EMC ISILON CUSTOMER TROUBLESHOOTING GUIDE

TROUBLESHOOT YOUR LDAP AUTHENTICATION PROVIDER

OneFS 7.2 - 8.1.0

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.

January 5, 2018

Contents and overview

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

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
   ```

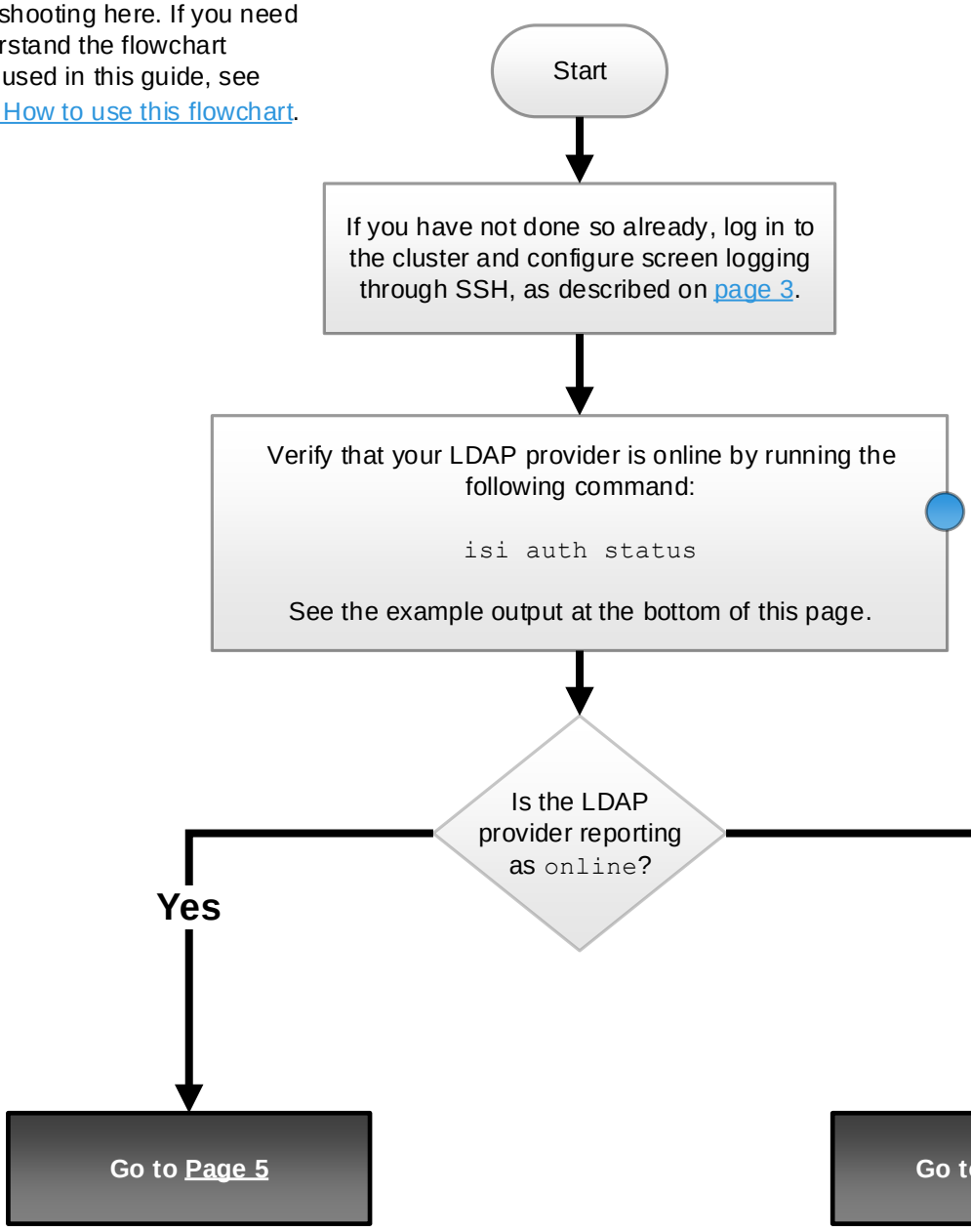
   This will create a file named screenlog.0 that will be appended to during your session.

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.



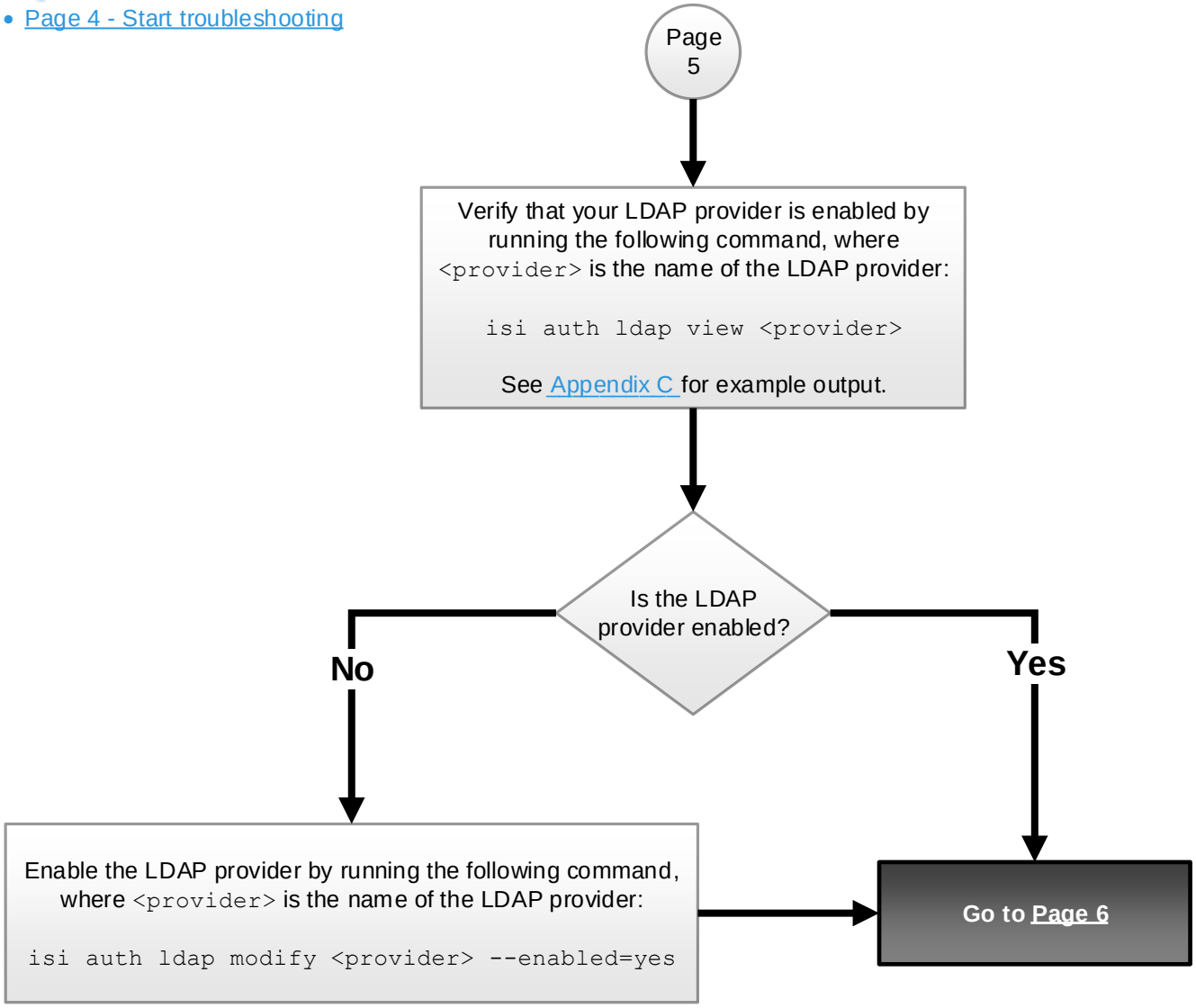
Example `isi auth status` output

```
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.

Page 7

Are all authentication providers enabled for the zone you are connecting to?

Yes → Go to Page 8

No

In the `isi zone zones list --verbose` output, is the LDAP provider listed as an authentication provider for the zone you are connecting to?

Yes → Go to Page 8

No

Add the LDAP provider to the zone by running the following command, where `<zone>` is the zone name and `<provider>` is the name of the LDAP provider:

```
isi zone zones modify <zone> --add-auth-providers=<provider-type>:<provider-name>
```

For example: `isi zone zones modify zone2 --add-auth-providers=ldap:ldap1`

Go to Page 8

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 and `<provider-name>` is the name of the provider:

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

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?

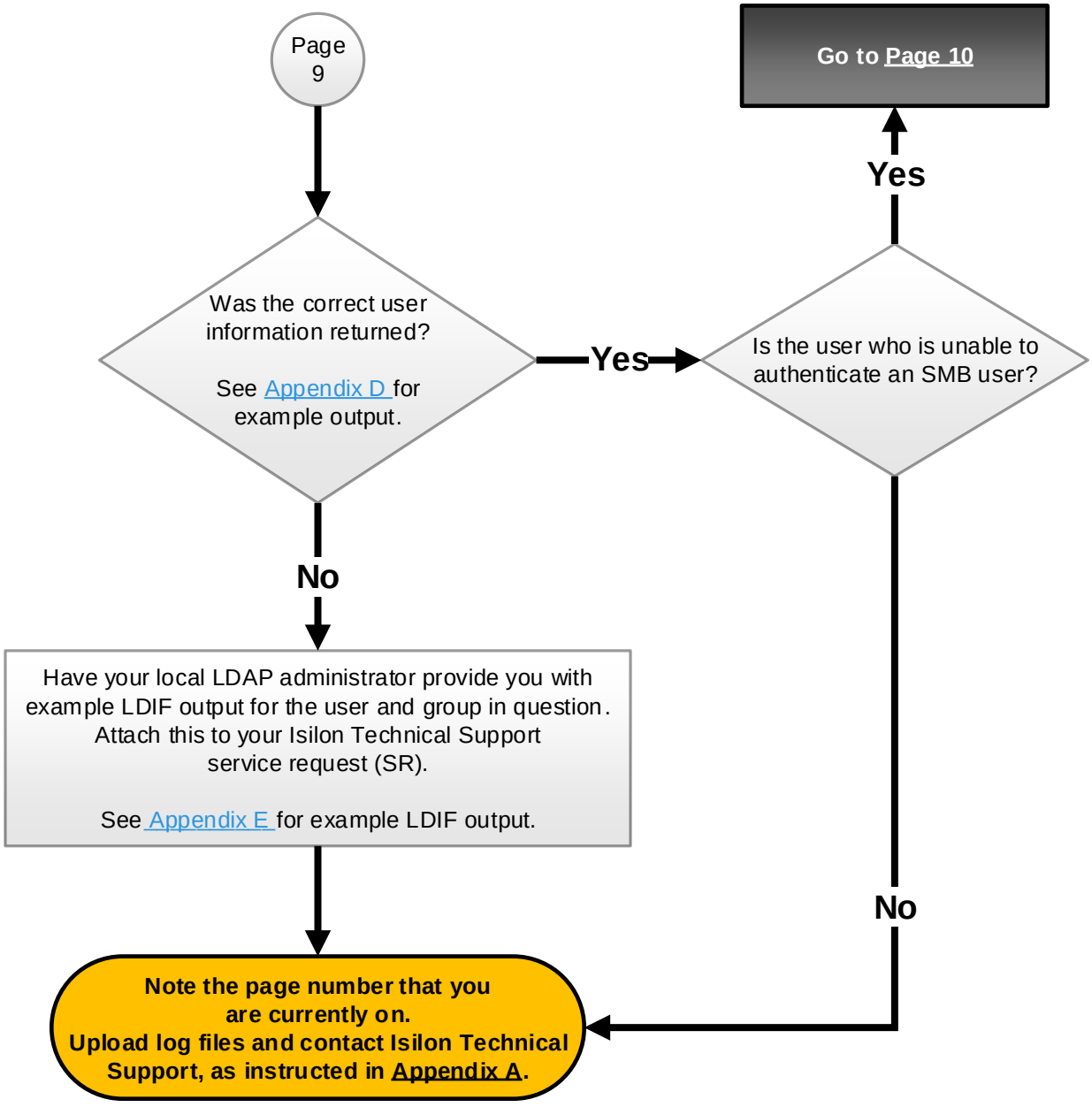
No → Go to Page 14

Yes → Go to Page 9

Verify required user attributes (2)

You could have arrived here from:

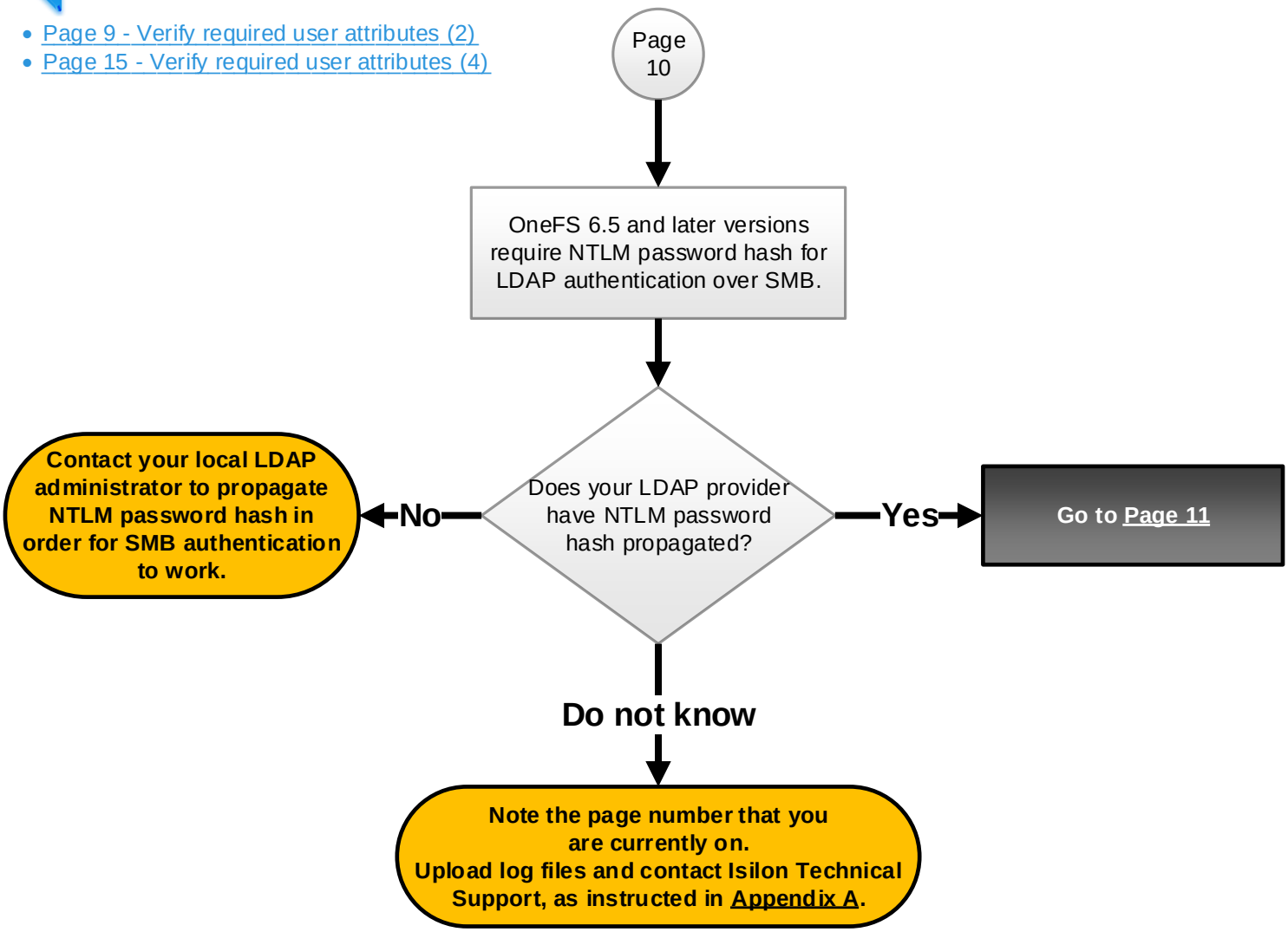
- Page 8 - Verify required user attributes



NTLM password hash

You could have arrived here from:

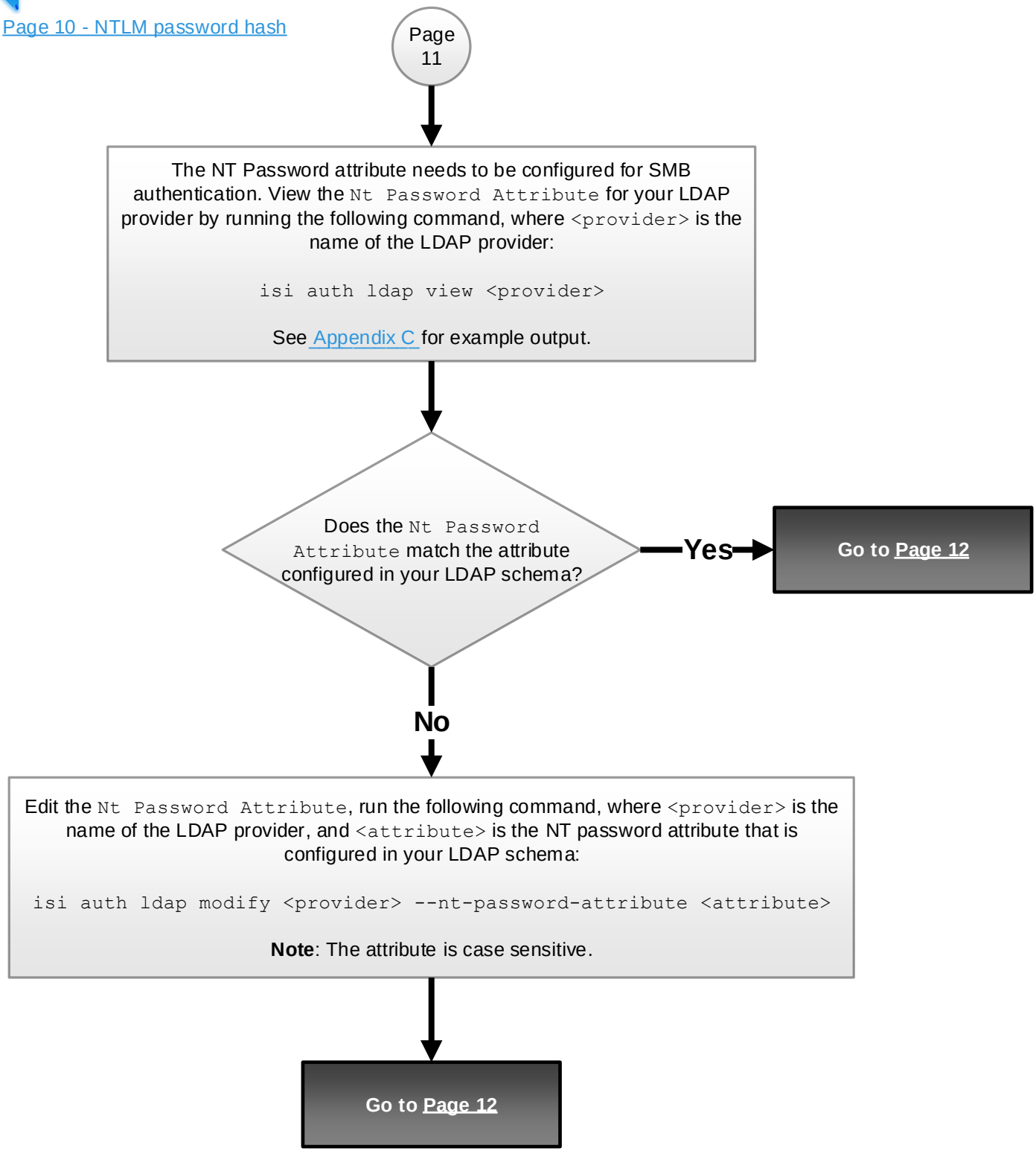
- Page 9 - Verify required user attributes (2)
- Page 15 - Verify required user attributes (4)



NT password attribute

You could have arrived here from:

- Page 10 - NTLM password hash



Test authentication

You could have arrived here from:

- Page 11 - NT password attribute

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

2. From a client, attempt to connect to the affected node by IP address and access a share. Type the following command in the run box, where `<nodeIP>` is the IP address of the node and `<share>` is the name of a share:

```
\\<nodeIP>\<share>
```

3. Test NTLM authentication by connecting to the affected node by IP address. Run the following command, where:

- `<drive>` is the letter of a drive that is not currently in use.
- `<nodeIP>` is the IP address of the node.
- `<share>` is the name of a share.
- `<user>` is the user name of the user.

```
net use <drive> \\<nodeIP>\<share> /user:<user>
```

Did the three test steps complete successfully?

Yes → **End troubleshooting**

No

Have your local LDAP administrator provide you with example LDIF output for the user and group in question. Attach this to your Isilon Technical Support service request (SR).

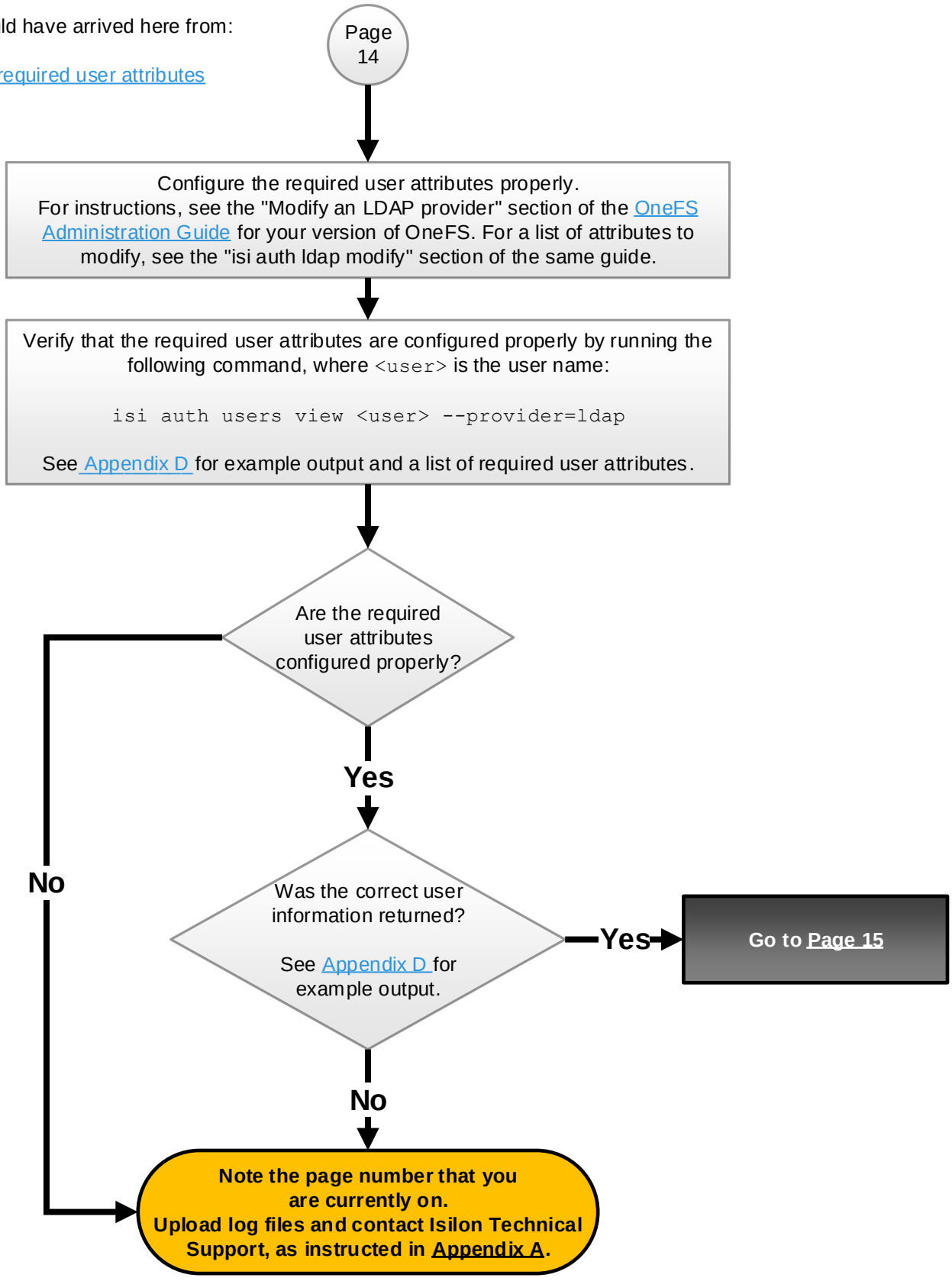
See Appendix E for example LDIF output.

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

Verify required user attributes (3)

You could have arrived here from:

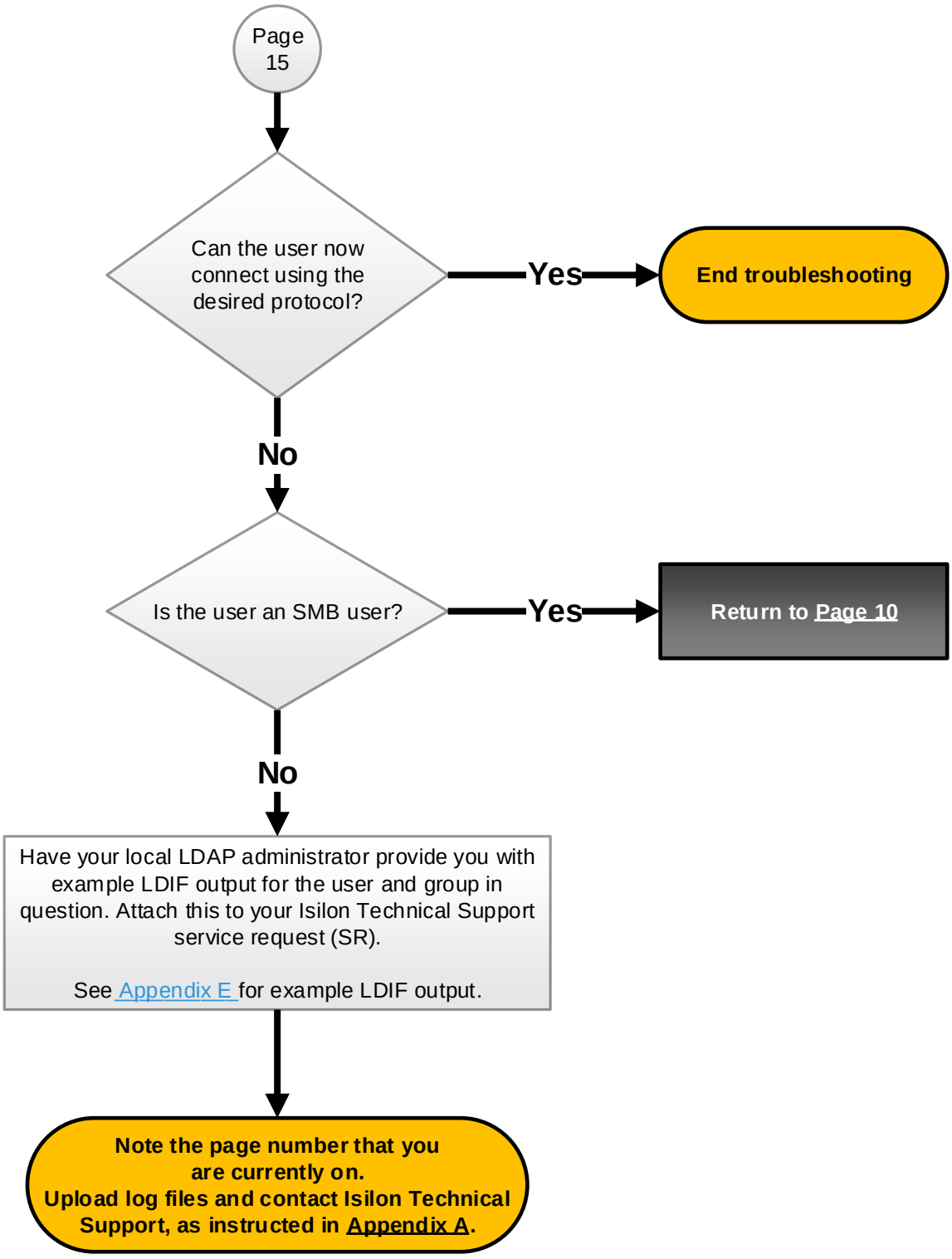
- Page 8 - Verify required user attributes



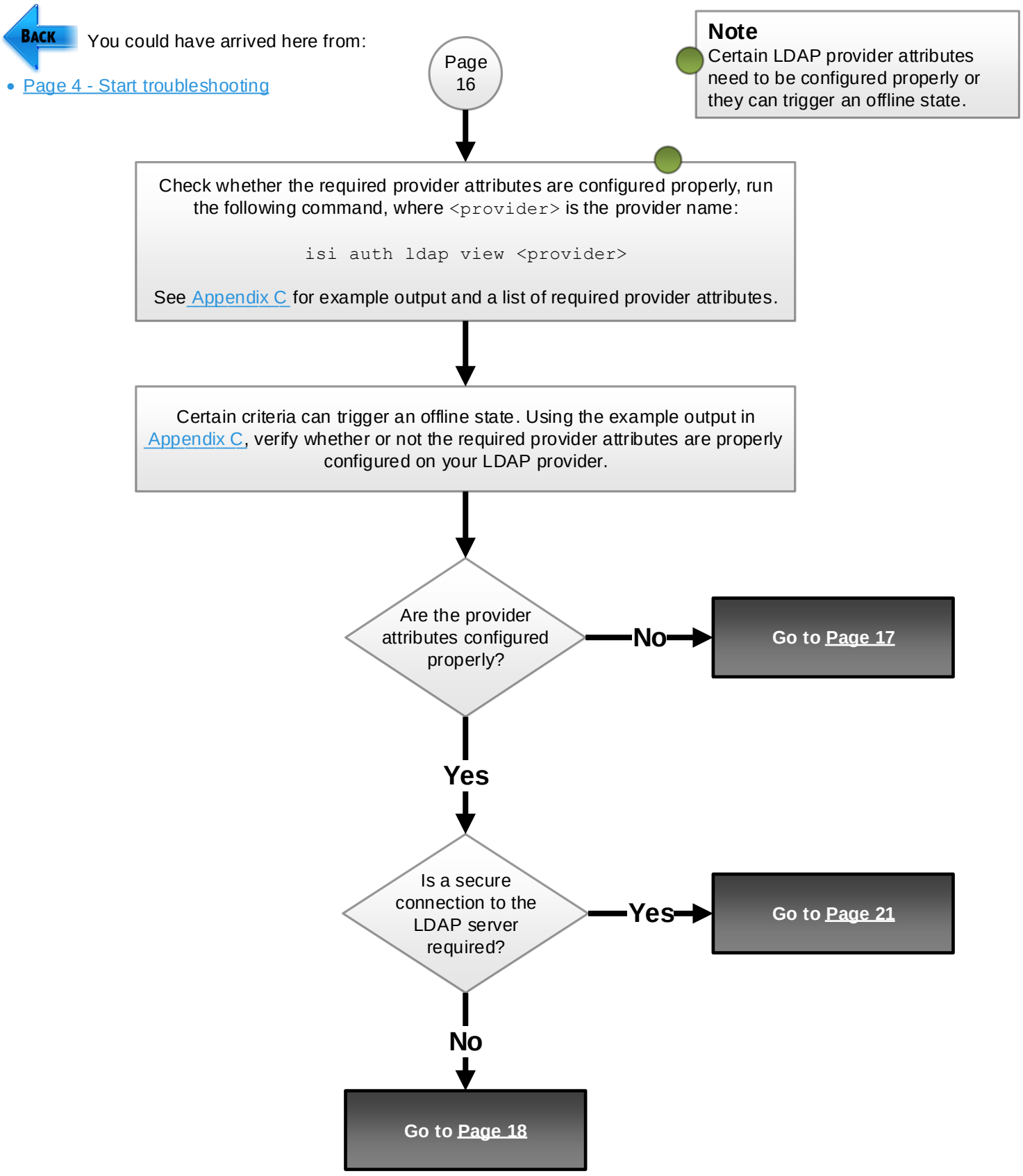
Verify required user attributes (4)

You could have arrived here from:

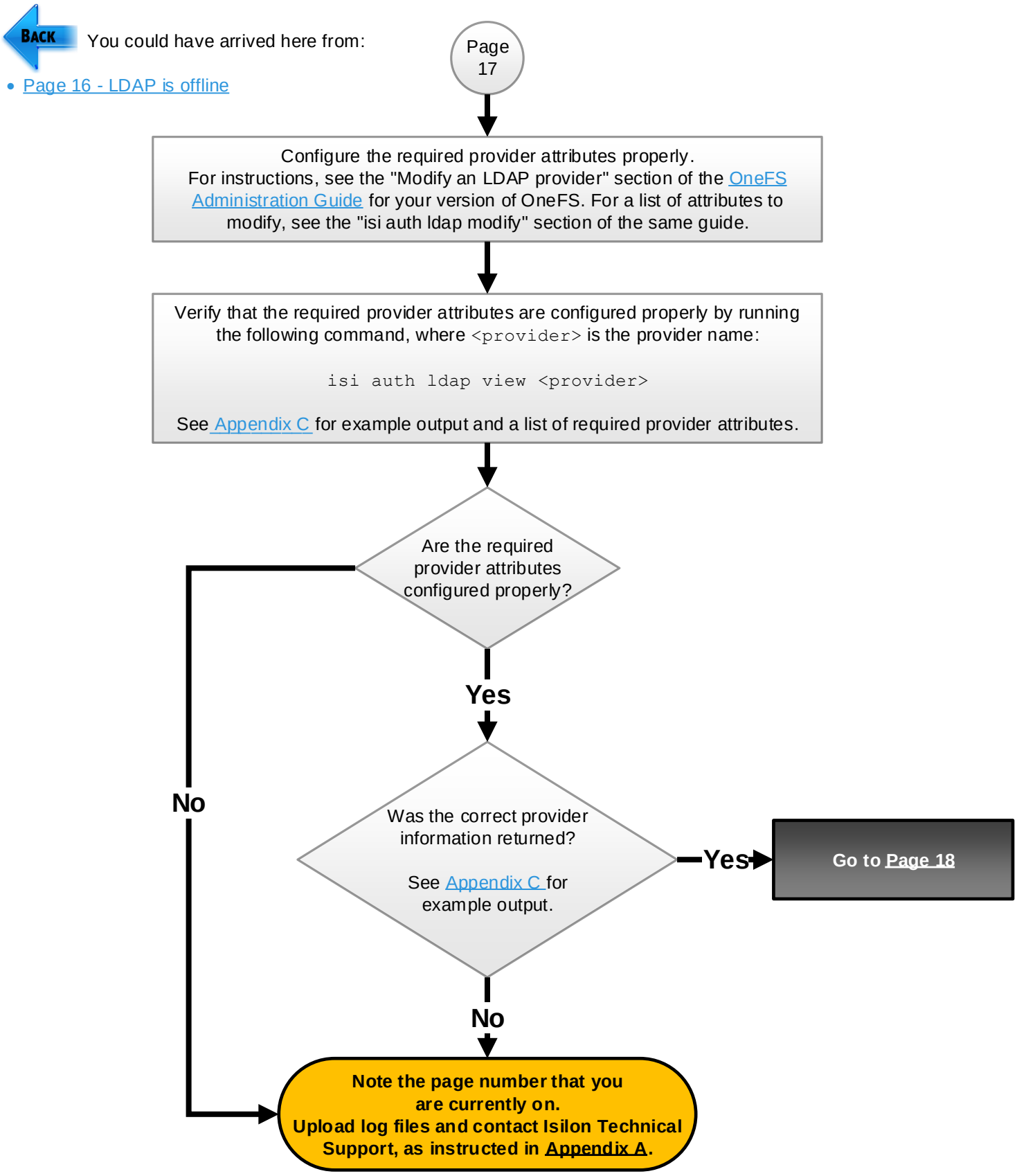
- Page 14 - Verify required user attributes (3)



LDAP is offline



Verify required user attributes (5)



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 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>
```

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:

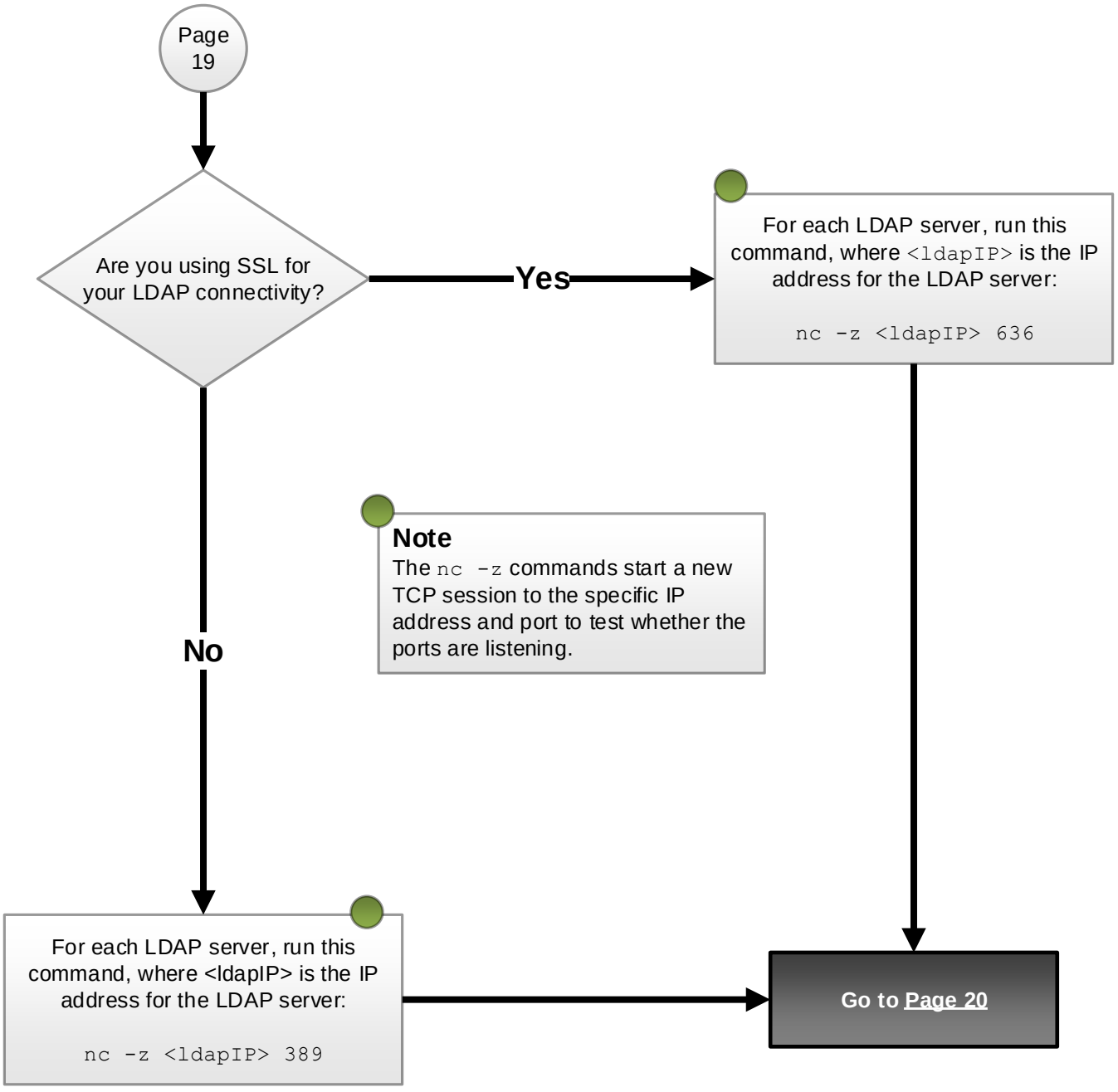
```
isi auth ldap modify --provider-name=<provider> --require-secure-connection=no
```

Go to Page 19

Test LDAP ports

You could have arrived here from:

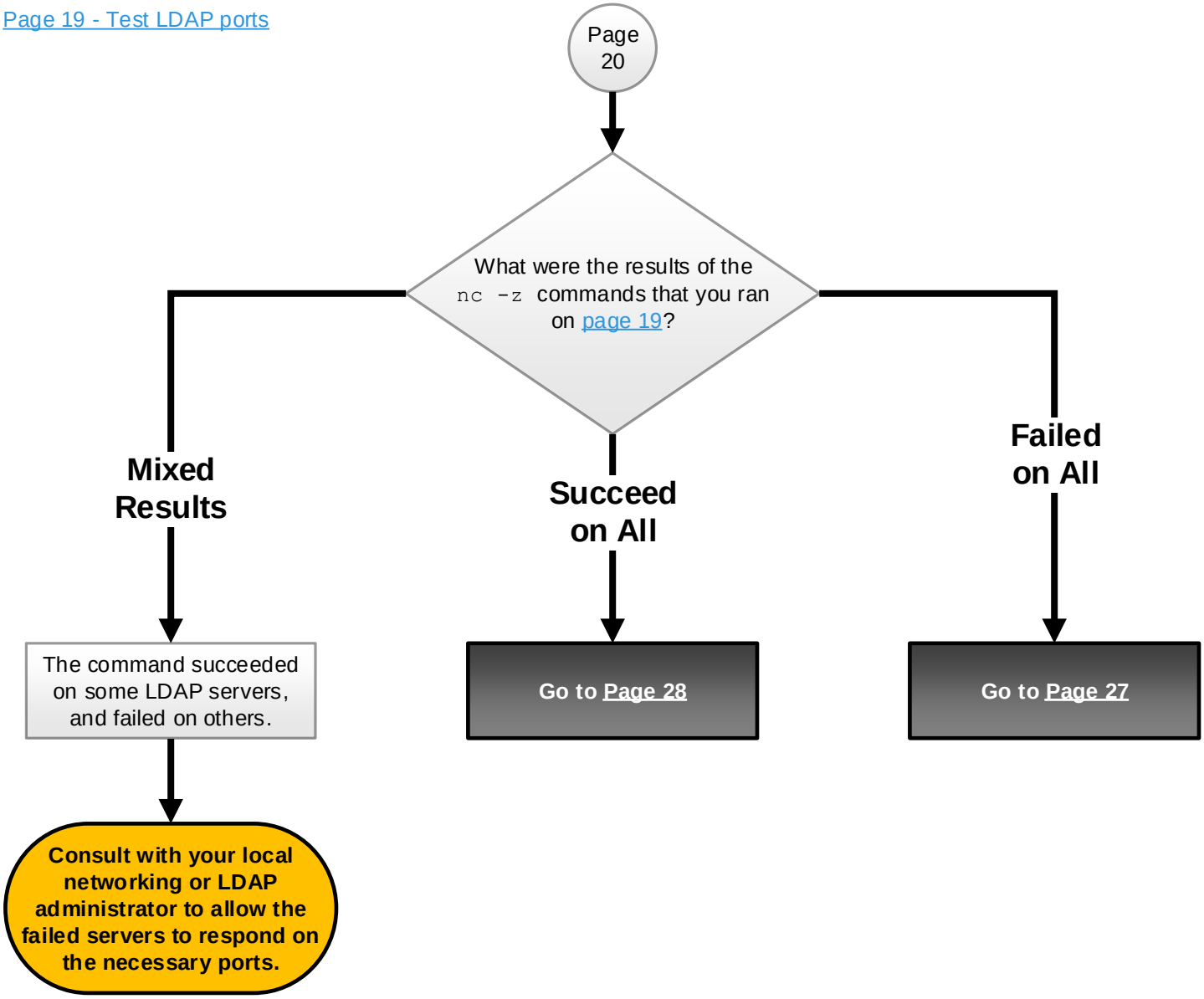
- Page 18 - Verify LDAP configuration
- Page 20 - Test LDAP ports (2)
- Page 25 - Verify secure LDAP configuration (3)
- Page 26 - Verify secure LDAP configuration (4)



Test LDAP ports (2)

You could have arrived here from:

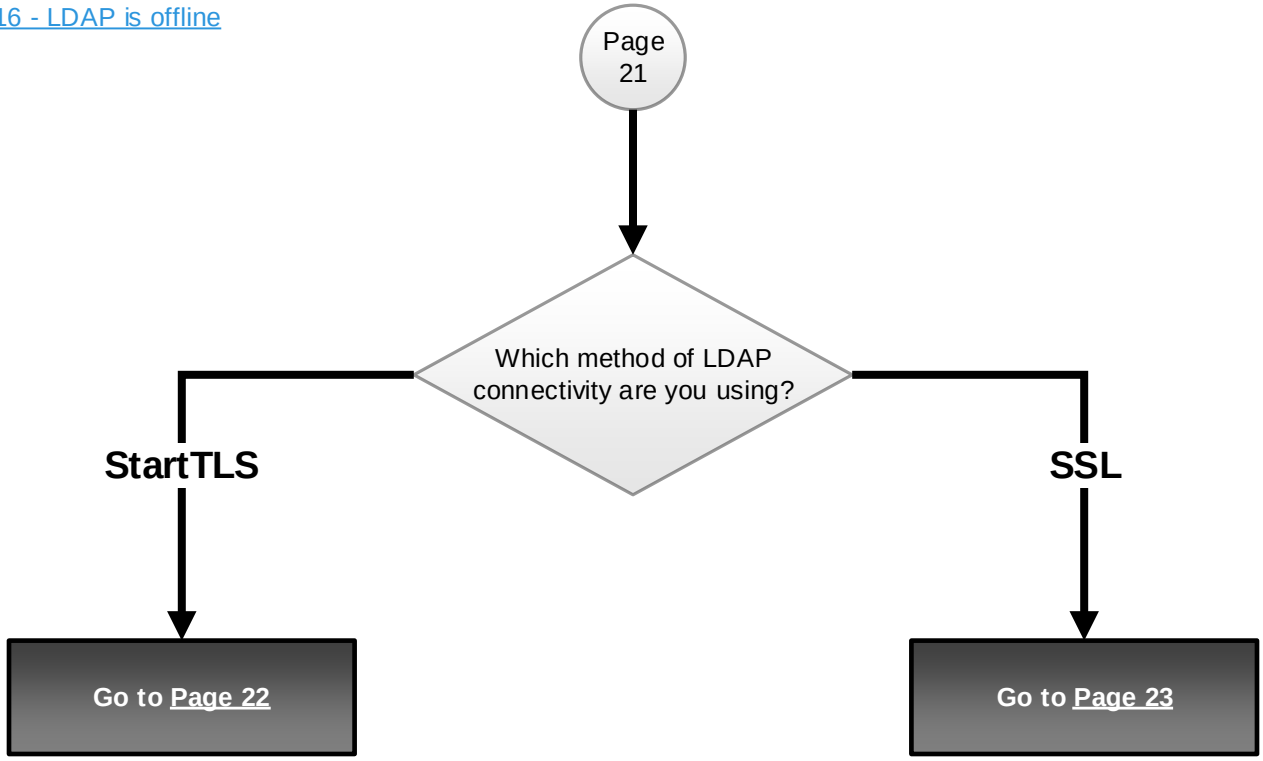
- Page 19 - Test LDAP ports



Test LDAP ports (3)

You could have arrived here from:

- Page 16 - LDAP is offline

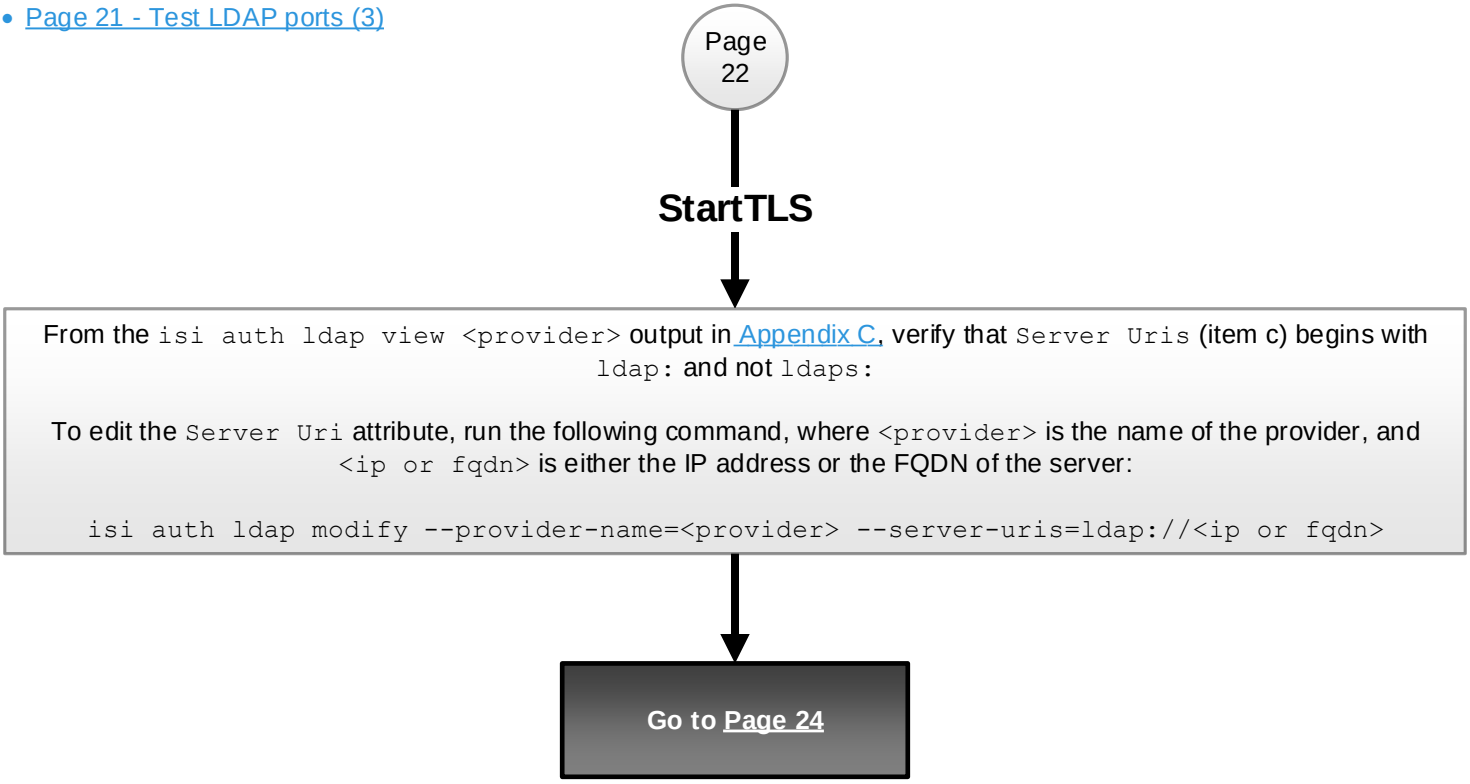


Verify secure LDAP configuration

StartTLS

You could have arrived here from:

- Page 21 - Test LDAP ports (3)

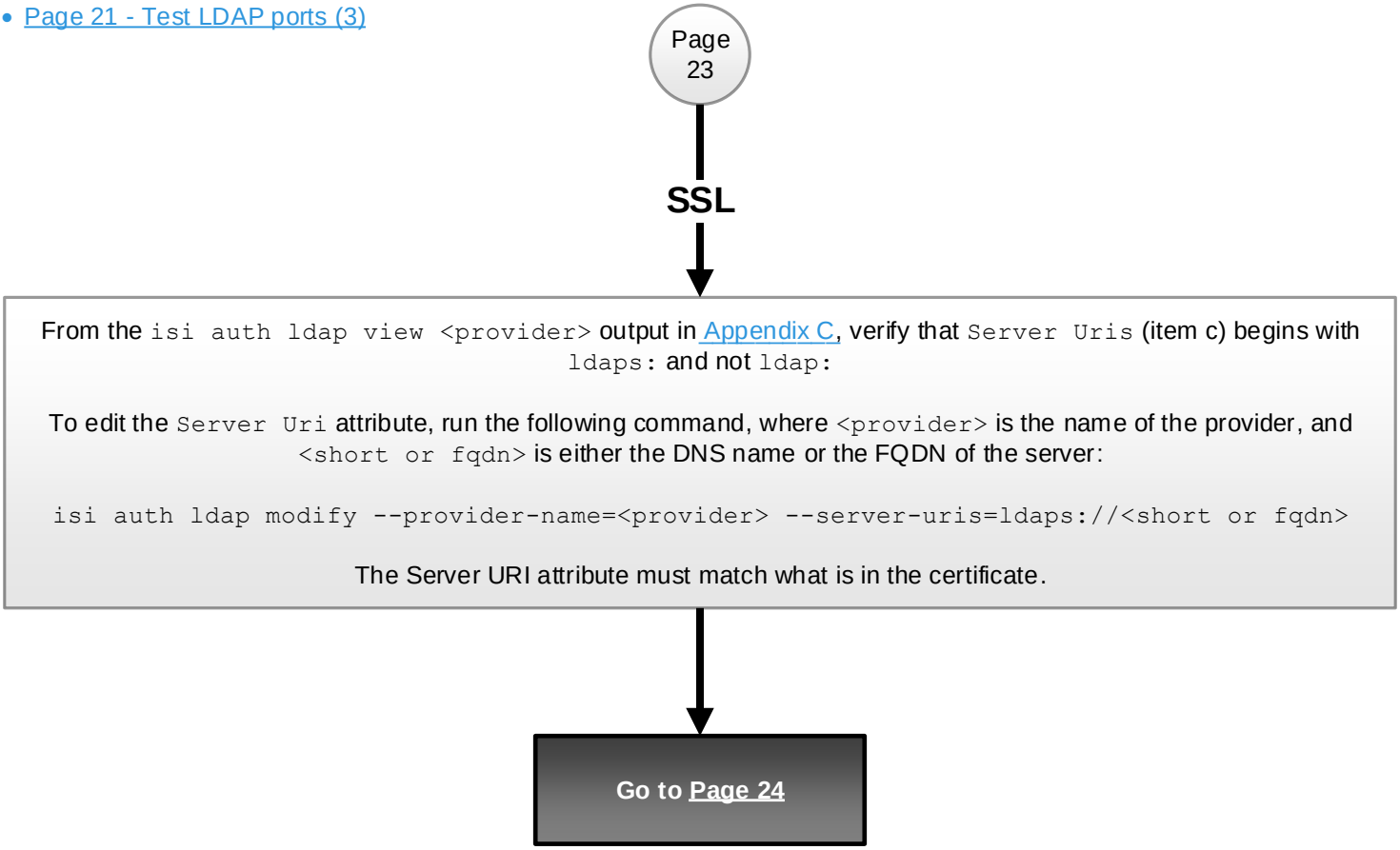


Verify secure LDAP configuration

SSL

You could have arrived here from:

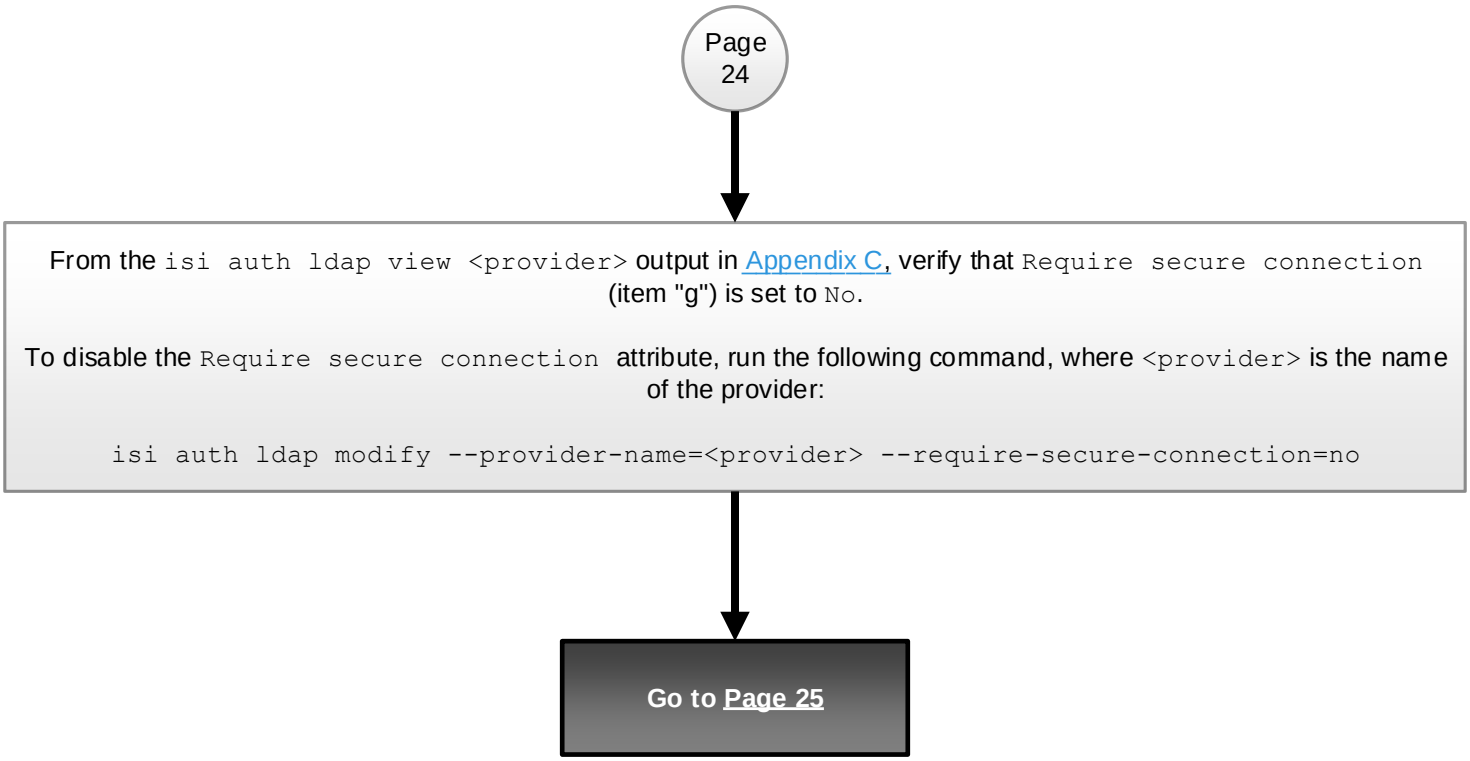
- Page 21 - Test LDAP ports (3)



Verify secure LDAP configuration (2)

You could have arrived here from:

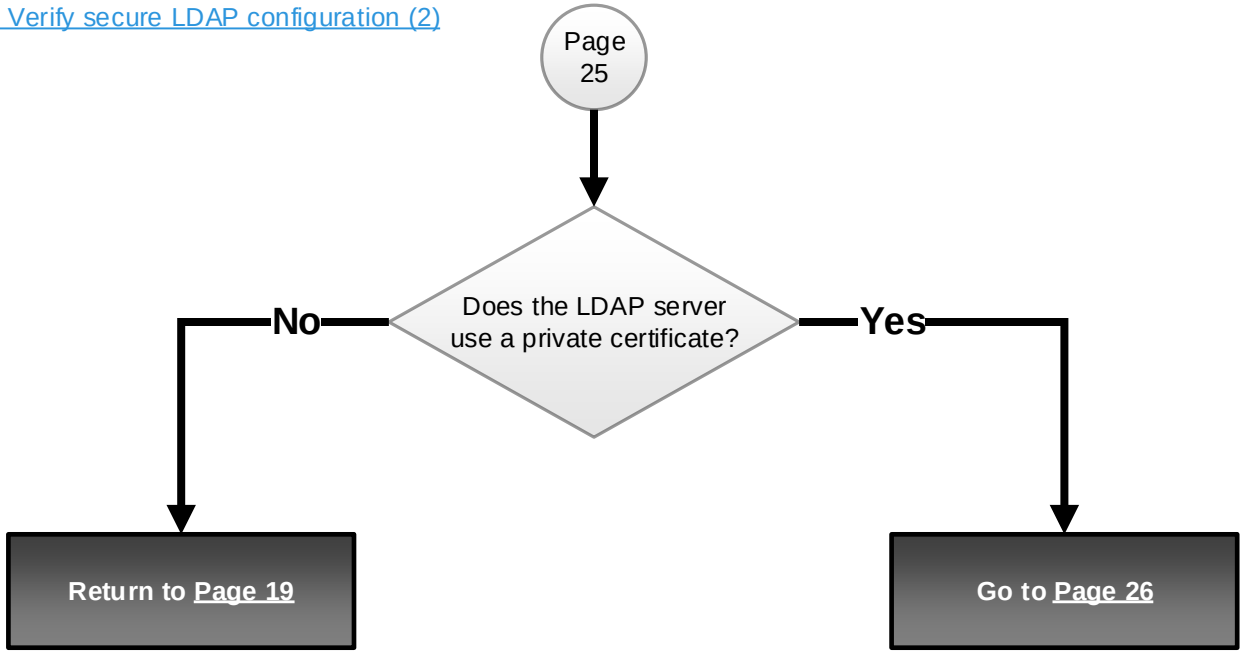
- Page 22 - Verify secure LDAP configuration, StartTLS
- Page 23 - Verify secure LDAP configuration, SSL



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.

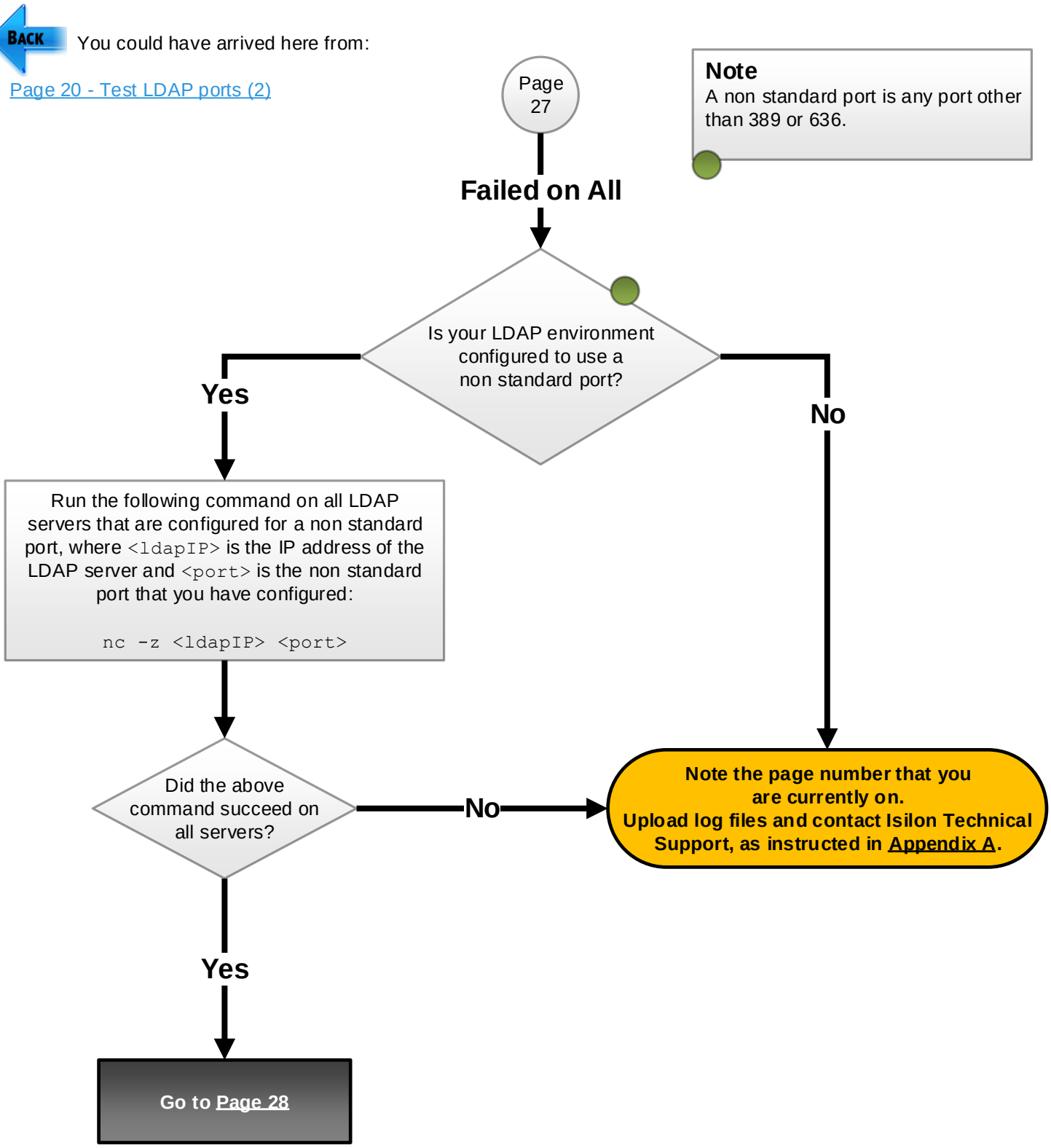
To specify the `Certificate Authority File`, run the following command, where `<provider>` is the name of the provider and `<location>` is the file path of the certificate authority file in */ifs*:

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

See Appendix C for example output.

Return to Page 19

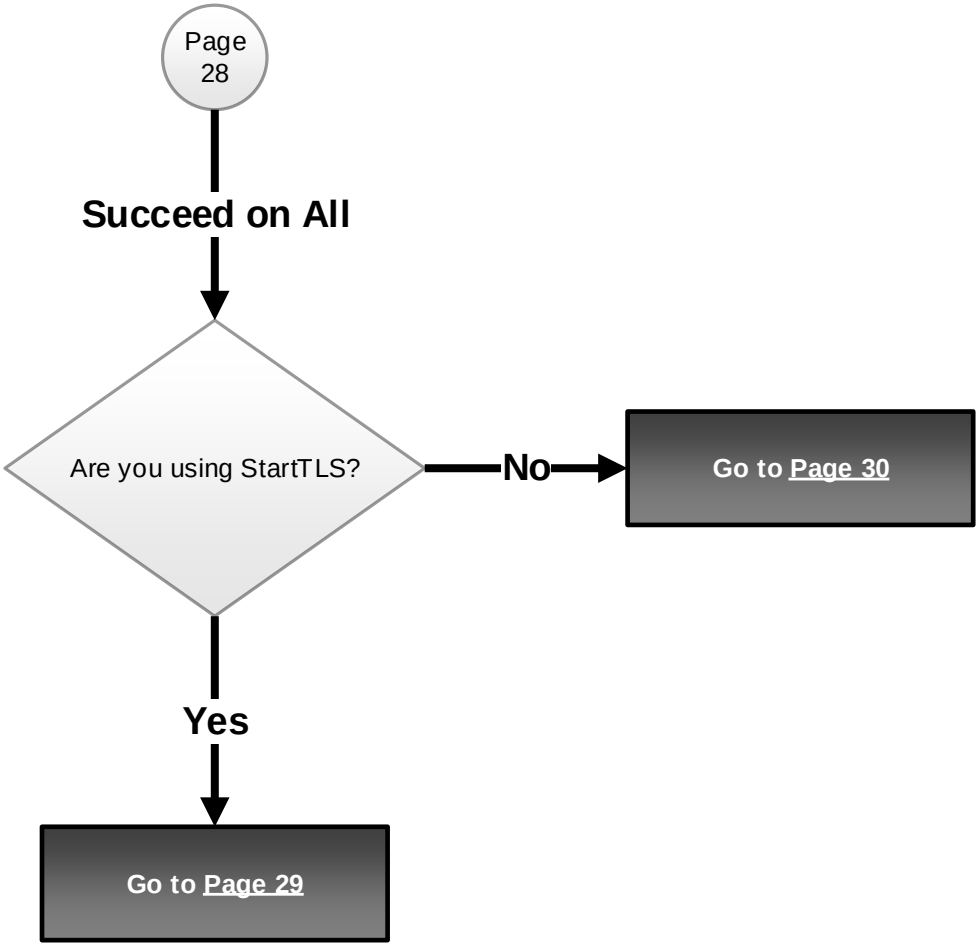
Test LDAP ports (4)



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:

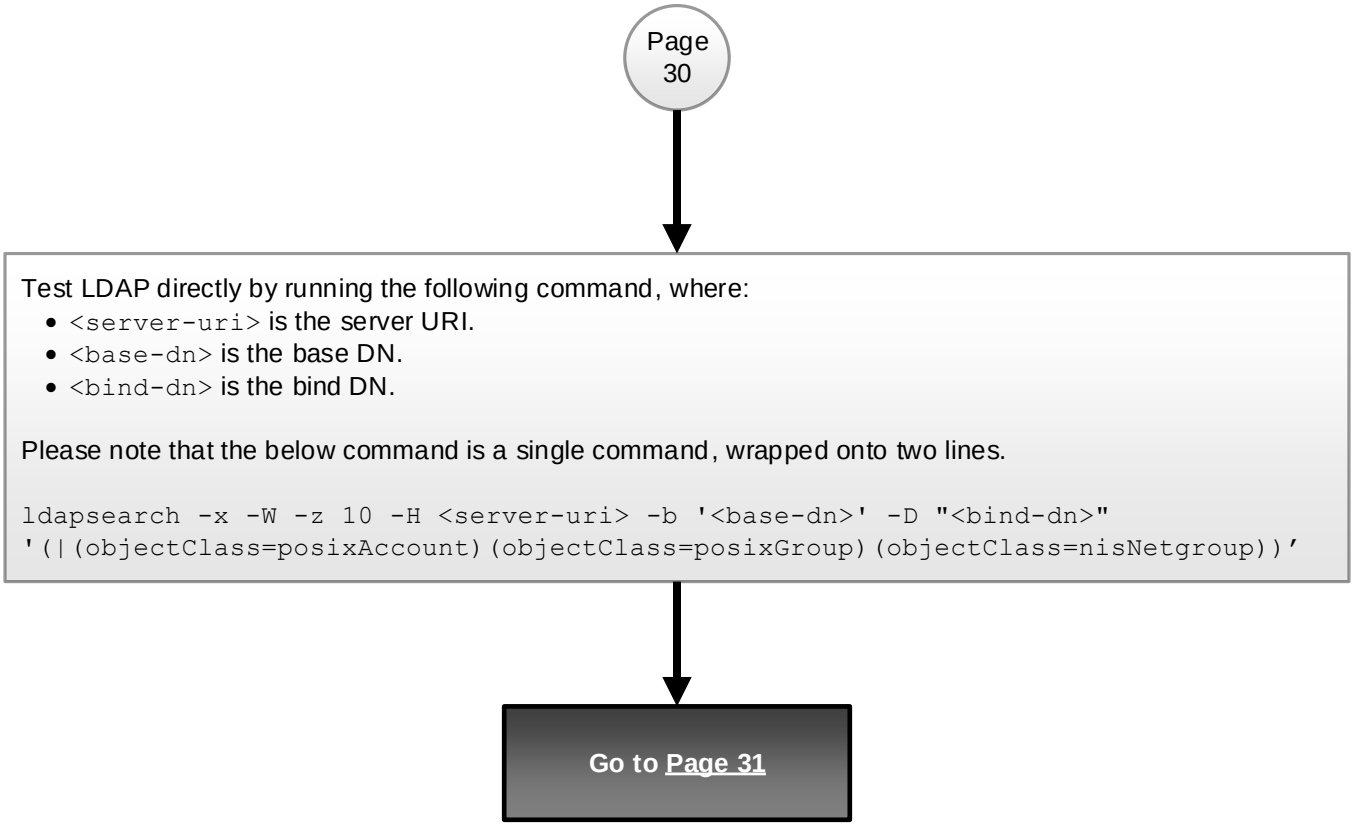
```
ldapsearch -x -W -z 10 -H <server-uri> -b '<base-dn>' -D "<bind-dn>" LDAPTLS_CACERT="<location>"
'(|(objectClass=posixAccount)(objectClass=posixGroup)(objectClass=nisNetgroup))'
```

Go to Page 31

Test LDAP (2)

You could have arrived here from:

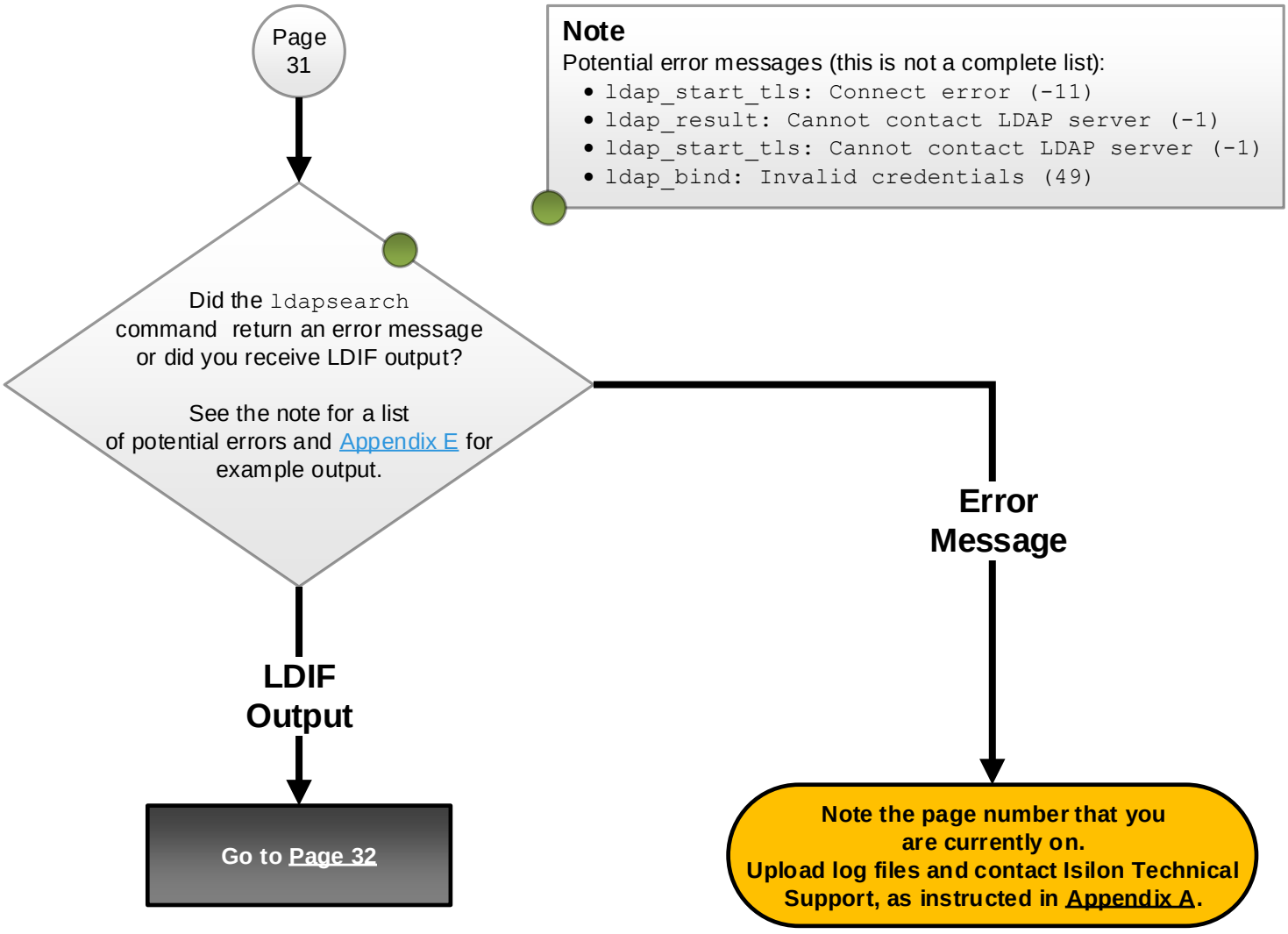
- Page 28 - Test LDAP ports (5)



Test LDAP (3)

You could have arrived here from:

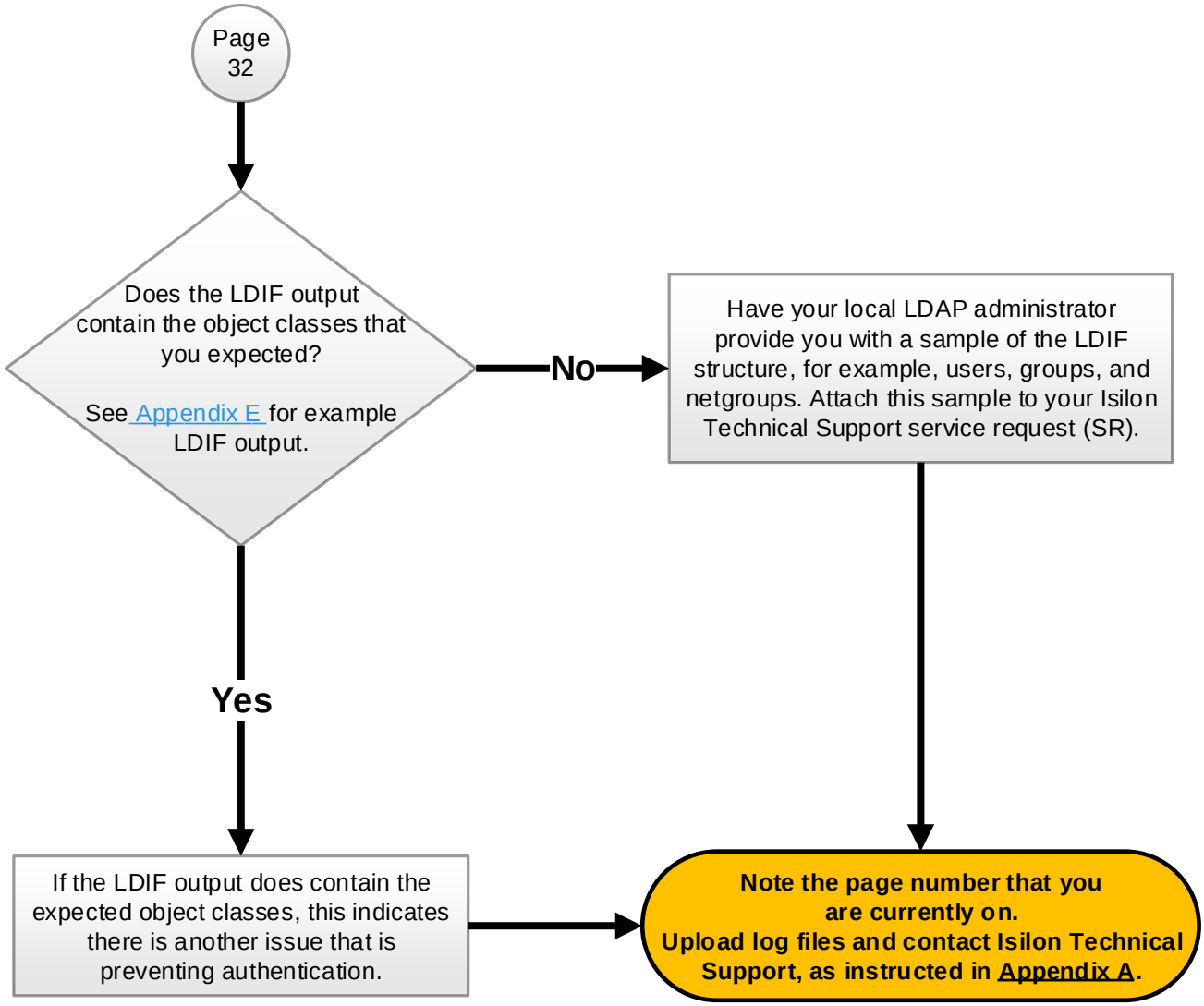
- Page 29 - Test LDAP
- Page 30 - Test LDAP (2)



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.

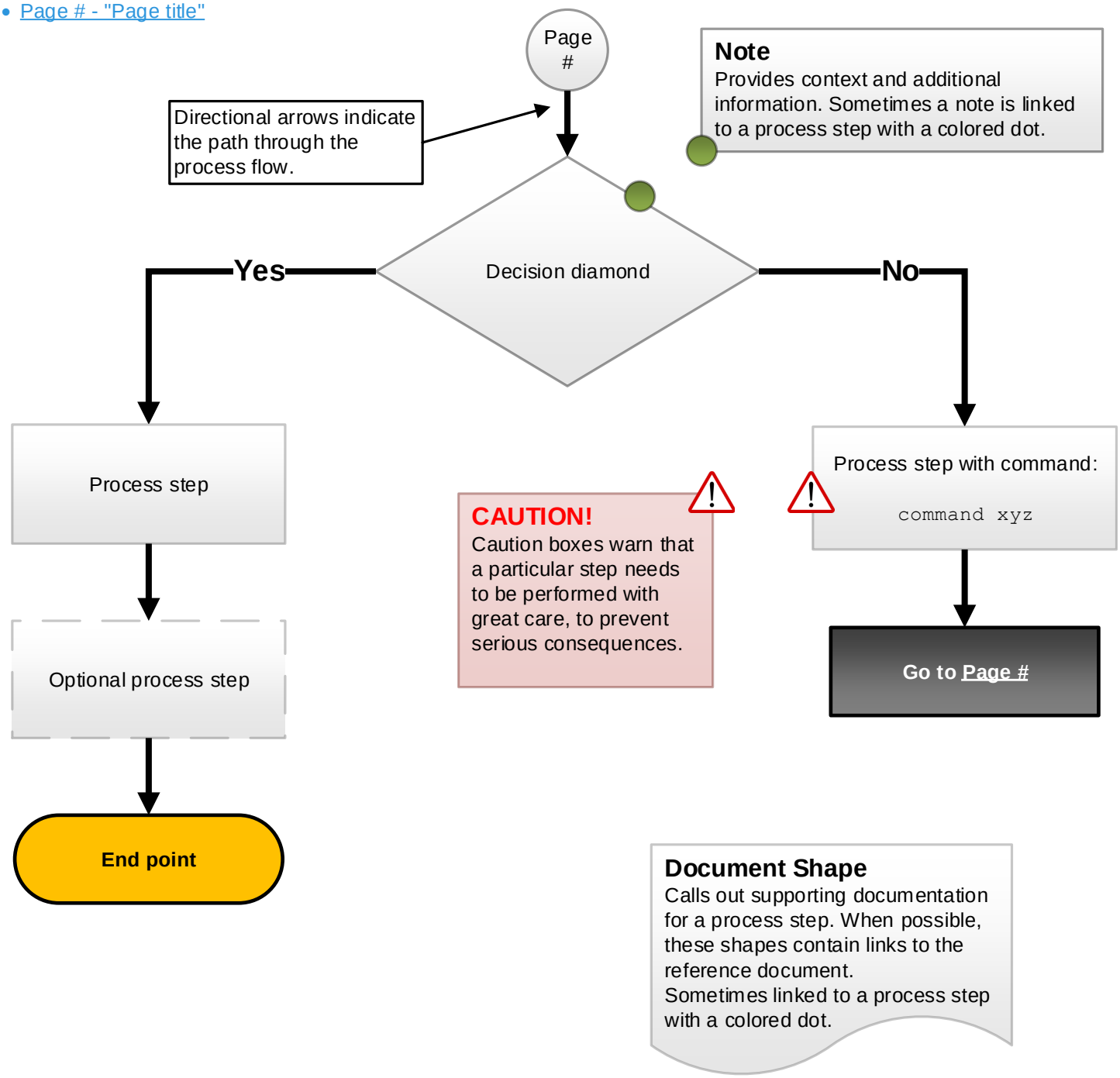
Appendix B: How to use this flowchart

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 Uris`
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)

```
cluster-1# isi auth ldap view ldap_example
Name: ldap_example
Base DN: cn=users,dc=10-9,dc=lab,dc=emc,dc=test
Server Uris: ldap://10.11.12.70
Status: online
Alternate Security Identities Attribute: -
Authentication: Yes
Balance Servers: Yes
Bind DN: uid=admin,cn=users,dc=10-9,dc=test
Bind Timeout: 10
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: gecos
GID Attribute: gidNumber
Group Base DN: -
Group Domain: LDAP_DOMAIN
Group Filter: (objectClass=posixGroup)
Group Members Attribute: memberUid
Group Search Scope: default
Groupnet: groupnet0
Home Directory Template: -
Homedir Attribute: homeDirectory
Ignore TLS Errors: No
Listable Groups: -
Listable Users: -
Login Shell: -
Member Of Attribute: -
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
Nt Password Attribute: ntPassword
Ntlm Support: all
Provider Domain: -
Require Secure Connection: No
Restrict Findable: Yes
Restrict Listable: No
Search Scope: subtree
Search Timeout: 100
Shadow User Filter: (objectClass=shadowAccount)
Shadow Expire Attribute: shadowExpire
Shadow Flag Attribute: shadowFlag
Shadow Inactive Attribute: shadowInactive
Shadow Last Change Attribute: shadowLastChange
Shadow Max Attribute: shadowMax
Shadow Min Attribute: shadowMin
Shadow Warning Attribute: shadowWarning
Shell Attribute: loginShell
UID Attribute: uidNumber
Unfindable Groups: wheel, 0, group1, 15, group2, 16
Unfindable Users: root, 0, user1, 15, user2, 16
Unique Group Members Attribute: -
Unlistable Groups: -
Unlistable Users: -
User Base DN: -
User Domain: domain_test
User Filter: (objectClass=posixAccount)
User Search Scope: default
```

a, b, c, d, 1, 2, e, 3, 6, g, 4, 5

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 tuser --provider=ldap
Name: tuser                                                    (1)
DN: CN=tuser,CN=Users,DC=dur,DC=example,DC=com
DNS Domain: -
Domain: LDAP_USERS
Provider: lsa-ldap-provider:ldap_example
Sam Account Name: tuser
UID: 1005                                                      (2)
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:
GID:1800                                                       (3)
Name: isilon
Home Directory: /home/user home                                (4)
Max Password Age: Never
Password Expired: No
Password Expiry: -
Password Last Set: -
Password Expires: Yes
Shell: /bin/tcsh                                               (5)
```

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=Test User,ou=Users,dc=nismaster,dc=example,dc=com
dn: cn=Test User,ou=Users,dc=nismaster,dc=example,dc=com
cn: Test User
(1) gidnumber: 1800
givenname: Test
(2) homedirectory: /home/users/tuser
(3) loginshell: /bin/tcsh
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: user
(4) uid: tuser
(5) uidnumber: 1005
userpassword: {MD5}Ho0TCNi6UB8gG7/JGpXU7w==
```

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 in North America 1-866-464-7381
www.EMC.com