete, get_security, logoff, logon, read, rename, set_security, tree_connect, write
Zone ID: 1
-----
Name: Zone2
Cache Size: 4.77M
Map Untrusted:
SMB Shares: Zone2 Files:Files, Home:Home
Auth Providers: lsa-local-provider:System, lsa-file-provider:System, lsa-ldap-provider:ldap_example, lsa-nis-
provider:nis_example
Local Provider: Yes
NetBIOS Name:
All SMB Shares: No
All Auth Providers: No
User Mapping Rules: -
Home Directory Umask: 0077
Skeleton Directory: /usr/share/skel
Audit Success: close, create, delete, get_security, logoff, logon, read, rename, set_security, tree_connect, write
Audit Failure: close, create, delete, get_security, logoff, logon, read, rename, set_security, tree_connect, write
Zone ID: 2
```

Access zone configuration (2)

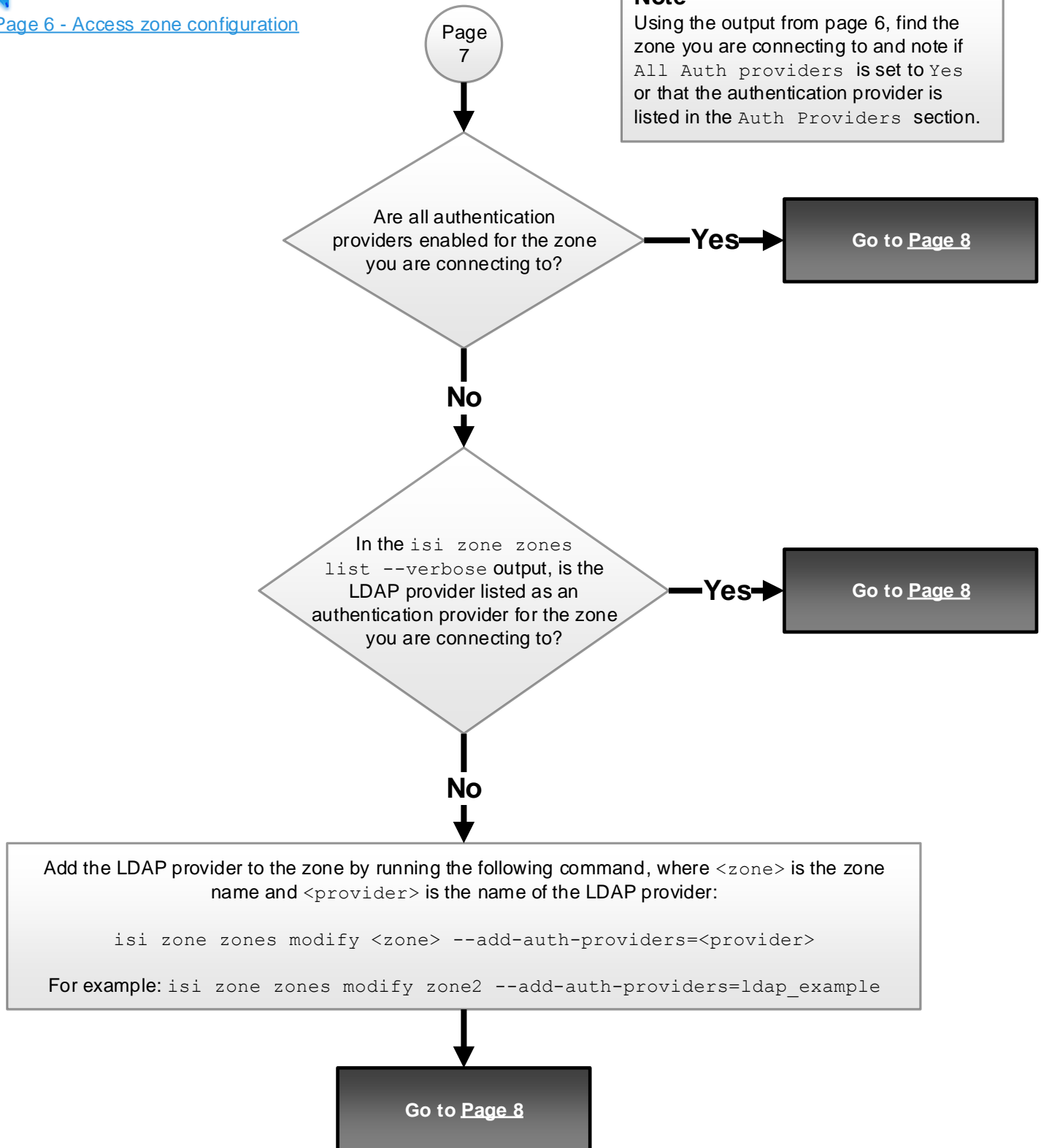


You could have arrived here from:

- [Page 6 - Access zone configuration](#)

Note

Using the output from page 6, find the zone you are connecting to and note if `All Auth providers` is set to `Yes` or that the authentication provider is listed in the `Auth Providers` section.



Verify required user attributes



You could have arrived here from:

- [Page 7 - Access zone configuration \(2\)](#)

Note

Certain LDAP user attributes need to be configured properly in order for user or group authentication to work.

Page
8

Check whether the required user attributes are configured properly, run the following command, where `<user>` is the user name of the user who cannot authenticate:

```
isi auth users view <user> --provider=ldap
```

See [Appendix D](#) for example output and a list of required user attributes.

To ensure user or group authentication, certain user attributes need to be configured. Using the example output in [Appendix D](#), verify whether or not the required user attributes are configured on your LDAP provider.

Are the required
user attributes
configured properly?

No

Go to [Page 14](#)

Yes

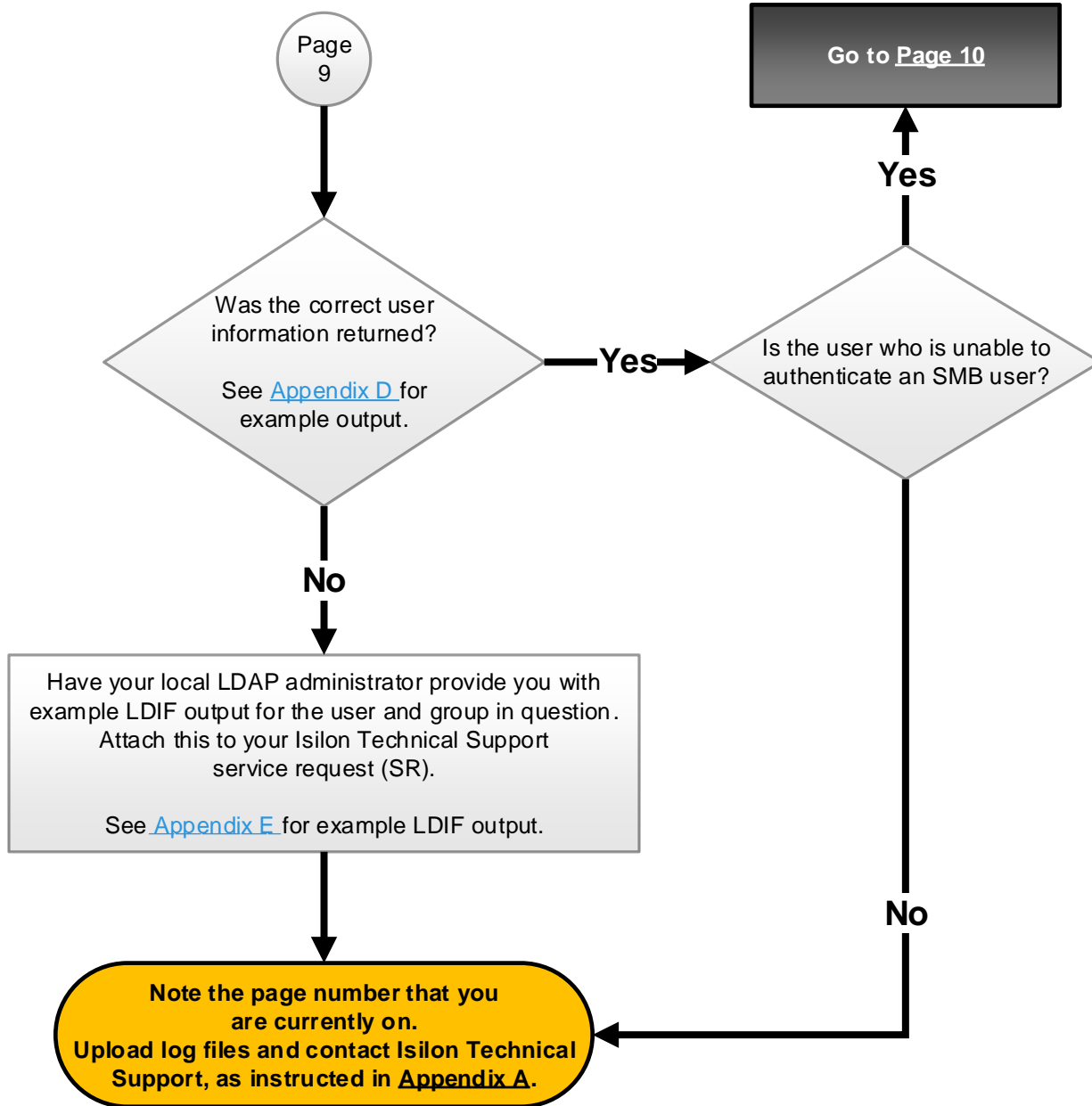
Go to [Page 9](#)

Verify required user attributes (2)



You could have arrived here from:

- [Page 8 - Verify required user attributes](#)

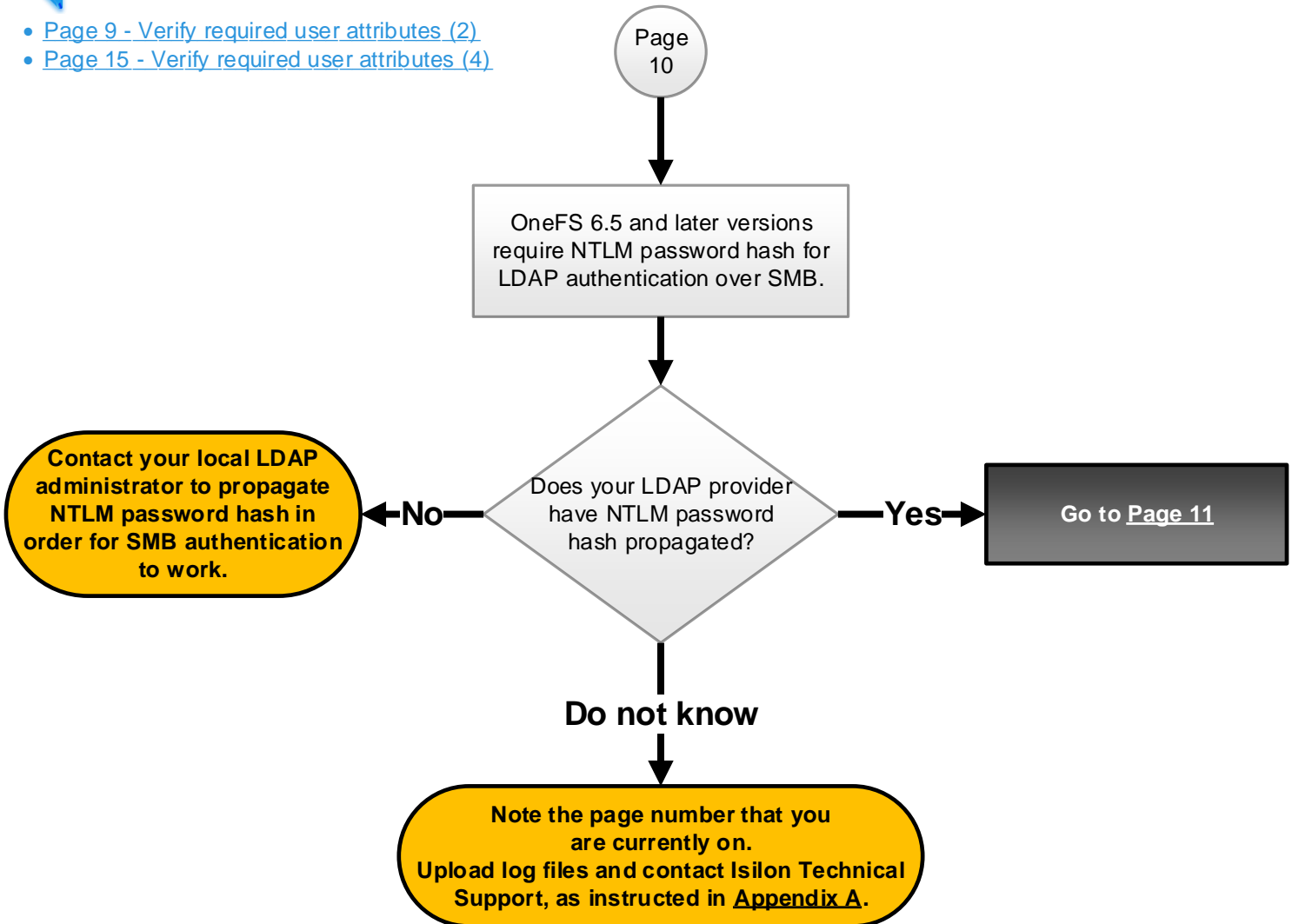


NTLM password hash



You could have arrived here from:

- [Page 9 - Verify required user attributes \(2\)](#)
- [Page 15 - Verify required user attributes \(4\)](#)



NT password attribute



You could have arrived here from:

- [Page 10 - NTLM password hash](#)

Page
11

The NT Password attribute needs to be configured for SMB authentication. View the Nt Password Attribute for your LDAP provider by running the following command, where <provider> is the name of the LDAP provider:

```
isi auth ldap view <provider>
```

See [Appendix C](#) for example output.

Does the Nt Password Attribute match the attribute configured in your LDAP schema?

Yes

Go to [Page 12](#)

No

Edit the Nt Password Attribute, run the following command, where <provider> is the name of the LDAP provider, and <attribute> is the NT password attribute that is configured in your LDAP schema:

```
isi auth ldap modify <provider> --nt-password-attribute <attribute>
```

Note: The attribute is case sensitive.

Go to [Page 12](#)

Test authentication



You could have arrived here from:

- [Page 11 - NT password attribute](#)

Page
12

Test authentication by performing the following three steps on the affected node.
If each step successfully completes, authentication is working.

1. Attempt to map a user token by running the following command, where `<user>` is the user name of the user:

```
isi auth mapping token --user="<user>"
```

See example output at the bottom of this page. An error message will be received if this step fails.

Go to [Page 13](#)

Example `isi auth mapping token --user="<user>"` output

```
Cluster-1# isi auth mapping token --user="testuser1"
User
  Name: TEST\testuser1
  UID: 11838
  SID: S-1-5-21-1606848-115176313-8392115-156283
  On Disk: 11838
  ZID: 1
  Zone: System
Privileges: -
Primary Group
  Name: TEST\domain users
  GID: 10006
  SID: S-1-5-21-1606848-115176313-8392115-513
  On Disk: 10006
Supplemental Identities
  Name: TEST\security_group_1
  GID: 11930
  SID: S-1-5-21-1606988-115176313-8395115-444484

  Name: TEST\building_access
  GID: 13320
  SID: S-1-5-21-1680848-115176313-8392115-921913
```

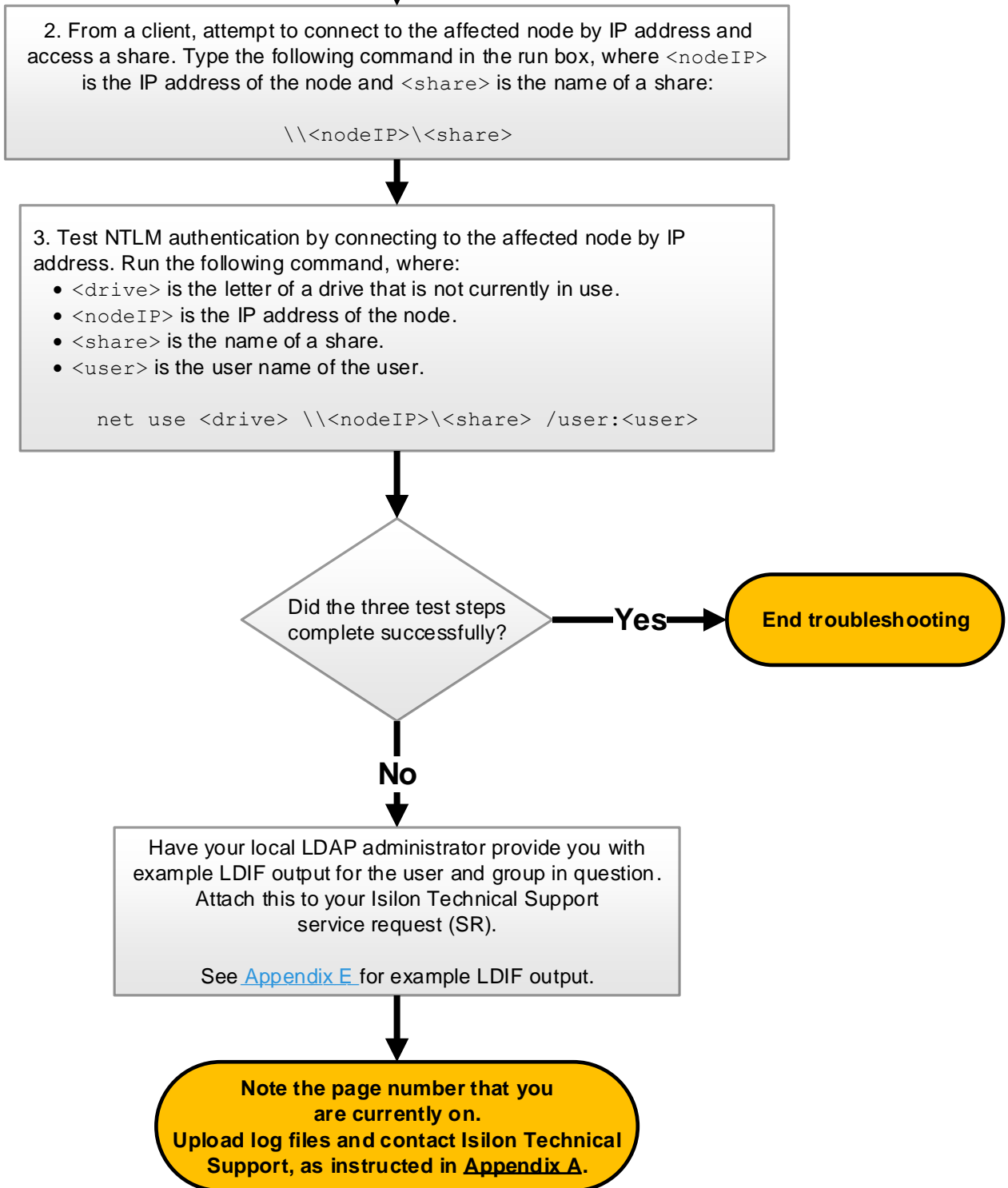
Test authentication (2)



You could have arrived here from:

- [Page 12 - Test authentication](#)

Page
13



Verify required user attributes (3)



You could have arrived here from:

- [Page 8 - Verify required user attributes](#)

Page
14

Configure the required user attributes properly.
For instructions, see the "Modify an LDAP provider" section of the [OneFS Administration Guide](#) for your version of OneFS. For a list of attributes to modify, see the "isi auth ldap modify" section of the same guide.

Verify that the required user attributes are configured properly by running the following command, where <user> is the user name:

```
isi auth users view <user> --provider=ldap
```

See [Appendix D](#) for example output and a list of required user attributes.

Are the required
user attributes
configured properly?

Yes

Was the correct user
information returned?

See [Appendix D](#) for
example output.

Yes

Go to [Page 15](#)

No

Note the page number that you
are currently on.
Upload log files and contact Isilon Technical
Support, as instructed in [Appendix A](#).

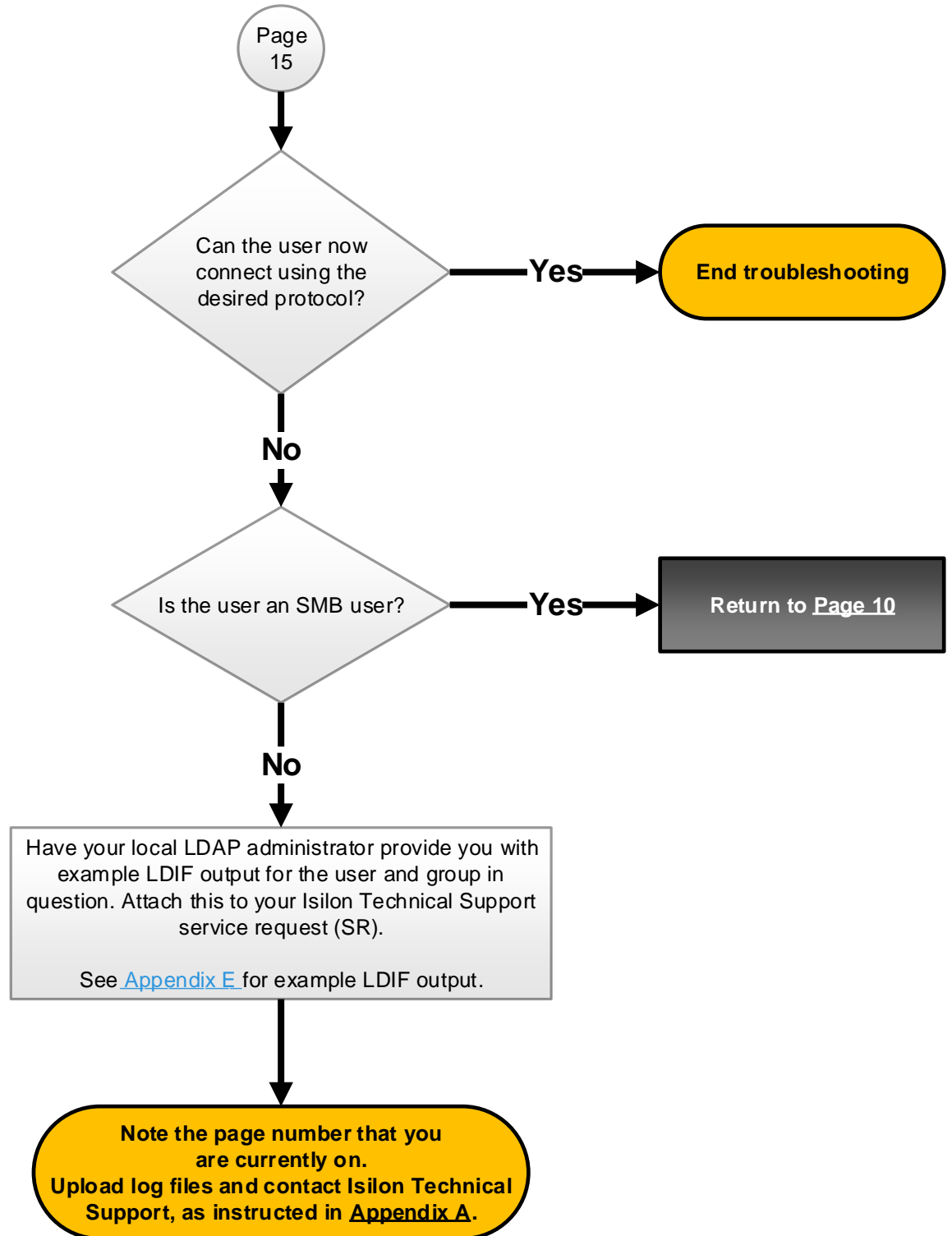
No

Verify required user attributes (4)



You could have arrived here from:

- [Page 14 - Verify required user attributes \(3\)](#)



LDAP is offline



You could have arrived here from:

- [Page 4 - Start troubleshooting](#)

Page
16

Note

Certain LDAP provider attributes need to be configured properly or they can trigger an offline state.

Check whether the required provider attributes are configured properly, run the following command, where <provider> is the provider name:

```
isi auth ldap view <provider>
```

See [Appendix C](#) for example output and a list of required provider attributes.

Certain criteria can trigger an offline state. Using the example output in [Appendix C](#), verify whether or not the required provider attributes are properly configured on your LDAP provider.

Are the provider attributes configured properly?

No

Go to [Page 17](#)

Yes

Is a secure connection to the LDAP server required?

Yes

Go to [Page 21](#)

No

Go to [Page 18](#)

Verify required user attributes (5)



You could have arrived here from:

- [Page 16 - LDAP is offline](#)

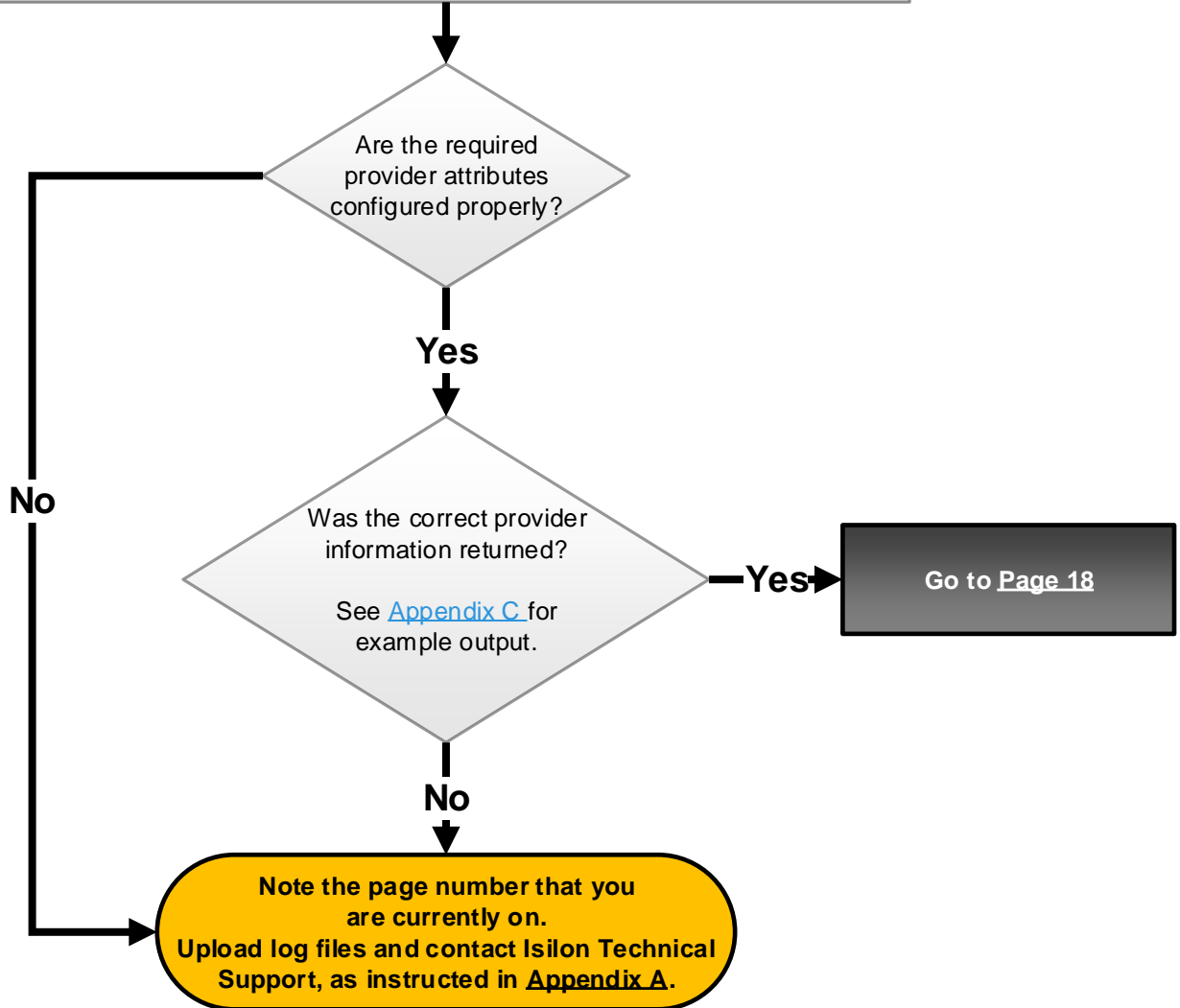
Page
17

Configure the required provider attributes properly.
For instructions, see the "Modify an LDAP provider" section of the [OneFS Administration Guide](#) for your version of OneFS. For a list of attributes to modify, see the "isi auth ldap modify" section of the same guide.

Verify that the required provider attributes are configured properly by running the following command, where <provider> is the provider name:

```
isi auth ldap view <provider>
```

See [Appendix C](#) for example output and a list of required provider attributes.



Verify LDAP configuration



You could have arrived here from:

- [Page 16 - LDAP is offline](#)
- [Page 17 - Verify required user attributes \(5\)](#)

Page
18

From the `isi auth ldap view <provider>` output in [Appendix C](#), verify that `Server Uri` (item c) begins with `ldap:` and not `ldaps:`

To edit the `Server Uri` attribute, run the following command where `<provider>` is the name of the provider, and `<ip or fqdn>` is either the IP address or the FQDN of the server:

```
isi auth ldap modify --provider-name=<provider> --server-uri=ldap://<ip or fqdn>
```

From the `isi auth ldap view <provider>` output in [Appendix C](#), verify that `Require secure connection` (item g) is set to `No`.

To disable the `Require secure connection` attribute, run the following command, where `<provider>` is the name of the provider:

```
isi auth ldap modify --provider-name=<provider> --require-secure-connection=no
```

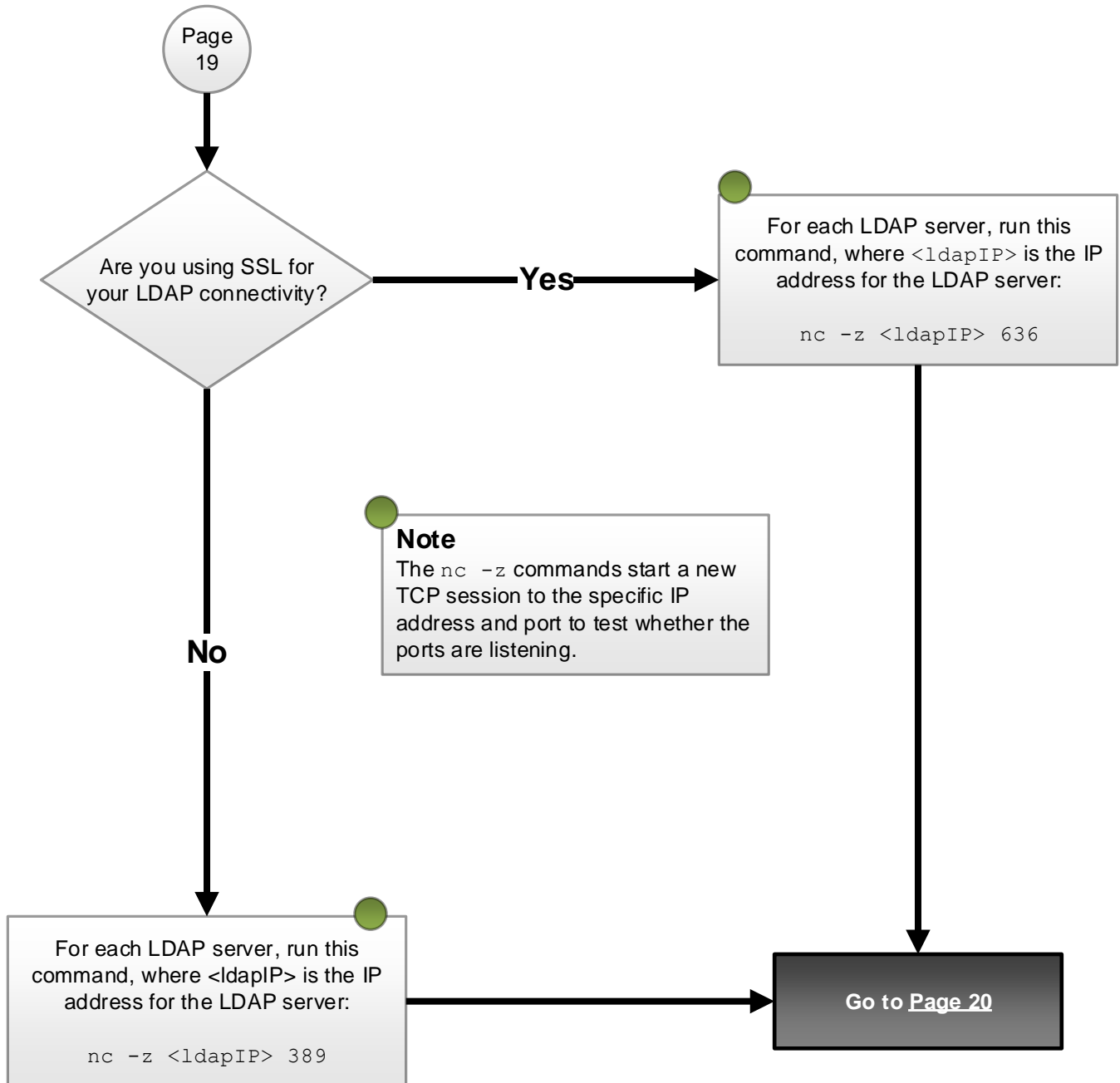
Go to [Page 19](#)

Test LDAP ports



You could have arrived here from:

- [Page 18 - Verify LDAP configuration](#)
- [Page 20 - Test LDAP ports \(2\)](#)
- [Page 25 - Verify secure LDAP configuration \(3\)](#)
- [Page 26 - Verify secure LDAP configuration \(4\)](#)

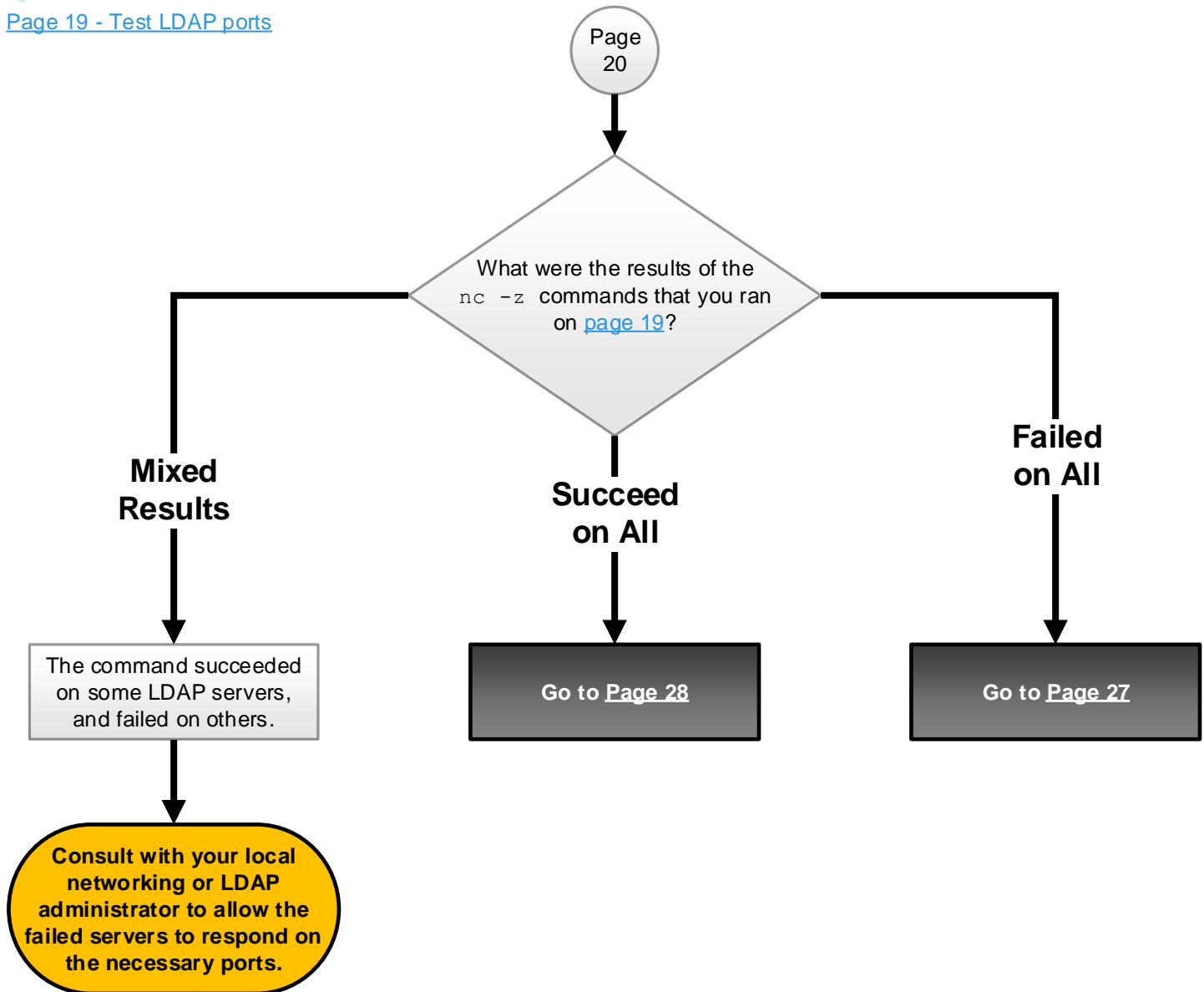


Test LDAP ports (2)



You could have arrived here from:

- [Page 19 - Test LDAP ports](#)

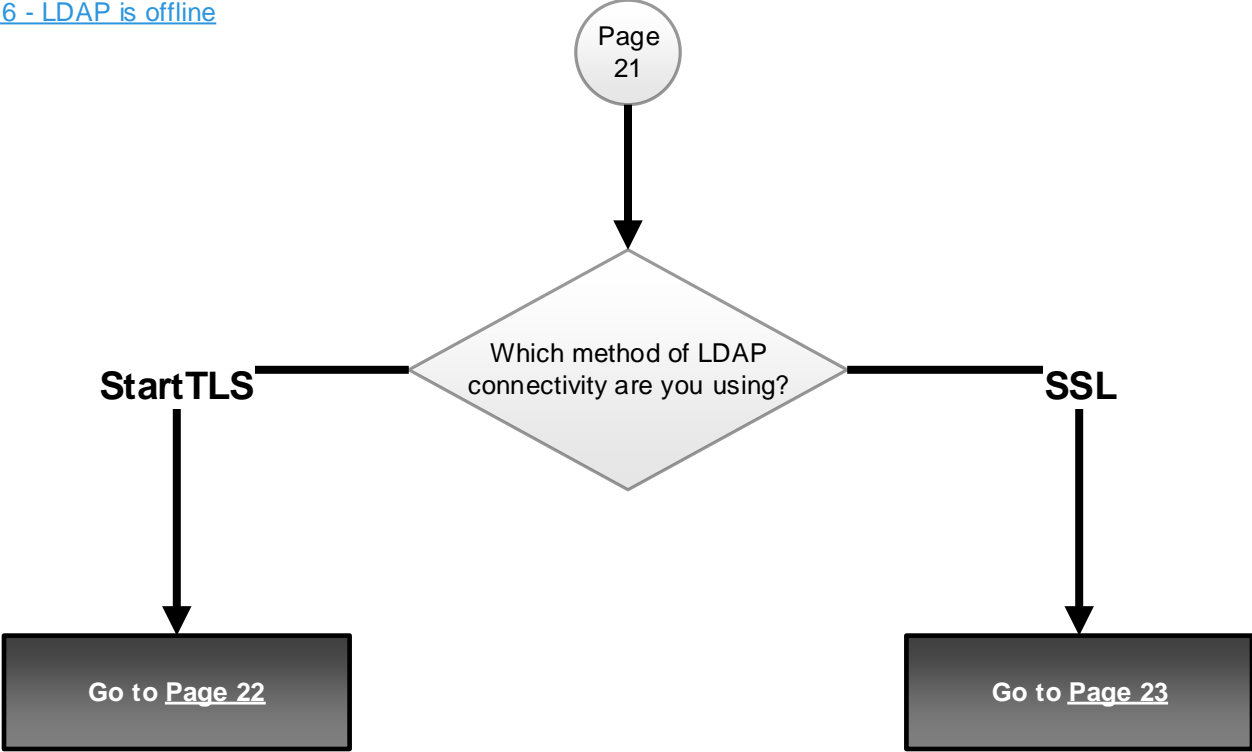


Test LDAP ports (3)



You could have arrived here from:

- [Page 16 - LDAP is offline](#)



Verify secure LDAP configuration

StartTLS



You could have arrived here from:

- [Page 21 - Test LDAP ports \(3\)](#)

Page
22

StartTLS

From the `isi auth ldap view <provider>` output in [Appendix C](#), verify that `Server Uris` (item c) begins with `ldap:` and not `ldaps:`

To edit the `Server Uri` attribute, run the following command, where `<provider>` is the name of the provider, and `<ip or fqdn>` is either the IP address or the FQDN of the server:

```
isi auth ldap modify --provider-name=<provider> --server-uris=ldap://<ip or fqdn>
```

Go to [Page 24](#)

Verify secure LDAP configuration

SSL



You could have arrived here from:

- [Page 21 - Test LDAP ports \(3\)](#)

Page
23

SSL

From the `isi auth ldap view <provider>` output in [Appendix C](#), verify that `Server Uri` (item c) begins with `ldaps:` and not `ldap:`

To edit the `Server Uri` attribute, run the following command, where `<provider>` is the name of the provider, and `<ip or fqdn>` is either the IP address or the FQDN of the server:

```
isi auth ldap modify --provider-name=<provider> --server-uris=ldaps://<ip or fqdn>
```

Go to [Page 24](#)

Verify secure LDAP configuration (2)



You could have arrived here from:

- [Page 22 - Verify secure LDAP configuration, StartTLS](#)
- [Page 23 - Verify secure LDAP configuration, SSL](#)

Page
24

From the `isi auth ldap` view `<provider>` output in [Appendix C](#), verify that `Require secure connection` (item "g") is set to `No`.

To disable the `Require secure connection` attribute, run the following command, where `<provider>` is the name of the provider:

```
isi auth ldap modify --provider-name=<provider> --require-secure-connection=no
```

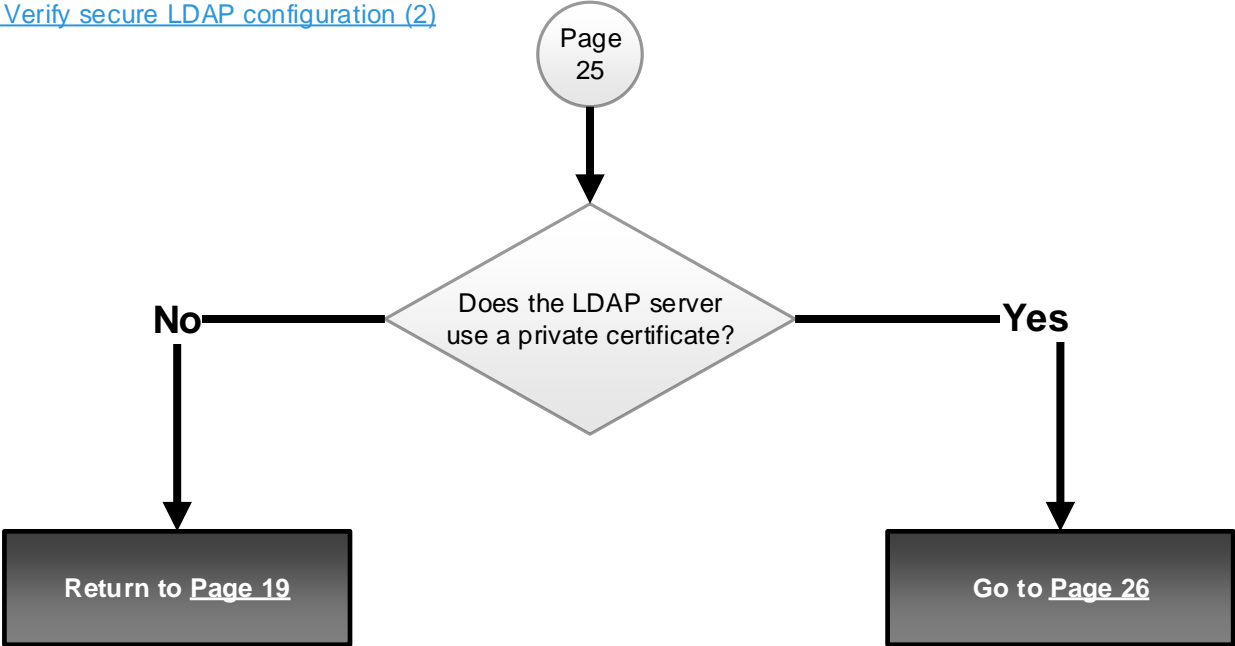
Go to [Page 25](#)

Verify secure LDAP configuration (3)



You could have arrived here from:

- [Page 24 - Verify secure LDAP configuration \(2\)](#)



Verify secure LDAP configuration (4)



You could have arrived here from:

- [Page 25 - Verify secure LDAP configuration \(3\)](#)

Page
26

Run the following command to configure the LDAP provider to ignore TLS errors, where `<provider>` is the name of the provider:

```
isi auth ldap modify <provider> --ignore-tls-errors=yes
```

See [Appendix C](#), item "e" for example output.

To specify the Certificate Authority File, run the following command, where `<provider>` is the name of the provider and `<location>` is the file path of the certificate authority file in `/ifs`:

```
isi auth ldap modify <provider> --certificate-authority-file=<location>
```

See [Appendix C](#) for example output.

Return to [Page 19](#)

Test LDAP ports (4)



You could have arrived here from:

- [Page 20 - Test LDAP ports \(2\)](#)

Page
27

Note

A non standard port is any port other than 389 or 636.

Failed on All

Is your LDAP environment configured to use a non standard port?

Yes

No

Run the following command on all LDAP servers that are configured for a non standard port, where <ldapIP> is the IP address of the LDAP server and <port> is the non standard port that you have configured:

```
nc -z <ldapIP> <port>
```

Did the above command succeed on all servers?

No

Note the page number that you are currently on.
Upload log files and contact Isilon Technical Support, as instructed in [Appendix A](#).

Yes

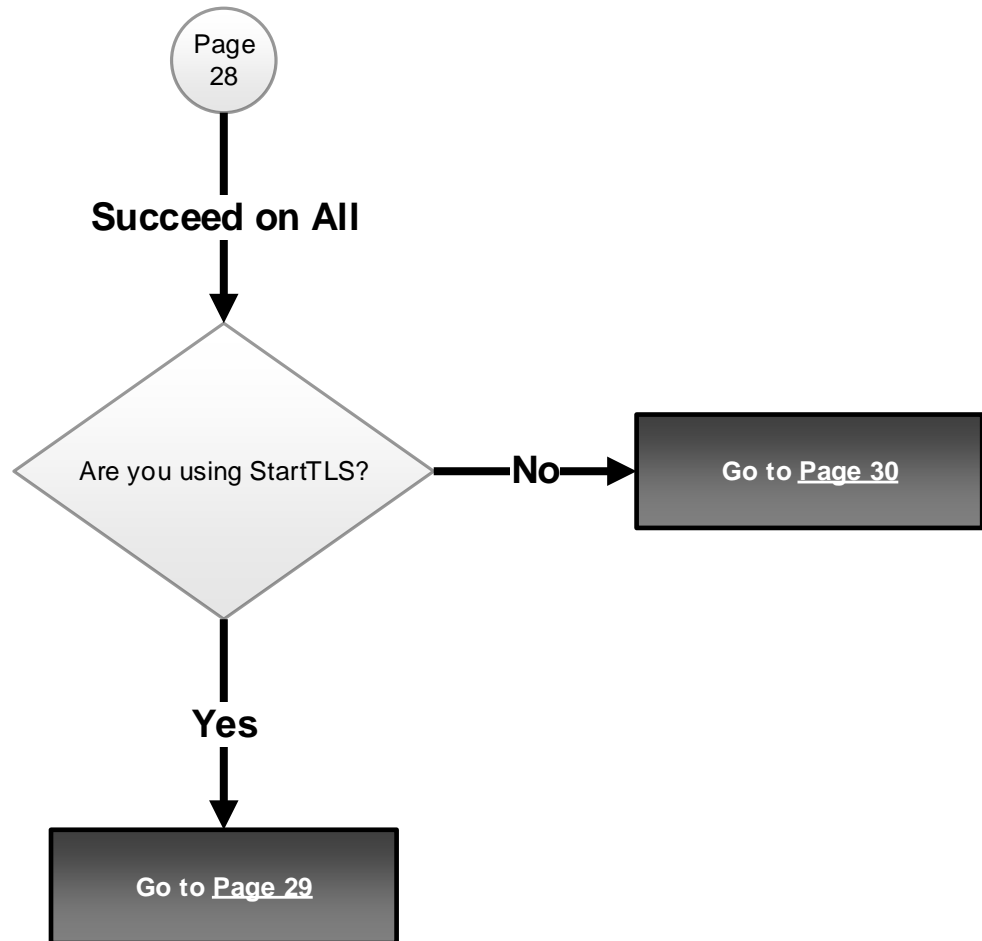
Go to [Page 28](#)

Test LDAP ports (5)



You could have arrived here from:

- [Page 20 - Test LDAP ports \(2\)](#)
- [Page 27 - Test LDAP ports \(4\)](#)



Test LDAP



You could have arrived here from:

- [Page 28 - Test LDAP ports \(5\)](#)

Page
29

Test LDAP directly by running the following command, where:

- <server-uri> is the server URI.
- <base-dn> is the base DN.
- <bind-dn> is the bind DN.

Please note that the below command is a single command, wrapped onto two lines.

```
ldapsearch -x -W -z 10 -H <server-uri> -b '<base-dn>' -D "<bind-dn>"  
'(|(objectClass=posixAccount)(objectClass=posixGroup)(objectClass=nisNetgroup))'
```

Add the certificate authority certificate, append the previous command with the following, where <location> indicates the file path to the certificate authority file:

```
LDAPTLS_CACERT="<location>"
```

The resulting command should look like:

```
ldapsearch -x -W -z 10 -H <server-uri> -b '<base-dn>' -D "<bind-dn>" LDAPTLS_CACERT="<location>"  
'(|(objectClass=posixAccount)(objectClass=posixGroup)(objectClass=nisNetgroup))'
```

Go to [Page 31](#)

Test LDAP (2)



You could have arrived here from:

- [Page 28 - Test LDAP ports \(5\)](#)

Page
30

Test LDAP directly by running the following command, where:

- <server-uri> is the server URI.
- <base-dn> is the base DN.
- <bind-dn> is the bind DN.

Please note that the below command is a single command, wrapped onto two lines.

```
ldapsearch -x -W -z 10 -H <server-uri> -b '<base-dn>' -D "<bind-dn>"  
'(|(objectClass=posixAccount)(objectClass=posixGroup)(objectClass=nisNetgroup))'
```

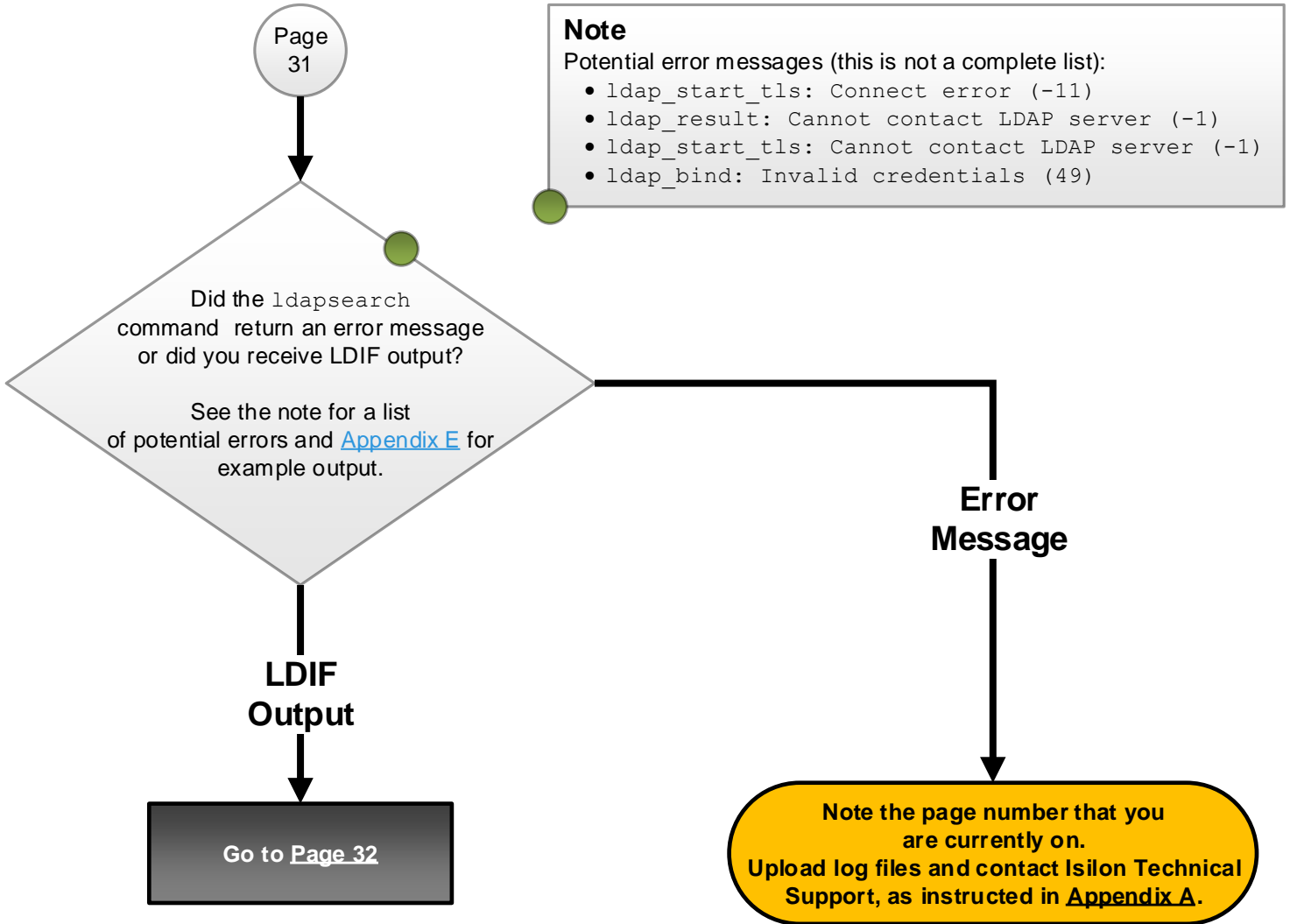
Go to [Page 31](#)

Test LDAP (3)



You could have arrived here from:

- [Page 29 - Test LDAP](#)
- [Page 30 - Test LDAP \(2\)](#)

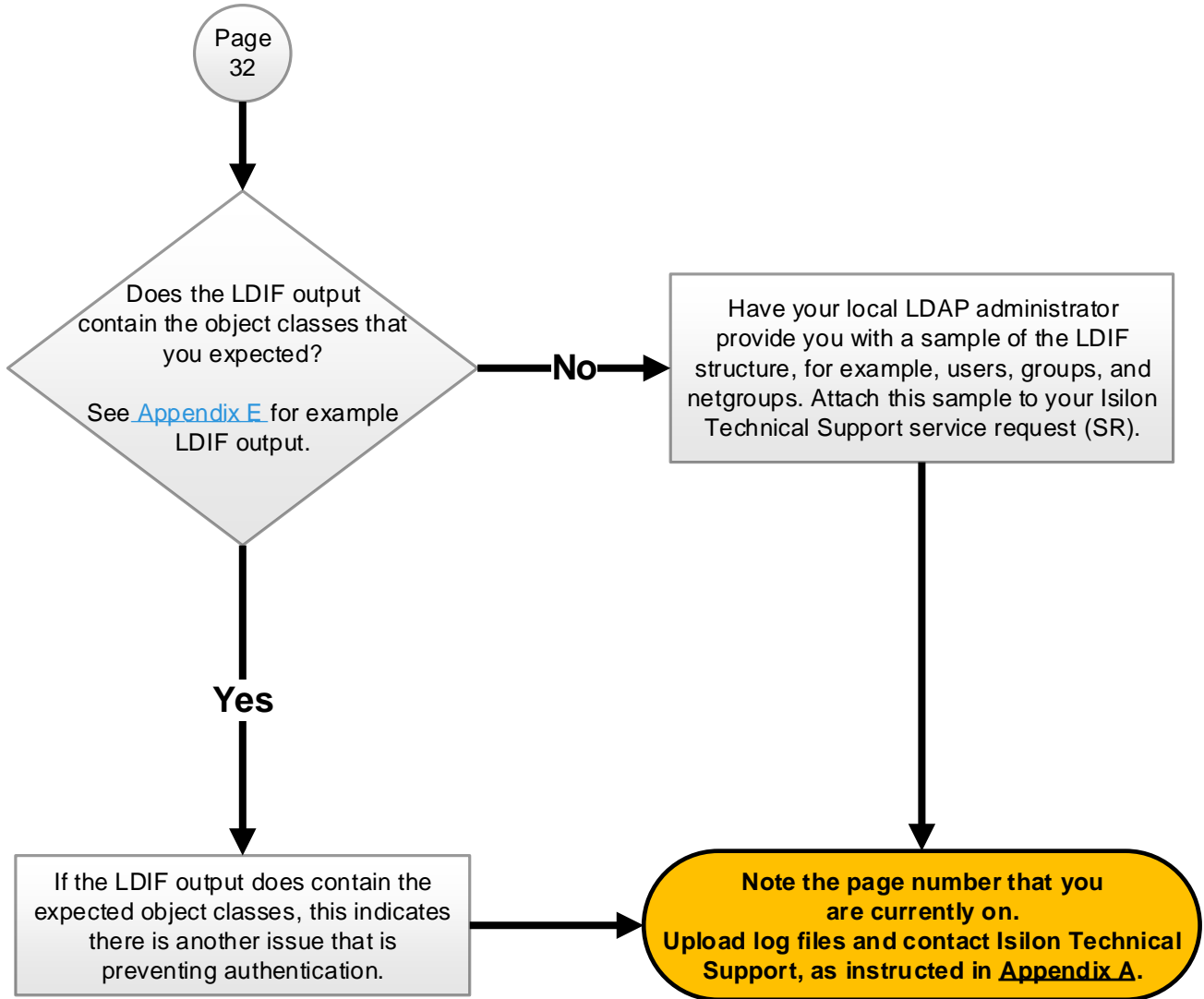


Test LDAP (4)



You could have arrived here from:

- [Page 31 - Test LDAP \(3\)](#)



Appendix A: If you need further assistance

Contact EMC Isilon Technical Support

If you need to contact [Isilon Technical Support](#) during troubleshooting, reference the page or step that you need help with. This information and the log file will help Isilon Technical Support staff resolve your case more quickly.

Upload node log files and the screen log file to EMC Isilon Technical Support

1. When troubleshooting is complete, type `exit` to end your screen session.
2. Gather and upload the node log set and include the SSH screen log file by using the command appropriate for your method of uploading files. If you are not sure which method to use, use FTP.

ESRS:

```
isi_gather_info --esrs --local-only -f /ifs/data/Isilon_Support/screenlog.0
```

FTP:

```
isi_gather_info --ftp --local-only -f /ifs/data/Isilon_Support/screenlog.0
```

HTTP:

```
isi_gather_info --http --local-only -f /ifs/data/Isilon_Support/screenlog.0
```

SMTP:

```
isi_gather_info --email --local-only -f /ifs/data/Isilon_Support/screenlog.0
```

SupportIQ:

Copy and paste the following command.

Note: When you copy and paste the command into the command-line interface, it will appear on multiple lines (exactly as it appears on the page), but when you press **Enter**, the command will run as it should.

```
isi_gather_info --local-only -f /ifs/data/Isilon_Support/screenlog.0 --noupload \  
--symlink /var/crash/SupportIQ/upload/ftp
```

3. If you receive a message that the upload was unsuccessful, refer to [article 16759](#) on the EMC Online Support site for directions on how to upload files over FTP.

Appendix B: How to use this flowchart

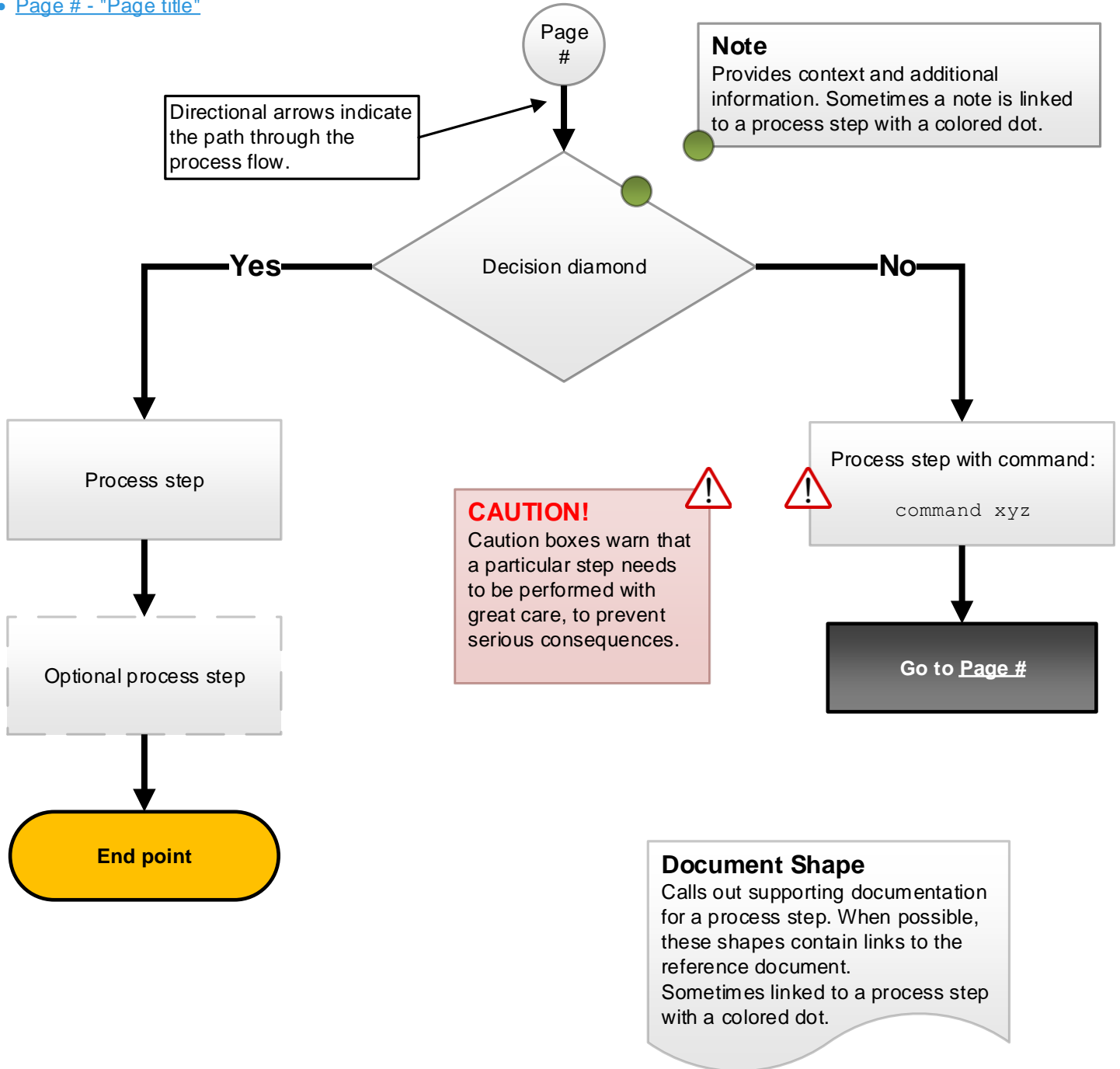
Introduction

Describes what the section helps you to accomplish.



You could have arrived here from:

- [Page # - "Page title"](#)



Appendix C: Example output

Example `isi auth ldap view <provider>` output



You could have arrived here from:

- [Page 5 - LDAP configuration](#)
- [Page 11 - NT password attribute](#)
- [Page 16 - LDAP is offline](#)
- [Page 17 - Verify required user attributes \(5\)](#)
- [Page 18 - Verify LDAP configuration](#)
- [Page 22 - Verify secure LDAP configuration, StartTLS](#)
- [Page 23 - Verify secure LDAP configuration, SSL](#)
- [Page 24 - Verify secure LDAP configuration \(2\)](#)
- [Page 26 - Verify secure LDAP configuration \(4\)](#)

Required provider attributes

There are certain criteria that can trigger an offline state. To ensure LDAP is online, be sure that the following settings are configured accurately:

- a. Name
- b. Base DN
- c. Server Uri
- d. Bind DN
- e. Ignore TLS errors
- f. Bind password (this setting is not displayed in the CLI output, instead it is configured in the OneFS web administration interface.)
- g. Require Secure Connection
- e. Ignore TLS Errors

Required user attributes

To ensure user or group authentication, be sure that the following attributes are configured properly:

1. gidNumber
2. homeDirectory
3. uid
4. loginShell
5. uidNumber
6. Nt Password Attribute (this attribute is required only for SMB authentication)

```
Cluster1# isi auth ldap view ldap_example
a Name: ldap_example
b Base DN: cn=users,dc=10-9,dc=cslab,dc=igs,dc=corp
c Server Uri: ldap://10.11.12.70
Status: online
Alternate Security Identities Attribute:
Authentication: Yes
Balance Servers: Yes
d Bind DN: uid=diradmin,cn=users,dc=10-9,dc=cslab,dc=igs,dc=corp
Bind Timeout: 10
Cache Entry Expiry: 15m
Certificate Authority File:
Check Online Interval: 3m
CN Attribute: cn
Create Home Directory: No
Crypt Password Attribute:
Email Attribute: mail
Enabled: Yes
Enumerate Groups: Yes
Enumerate Users: Yes
Findable Groups: -
Findable Users: -
GECOS Attribute: gecoc
1 GID Attribute: gidNumber
Group Base DN:
Group Domain: LDAP_GROUPS
Group Filter: (objectClass=posixGroup)
Group Members Attribute: memberUid
Group Search Scope: default
Home Directory Template:
2 Homedir Attribute: homeDirectory
e Ignore TLS Errors: No
Listable Groups: -
Listable Users: -
Login Shell:
Member Of Attribute:
3 Name Attribute: uid
Netgroup Base DN:
Netgroup Filter: (objectClass=nisNetgroup)
Netgroup Members Attribute: memberNisNetgroup
Netgroup Search Scope: default
Netgroup Triple Attribute: nisNetgroupTriple
Normalize Groups: No
Normalize Users: No
6 Nt Password Attribute: ntPassword
Ntlm Support: all
Provider Domain:
g Require Secure Connection: No
Restrict Findable: No
Restrict Listable: No
Search Scope: subtree
Search Timeout: 100
4 Shell Attribute: loginShell
5 UID Attribute: uidNumber
Unfindable Groups: -
Unfindable Users: -
Unique Group Members Attribute:
Unlistable Groups: -
Unlistable Users: -
User Base DN:
User Domain: LDAP_USERS
User Filter: (objectClass=posixAccount)
User Search Scope: default
```

Appendix D: Example output

Example `isi auth users view <user> --provider=ldap` output



You could have arrived here from:

- [Page 8 - Verify required user attributes](#)
- [Page 9 - Verify required user attributes \(2\)](#)
- [Page 14 - Verify required user attributes \(3\)](#)

Required user attributes

To ensure user or group authentication, be sure that the following attributes are configured properly:

1. Name
2. UID
3. GID
4. Home Directory
5. Shell

```
Cluster-1# isi auth users view jblogs --provider=ldap
1 Name: jblogs
  DN: CN=jblogs,CN=Users,DC=dur,DC=example,DC=com
  DNS Domain: -
  Domain: LDAP_USERS
  Provider: lsa-ldap-provider:ldap_example
  Sam Account Name: jblogs
2 UID: 1005
  SID: S-1-22-1-1005
  Enabled: Yes
  Expired: No
  Expiry: -
  Locked: No
  Email: -
  GECOS: -
  Generated GID: No
  Generated UID: No
  Generated UPN: -
  Primary Group
  ID:
3 GID:1800
  Name: isilon
4 Home Directory: /home/user home
  Max Password Age: Never
  Password Expired: No
  Password Expiry: -
  Password Last Set: -
  Password Expires: Yes
5 Shell: /bin/tcsh
```

Appendix E: Example output

Example LDIF output



You could have arrived here from:

- [Page 9 - Verify required user attributes \(2\)](#)
- [Page 13 - Test authentication \(2\)](#)
- [Page 15 - Verify required user attributes \(4\)](#)
- [Page 31 - Test LDAP \(3\)](#)
- [Page 32 - Test LDAP \(4\)](#)

Required user attributes

To ensure user or group authentication, be sure that the following attributes are configured properly:

1. `gidnumber`
2. `homedirectory`
3. `loginshell`
4. `uid`
5. `uidnumber`

```
# Entry 23: cn=Joe Blogs,ou=Users,dc=nismaster,dc=example,dc=com
dn: cn=Joe Blogs,ou=Users,dc=nismaster,dc=example,dc=com
cn: Joe Blogs
① gidnumber: 1800
givenname: Joe
② homedirectory: /home/users/jblogs
③ loginshell: /bin/tcsh
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: blogs
④ uid: jblogs
⑤ uidnumber: 1005
userpassword: {MD5}Ho0TCNi6UB8gG7/JGpXU7w==
```

Copyright © 2015 EMC Corporation. All rights reserved. Published in USA.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).