EMC ISILON CUSTOMER TROUBLESHOOTING GUIDE

TROUBLESHOOT WINDOWS FILE SYSTEM PERMISSIONS FOR YOUR ISILON CLUSTER

Abstract

This guide will help you to troubleshoot problems with gaining access to the Isilon cluster.

January 6, 2016

Contents and overview

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

We appreciate your help in improving this document. Submit your feedback at http://bit.ly/isi-docfeedback.

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 connect through either 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, please 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
   ```

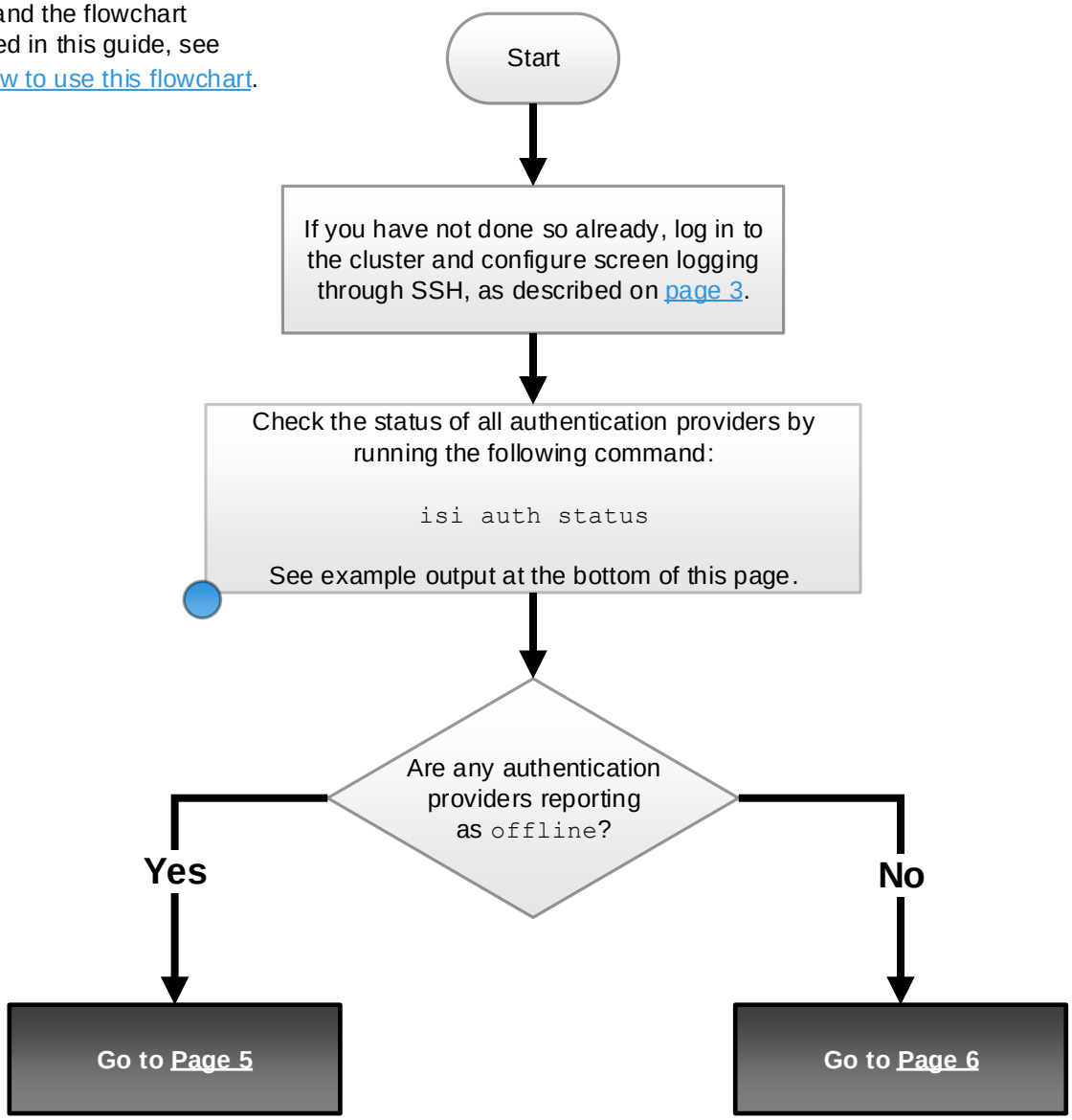
   This will create a file named `screenlog.0` that will be appended to during your session.

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.



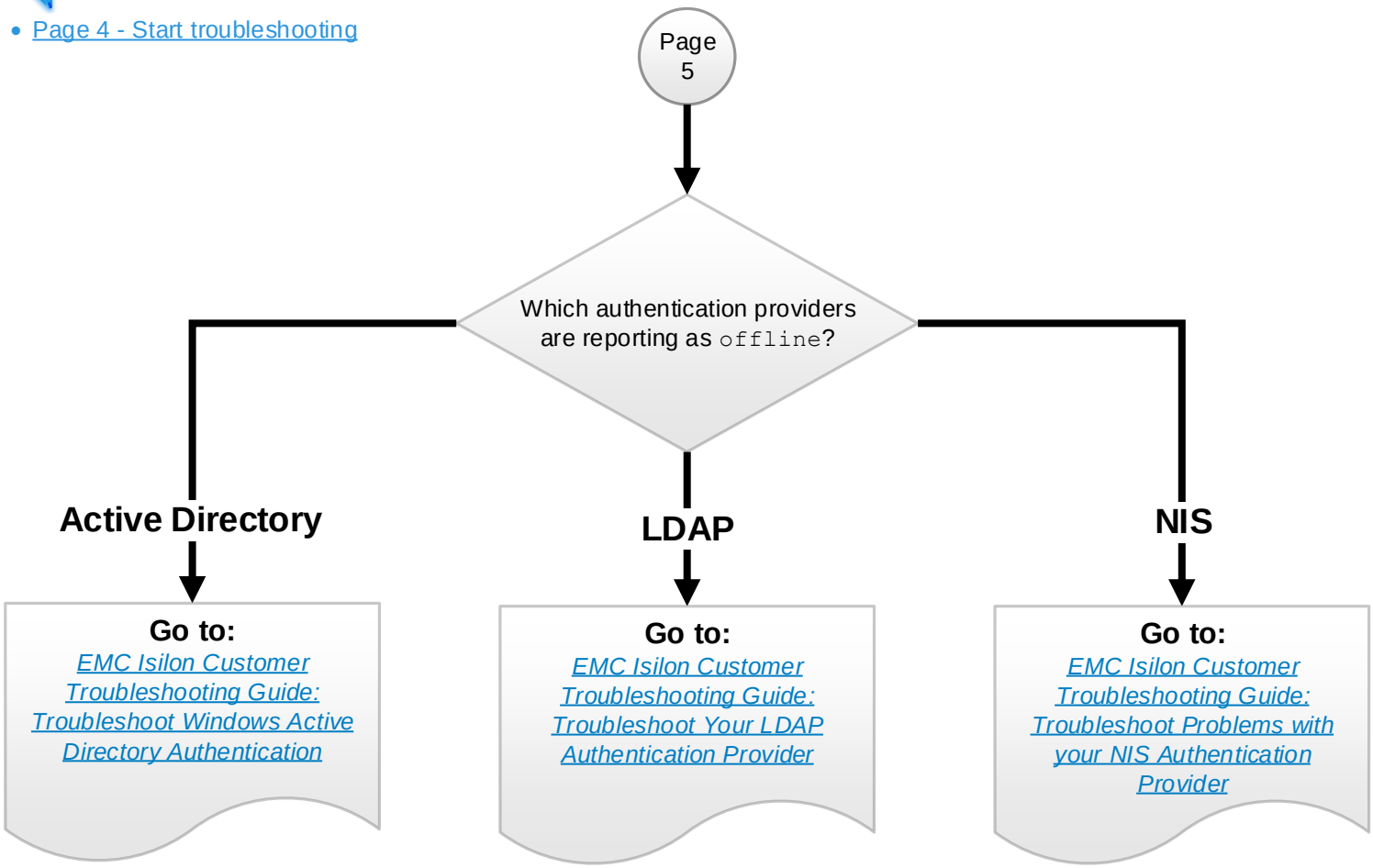
Example `isi auth status` output

```
Cluster-1# isi auth status
ID                          Active Server  Status
-------------------------------------------------
lsa-local-provider:System   -              active
lsa-local-provider:ZONE2    -              active
lsa-file-provider:System    -              active
lsa-ldap-provider:LDAPTest  -              online
lsa-nis-provider:NIStest    -              offline
lsa-ads-provider:ADtest     -              online
-------------------------------------------------
Total: 5
```

Authentication provider status

You could have arrived here from:

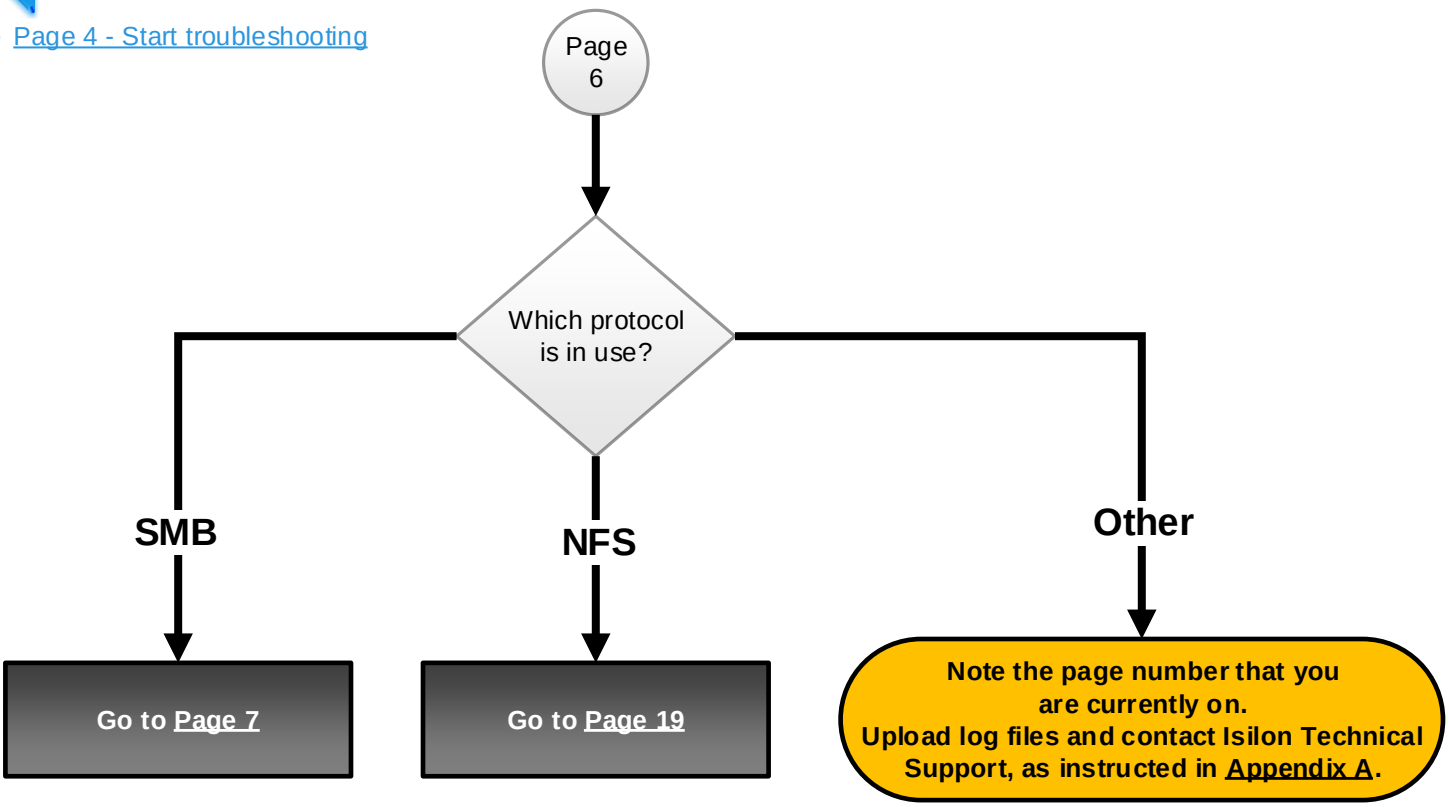
- Page 4 - Start troubleshooting



Protocol

You could have arrived here from:

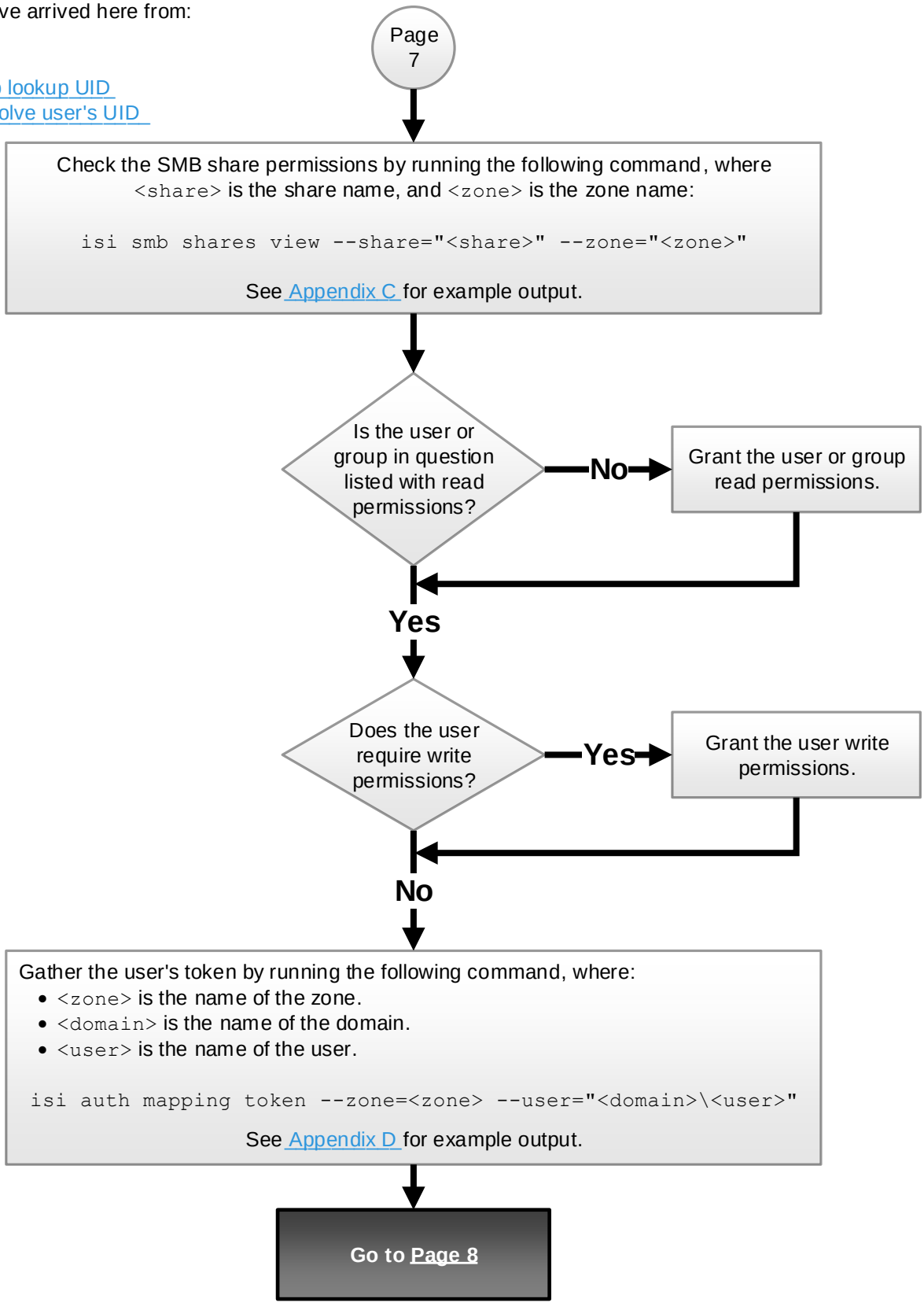
- Page 4 - Start troubleshooting



SMB protocol

You could have arrived here from:

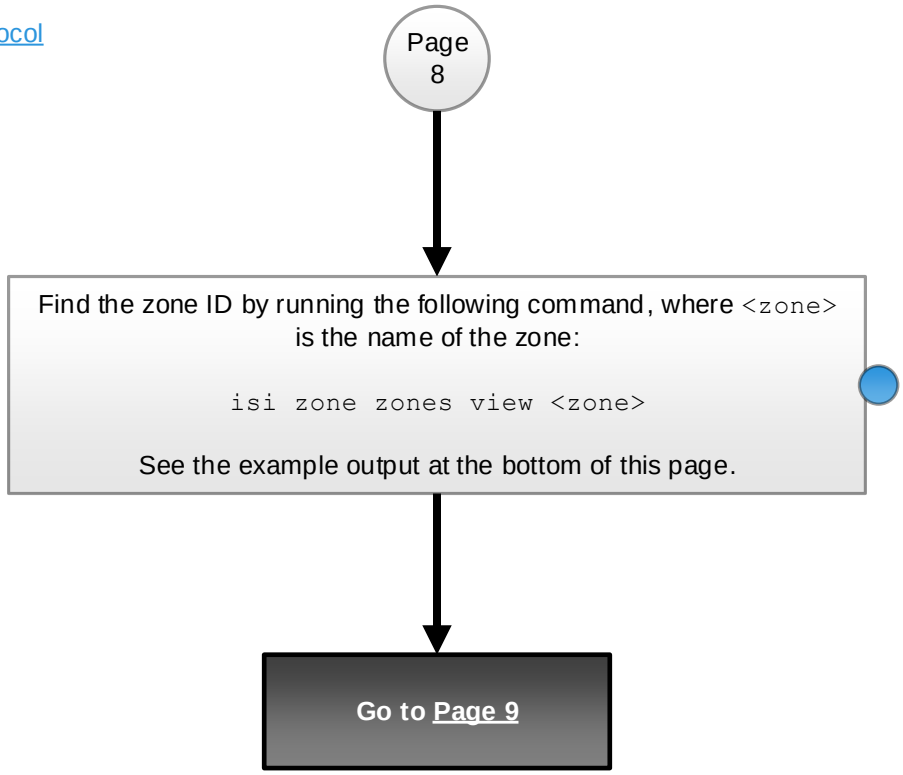
- Page 6 - Protocol
- Page 20 - NFS - Map lookup UID
- Page 21 - NFS - Resolve user's UID



SMB protocol (2)

You could have arrived here from:

- Page 7 - SMB protocol



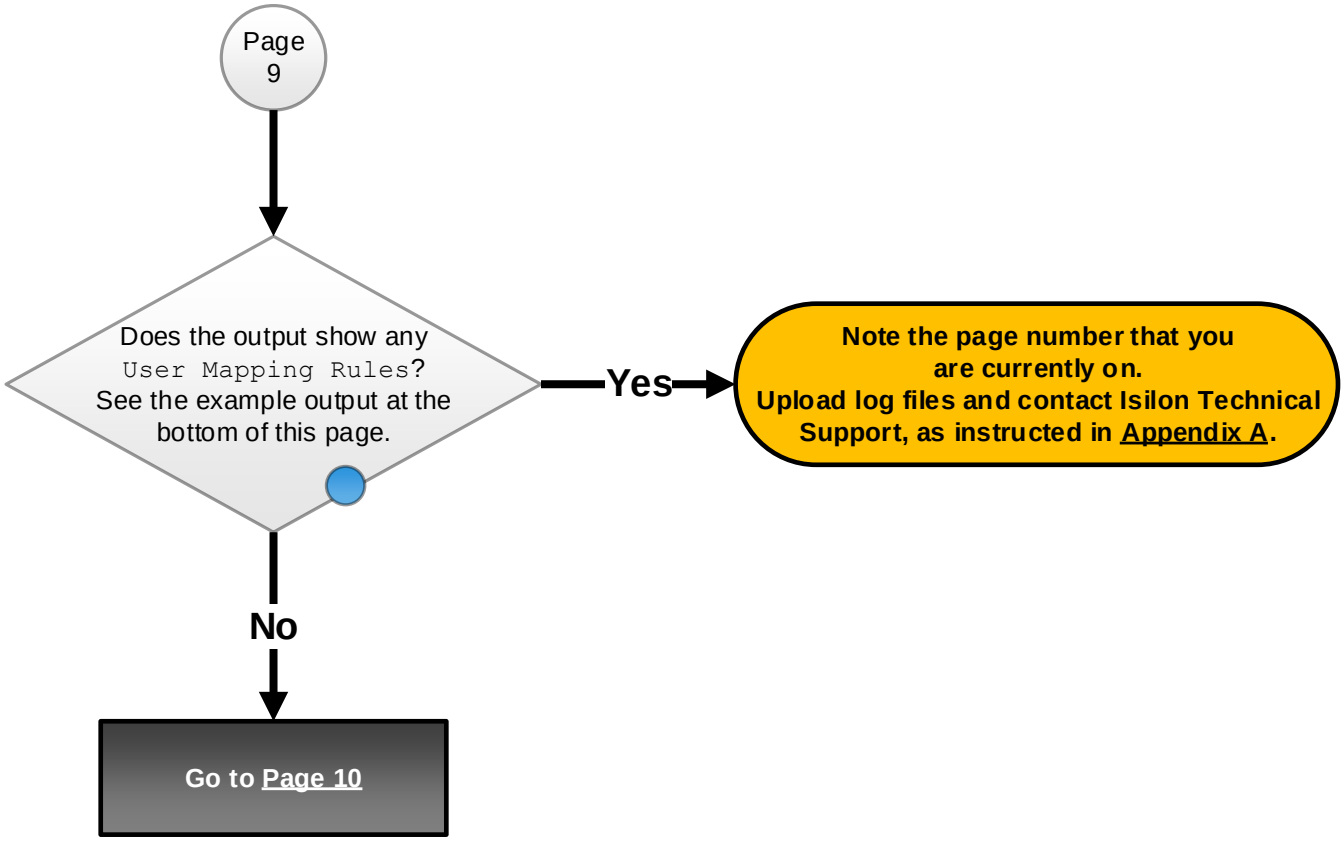
Example `isi zone zones view <zone>` output

```
Cluster-1# isi zone zones view System
                      Name: System
                      Path: /ifs
                Cache Size: 9.54M
             Map Untrusted:
            Auth Providers: -
              NetBIOS Name:
       All Auth Providers: Yes
       User Mapping Rules: -
     Home Directory Umask: 0077
       Skeleton Directory: /usr/share/skel
            Audit Success: create, delete, rename, set_security, close
            Audit Failure: create, delete, rename, set_security, close
      HDFS Authentication: all
              HDFS Keytab: /etc/hdfs.keytab
      HDFS Root Directory: /ifs
          WebHDFS Enabled: Yes
Syslog Forwarding Enabled: No
      Syslog Audit Events: create, delete, rename, set_security
                  Zone ID: 1
```

Multiprotocol

You could have arrived here from:

- Page 8 - SMB protocol (2)



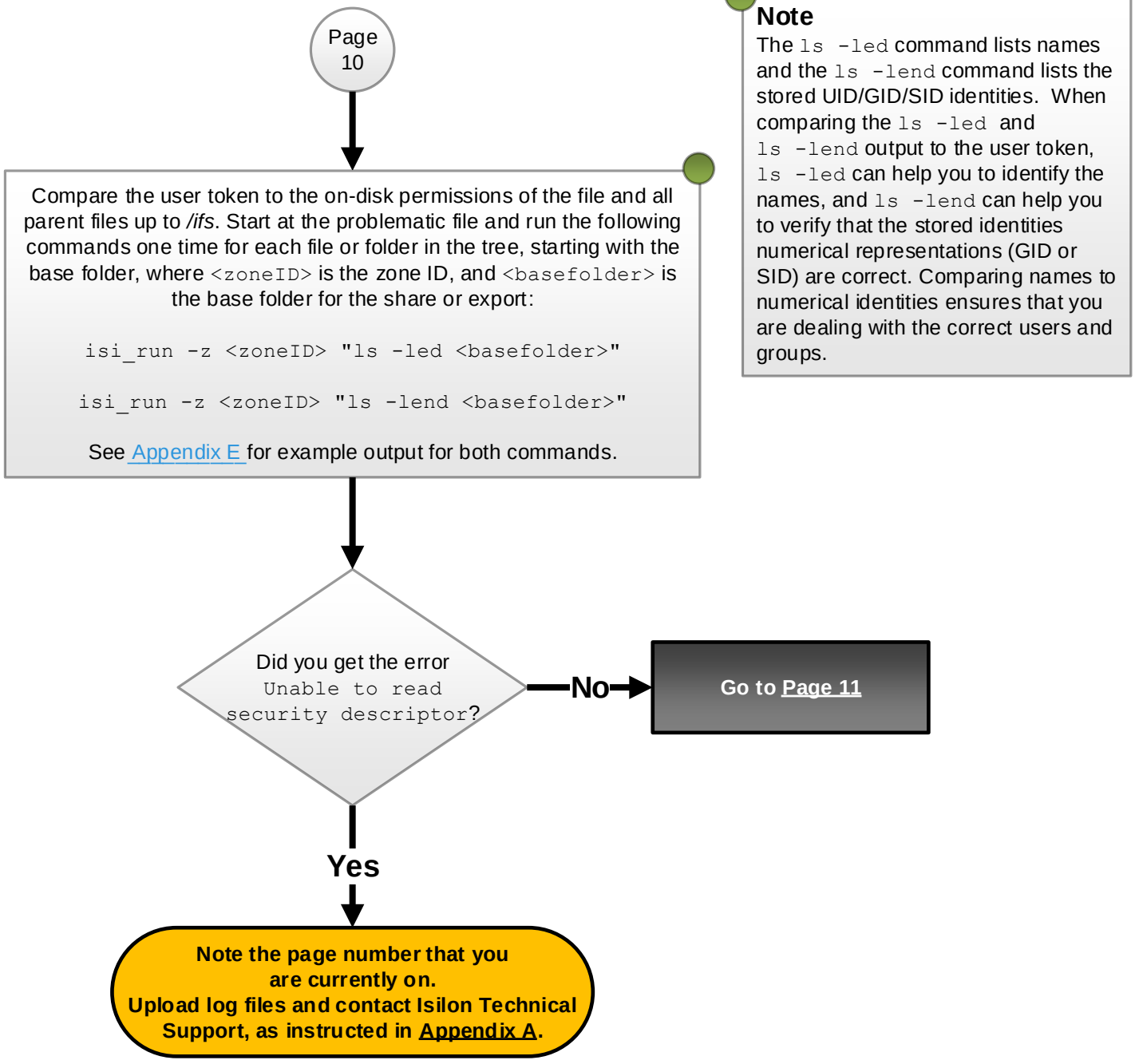
Example `isi zone zones view <zone>` output

```
Cluster-1# isi zone zones view System
                      Name: System
                      Path: /ifs
                Cache Size: 9.54M
             Map Untrusted:
            Auth Providers: -
              NetBIOS Name:
       All Auth Providers: Yes
       User Mapping Rules: -
     Home Directory Umask: 0077
       Skeleton Directory: /usr/share/skel
            Audit Success: create, delete, rename, set_security, close
            Audit Failure: create, delete, rename, set_security, close
      HDFS Authentication: all
              HDFS Keytab: /etc/hdfs.keytab
      HDFS Root Directory: /ifs
          WebHDFS Enabled: Yes
Syslog Forwarding Enabled: No
      Syslog Audit Events: create, delete, rename, set_security
                  Zone ID: 1
```

Multiprotocol (2)

You could have arrived here from:

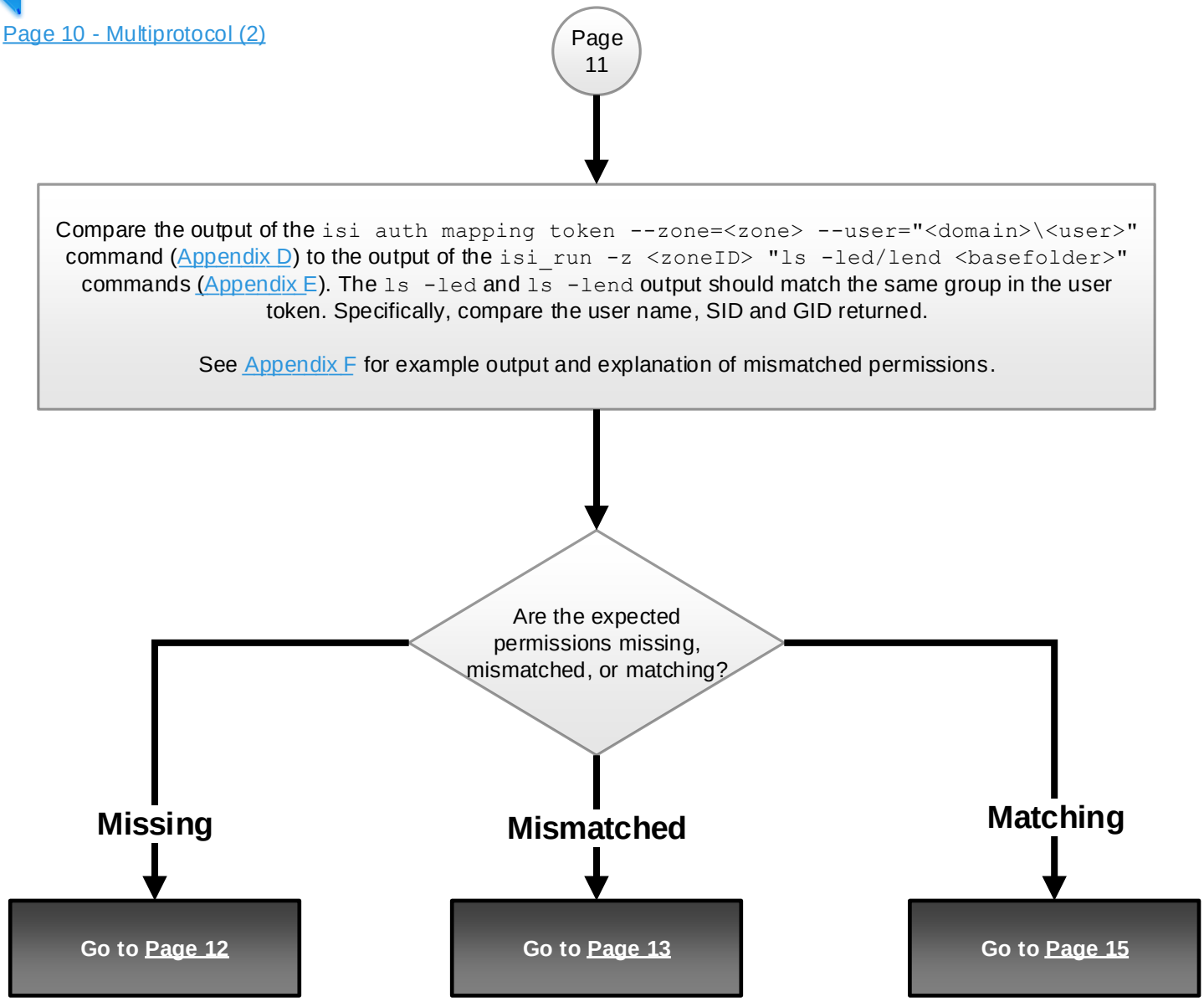
- Page 9 - Multiprotocol



Multiprotocol (3)

You could have arrived here from:

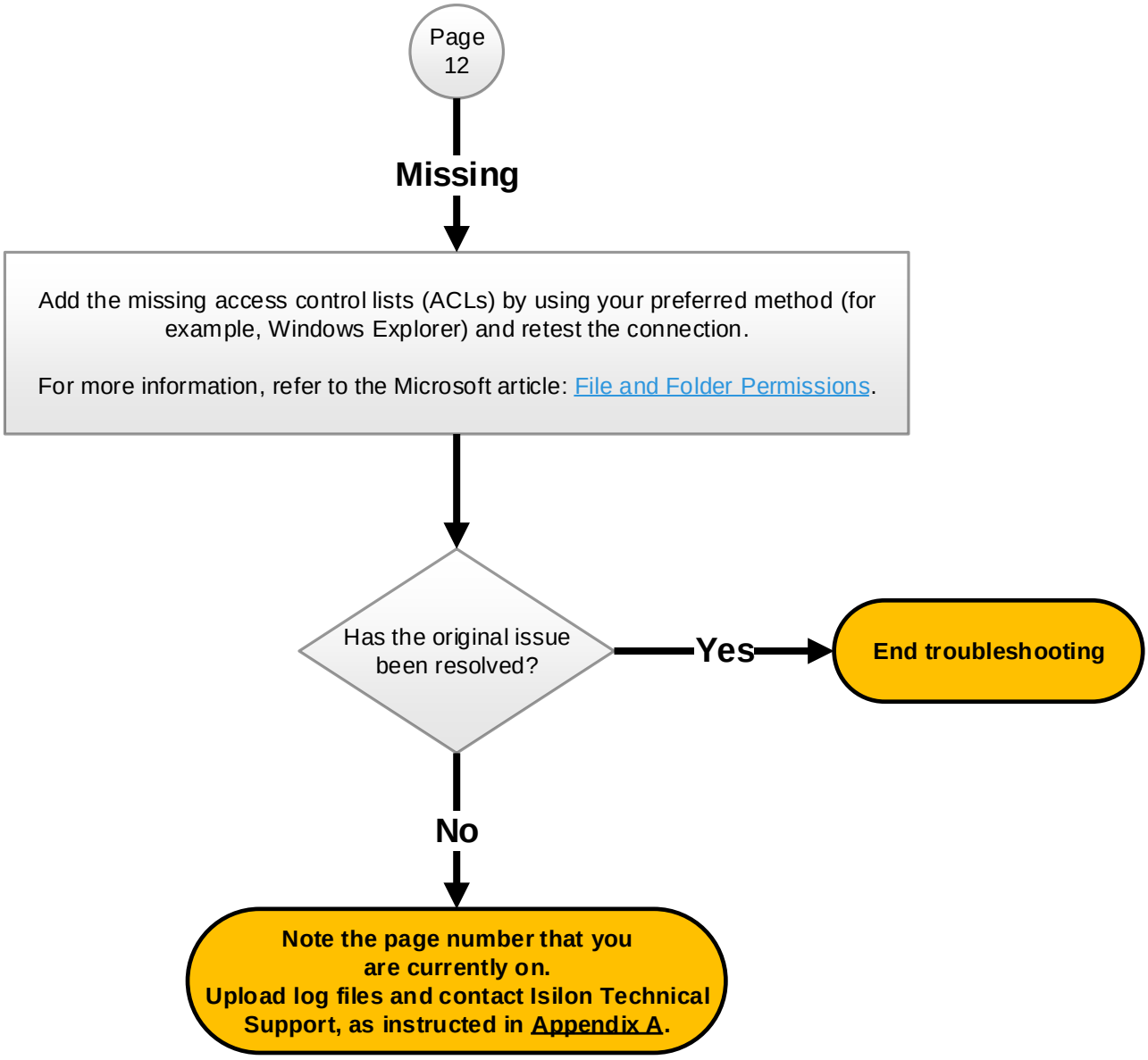
- Page 10 - Multiprotocol (2)



Missing permissions

You could have arrived here from:

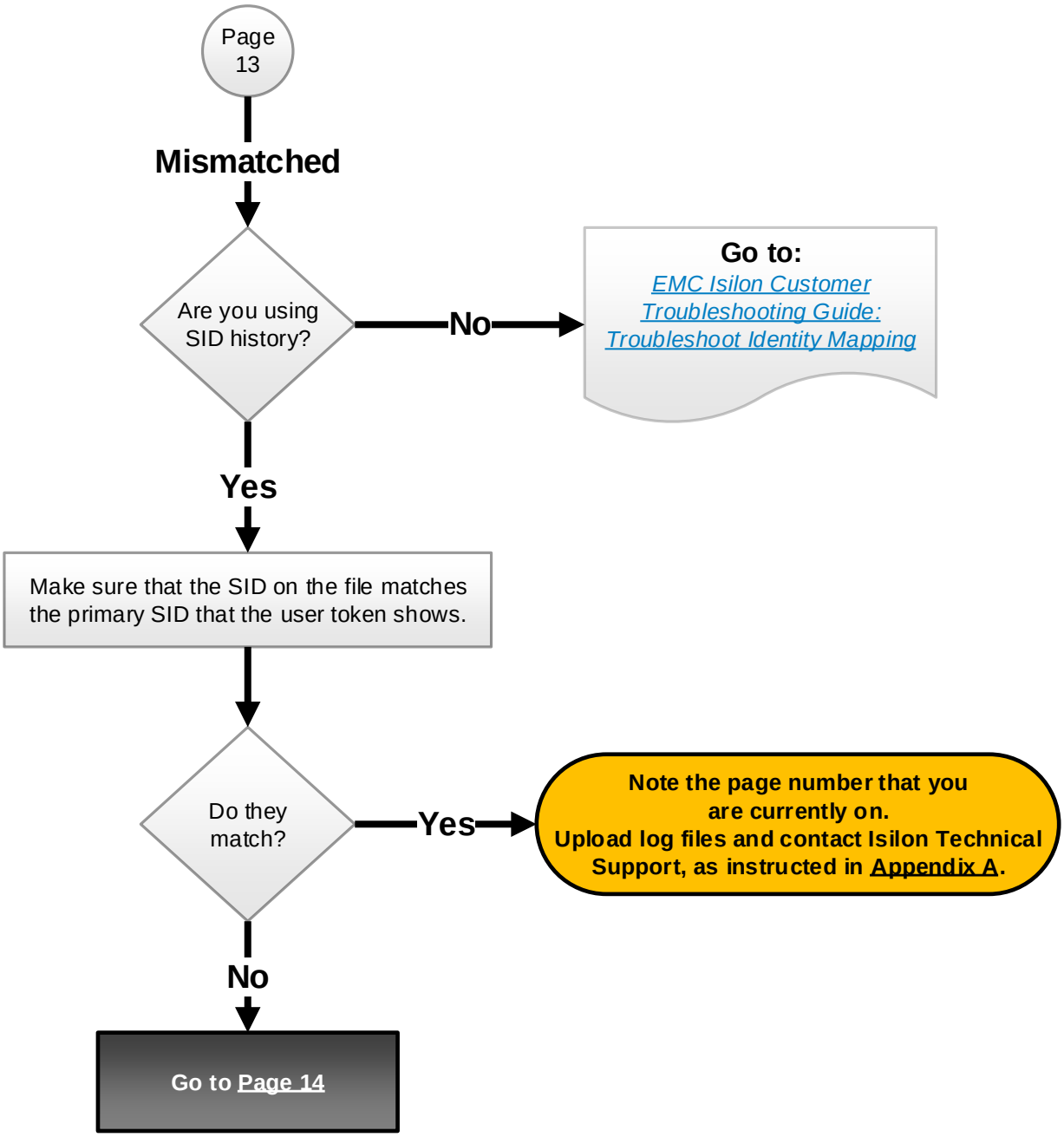
- Page 11 - Multiprotocol (3)



Mismatched permissions

You could have arrived here from:

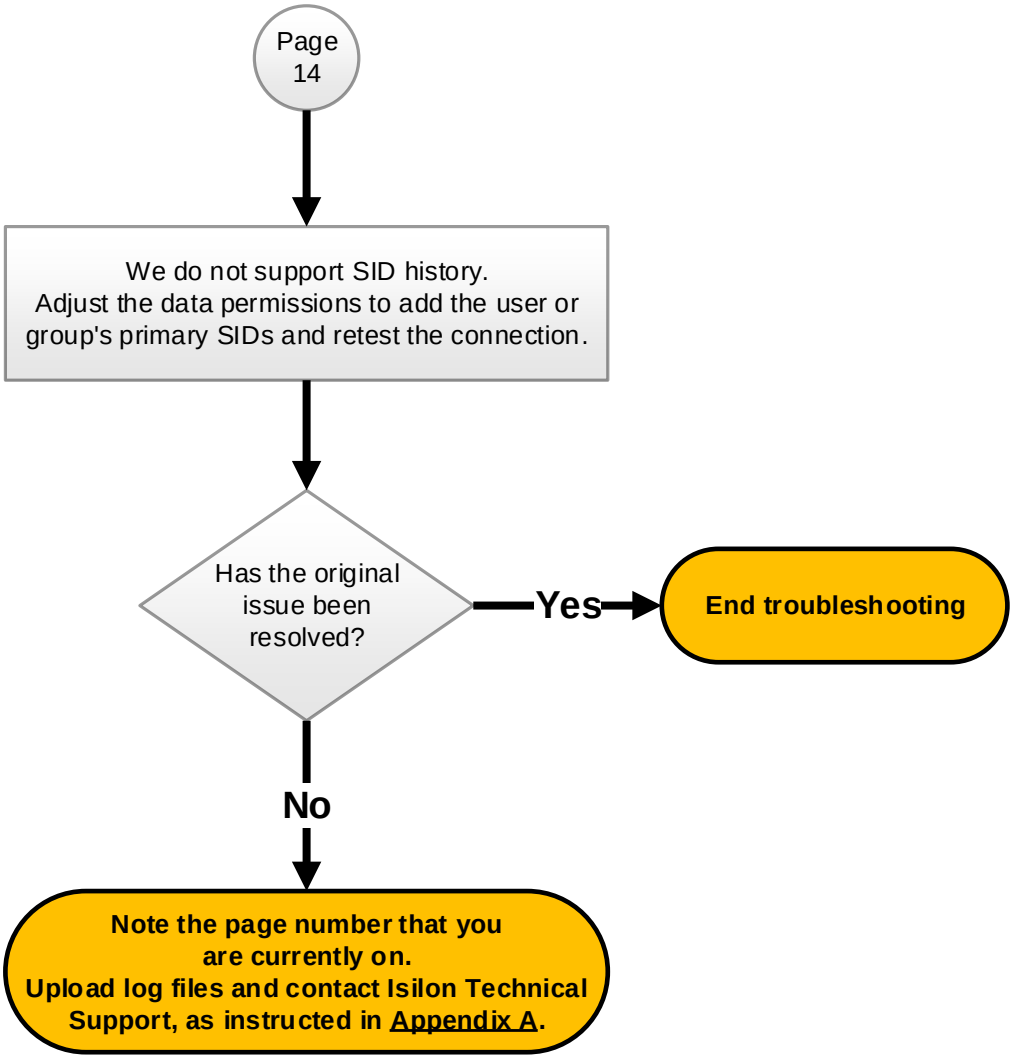
- Page 11 - Multiprotocol (3)



Mismatched permissions (2)

You could have arrived here from:

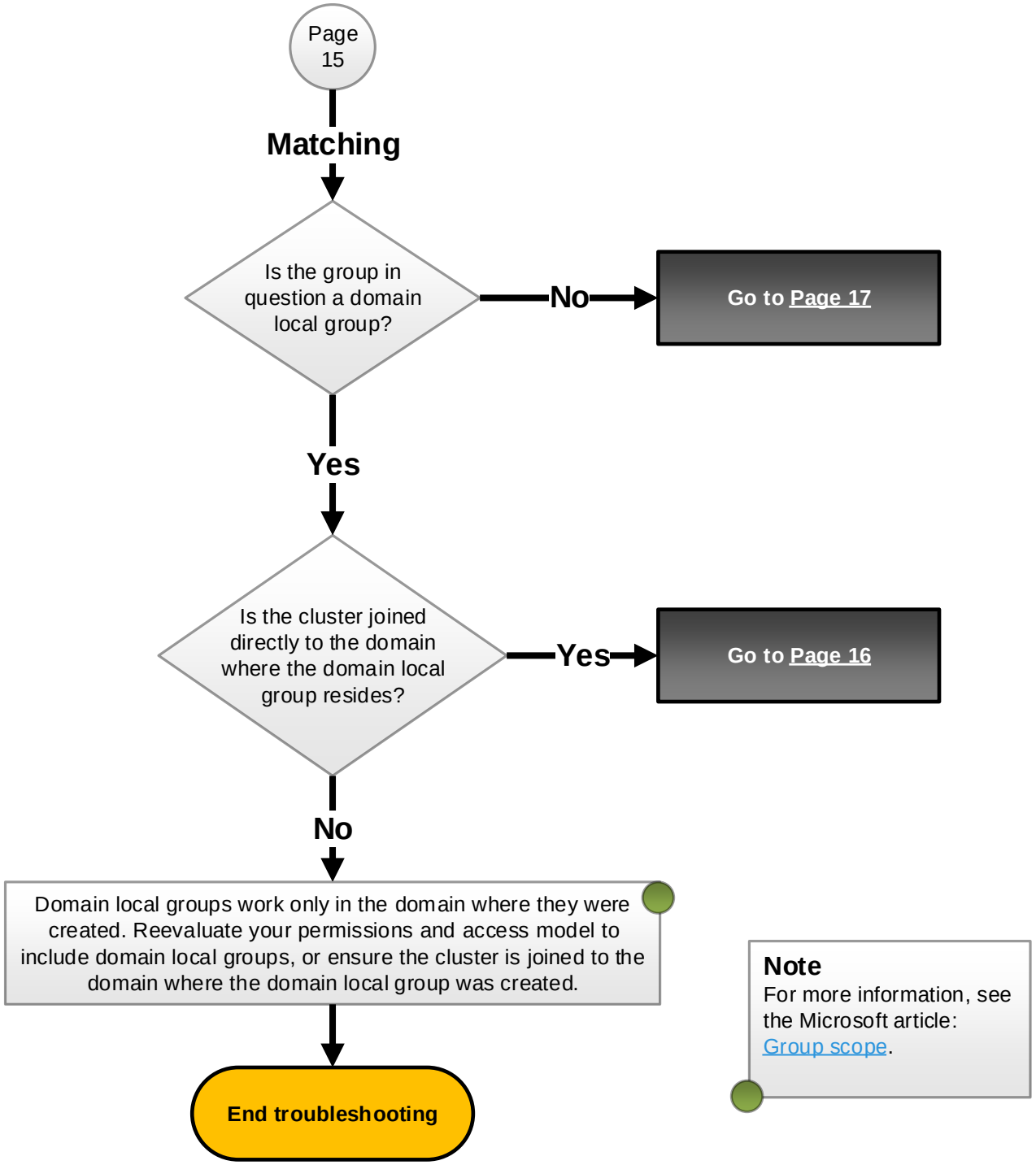
- Page 13 - Mismatched permissions



Matching permissions

You could have arrived here from:

- Page 11 - Multiprotocol (3)

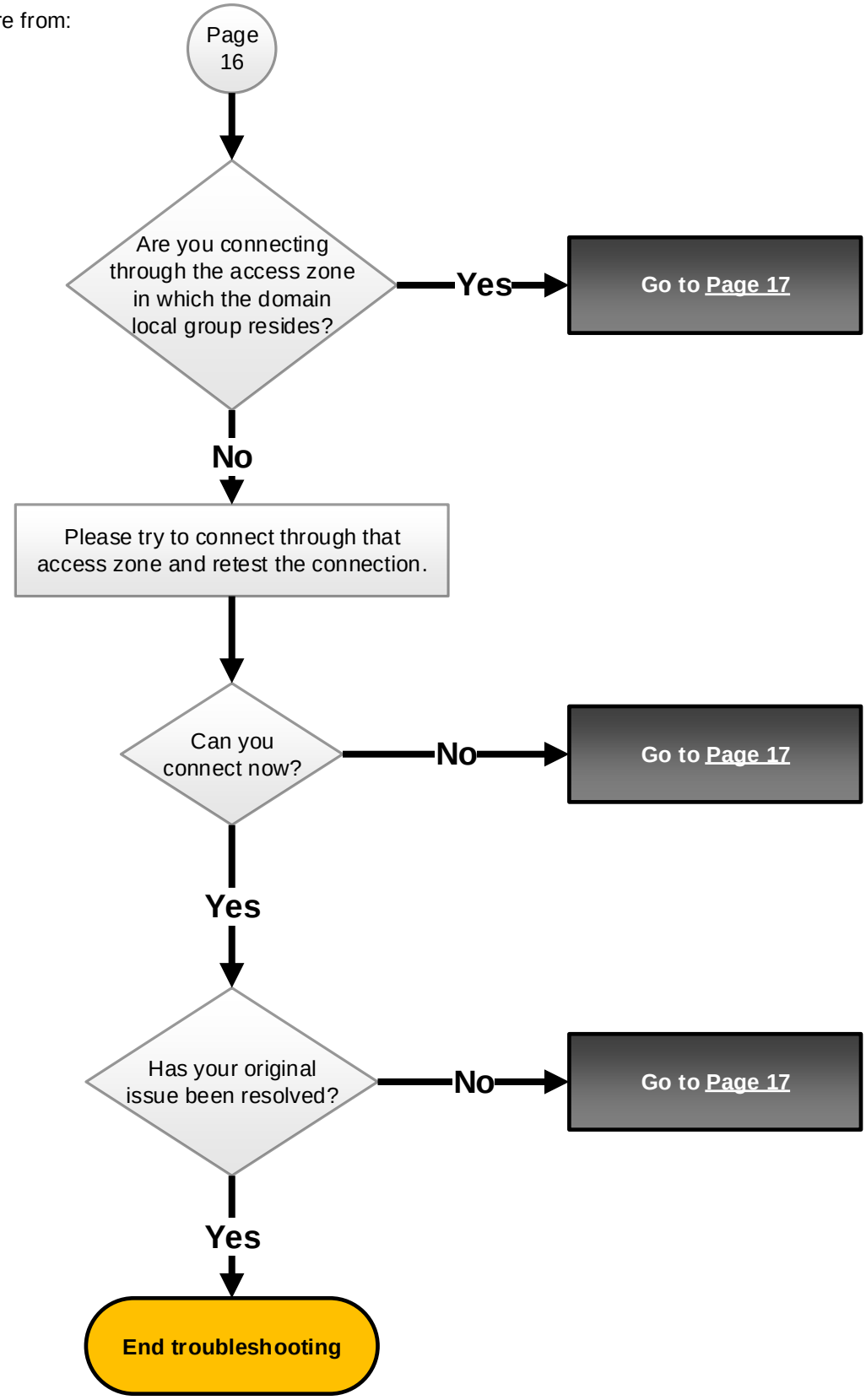


Note
For more information, see the Microsoft article: Group scope.

Multiprotocol (4)

You could have arrived here from:

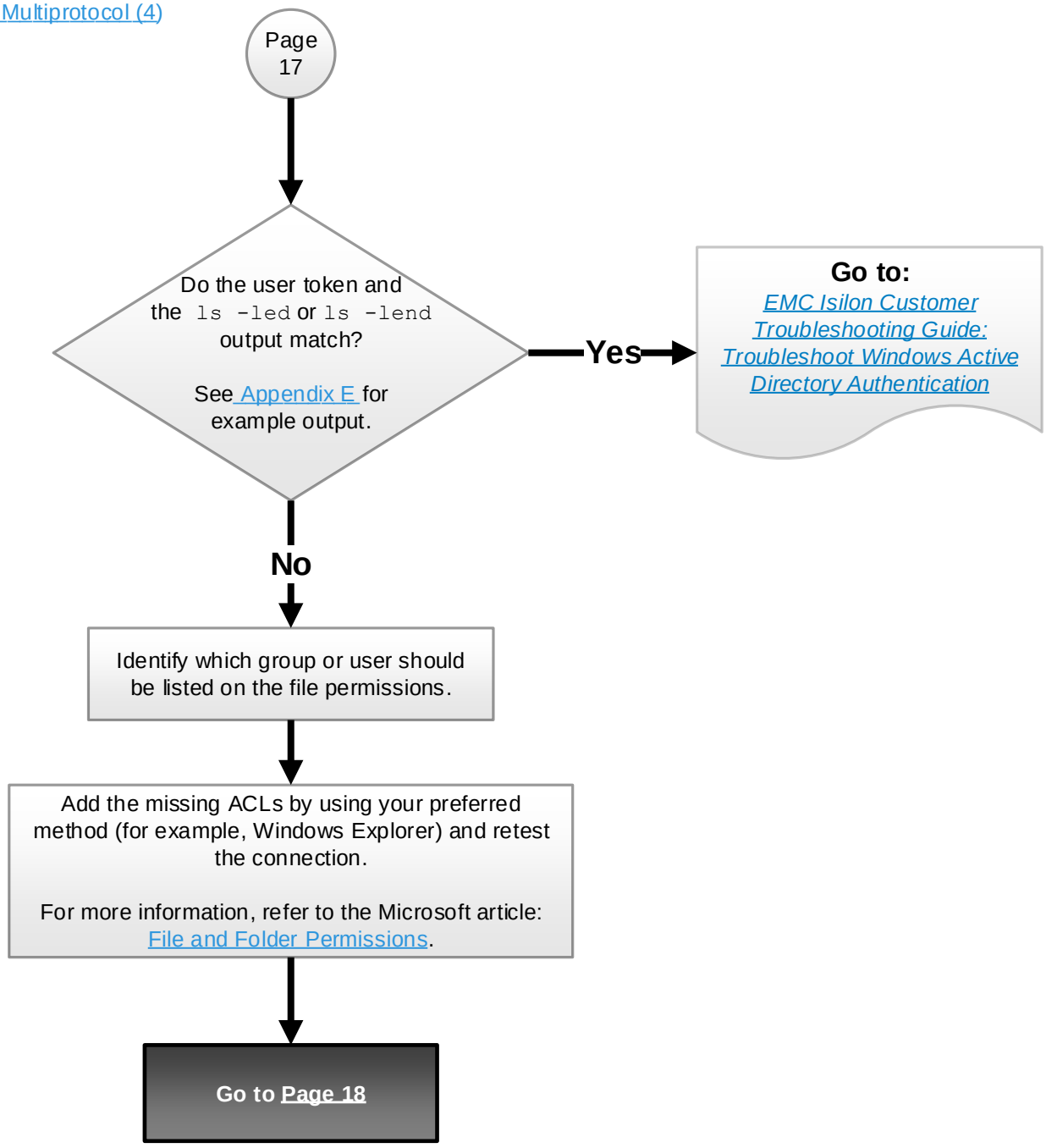
- Page 15 - Matching permissions



Multiprotocol (5)

You could have arrived here from:

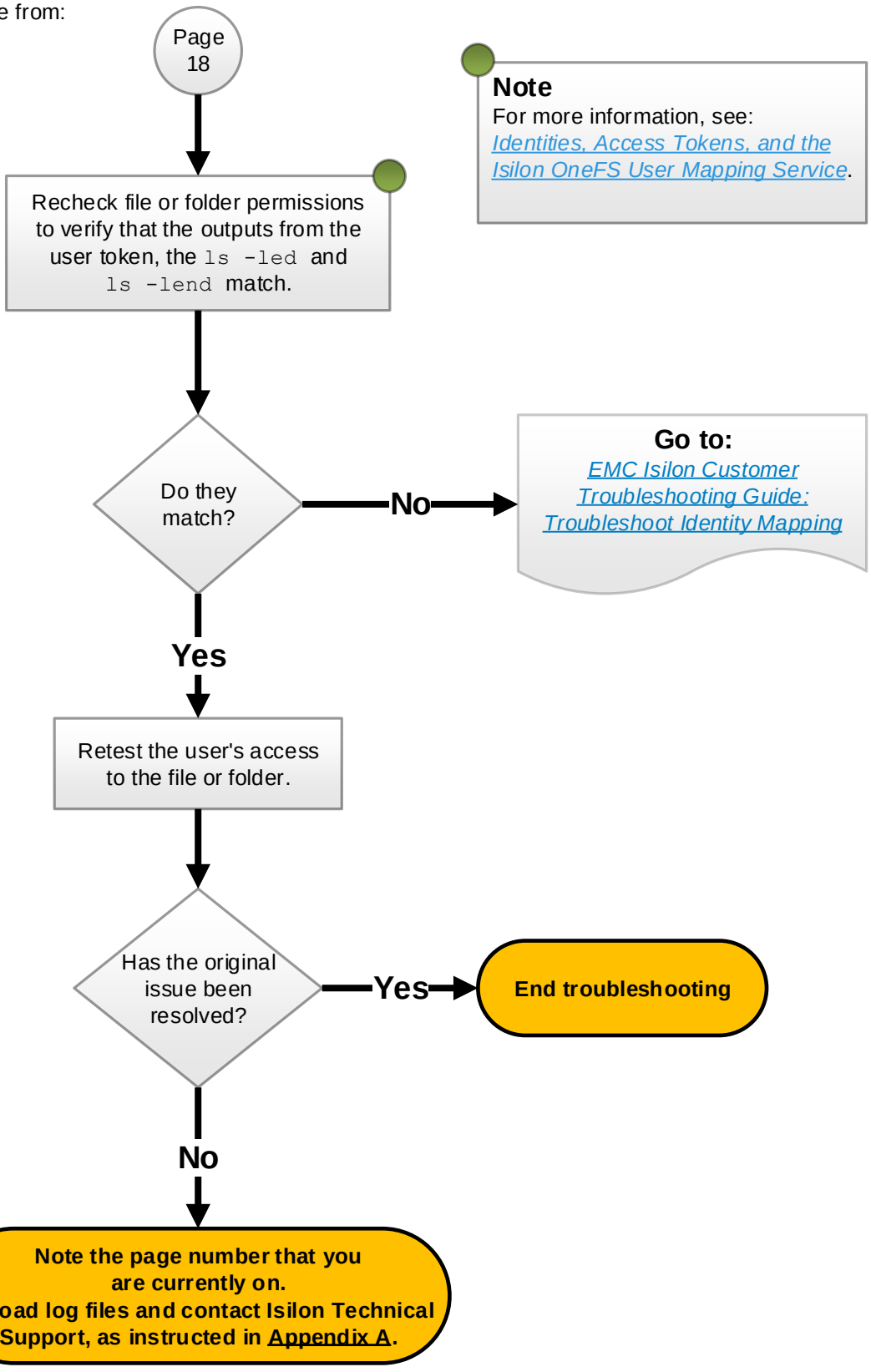
- Page 15 - Matching permissions
- Page 16 - Multiprotocol (4)



Multiprotocol (6)

You could have arrived here from:

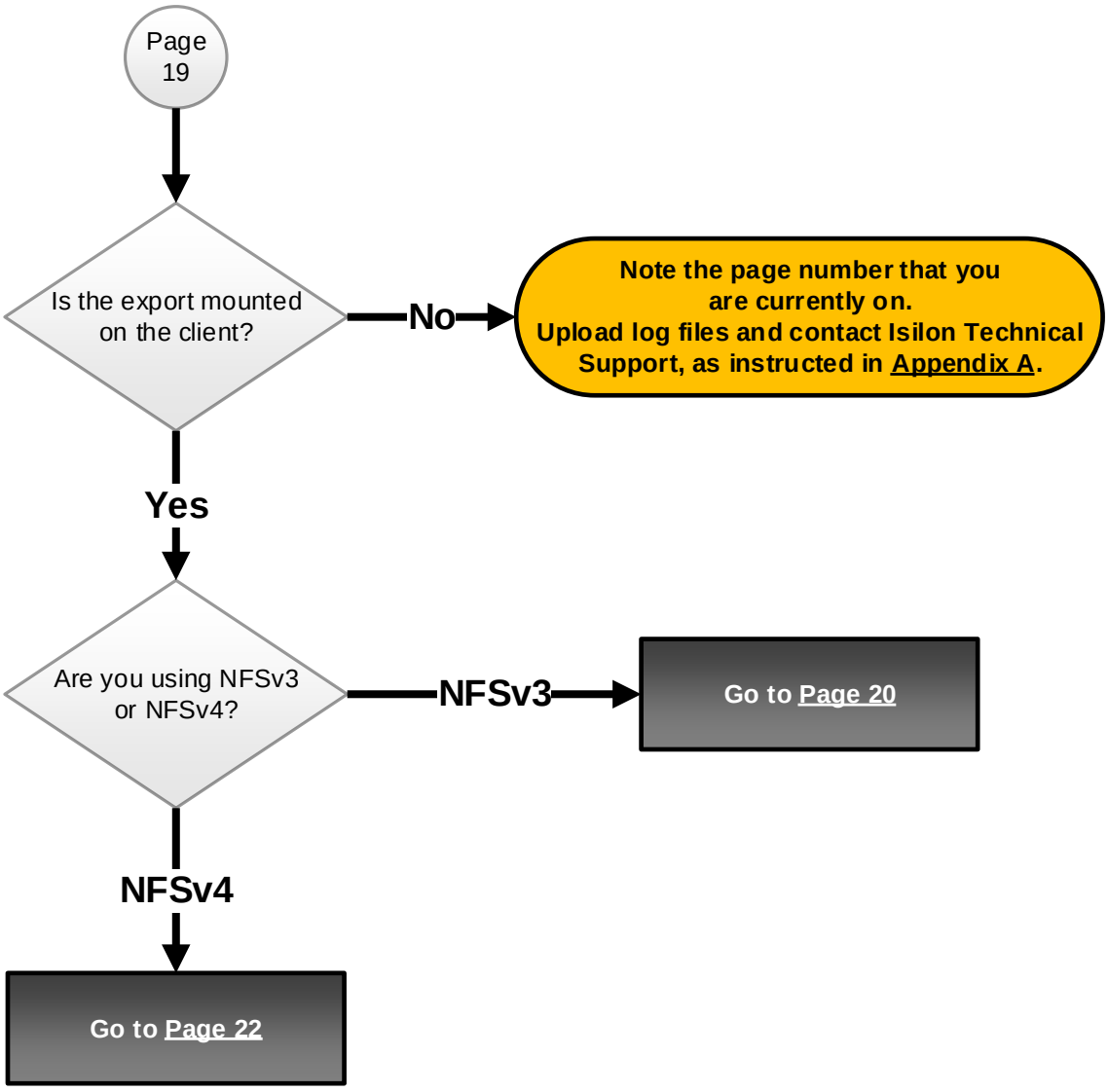
- Page 17 - Multiprotocol (5)



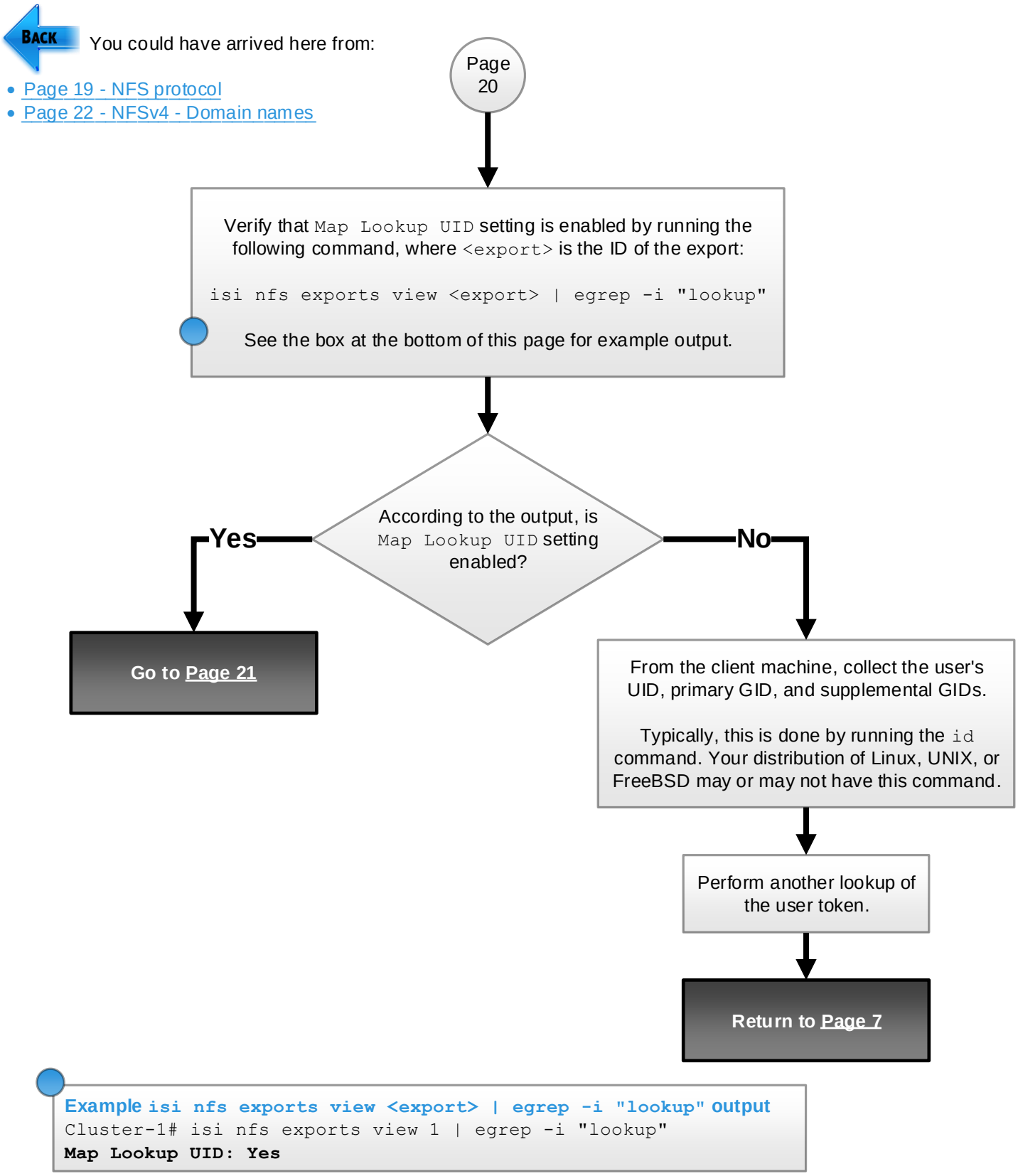
NFS Protocol

You could have arrived here from:

- Page 6 - Protocol



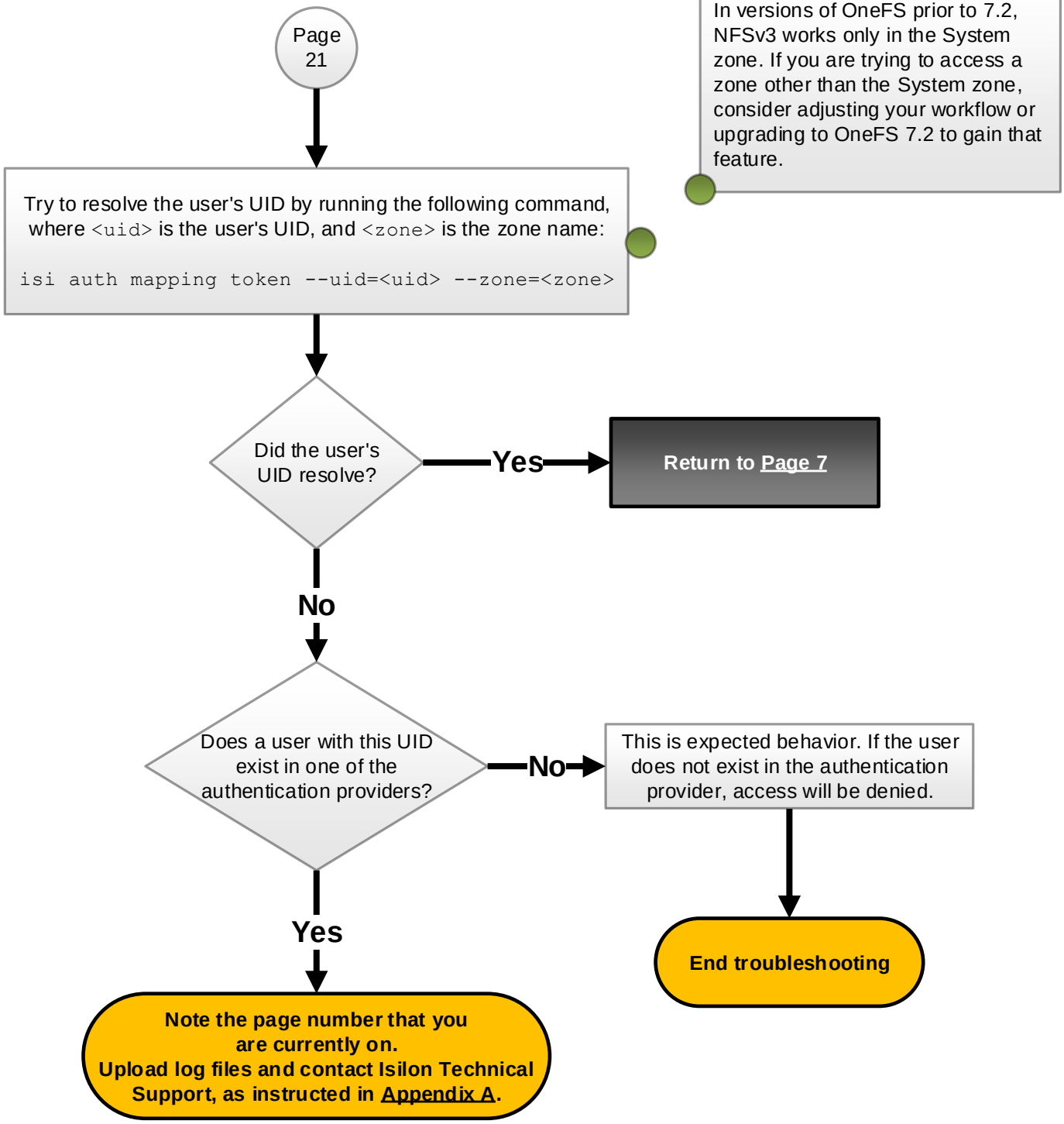
NFS - Map lookup UID



NFS - Resolve user's UID

You could have arrived here from:

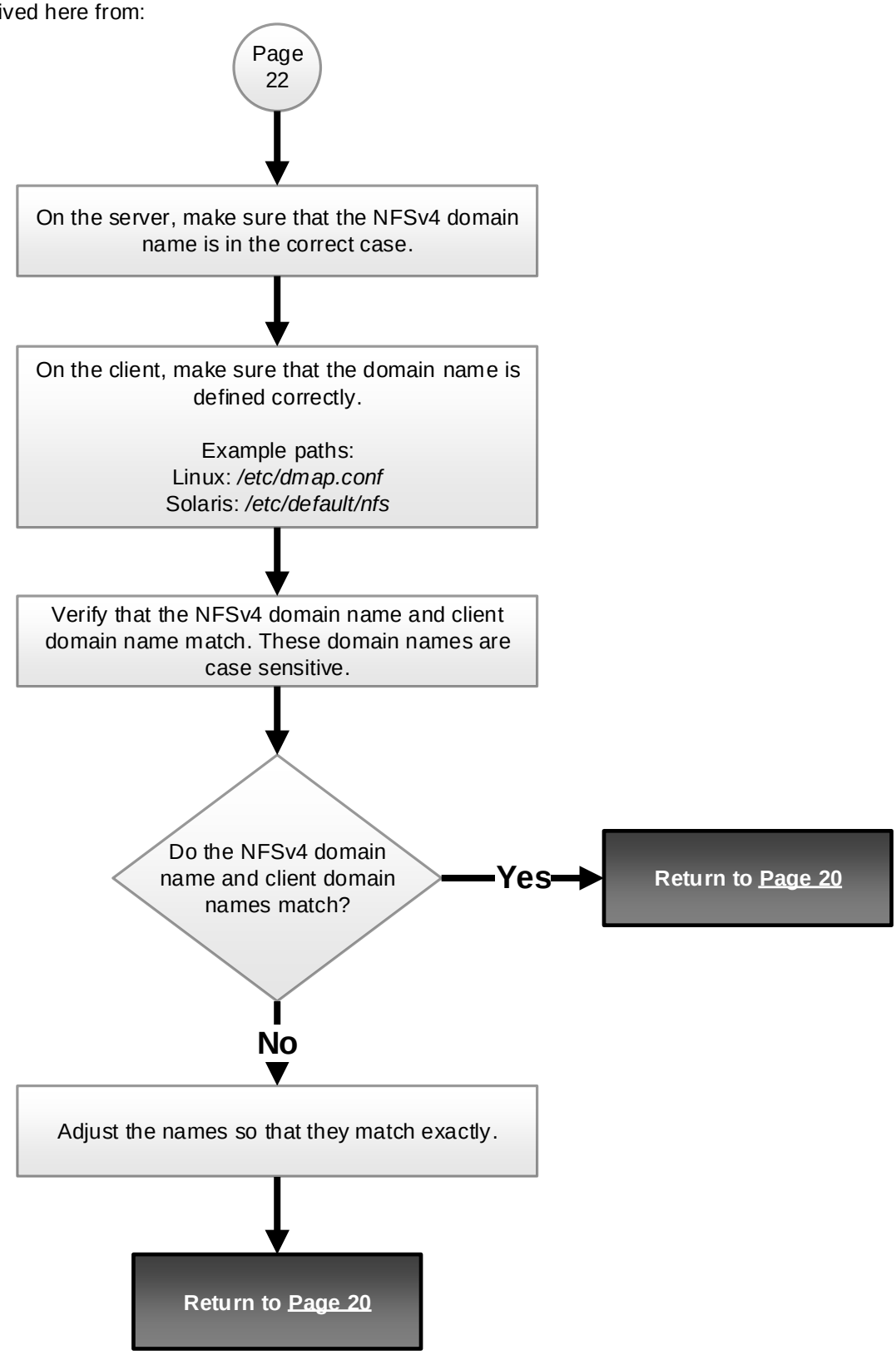
- Page 20 - NFS - Map lookup UID



NFSv4 - Domain names

You could have arrived here from:

- Page 19 - NFS protocol



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.

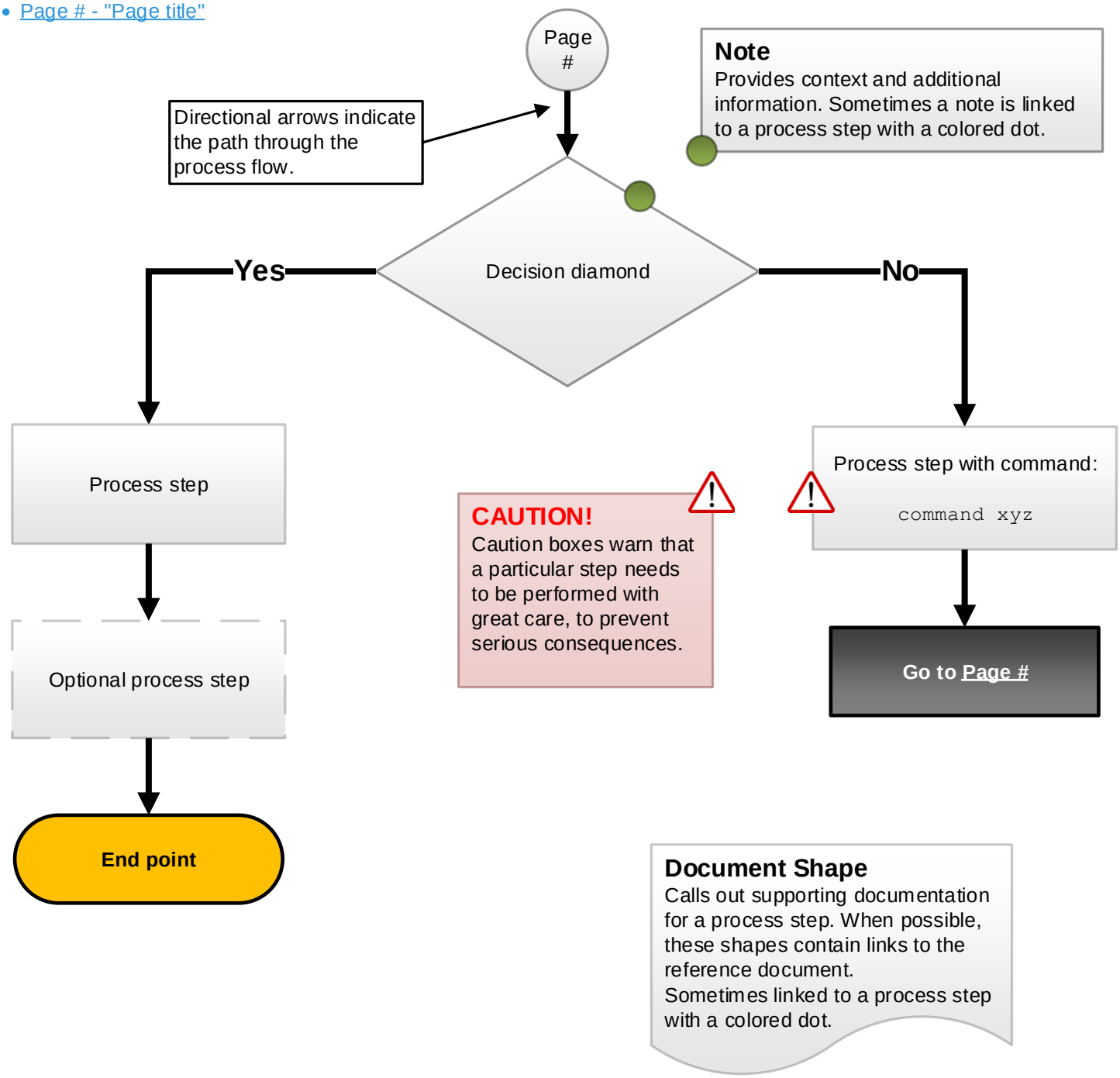
Appendix B: How to use this flowchart

Introduction

Describes what the section helps you to accomplish.

You could have arrived here from:

- Page # - "Page title"



Appendix C: Example output

Example `isi smb shares view --share=<share> --zone=<zone>` output

You could have arrived here from:

- Page 7 - SMB protocol

Example `isi smb shares view --share=<share> --zone=<zone>` output

```
Cluster-1# isi smb shares view --share=testshare --zone=system
                                     Share Name: testshare
                                           Path: /ifs/home
                                    Description:
                        Client-side Caching Policy: manual
Automatically expand user names or domain names: False
Automatically create home directories for users: False
                                      Browsable: True
Permissions:
Account    Account Type    Run as Root   Permission Type   Permission
-------------------------------------------------------------------
Everyone   wellknown       False         allow             read
TestUser   wellknown       False         allow             write
-------------------------------------------------------------------
Total: 1

          Access Based Enumeration: No
Access Based Enumeration Root Only: No
              Allow Delete Readonly: No
               Allow Execute Always: No
                      Change Notify: norecurse
                 Create Permissions: default acl
              Directory Create Mask: 0700
              Directory Create Mode: 0000
                   File Create Mask: 0700
                   File Create Mode: 0100
                     Hide Dot Files: No
                            Host ACL: -
                  Impersonate Guest: never
                   Impersonate User:
                  Mangle Byte Start: 0XED00
                        Mangle Map: 0x01-0x1F:-1, 0x22:-1, [snip]
                   Ntfs ACL Support: Yes
                            Oplocks: Yes
                       Strict Flush: Yes
                     Strict Locking: No
```

Appendix D: Example output

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

You could have arrived here from:

- Page 7 - SMB protocol
- Page 11 - Multiprotocol (3)

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

```
Cluster-1# isi auth mapping token --zone=System --user="TEST\testuser1"
                  User
                      Name: TEST\testuser1
                       UID: 3501
                       SID: S-1-5-21-377814043-3192668432-1337460308-1886
                   On Disk: 3501
                   ZID: 1
                  Zone: System
              Privileges: -
           Primary Group
                      Name: TEST\domain users
                       GID: 1000000
                       SID: S-1-5-21-377814043-319232-133708-513
                   On Disk: S-1-5-21-377814043-319232-133708-513
Supplemental Identities
                      Name: TEST\ad_group-1
                       GID: 1000001
                       SID: S-1-5-21-377814043-319232-1337460308-1887

                      Name: TEST\ad_group-2
                       GID: 1000002
                       SID: S-1-5-21-377814043-319232-1337460308-1888

                      Name: TEST\ad_group-3
                       GID: 1000003
                       SID: S-1-5-21-377814043-319232-1337460308-1889

                      Name: Users
                       GID: 1545
                       SID: S-1-5-32-545

                      Name: Authenticated Users
                       UID: -
                       GID: -
                       SID: S-1-5-11

                      Name: NIS_Group-2
                       GID: 3002
                       SID: S-1-22-2-3002

                      Name: NIS_Group-1
                       GID: 3001
                       SID: S-1-22-2-3001

                      Name: NIS_Group-3
                       GID: 3003
                       SID: S-1-22-2-3003
```

Appendix E: Example output

Example `isi_run -z <zoneID> "ls -led/lend <basefolder>"` output

You could have arrived here from:

- Page 10 - Multiprotocol (2)
- Page 11 - Multiprotocol (3)
- Page 17 - Multiprotocol (5)

Example `isi_run -z <zoneID> "ls -led <basefolder>"` output

```
Cluster-1# isi_run -z 1 "ls -led /ifs"
drwxrwxrwx 5 root  wheel  65 Apr 21 12:01 /ifs
 OWNER: user:root
 GROUP: group:wheel
 SYNTHETIC ACL
 0: user:root allow
dir_gen_read,dir_gen_write,dir_gen_execute,std_write_dac,delete_child
 1: group:wheel allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
 2: everyone allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
```

Example `isi_run -z <zoneID> "ls -lend <basefolder>"` output

```
Cluster-1# isi_run -z 1 "ls -lend /ifs"
drwxrwxrwx 5 0  0  65 Apr 21 12:01 /ifs
 OWNER: user:0
 GROUP: group:0
 SYNTHETIC ACL
 0: user:0 allow dir_gen_read,dir_gen_write,dir_gen_execute,std_write_dac,delete_child
 1: group:0 allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
 2: SID:S-1-1-0 allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
```

Appendix F: Examples of permissions

You could have arrived here from:

- Page 11 - Multiprotocol (3)

Example of a permission that should have matched but shows the wrong identity.

In this example the user is: `TEST\testuser1`, the SID is `S-1-5-21-4087762976-3323327-7495-1118`, and the UID is `1001`.

```
Cluster-1# ls -led multi
-rw-r--r--    1 TEST\testuser1  wheel  0 Sep  4 15:41 multi
OWNER: user:TEST\testuser1
GROUP: group:wheel
SYNTHETIC ACL
0: user:TEST\testuser1 allow file_gen_read,file_gen_write,std_write_dac
1: group:wheel allow file_gen_read
2: everyone allow file_gen_read
```

`TEST\testuser1` exists in AD and LDAP and this is the expected output:

```
Cluster-1# ls -lend multi
-rw-r--r--    1 1001  0  0 Sep  4 15:41 multi
OWNER: user:1001
GROUP: group:0
SYNTHETIC ACL
0: user:1001 allow file_gen_read,file_gen_write,std_write_dac
1: group:0 allow file_gen_read
2: SID:S-1-1-0 allow file_gen_read
```

If the identities were not correctly matched, the output might look like this:

```
Cluster-1# ls -lend multi
-rw-r--r--    1 1001  0  0 Sep  4 15:41 multi
OWNER: SID:S-1-5-21-4087762976-3323327-7495-1118
GROUP: group:0
SYNTHETIC ACL
0: SID:S-1-5-21-4087762976-3323327-7495-1118 allow file_gen_read,file_gen_write,std_write_dac
1: group:0 allow file_gen_read
2: SID:S-1-1-0 allow file_gen_read
```

Continued on next page.

Appendix F: Examples of permissions (2)

You could have arrived here from:

- Page 28 - Appendix F: Examples of permissions

Example of permissions that match but that give the wrong permissions

An extra ACE has been added to the example on the previous page, giving users in TEST\testgroup1 read access. If the expectation was that users in TEST\testgroup1 should be able to write or modify, then this is the wrong permission:

```
Cluster-1# ls -led multi
-rw-r--r-- +  1 TEST\testuser1  wheel  0 Sep  4 15:41 multi
OWNER: user:TEST\testuser1
GROUP: group:wheel
0: group:TEST\testgroup1 allow file_gen_read
1: user:TEST\testuser1 allow file_gen_read,std_write_dac
2: group:wheel allow file_gen_read
3: everyone allow file_gen_read

Cluster-1# ls -lend multi
-rw-r--r-- +  1 1001  0  0 Sep  4 15:41 multi
OWNER: user:1001
GROUP: group:0
0: group:1001 allow file_gen_read
1: user:1001 allow file_gen_read,std_write_dac
2: group:0 allow file_gen_read
3: SID:S-1-1-0 allow file_gen_read
```