

Open Enterprise Server 2018 SP1

Novell Apple Filing Protocol for Linux Administration Guide

February 2019

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Copyright © 2019 Micro Focus Software, Inc. All Rights Reserved.

Contents

About This Guide	7
1 Overview of AFP	9
1.1 Understanding AFP	9
1.1.1 AFP and Universal Password	10
1.2 AFP Features and Capabilities	10
1.3 Limitations	10
1.4 What's Next	11
2 What's New or Changed in AFP	13
2.1 What's New (Update 2 - OES 2018 SP1)	13
2.2 What's New (OES 2018 SP1)	13
2.3 What's New (OES 2018)	13
3 AFP Monitoring and Management	15
3.1 Overview of AFP Monitoring and Management	15
3.2 Using AFP Monitoring and Management	15
3.3 Monitoring Connections	15
3.4 Monitoring Files	16
3.5 Monitoring Configuration Parameters	17
4 Planning and Implementing AFP	19
4.1 Supported Platforms	19
4.2 Requirements	19
4.3 Antivirus Support	19
4.4 Unsupported Service Combinations	20
4.5 What's Next	20
5 Installing and Setting Up AFP	21
5.1 Installing AFP during OES Installation	21
5.2 Installing AFP after OES Installation	23
5.3 Installing AFP NMAS Methods	23
5.3.1 Installing AFP NAMS Methods during a New Installation	23
5.3.2 Installing AFP NAMS during an Upgrade	23
5.3.3 Installing Patches for the AFP NMAS Methods	24
5.4 Verifying the Installation	24
5.4.1 Checking Files and Directories	24
5.4.2 Verifying LSM Installation	25
5.5 What's Next	25
6 Administering the AFP Server	27
6.1 Prerequisite	27
6.2 Selecting a Server to Manage	27

6.3	Configuring General Parameters	28
6.3.1	Security and Rights	28
6.3.2	Threads and Connections	29
6.3.3	Version and Logging	30
6.3.4	Other	31
6.3.5	Subtree Search	31
6.3.6	Rights to a File or Folder	32
6.4	Configuring Volume Details	33
6.4.1	Adding a New Volume Name	34
6.4.2	Editing an Existing Volume Name	34
6.4.3	Deleting a Volume Name	35
6.4.4	Resetting the Desktop	35
6.5	Configuring Context Details	36
6.5.1	Adding a Context	36
6.5.2	Removing a Context	36
7	Migrating AFP to OES 2018 SP1	37
8	Running AFP in a Virtualized Environment	39
9	Configuring AFP with Novell Cluster Services for an NSS File System	41
9.1	Benefits of Configuring AFP for High Availability	41
9.2	Volumes in a Cluster	41
9.2.1	Volume Name Management in a Cluster	42
9.3	Configuring AFP in a Cluster	42
9.3.1	Identifying the Nodes to Host the AFP Service	42
9.3.2	Installing Novell Cluster Services	42
9.3.3	Creating Shared NSS Pools	43
9.3.4	Configuring the Monitoring Script	43
9.3.5	Reviewing Load and Unload Scripts	44
10	Working with Macintosh Computers	47
10.1	Administrator Tasks for Macintosh	47
10.1.1	Configuring a Guest User Account	47
10.1.2	Editing the Volume File	48
10.1.3	Editing the Configuration File	48
10.2	Macintosh End User Tasks	48
10.2.1	Accessing Network Files	49
10.2.2	Logging In to the Network as a Guest	49
10.2.3	Changing Passwords from a Macintosh Computer	49
10.2.4	Changing Expired Passwords from a Macintosh Computer	50
10.2.5	Assigning Rights and Sharing Files from a Macintosh Computer	50
11	Monitoring the AFP Server	53
11.1	Understanding the Monitoring Process	53
11.2	Enabling Monitoring	53
11.3	Viewing Logs through iManager	53
11.4	Understanding Performance Parameters	54
12	Auditing the AFP Server	55
12.1	Understanding the Auditing Process	55
12.2	Enabling Auditing	55

12.3	Viewing Auditing Information	56
13	Troubleshooting AFP	57
13.1	Known Issues	57
13.1.1	AFP Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured	57
13.1.2	AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit	58
13.1.3	Owner's Name Not Displayed in the Macintosh Client	58
13.1.4	File Level Trustees Are Deleted When a File is Modified	58
13.1.5	AFP Does Not Support DST Shadow Volumes	59
13.2	AFP Login Issues	59
13.2.1	Cannot See the Login Dialog Box	59
13.2.2	AFP User Login to a Macintosh 10.5 Client Fails With a "Connection Failed" Error	59
13.2.3	Invalid Username and Password Error	59
13.2.4	Cleartext Authentication Fails on Mac Clients	59
13.2.5	One-Way or Two-Way Random Exchange Authentication Fails on Mac Clients	60
13.2.6	Enabling Authentication Mechanisms for a Mac 10.7 Client	60
13.3	Starting the AFP Server	60
13.3.1	Starting the AFP Daemon Failed	60
13.4	File Creation	60
13.4.1	Failure to Create a File on a Macintosh Client	60
13.5	Displaying Volumes	61
13.5.1	Volumes Tab on a Macintosh 10.4 Client Displays an Empty Volume List	61
13.6	Log Messages	61
13.6.1	NWDSResolveName failed to resolve supplied name <user name>	61
13.6.2	zOpen on volume <VOLUME_NAME> failed	61
13.6.3	zAFPCountByScanDir: scandir failed	61
13.7	AFP Server Responds Slowly	61
13.8	Operation Fails When a Macintosh Client Mounts an NSS Volume and Opens Files	62
13.9	Hard Links are Broken When Files Are Accessed from an AFP Mount Point	62
13.10	AFP Subtree Search Fails	62
13.11	Cannot Access an AFP Share by Using an Alias	62
14	Security Guidelines for AFP	63
14.1	Recommended Authentication Protocol	63
14.2	Storing Credentials	63
14.3	Intruder Detection	63
14.4	Timeout Values	64
A	Command Line Utilities for AFP	65
A.1	novafp	65
A.2	afpdreset	65
A.3	afpstat	66
A.4	afptcpd	66
A.5	afpbinding	66
A.6	afpnames	66
A.7	migafp	67
B	Comparing AFP on NetWare and AFP on Linux	69

About This Guide

This guide describes how to use the Novell Apple Filing Protocol (AFP) service on a Open Enterprise 2018 SP1 server to access and manage Macintosh systems.

This guide is divided into the following sections:

- ♦ Chapter 1, “Overview of AFP,” on page 9
- ♦ Chapter 2, “What’s New or Changed in AFP,” on page 13
- ♦ Chapter 3, “AFP Monitoring and Management,” on page 15
- ♦ Chapter 4, “Planning and Implementing AFP,” on page 19
- ♦ Chapter 5, “Installing and Setting Up AFP,” on page 21
- ♦ Chapter 6, “Administering the AFP Server,” on page 27
- ♦ Chapter 7, “Migrating AFP to OES 2018 SP1,” on page 37
- ♦ Chapter 8, “Running AFP in a Virtualized Environment,” on page 39
- ♦ Chapter 9, “Configuring AFP with Novell Cluster Services for an NSS File System,” on page 41
- ♦ Chapter 10, “Working with Macintosh Computers,” on page 47
- ♦ Chapter 11, “Monitoring the AFP Server,” on page 53
- ♦ Chapter 12, “Auditing the AFP Server,” on page 55
- ♦ Chapter 13, “Troubleshooting AFP,” on page 57
- ♦ Chapter 14, “Security Guidelines for AFP,” on page 63
- ♦ Appendix A, “Command Line Utilities for AFP,” on page 65
- ♦ Appendix B, “Comparing AFP on NetWare and AFP on Linux,” on page 69

Audience

This document is intended for network administrators. It is not intended for users of the network.

Documentation Updates

For the most recent version of the *Novell AFP for Linux Administration Guide*, see the [Open Enterprise Server 2018 SP1 documentation](#).

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with OES. Please use the User Comment feature at the bottom of each page of the OES 2018 SP1 online documentation.

1 Overview of AFP

Novell Apple Filing Protocol (AFP) for Linux operating systems is provided with Open Enterprise Server (OES) 2 SP1 and later versions. AFP is a network protocol that offers file services for Macintosh clients. OES currently supports AFP version 3.1.

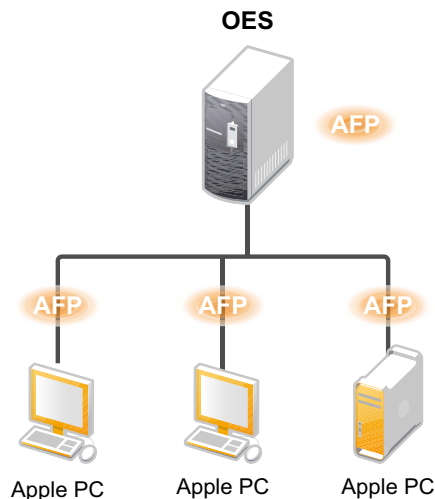
- [Section 1.1, “Understanding AFP,” on page 9](#)
- [Section 1.2, “AFP Features and Capabilities,” on page 10](#)
- [Section 1.3, “Limitations,” on page 10](#)
- [Section 1.4, “What’s Next,” on page 11](#)

1.1 Understanding AFP

AFP (Apple Filing Protocol) lets Macintosh workstations access and store files on OES server without installing any additional software. The AFP software is installed as part of OES and provides out-of-the-box network access. Join the Macintosh computer to your enterprise network to access files on the OES server.

Novell AFP enables the Linux server to use the same protocol as the client workstation to copy, create, delete, move, save, and open files on a Macintosh workstation.

Figure 1-1 Novell AFP Overview



Macintosh users can use Chooser or the Go menu to access network files and even create aliases. The native protocols that run on a Linux server enable the users to seamlessly copy, delete, move, create, save, and open network files—just like they do when they work locally.

AFP also provides integration with NetIQ eDirectory. Consolidation of user management through eDirectory simplifies network administration. All users who need access to the network are represented in eDirectory through user objects, which enables you to easily and effectively assign trustee rights, control access, and manage all user objects from a single location on the network.

IMPORTANT: Novell AFP is currently supported only on the NSS file system. It can be used for accessing files on NSS volumes.

1.1.1 AFP and Universal Password

Universal Password helps to manage password-based authentication schemes. Each AFP user must be Universal Password enabled to be able to log in to the AFP server.

The Universal Password is not enabled by default.

For details on Universal Password, see [Novell Password Management](#).

1.2 AFP Features and Capabilities

AFP has many features that can help you manage users, workstations, and networks.

- ♦ AFP parameter configuration and administration through iManager. For more information, see [Chapter 6, “Administering the AFP Server,” on page 27](#).
- ♦ Support for Macintosh OS 10.12 and later.
- ♦ Integration with NetIQ eDirectory.
- ♦ Migration capability from NetWare to SUSE Linux Enterprise Server. For more information, see [Chapter 7, “Migrating AFP to OES 2018 SP1,” on page 37](#).
- ♦ Cross-protocol file locking support between AFP, CIFS, and NCP. For more information, see “[Configuring Cross-Protocol File Locks for NCP Server](#)” in the *OES 2018: SP1 NCP Server for Linux Administration Guide*.
- ♦ Auditing support for file operations and changes to AFP configuration. For more information, see [Chapter 12, “Auditing the AFP Server,” on page 55](#).
- ♦ Support for using the Bonjour protocol for the AFP service discovery.
- ♦ Auditing and Monitoring support. The Auditing framework helps you to monitor the authentication process and the Monitoring framework helps you assess the performance of the AFP server. For more information, see [Chapter 12, “Auditing the AFP Server,” on page 55](#) and [Chapter 11, “Monitoring the AFP Server,” on page 53](#).
- ♦ Support for Unicode filenames.
- ♦ Support for Universal Passwords longer than 8 characters.
- ♦ Clustering support for high availability. For more information, see [Chapter 9, “Configuring AFP with Novell Cluster Services for an NSS File System,” on page 41](#).
- ♦ Support for subtree searching. For more information, see [Section 6.3.5, “Subtree Search,” on page 31](#)

1.3 Limitations

- ♦ If you restart eDirectory, ensure that you restart the AFP service by using the `rcnovell-afptcpd restart` command or through iManager.

- ♦ When you map the NSS volume with ZID value greater than the 32-bit limit (0xffffffff), AFP users might experience abnormal behavior while performing the file operations on that volume. For more information, see [Section 13.1.2, “AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit,”](#) on page 58.
- ♦ The following table illustrates the limitations associated with using dot notation in login names.

Login with	Example	Supported
Dot in user name component	juan.garcia	Yes
Full context without dot in user name component	juangarcia.users.novell	Yes
Full context with dot in user name component	juan.garcia.users.novell	No
Partial context without dot in user name component	juangarcia.users	No
Partial context with dot in user name component	juan.garcia.users	No

1.4 What’s Next

For information on new features in this release of AFP see, [Chapter 2, “What’s New or Changed in AFP,”](#) on page 13

2 What's New or Changed in AFP

This section describes enhancements and changes to AFP from Micro Focus Open Enterprise Server (OES) 2018.

2.1 What's New (Update 2 - OES 2018 SP1)

Before OES 2018 SP1 (Update 2) patch, when you access the NSS volume with ZID value greater than the 32-bit limit using AFP, users might experience abnormal behavior while performing the file operations on that volume because of Apple Filing Protocol (AFP) limitation. Beginning with this patch, few commands are introduced in `nss` utility to restrict the ZID value from crossing the 32-bit limit.

For more information, see [AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit](#) in the [OES 2018 SP1: Novell AFP for Linux Administration Guide](#).

2.2 What's New (OES 2018 SP1)

AFP in OES 2018 SP1 has been modified for bug fixes. There are no new features or enhancements in OES 2018 SP1.

2.3 What's New (OES 2018)

AFP in OES 2018 has been modified for bug fixes. There are no new features or enhancements in OES 2018.

3 AFP Monitoring and Management

In the Open Enterprise Server, the command line novafp utility lets you manage open files and AFP connections.

3.1 Overview of AFP Monitoring and Management

You can close connections that are stale and persistent. With the file monitoring options, you can view details of open files and close open files within a volume, by connection, and file handles associated with a file.

3.2 Using AFP Monitoring and Management

novafp - A command line utility to configure, monitor, and manage the AFP service (**afptcpd** daemon). To run the **novafp** utility from the command line, the user must log in as root.

To know more about various options provided, enter **man novafp** at the command prompt.

You can also monitor and manage AFP service using the **Manage AFP Services** menu option provided in NRM.

3.3 Monitoring Connections

Table 3-1 Connection Monitoring command options

Option	Description
-Cl, --Conn --list	Lists all active connections.
-C, --Conn	Displays the consolidated list of active and expired connections.
-Cn CONNECTION_ID, --Conn --connection CONNECTION_ID	Displays details of the specified connection number. The Privileges field displaying Supervisor for the logged in user implies that the user has Supervisor privileges for Entry Rights over NCP Server object. The user with such privileges gets full access to all the mounted volumes irrespective of user rights at file system level.
-Clx, --Conn --list --exp	Lists all expired connections. A session is called an expired session if there is no request/response packet flow (not even a keep-alive request DSI Tickle) between the server and the client for 2 minutes. Normally expired sessions are cleared by the server at intervals specified by the RECONNECT_PERIOD configuration parameter.

Option	Description
-Ccn CONNECTION_ID, --Conn --clear CONNECTION_ID	Closes the connection with the specified connection number.

By querying or listing all open connections you can find how many sessions are opened at any moment. The details include session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received.

You can also drill down to extract per-connection details such as the group the user is a member of.

If the connections are stale and persistent, for example, and if there is no activity for a considerable amount of time, this session occupies a considerable amount of memory. If this happens, you can close the connection/session based on the qualitative analysis of various connection parameters dumped by the new commands and options.

IMPORTANT: Closing a connection by using this utility can leave the associated open files in an incomplete state, so use this command sparingly.

3.4 Monitoring Files

Table 3-2 File Monitoring command options

Option	Description
-Flv VOLUME_NAME, --Files --list --volume VOLUME_NAME	Lists all open files by the specified volume. NOTE: Listing all files on a volume is a time-consuming operation if too many files are open, so use this option sparingly.
-Fln CONNECTION_ID, --Files --list -- connection CONNECTION_ID	Lists files opened by the user session with the specified connection number.
-Flp FILE_PATH, --Files --list --path FILE_PATH	Lists users who opened the file with the specified file path.
-FCv VOLUME_NAME, --Files --Close -- volume VOLUME_NAME	Closes all open files with the specified volume.
-FCn CONNECTION_ID, --Files --Close -- connection CONNECTION_ID	Closes the files opened by the user session with the specified connection number.
-FCp FILE_PATH, --Files --Close --path FILE_PATH	Closes the file with the specified file path.
-Vl, --Vols --list	Lists all AFP configured volumes.
-Va VOLUME_NAME:ALIAS_NAME, --Vols --add VOLUME_NAME:ALIAS_NAME	Add or modify entries in volume configuration file. An alias name is optional.

You use the file listing options to view the following:

- ♦ All open files within a particular volume
- ♦ All open files by connection
- ♦ All users who have open file handles for a particular file

You use the file closing options to close the following:

- ♦ All open files within a particular volume
- ♦ All open files by a particular connection
- ♦ All open file handles associated with a particular file

If a user tries to perform any operation on an open file that was closed by using this utility, the changes might appear next time the file is opened. This depends on the application. The data that was saved before the file was closed will be intact.

IMPORTANT: This is not the recommended way to close files. It is provided as a tool to administrators to force close open files.

3.5 Monitoring Configuration Parameters

Use the following commands to set a particular configuration parameter of AFP:

Table 3-3 Configuration Parameters Monitoring command options

Option	Description
<code>-o, --conf-params</code>	Lists all AFP configuration parameters. If you change the AFP server parameters through iManager, reload the AFP service by running <code>rcnovell-afptcpd reload</code> command before you run <code>novafp -o</code> or <code>novafp --conf-params</code> command options.
<code>--uam=cleartext random two-way DHX DHX2</code>	Sets an authentication method. The default authentication mode is DHX2.
<code>--minthreads=NO_OF_THREADS</code>	Sets the minimum number of threads that should be set for the <code>afptcpd</code> daemon to start. The number should be between 3 and 32. The default value is 3.
<code>--maxthreads=NO_OF_THREADS</code>	Sets the maximum number of threads. The number should be between 4 and 512. The default value is 32.
<code>--recon=NO_OF_MINUTES</code>	Sets the number of minutes the AFP server waits before attempting to reconnect. The minimum waiting time is 2 minutes and can extend to 1440 minutes. The default value is 1440 minutes.
<code>--afp-version=2.2 3.0 3.1 ALL</code>	Sets the AFP versions that the AFP server can support. The default value is All.
<code>-r all default no, --rights=all default no</code>	Sets the sharing rights. The default option is no.
<code>--log=no status debug error all</code>	Sets the log levels for the AFP server to log messages.
<code>-g yes no, --guest-login=yes no</code>	Allows guest login.
<code>-U USER_NAME, --guest-user=USER_NAME</code>	Sets a guest user name.
<code>-w yes no, --no-manage-world-rights=yes no</code>	Enables or disables No Manage World Rights.

Option	Description
<code>--audit=yes no</code>	Enables or disables the AFP server to audit and log authentication process and configuration parameters changes.
<code>-e yes no, --export-all-volumes=yes no</code>	Enables or disables NSS volume export.
<code>-s yes no, --subtree-search=yes no</code>	Enables or disables subtree search. By default, this option is disabled.

4 Planning and Implementing AFP

This section describes requirements and guidelines for using the Apple Filing Protocol (AFP) for Open Enterprise Server (OES).

- ♦ [Section 4.1, “Supported Platforms,” on page 19](#)
- ♦ [Section 4.2, “Requirements,” on page 19](#)
- ♦ [Section 4.3, “Antivirus Support,” on page 19](#)
- ♦ [Section 4.4, “Unsupported Service Combinations,” on page 20](#)
- ♦ [Section 4.5, “What’s Next,” on page 20](#)

4.1 Supported Platforms

Macintosh 10.12 or later

4.2 Requirements

- ♦ The install administrator must have Compare, Read, and Write right on ACL Attribute to add the Common Proxy user as a trustee of AFP user contexts selected at the time of installation.
- ♦ The AFP proxy user must have inheritable Read and Compare rights on CN attribute of user contexts.
- ♦ The AFP administrator must have Compare, Read, and Write rights on ACL Attribute of user contexts being added for authentication.
- ♦ If your eDirectory replica is stored on an eDirectory server earlier than 8.8.3, make sure that you upgrade the server by using the [Security Services 2.0.6 patch](#).
- ♦ The AFP server requires at least one Read/Write replica in an eDirectory tree with NMAS version 3.2 or later.
- ♦ Ensure that the Novell AFP NMAS method is installed and synchronized across the eDirectory tree:
 1. Install `novell-afp-nmasmethods.rpm`.
 2. Execute the `/opt/novell/afptcpd/bin/install_afp_lsm.sh` script.

For more information on installing AFP NMAS methods during a new installation or an upgrade , see [Section 5.3, “Installing AFP NMAS Methods,” on page 23](#).

4.3 Antivirus Support

The Apple Filing Protocol (AFP) support for NSS files is implemented via a technology that bypasses the real-time scanning employed by most OES antivirus solutions.

To protect NSS files that are shared through an AFP connection, set up an antivirus solution that supports on-demand scanning on the OES server, or real-time and on-demand scanning on the Apple client.

4.4 Unsupported Service Combinations

Do not install any of the following service combinations on the same server with Novell AFP. Although the combinations might not cause pattern conflict warnings, Micro Focus does not support any of the combinations shown.

- ☐ Netatalk
- ☐ Novell Domain Services for Windows
- ☐ Xen Virtual Machine Host Server
- ☐ DST Shadow Volumes
- ☐ DFS Junction
- ☐ Novell Storage Services AD Support

4.5 What's Next

To proceed with installation of AFP, see [Chapter 5, "Installing and Setting Up AFP,"](#) on page 21.

5 Installing and Setting Up AFP

This section describes how to install and configure the Novell Apple Filing Protocol (AFP) on Open Enterprise Server (OES) 2018 and later.

- ♦ [Section 5.1, “Installing AFP during OES Installation,” on page 21](#)
- ♦ [Section 5.2, “Installing AFP after OES Installation,” on page 23](#)
- ♦ [Section 5.3, “Installing AFP NMAS Methods,” on page 23](#)
- ♦ [Section 5.4, “Verifying the Installation,” on page 24](#)
- ♦ [Section 5.5, “What’s Next,” on page 25](#)

5.1 Installing AFP during OES Installation

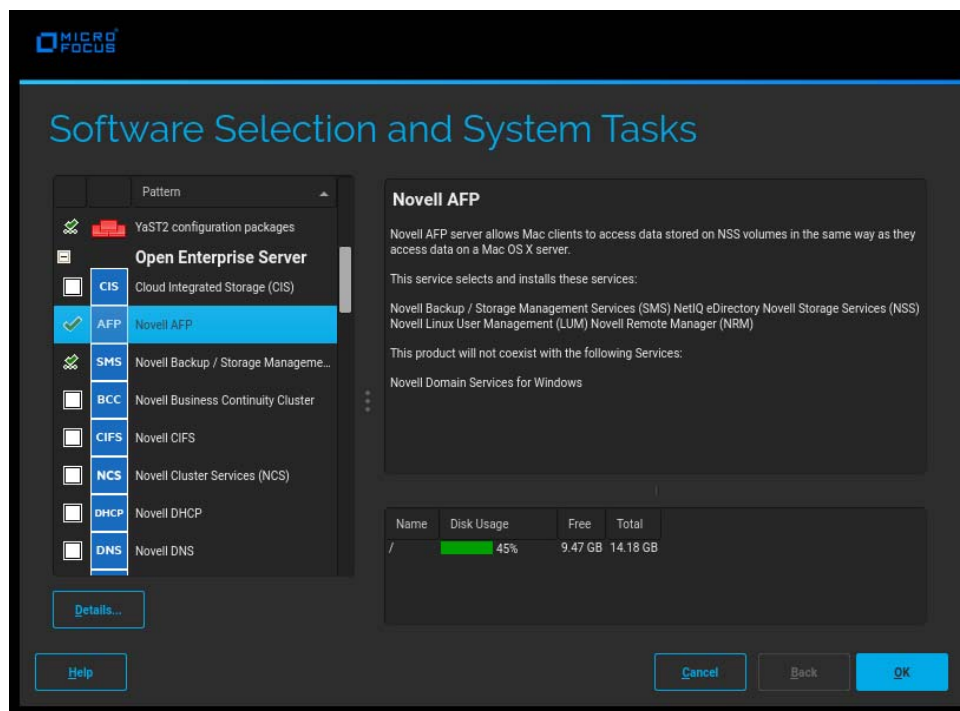
- 1 In the YaST install for OES, on the **Installation Settings** page, click **Software** to go to the **Software Selections** page.

For information about the entire OES installation process, see the [OES 2018 SP1: Installation Guide](#).

- 2 From the **OES Services** option, select **Novell AFP**. Click **Accept**.

The following additional services are automatically selected:

- ♦ Novell Backup / Storage Management Services (SMS)
- ♦ NetIQ eDirectory
- ♦ Novell Linux User Management (LUM)
- ♦ Novell NCP Server
- ♦ Novell Storage Services (NSS)
- ♦ Novell Remote Manager (NRM)



- 3 Select an appropriate install option.

Typical Configuration: A two-click express installation with minimal user inputs. This method collects only essential information to proceed with the OES configuration and uses default values for most options. In case you want to modify the default configuration parameters; in the OES install summary screen, click the respective links and modify them.

Custom Configuration: This method of OES configuration requires inputs for all parameters.

- 4 On the Open Enterprise Server Configuration window, click **Change** and then click **Novell AFP Services**.
- 5 Select the IP address of the LDAP server from the **Directory Server Address** drop-down list. If you do not want to use the default, select a different LDAP server in the list.

Add Proxy User as Trustee of User Contexts: This option is selected by default. Deselecting this option will not grant the AFP proxy user the rights required over eDirectory contexts to search for a AFP user in the subtree.

Enable Subtree Search: This option is not selected by default. Selecting this option enables AFP to search for a user in the entire subtree of selected contexts.

- 6 Browse or specify a user (existing or created here) with rights to search the LDAP tree for AFP objects.

If you selected the **Use Common Proxy User as default for OES Products** check box during eDirectory configuration, the Proxy user name and password fields are auto-populated. If a common proxy is not configured, the **AFP Proxy User Name** field is populated with a system-generated proxy user name.

- 7 Specify a password (existing or created here) for the Proxy user.

This field is disabled if you selected the **Use Common Proxy User as default for OES Products** check box during eDirectory configuration. If a common proxy is not configured, the **Proxy Password** field is auto-populated with a system-generated proxy password.

- 8 Retype the same password in the **Verify Proxy User Password** field.

- 9 Click **Add**, then browse to search for an existing eDirectory context. Specify the list of contexts to search for AFP users. They will be sequentially searched when AFP users enter their credentials.

The AFP server searches through each context in the list until it finds the correct user object. For example, if users exist in ou=users, provide the context. If there are any users in ou=user1,ou=users, it is not resolved unless you have a subtree search enabled. The ou=user1,ou=users context must be added explicitly.

- 10 Click **Next**.
- 11 Click **Apply** to save the changes.

5.2 Installing AFP after OES Installation

If you did not install Novell AFP Services during the OES installation, you can install it later by using **YaST > Open Enterprise Server > OES Install and Configuration**.

- 1 Open the YaST Control Center. In the left panel under **Groups** section, click **Open Enterprise Server**, then click **OES Install and Configuration** to open the **Software Selection** page.
- 2 Select **Novell AFP**, then click **Accept**.

After the install is finished, YaST displays a summary page indicating that AFP configuration is enabled. All the configured services are disabled on this page.
- 3 Select **AFP** to go to the configuration page.
- 4 Browse or specify a user (existing or created here) with rights to search the LDAP tree for AFP objects.

If you selected the **Use Common Proxy User as default for OES Products** check box during eDirectory configuration, the Proxy user name and password fields are auto-populated. If a common proxy is not configured, the **AFP Proxy User Name** field is populated with a system-generated proxy user name.
- 5 Click **Next** to continue.

5.3 Installing AFP NMAAS Methods

The AFP NMAAS methods were introduced in OES 2 SP3 for secure authentication purposes.

- [Section 5.3.1, “Installing AFP NAMS Methods during a New Installation,” on page 23](#)
- [Section 5.3.2, “Installing AFP NAMS during an Upgrade,” on page 23](#)
- [Section 5.3.3, “Installing Patches for the AFP NMAAS Methods,” on page 24](#)

5.3.1 Installing AFP NAMS Methods during a New Installation

For a new installation, you are not required to install the AFP NMAAS methods. The methods are installed during the AFP server installation.

5.3.2 Installing AFP NAMS during an Upgrade

If you are upgrading from an OES 2 SP2 server or an OES 2 SP3 server to an OES 2018 or later server, make sure you install the `novell-afp-nmasmethods.rpm`.

5.3.3 Installing Patches for the AFP NMAS Methods

It is important to ensure that the AFP NMAS methods have the latest updates.

To install patches for the AFP NMAS methods, run the following script:

```
/opt/novell/afptpd/bin/install_afp_lsm.sh
```

This script prompts you to enter the Tree Admin name and password for the eDirectory user.

After installing or upgrading the NMAS methods, ensure that s NMAS methods are synchronized in eDirectory.

5.4 Verifying the Installation

- ♦ [Section 5.4.1, “Checking Files and Directories,” on page 24](#)
- ♦ [Section 5.4.2, “Verifying LSM Installation,” on page 25](#)

5.4.1 Checking Files and Directories

After the installation is done, you can verify if the installation was successful by using the following procedure:

- 1 Check for the following files in the `/etc/opt/novell/afptcpd` directory:
 - ♦ `afpdirxt.conf`
 - ♦ `afptcpd.conf`
 - ♦ `afpvols.conf`
- 2 Check the `afpdirxt.conf` file for the context added during the installation.
- 3 Check for the `/usr/share/mof/novell-afp-providers/AFPServices.mof` file.
- 4 Check for the following libraries under `/usr/lib64/cmpi` directory:

```
libcmpiOSBase_BaseBoardProvider.so
libcmpiOSBase_CSBaseBoardProvider.so
libcmpiOSBase_CSProcessorProvider.so
libcmpiOSBase_ComputerSystemProvider.so
libcmpiOSBase_OSProcessProvider.so
libcmpiOSBase_OperatingSystemProvider.so
libcmpiOSBase_OperatingSystemStatisticalDataProvider.so
libcmpiOSBase_OperatingSystemStatisticsProvider.so
libcmpiOSBase_ProcessorProvider.so
libcmpiOSBase_RunningOSProvider.so
libcmpiOSBase_UnixProcessProvider.so
libnovell_lum_config.so
libnovell_pam_module.so
libnovell_pam_settingdata.so
libnovell_pammodule_lumsettingdata.so
libnovell_pammodule_settingdata.so
libpyCmpiProvider.so
```

- 5 Check for the `libafplinlcm.so` library in the `/opt/novell/lib64` directory.

LCM (Login Client Module) is the NMAS client component of an NMAS Login method. The new AFP NMAS LCM is the shared object (`.so`) loaded by the NMAS Client that is loaded into AFP Server address space.

5.4.2 Verifying LSM Installation

LSM installation can be verified either through iManager or the local file system.

Verifying through iManager

In iManager, click **NMAS**. Under **NMAS Login Methods** and **NMAS Login Sequences**, verify that `afplinlsm` is present.

Verifying through the Local File System

Verify that `AFPLINLSM_X64.S0` is present in the `/var/opt/novell/eDirectory/data/nmas-methods` directory.

5.5 What's Next

For details on administering the AFP service, see [“Administering the AFP Server” on page 27](#).

6 Administering the AFP Server

After AFP services are installed on the Open Enterprise Server (OES) server, you can use iManager to change the configuration details of the AFP server.

- ♦ [Section 6.1, “Prerequisite,” on page 27](#)
- ♦ [Section 6.2, “Selecting a Server to Manage,” on page 27](#)
- ♦ [Section 6.3, “Configuring General Parameters,” on page 28](#)
- ♦ [Section 6.4, “Configuring Volume Details,” on page 33](#)
- ♦ [Section 6.5, “Configuring Context Details,” on page 36](#)

6.1 Prerequisite

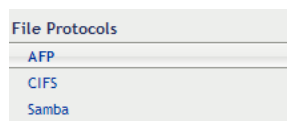
- ♦ To manage AFP server through the AFP iManager plug-in, ensure that the admin user or the container admin user is LUM-enabled. For more information, refer to [Using iManager for Linux User Management](#) in the [OES 2018 SP1: Linux User Management Administration Guide](#).
- ♦ The install administrator must have Compare, Read, Write on ACL Attribute to add the Common Proxy user as a trustee of AFP user contexts selected at the time of installation.

6.2 Selecting a Server to Manage

- 1 Open a browser and enter the URL for iManager.



The URL is `https://server_ip_address/nps/imanager.html`. Replace `server_ip_address` with the IP address or DNS name of the Linux server running AFP.

- 2 Enter your user name and password.
- 3 In the left pane, locate and select the **AFP** task.









- 4 Use one of the following methods to select a server in the tree where you are logged in:
 - ♦ In the **Server** field, type the NetIQ eDirectory distinguished server name for the server you want to manage, then press the Tab key or click somewhere on the page outside of the **Server** field to confirm your selection. For example:

```
afpserver.novell
```

- ♦ Click the **Search** icon  to open the eDirectory Object Selector. Browse or search the list to locate the server you want to manage, then click the server name.
 - ♦ Click the **Object History** icon  to select a server you have recently managed.
- 5 Wait for iManager to retrieve information about that server and display the appropriate information to the task page you are in. It might take several seconds to retrieve the information, depending on the amount of the data in the server.

The status of the server is displayed in the status bar below the **Server** text field.

Button	Description
	Indicates that the AFP server is stopped. To start the server, click  .
	Indicates that the AFP server is up and functional. To stop the server, click  .
	Click this button to view log details of the AFP server.
	Click this button to save and load the configuration changes on the AFP server. This saves and loads configuration changes for all the parameters except for Authentication Mode , Reconnect Period , and Export All Volumes . Any change in these two parameters requires restarting the AFP server. Reloading does not affect the existing client connections to the AFP server.

6.3 Configuring General Parameters

The general parameters help you define the security and rights features of the AFP server.

- 1 Open a browser and enter the URL for iManager.
The URL is `https://server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Select the **General** tab.
The following details are displayed:
 - ♦ [Section 6.3.1, “Security and Rights,” on page 28](#)
 - ♦ [Section 6.3.2, “Threads and Connections,” on page 29](#)
 - ♦ [Section 6.3.3, “Version and Logging,” on page 30](#)
 - ♦ [Section 6.3.4, “Other,” on page 31](#)
 - ♦ [Section 6.3.5, “Subtree Search,” on page 31](#)
 - ♦ [Section 6.3.6, “Rights to a File or Folder,” on page 32](#)
- 5 Modify the parameters, click **Ok**.
- 6 Restart the AFP service, if you have modified **Authentication Mechanism** and **Export All Volumes** parameters. For other parameters, reload the AFP service.

6.3.1 Security and Rights

The Security and Rights parameters let you define and set access permissions for the AFP server.

Setting	Description
Allow Guest Login	Select this option to allow users to log in as a guest.
World No Rights Management	<p>Select this option to let users set permissions and give access to network directories and their contents to everyone (world).</p> <p>If this option is not selected, the AFP server ignores the <code>Set Rights</code> requests coming from Macintosh clients, so the users cannot set permissions to give access to others.</p>
Sharing Rights	<p>Select this option to turn off retrieval rights for the owner, groups, and everyone.</p> <p>Returns a set of default rights when queried.</p> <p>The default option is No.</p>
Authentication Mode	<p>Indicates the authentication mechanism to use. The supported methods are:</p> <ul style="list-style-type: none"> ♦ Two-Way Random Key Exchange ♦ Cleartext ♦ Random Exchange ♦ Diffie Hellman ♦ DHX2 <p>The default authentication mode is DHX2.</p> <p>IMPORTANT: The authentication mechanism for Mac 10.7 clients is Diffie-Hellman 2 (DHX2).</p> <p>If you want to connect to a Mac 10.7 client, ensure that the authentication mode is set to <code>Diffie-Hellman 2</code>.</p>

6.3.2 Threads and Connections

These parameters help you define the processing capabilities of the AFP server.

Setting	Description
Minimum Threads	<p>Indicates the minimum number of threads that should be set for the <code>afptcpd</code> daemon to start.</p> <p>The minimum number of threads that can be supported is 32.</p> <p>The default value is 3 threads.</p>
Maximum Threads	<p>Indicates the maximum number of threads that the AFP server can support.</p> <p>The maximum number of threads that can be supported is 512.</p> <p>The default value is 32 threads.</p>

Setting	Description
Reconnect Period	<p>Indicates the number of minutes the AFP server waits before attempting to reconnect.</p> <p>The minimum waiting time is 2 minutes and can extend up to 24 hours (1440 minutes).</p> <p>The default value is 1440 minutes.</p>

IMPORTANT: Maximum and Minimum Thread Range is Changed

Up until OES 11 SP1, valid range for min/max threads is as follows:

Minimum threads: 1 to 32767, default value: 3

Maximum threads: 4 to 32768, default value: 32

In OES11 SP2 or later, the valid thread range is changed to as follows:

Minimum threads: 3 to 32, default value: 3

Maximum threads: 4 to 512, default value: 32

Before migration, manually edit `afptcpd.conf` file and set the number of threads within the valid range and proceed with the migration procedure. If it is not changed and the minimum or maximum threads is out of the range, then AFP server will use default number of threads.

In case of upgrade, AFP server will auto adjust the minimum or maximum threads values if required. If values of minimum or maximum threads set in the `afptcpd.conf` file is outside the new range of values, AFP server will adjust it to the nearest valid value and update the `afptcpd.conf` file.

In OES 2018 or later, iManager 3.1 user interface has been modified to reflect the change in thread range. If an OES 2018 or later version of AFP server is accessed with an older version of iManager, then it will not show the new thread range.

6.3.3 Version and Logging

These parameters help you define the logging capabilities of the AFP server.

AFP makes use of `syslog` daemon for logging. This daemon keeps track of the log file that it writes to if the log file is renamed or the location is changed.

Setting	Description
AFP Version	<p>Indicates the AFP versions that the AFP server can support.</p> <p>If you select All, AFP versions 2.2, 3.0, and 3.1 are supported.</p> <p>The default value is All.</p>
Enable Log	<p>Select this option to turn the logging feature on and add an entry to the log file.</p> <p>When logging is activated, AFP error messages are written to the <code>/var/log/afptcpd/afptcp.log</code> file.</p>
Enable Status	<p>Select this option if you want status messages to be recorded in the <code>/var/log/afptcpd/afptcp.log</code> file.</p>

Setting	Description
Enable Debug	Select this option if you want debug messages to be recorded in the <code>/var/log/afptcpd/afptcp.log</code> file.
Enable Error	Select this option if you want error messages to be recorded in the <code>/var/log/afptcpd/afptcp.log</code> file.
Auditing	Select this option to check the authentication process and any changes that occur to the configuration parameters of the AFP server. Details of any changes that occur are recorded in the <code>/var/log/audit/audit.log</code> file

6.3.4 Other

These parameters let you define the search boundaries and determine if all volumes need to be exported. Novell AFP supports only Storage Services (NSS) volumes.

Setting	Description
Export All Volumes	When this option is selected, all the NSS volumes on the server are exported. When this option is deselected, only the volumes listed in the <code>afpvols.conf</code> file are exported. NOTE: When the Export All Volumes option is turned off, specifying the alternate name is not mandatory. The volume name is displayed for export. However, if the alternate name is specified, the alternate name of the volume is displayed for export.
Subtree Search	If the subtree search option is enabled, AFP searches for the user in the base context as well as in the subtree under the contexts specified in the <code>/etc/opt/novell/afptcpd/afpdirxt.conf</code> file. By default, this feature is disabled.

IMPORTANT: The following options have been removed from OES 2 SP2 and later:

- ♦ `CROSS_PROTOCOL_LOCKS`
- ♦ `NO_UNLOAD_TIME_CHECK`
- ♦ `NO_COUNT_ON_OFFSPRING`

If you use an OES 2 SP1 AFP iManager plug-in to manage an OES 2 SP2 or later AFP server, these configuration settings cannot be managed.

The `GUEST_USER` and `EXPORT_ALL_VOLUMES` options was added in OES 2 SP2 and the *Subtree Search* option was added in OES 11 SP1. If you use an OES 2 SP1 iManager plug-in, these options are not available.

6.3.5 Subtree Search

A subtree search enables AFP to search for a user in the base contexts defined in the `/etc/opt/novell/afptcpd/afpdirxt.conf` file as well as in all the sub-contexts (subtrees) underlying those base contexts. If a subtree search is enabled, all the users existing in any subcontexts in the `afpdirxt.conf` file can authenticate to the AFP server if the users have sufficient rights on volumes or folders.

NOTE: It might take longer to authenticate with subtree search enabled, depending on the tree structure. Having local replicas for all AFP users can improve the authentication performance.

- ♦ [“Prerequisites” on page 32](#)
- ♦ [“Enabling Subtree Search” on page 32](#)
- ♦ [“Disabling Subtree Search” on page 32](#)
- ♦ [“Subtree Search in a Cluster Setup” on page 32](#)

Prerequisites

To use the subtree search feature, the AFP proxy user should have read rights over all the search contexts and their subcontexts mentioned in `afpdirctx.conf` file. These rights are assigned automatically either during AFP installation or through iManager when the context is added from AFP iManager plug-in.

Enabling Subtree Search

Subtree search is disabled, by default. To enable subtree search, go to iManager > **File Protocols** > **AFP** > select the server > **General** tab > select the **Subtree Search** check box > **OK** > click **Reload**.

Disabling Subtree Search

To disable subtree search, go to iManager > **File Protocols** > **AFP** > select the server > **General** tab > clear the **Subtree Search** check box > **OK** > click **Reload**.

Subtree Search in a Cluster Setup

Subtree search can be configured only at a physical server or node level. In a cluster setup, subtree search should be enabled on all nodes and all nodes should be configured with same contexts in the `afpdirctx.conf` file.

6.3.6 Rights to a File or Folder

Rights to a file or a folder on the AFP server are controlled through the rights configuration parameter.

There are three options: **All**, **Default**, and **No**. If you do not want to use the **All** parameter option, set the option to **Default** or **No**. The following table lists the details of the configuration parameters:

Parameter	Description
No	<p>If you set the Rights parameter to No, rights returned by the AFP server are set to returning the owner ID for files or folders.</p> <p>The AFP server does not calculate group and other rights for files and folders when Rights is set to No. In this case, the AFP server returns the default server ID 0, which is mapped to the user name Root for group and other rights</p>

Parameter	Description
Default	<p>If you set the Rights parameter to <code>Default</code>, the AFP server turns off rights calculations for all the rights.</p> <p>The AFP server returns the AFP server ID, which is set to 0 for owner, group, and other rights. This is because, after setting the Rights configuration option to <code>Default</code>, no rights calculations are performed for files and folders.</p> <p>Setting this option results in improved performance (compared to when Rights option is set to <code>All</code>) when files and folders have a large number of trustees, which requires more processing for calculating group rights.</p>
All	<p>If you set the Rights parameter to <code>All</code>, the AFP server returns the correct owner ID that is set on a file or folder. For other IDs, the AFP server finds the group or user trustee that has maximum rights on the file/folder. This group or user is then returned to the other ID parameter when the Rights option is set to <code>All</code>. For finding a group or user name with maximum rights, the AFP server scans all the trustees assigned to a file or folder.</p> <p>This calculation takes more time when a large number of trustees are assigned to a file or folder.</p>

6.4 Configuring Volume Details

The logical volumes you create on NSS storage pools are called NSS volumes.

Novell AFP supports only Storage Services (NSS) volumes. NSS storage object names are case insensitive. Names such as AURORA, Aurora, and aurora are the same. Because NSS volume names are case insensitive, volumes that can be exported from AFP are also case insensitive.

NSS volumes are identified by the machine name and volume name combination. For instance, if you create a volume titled `AFP_Volume` on a server named `ACME`, the volume name is represented as `ACME.AFP_Volume`. The Volume Name Management feature helps you specify an alternate name for the NSS volume. For instance, you can represent `ACME.AFP_Volume` as `AFP_Volume`. This is mandatory in a cluster setup where you need to identify volumes without the machine name prefix.

Renaming of AFP server volumes in the `afpvols.conf` file is required when using NCS clustered volumes.

The AFP volume share name supports all ASCII characters except NULL, colon(:), and forward slash(/).

IMPORTANT: Do not edit the `afpvols.conf` file for a volume that is already mounted and is already in use (mounted on AFP clients).

However, if there is a need to modify the file, restart the server after modification instead of reloading it. This ensures the volumes mounted on clients have a clean unmount.

Using the reload option for modification leads to anomalies and should be avoided.

You must restrict access to NSS volumes whose ZID value is greater than the 32-bit limit (`0xffffffff`). For more information, see [Section 13.1.2, “AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit,” on page 58](#).

The AFP server now dynamically detects when a new NSS volume is added or mounted, and when an existing NSS volume is deleted or unmounted. The AFP server updates itself with the current set of volumes on the OES 2015 or later server. An explicit reload of the server is not required.

Dynamic detection is applicable to standalone servers as well as cluster nodes.

Use the following tasks to administer AFP volume names:

- ♦ [Section 6.4.1, “Adding a New Volume Name,” on page 34](#)
- ♦ [Section 6.4.2, “Editing an Existing Volume Name,” on page 34](#)
- ♦ [Section 6.4.3, “Deleting a Volume Name,” on page 35](#)
- ♦ [Section 6.4.4, “Resetting the Desktop,” on page 35](#)

6.4.1 Adding a New Volume Name

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https:// server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Volume** tab. Click the **Object Selector** button, then select the server for which you want to specify new volume names.
- 6 Select **Add**. This opens the Add New Volume dialog box.
- 7 Click the **Object Selector** button, then select an existing volume. If you want to see the volumes you selected earlier, click the **Object History** icon.
- 8 (Optional) Specify a name for the selected NSS volume. This changes the volume name visible to the AFP clients.
- 9 Click **OK** to save the changes.
- 10 Restart the AFP server by using the `rcnovell-afptcpd restart` command.

NOTE: Volumes renamed through **Adding a New Volume Name** are updated in the `afpvols.conf` file.

6.4.2 Editing an Existing Volume Name

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https:// server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Volume** tab, then use the **Object Selector** button to select the server for which you want to specify new volume names.
The volumes created on the server are displayed.
- 6 Select the volume you want to modify and click **Edit**.
- 7 (Optional) Specify a new name for the shared volume. This changes the volume name visible to the AFP clients.

- 8 Click **OK**.
- 9 Restart the AFP server by using the `rcnovell-afptcpd restart` command.

IMPORTANT: The default namespace of a volume is the Long format. If you change the volume namespace by using NSSMU or iManager, the AFP server needs to be restarted for the changes to take effect.

6.4.3 Deleting a Volume Name

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https://server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Volume** tab. Use the **Object Selector** to select the server you want to modify.
The volumes created on the server are displayed.
- 6 Select the volume name you want to remove and click **Delete**.
- 7 Click **OK**.
- 8 Restart the AFP server by using the `rcnovell-afptcpd restart` command.

6.4.4 Resetting the Desktop

In Macintosh, each application is bundled with an icon. The AFP server scans all the applications on each volume and stores the application details and icon details in the `Desktop.AFP/APPL` and `Desktop.AFP/ICONS` directories.

The **Reset Desktop** option can be used to restore the application or icon configuration to its original state.

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https://server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Volume** tab. Use the **Object Selector** to select the server you want to modify.
The volumes created on the server are displayed.
- 6 Select the volume for which you want to reset the desktop, then click the **Reset Desktop** option.

6.5 Configuring Context Details

The context defines the position of an object within the Directory tree structure. It is a list of container objects leading from the object to the root of the tree. Specifying the context preempts the need to specify the FQDN (fully qualified distinguished name) of the user.

A context search file allows Macintosh users to log in to the network without specifying their full context. When the Macintosh user enters a user name, the server searches through each context in the list until it finds the correct user object.

- ♦ [Section 6.5.1, “Adding a Context,” on page 36](#)
- ♦ [Section 6.5.2, “Removing a Context,” on page 36](#)

6.5.1 Adding a Context

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https:// server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Contexts** tab. The contexts created on the server are displayed.
- 6 Click **Add**. This opens the Add New Context dialog box.
- 7 Specify a context name or browse to select an existing context.
- 8 Click **OK** to save the changes.

6.5.2 Removing a Context

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https:// server_ip_address/hps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In the left column, select **File Protocols**, then click **AFP**.
- 4 Browse and select the AFP server that you want to administer.
- 5 Select the **Contexts** tab. The contexts created on the server are displayed.
- 6 Select the context you want to delete.
To remove all of the contexts in the list, click the top-level check box, then click **Delete**.
To remove one or more contexts, click the check boxes next to them, then click **Delete**.

7 Migrating AFP to OES 2018 SP1

The Open Enterprise Server (OES) Migration Tool has a plug-in architecture and is made up of Linux command line utilities with a GUI wrapper. You can migrate AFP to OES 2018 or later through the GUI Migration Tool or through the command line utilities.

To get started with migration, see “[Overview of the Migration Tools](#)” in the *OES 2018 SP1: Migration Tool Administration Guide*.

For more information on migrating AFP, see “[Migrating AFP to OES 2018 SP1](#)” in the *OES 2018 SP1: Migration Tool Administration Guide*.

8 Running AFP in a Virtualized Environment

AFP services run in a virtualized environment just as they do on a physical NetWare server, or on a physical server running Open Enterprise Server (OES) 2018 or later and require no special configuration or other changes.

To get started with Xen virtualization or with KVM virtualization, see the SLES 12 [Virtualization Guide](#)

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product you are using.

For information on setting up virtualized OES 2018 SP1, see “[Installing, Upgrading, or Updating OES on a VM](#)” in the *OES 2018 SP1: Installation Guide*.

9 Configuring AFP with Novell Cluster Services for an NSS File System

Novell Apple Filing Protocol can be used in a cluster environment with Novell Cluster Services on your Open Enterprise Server (OES) server.

- ♦ [Section 9.1, “Benefits of Configuring AFP for High Availability,” on page 41](#)
- ♦ [Section 9.2, “Volumes in a Cluster,” on page 41](#)
- ♦ [Section 9.3, “Configuring AFP in a Cluster,” on page 42](#)

9.1 Benefits of Configuring AFP for High Availability

When you configure AFP in an OES cluster, resources can be dynamically switched or moved to any server in the cluster. Resources can be configured to automatically switch or be moved if there is a server failure, or they can be moved manually to troubleshoot hardware or balance the workload.

An equally important benefit of implementing AFP in a cluster setup is that you can reduce unplanned service outages as well as planned outages for software and hardware maintenance and upgrades.

Before you attempt to implement this solution, familiarize yourself with how Cluster Services works. For information, see the [OES 2018 SP1: Novell Cluster Services for Linux Administration Guide](#).

9.2 Volumes in a Cluster

In a cluster setup, when a Macintosh client connects to the physical IP of the AFP server, both the local volumes and the cluster-enabled shared volumes are exported to the client.

However, if the client connects to the cluster/virtual IP, then only the cluster-enabled shared volumes associated with the cluster IP are exported.

For example, consider a cluster setup with two AFP servers running on nodes A and B. If the cluster resource is bound to node A, a Mac client connecting to the physical IP of node A can access both the local and the cluster-enabled shared volumes.

If the client connects to the physical IP of node B, then only local volumes on node B are exported, because the cluster resource is now on node A. However, if the cluster resource moves to node B because of migration or failover, then clients connecting to node B can see both local and shared volumes.

NSS volumes are identified by the machine name and volume name combination. For instance, if you create a volume titled AFP_Volume on a server named ACME, the volume is represented as ACME.AFP_Volume. The Volume Name Management feature helps you specify an alternate name for the NSS volume. For instance, you can rename ACME.AFP_Volume to AFP_Volume. This is mandatory in a cluster setup where you need to identify volumes without the machine name prefix.

The following example illustrates how cluster nodes map to shared volumes.

```

Example 3: Renaming cluster volumes
afpvols.conf for serverA:
serverA.vol1      sharedVol1
serverA.vol2      sharedVol2

afpvols.conf for serverB:

serverB.vol1      sharedVol1
serverB.vol2      sharedVol2

```

9.2.1 Volume Name Management in a Cluster

Volume management is done in two ways in a cluster:

- ♦ By using the iManager AFP Management plug-in:

The iManager AFP Management plug-in requires a volume to be locally mounted on the cluster node before adding it to the AFP configuration. You migrate the volume resource to each node and use the iManager AFP Management plug-in to add the volume to the AFP configuration.

- ♦ By editing the `/etc/opt/novell/afptcpd/afpvols.conf` on each cluster node. This is done without migrating the resource to each node. Use the following syntax: `ServerName.VolumeName` `VolumeName`.

Replace `ServerName` with the host name of the local cluster node and replace `VolumeName` with the name of the shared, cluster-enabled volume.

9.3 Configuring AFP in a Cluster

Configuring or enabling AFP and making it available in a cluster environment requires you to perform the following tasks:

- ♦ [Section 9.3.1, “Identifying the Nodes to Host the AFP Service,” on page 42](#)
- ♦ [Section 9.3.2, “Installing Novell Cluster Services,” on page 42](#)
- ♦ [Section 9.3.3, “Creating Shared NSS Pools,” on page 43](#)
- ♦ [Section 9.3.4, “Configuring the Monitoring Script,” on page 43](#)
- ♦ [Section 9.3.5, “Reviewing Load and Unload Scripts,” on page 44](#)

9.3.1 Identifying the Nodes to Host the AFP Service

- 1 Install the AFP server on all the nodes in cluster or on the nodes identified for running AFP. For instructions on installing, see [Chapter 5, “Installing and Setting Up AFP,” on page 21](#).
- 2 Continue with [Section 9.3.2, “Installing Novell Cluster Services,” on page 42](#).

9.3.2 Installing Novell Cluster Services

- 1 Install Novell Cluster Services 2.0 on the OES server. For details, see [“Installing, Configuring, and Repairing Novell Cluster Services.”](#)
- 2 When you have finished installing Novell Cluster Services, continue with [Section 9.3.3, “Creating Shared NSS Pools,” on page 43](#).

9.3.3 Creating Shared NSS Pools

You can create a pool by using iManager, the NSSMU utility, or the NLVM create command.

- ♦ [“Using iManager to Create Pools” on page 43](#)
- ♦ [“Using NSSMU to Create Pools” on page 43](#)
- ♦ [“Using NLVM to Create Pools” on page 43](#)

Using iManager to Create Pools

For information on creating pools by using iManager, see [“Creating a Pool”](#) in the *OES 2018 SP1: NSS File System Administration Guide for Linux*.

Using NSSMU to Create Pools

For information on creating pools by using NSSMU, see [“NSS Management Utility \(NSSMU\) Quick Reference”](#) in the *OES 2018 SP1: NSS File System Administration Guide for Linux*.

Using NLVM to Create Pools

For information on creating pool by using NLVM, see [“NLVM Commands”](#) in the *OES 2018 SP1: NLVM Reference*.

9.3.4 Configuring the Monitoring Script

You use a script to configure resource monitoring to let a cluster fail over to the next node in the preferred nodes list.

The default monitor script is:

```
#!/bin/bash

. /opt/novell/ncs/lib/ncsfuncs

exit_on_error status_fs /dev/pool/P_E /opt/novell/nss/mnt/.pools/P_E nsspool

exit_on_error status_secondary_ipaddress 10.10.10.44

exit_on_error ncpcon volume V_E

exit_on_error afpstat

exit 0
```

For details on configuring resource monitoring scripts, see [“Configuring Resource Monitoring”](#) in the *OES 2018 SP1: Novell Cluster Services for Linux Administration Guide*

9.3.5 Reviewing Load and Unload Scripts

Cluster resource load and unload scripts are automatically generated for pools when they are cluster-enabled.

- ♦ [“Reviewing and Editing Scripts” on page 44](#)
- ♦ [“Load Script” on page 44](#)
- ♦ [“Unload Script” on page 45](#)

Reviewing and Editing Scripts

You can review the load and unload scripts for the AFP cluster by using the following procedure:

- 1 Open an Internet browser and enter the URL for iManager.
The URL is `https:// server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running AFP.
- 2 Enter your user name and password.
- 3 In Roles and Tasks, locate and select the **Clusters > My Clusters** task, then select the cluster.
or
If the cluster does not appear in your personalized list of clusters to manage, you can add it. Click **Add**, browse and select the cluster, then click **OK**. Wait for the cluster to appear and report its status, then select the cluster.
- 4 On the Cluster Manager page or Cluster Options page, select the cluster resource to view its properties, then click the **Scripts** tab.
- 5 Click the **Load Script**, **Unload Script**, or **Monitor Script** links to view or modify the scripts. If you modify a script, click **Apply** to save your changes before you leave the page.
Changes do not take effect until you take the resource offline, and bring it online again.

Load Script

```
#!/bin/bash

. /opt/novell/ncs/lib/ncsfuns

exit_on_error nss /poolact=P_E

exit_on_error ncpcon mount V_E=254

exit_on_error add_secondary_ipaddress 10.10.10.44

exit_on_error ncpcon bind --ncpservname=CLUSTER-P-E-SERVER --
ipaddress=10.10.10.44

exit_on_error cluster_afp.sh add CLUSTER-P-E-SERVER 10.10.10.44

exit 0
```

Unload Script

```
#!/bin/bash

. /opt/novell/ncs/lib/ncsfuns

ignore_error cluster_afp.sh del CLUSTER-P-E-SERVER 10.10.10.44

ignore_error ncpcon unbind --ncpservername=CLUSTER-P-E-SERVER --
ipaddress=10.10.10.44

ignore_error del_secondary_ipaddress 10.10.10.44

ignore_error nss /pooldeact=P_E

exit 0
```


10 Working with Macintosh Computers

This section contains the following information:

- ♦ [Section 10.1, “Administrator Tasks for Macintosh,” on page 47](#)
- ♦ [Section 10.2, “Macintosh End User Tasks,” on page 48](#)

10.1 Administrator Tasks for Macintosh

This section provides several ways to simplify your administration tasks and customize how Macintosh workstations interact with the network.

- ♦ [Section 10.1.1, “Configuring a Guest User Account,” on page 47](#)
- ♦ [Section 10.1.2, “Editing the Volume File,” on page 48](#)
- ♦ [Section 10.1.3, “Editing the Configuration File,” on page 48](#)

10.1.1 Configuring a Guest User Account

AFP lets you configure a guest user account through iManager.

- 1 In iManager, click the **Roles and Tasks** button.

For more information, see the [NetIQ iManager Administration Guide](#).

- 2 Click **Users > Create User**.

- 3 Specify a user name and a last name for the user.

- 4 Specify the context for the user.

- 5 Click **OK** to save the changes.

The guest user is now created.

- 6 After creation of the guest user, query for the user by using the **User > Modify User** task in iManager.

- 7 Remove the ability for the user to change the password by clicking **Restrictions**, then deselect **Allow User to Change Password**.

- 8 Enable the Guest account by adding the full eDirectory context of the guest object to the context search file.

- 9 Click **File Protocols > AFP**.

- 10 Select the **Allow Guest Login** option and specify the name of the guest user by using the instructions in [Section 6.3.1, “Security and Rights,” on page 28](#)

- 11 Reload the AFP server to make the **Guest** button available on the login screen.

To reload the AFP server through iManager, see [Section 6.2, “Selecting a Server to Manage,” on page 27](#).

10.1.2 Editing the Volume File

Information about volumes is stored in the `/etc/opt/novell/afptcpd/afpvols.conf` file.

To edit the `afpvols.conf` file and store volume information:

- 1 Use a text editor to open the `afpvols.conf` file.
- 2 On separate lines, enter the current name of the volume and the new name of the volume, separated by a space. For example:

```
server1.Volume1 AFPVol1  
  
server1.Volume2 AFPVol2
```

- 3 Unload and reload the AFP server by using the `rcnovell-afptcpd reload` command, or use [iManager](#) to reload the server.

10.1.3 Editing the Configuration File

The AFP server configuration parameters are stored in the `/etc/opt/novell/afptcpd/afptcpd.conf` file. After you install the AFP server, this configuration file has all the parameters, commented with their default values.

The following sample shows a typical `afptcpd.conf` file:

```
# Authentication module to use.  
  
# It is advisable not to use - cleartext - as the option # for this. The possible  
# options currently are: # cleartext, random random key exchange), two-way (two way  
# random # key exchange), DHX (Diffie-Hellman exchange 2).  
  
#  
# AUTH_UAM <name>  
  
AUTH_UAM DHX  
  
#  
# Minimum Number of threads that the daemon must always  
# have waiting for work, notwithstanding the complimentary  
# parameter - Maximum Number of threads (described next)  
# This can not be more than MAX_THREADS parameter.  
#  
# MIN_THREADS <num>#  
  
MIN_THREADS 3
```

10.2 Macintosh End User Tasks

When the Novell Apple Filing Protocol (AFP) is properly configured, the Macintosh users on your network can perform the following tasks:

- ♦ [Section 10.2.1, “Accessing Network Files,” on page 49](#)
- ♦ [Section 10.2.2, “Logging In to the Network as a Guest,” on page 49](#)

- [Section 10.2.3, “Changing Passwords from a Macintosh Computer,” on page 49](#)
- [Section 10.2.4, “Changing Expired Passwords from a Macintosh Computer,” on page 50](#)
- [Section 10.2.5, “Assigning Rights and Sharing Files from a Macintosh Computer,” on page 50](#)

10.2.1 Accessing Network Files

Macintosh users can use the Chooser option to access files and directories.

- 1 In Macintosh OS X, click **Go > Connect to Server**.
- 2 Specify `afp://IP address of the OES 2018 or later server` or `afp://DNS name of the OES 2018 or later server`, then click **Connect**.
- 3 Specify the user name and password, then click **Connect**.
- 4 Select a volume to be mounted on the desktop.

Although you now have access to the files, mounting the volume to the desktop does not make it available after rebooting. You need to create an alias to make it available after rebooting.

- 5 (Optional) Create an alias to the desired volume or directory:

5a Click the Linux server icon.

5b Click **File > Make Alias**.

The alias icon appears on the desktop.

- 6 (Optional) To access AFP share via the terminal, execute the following command:

```
mount_afp
```

The following example illustrates how to mount the afp volume `server.company.com/volumename/` at the mount point `/Volumes/mntpnt`:

```
mkdir /Volumes/mntpnt
```

```
mount_afp afp://username:userpass@server.company.com/volumename/ /Volumes/mntpnt
```

10.2.2 Logging In to the Network as a Guest

If the network administrator has set up the Guest User object account as described in [“Configuring a Guest User Account” on page 47](#), Macintosh users can log in to the network as a Guest.

- 1 In Macintosh OS X, click **Go > Connect to Server**.
- 2 Type the IP address or DNS name of the Linux server, then click **Connect**.
- 3 Click **Guest Login > Connect**.

The Guest user has rights to access network resources as configured by the network administrator.

10.2.3 Changing Passwords from a Macintosh Computer

Macintosh users can change their passwords. When they change the simple password, the eDirectory password is automatically synchronized.

- 1 In Macintosh OS, click the **Apple** menu > **Chooser > AppleTalk > Server IP Address**.
or
In Macintosh OS X, click **Go > Connect to Server**.
- 2 Type the IP address or DNS name of the Linux server, then click **Connect**.

- 3 Specify the user name.
- 4 Click **Change Password**.
- 5 Type the old password and the new password, then click **OK**.

10.2.4 Changing Expired Passwords from a Macintosh Computer

When the existing user's password expires, a pop-up is displayed as a reminder to change the password. Change the password from the Mac computer.

10.2.5 Assigning Rights and Sharing Files from a Macintosh Computer

Although using iManager is the recommended method for managing rights, Macintosh users have some file sharing and management capability through Chooser.

- ♦ [“NSS Rights versus Macintosh Rights” on page 50](#)
- ♦ [“Owner Rights” on page 51](#)
- ♦ [“User / Group” on page 51](#)
- ♦ [“Everyone” on page 51](#)

NSS Rights versus Macintosh Rights

Using Chooser/Finder to access network files and folders is consistent with the Macintosh environment, but there are some differences between NSS and Macintosh file sharing. Macintosh users can view the sharing information about specific folders by clicking **Get Info/Sharing**.

- ♦ [“Inherited Rights and Explicit Rights” on page 50](#)
- ♦ [“Owner, User/Group, and Everyone Rights” on page 51](#)

Inherited Rights and Explicit Rights

The Macintosh file system uses either inherited rights (which use the enclosing folder's privileges) or explicit rights (which assign rights to a group or user). A folder in the Macintosh file system cannot have both inherited and explicit rights.

NSS uses both inherited and explicit rights to determine the actual rights that a user has. NSS allows a folder (or directory) to hold file rights for multiple groups and users. Because of these differences, Macintosh users will find that access rights to folders and files might function differently than expected.

NSS uses inherited rights, so the **Macintosh Use Enclosing Folder's Privileges** option is automatically turned off. When a Macintosh user views the Get Info/Sharing dialog box for an NSS folder, only the User/Group assignments are visible if there is an explicit assignment on the folder. If the NSS folder inherits User/Group rights from a parent group or container, those rights are not displayed in the dialog box, nor is there any indication that the folder is inheriting rights from a group or container.

Owner, User/Group, and Everyone Rights

Because NSS allows multiple groups and users to have rights to a single folder, users cannot delete rights assignments by using the Apple Macintosh interface. Users can add assignments to allow basic file sharing, but more complex rights administration must be done through iManager. When specifying Owners, Users, and Groups, there is no way to select from current groups. You must specify the correct Linux name and context (fully distinguished eDirectory name).

TIP: No context is required if the context is specified in the context search file.

Owner Rights

In the Apple File Sharing environment, an owner is a user who can change access rights. In the NSS environment, users can change access rights if they have been granted the Access Control right for the folder. In NSS, an owner is the user who created the file. An NSS owner has no rights by virtue of ownership. In the NSS environment, the owner is the current user if he or she has access control rights to the folder.

If the user has access control rights, then he or she is shown as the owner of the file. If the user does not have access control rights, the actual NSS owner is shown as the owner. However, for directories, the NSS owner is always displayed.

In Apple File Sharing, there can be more than one owner. If you change the owner, access control rights are added to the new owner, but are not removed from the current owner. In NSS, there are two ways to have access control rights: 1) have the Access Control right and 2) have the Supervisor right. Adding a new owner only adds the Access Control right, not the Supervisor right. If the current owner already has the Supervisor right through other management utilities, that right remains. The Supervisor right also gives full file access rights. This means that if you are the current user and have the Supervisor right, you also have read/write access and you cannot change those rights.

The display only shows one owner. If multiple users have file access rights, only the current user is shown in the **Owner** field.

User / Group

Only one user or group can be displayed for a folder, although NetWare allows multiple users and groups to be assigned file access rights.

If both users and groups have access to an NSS folder, groups are displayed before users. The group with the most access rights is preferred over groups with fewer access rights. Only users or groups with explicit rights (not inherited rights) are shown in the **User/Group** field. Users and groups with inherited rights are not shown in the dialog box, nor is there any indication that there are users and groups with inherited rights.

Rights set through this interface are inherited by the folder's subfolders. It is impossible to manage all inherited rights from the Macintosh interface. (Although it is not recommended, you could set the inherited rights filters from the management utilities to turn off inherited rights.)

Everyone

Assigning rights to Everyone acts like the Macintosh user expects, with the exception that Everyone's rights are inherited. In NetWare, the object that represents the rights of any authenticated user is used to set Everyone's rights. Everyone's rights can change from folder to folder, but when they are set, they are inherited by subfolders.

11

Monitoring the AFP Server

The AFP server provides a monitoring feature for you to use.

- ♦ [Section 11.1, “Understanding the Monitoring Process,” on page 53](#)
- ♦ [Section 11.2, “Enabling Monitoring,” on page 53](#)
- ♦ [Section 11.3, “Viewing Logs through iManager,” on page 53](#)
- ♦ [Section 11.4, “Understanding Performance Parameters,” on page 54](#)

11.1 Understanding the Monitoring Process

The monitoring framework helps you assess the performance of the AFP server. The details provided by the AFP server logs are beneficial if you want to tune the performance of the server based on your needs. This framework records the following runtime information:

- ♦ Number of active threads in the AFP server
- ♦ Load capacity of the AFP server
- ♦ Query processing ability
- ♦ AFP server efficiency ratio

11.2 Enabling Monitoring

You enable monitoring through the command line interface by using the following command:

```
afpstat
```

11.3 Viewing Logs through iManager


- 1 In iManager, use one of the following methods to select a server in the tree where you are logged in:

- ♦ In the **Server** field, type the NetIQ eDirectory distinguished server name for the server you want to manage, then press the Tab key or click somewhere on the page outside of the **Server** field to enter your selection. For example:

```
afpserver.novell
```

- ♦ Click the **Search** icon to open the eDirectory Object Selector. Browse or search the list to locate the server you want to manage, then click the server name.
- ♦ Click the **Object History** icon to select a server you have recently managed.

Wait for iManager to retrieve information about that server and display the appropriate information to the task page you are in.

- 2 The status of the server is displayed in the status bar below the **Server** field. Click  to view the log details.

- 3 Select the **General** tab and scroll down to **Version and Logging**.
- 4 Select the **Enable Log** option. This option turns the logging feature on and adds an entry to the log file. When logging is activated, AFP log and error messages are written to the `/var/log/afptcpd/afptcp.log` file.

If you want to record the status, debug, and error messages in the `afptcp.log` file, ensure that the **Enable Status**, **Enable Debug**, and **Enable Error** options are selected.

11.4 Understanding Performance Parameters

When you click , the AFP server statistics window is displayed with the following information:

Table 11-1 AFP Server Performance Parameters

Parameter	Description
Active Threads	The number of threads that are presently active on the AFP server.
Load Ratio	The ratio of the total number of active threads to the total number of threads in the AFP server.
Availability	The ratio of the total number of events required for creation of a new thread compared to the number of events required to execute an AFP task.
Efficiency Ratio	<p>The ratio of the total number of times that threads complete a task and then terminate themselves compared to the total number of times that threads complete a task. AFP always maintains a minimum number of threads in the pool. The minimum count of threads is set to 3 during installation, but you can modify it to increase the thread count in the pool. For more information on threads and connections, see Section 6.3, "Configuring General Parameters," on page 28.</p> <p>When the list of tasks to be executed by the AFP server is high and there are no idle threads in the thread pool, the AFP server creates a new pool of threads. After a thread finishes its assigned task, if it finds a minimum number of threads in the thread pool, the thread terminates itself. The AFP server maintains a record of such events.</p>
Connections	Number of AFP client sessions that are currently connected to the AFP server.

You can control the number of log entries shown at one time by specifying your preference in the corresponding text field. For example: If you want to view the last 10 log entries of the AFP server, specify 10 in the **Latest Log Entries to display** field.

12 Auditing the AFP Server

The AFP server provides an auditing feature for you to use.

- ♦ [Section 12.1, “Understanding the Auditing Process,” on page 55](#)
- ♦ [Section 12.2, “Enabling Auditing,” on page 55](#)
- ♦ [Section 12.3, “Viewing Auditing Information,” on page 56](#)

12.1 Understanding the Auditing Process

The auditing framework helps you to monitor the authentication process and track any changes that occur to the configuration parameters of the server. Details of any changes that occur are recorded in the `/var/log/audit/audit.log` file. The audit daemon keeps track of the changes to the `audit.log` file.

Auditing is disabled by default in OES 2015 or later.

However, if it is enabled, you can disable the Audit configuration option in the `/etc/opt/novell/afptcpd/afptcpd.conf` file manually or through [iManager](#).

When the auditing option is enabled, the AFP server reports changes for the following events:

- ♦ AFP user login and logout events
- ♦ Changes to the configuration parameters of the `afptcpd.conf` file.

12.2 Enabling Auditing

You can enable auditing through iManager.

- 1 In iManager, use one of the following methods to select a server in the tree where you are logged in:
 - ♦ In the **Server** field, type the NetIQ eDirectory distinguished server name for the server you want to manage, then press the Tab key or click somewhere on the page outside of the **Server** field to enter your selection. For example:
`afpserver.novell`
 - ♦ Click the **Search** icon to open the eDirectory Object Selector. Browse or search the list to locate the server you want to manage, then click the server name.
 - ♦ Click the **Object History** icon to select a server you have recently managed.
Wait for iManager to retrieve information about that server and display the appropriate information to the task page you are in.
- 2 Select the **General** tab and scroll down to **Version and Logging**.
- 3 Select the **Auditing** option. This checks the authentication process, and any changes that occur to the configuration parameters of the AFP server are logged in `/var/log/audit/audit.log` file.
- 4 Click **OK** to save and apply the changes.

12.3 Viewing Auditing Information

To view the audit logs, open the `/var/log/audit/audit.log` file in a text editor.

Your log file will resemble the following example:

```
*****

type=DAEMON_START msg=audit(1185934048.314:4312) auditd start, ver=1.2.9,
format=raw, auid=4294967295 pid=27992 res=success, auditd pid=2

type=CONFIG_CHANGE msg=audit(1185934048.418:4): audit_enabled=0 old=0 by
auid=4294967295
type=CONFIG_CHANGE msg=audit(1185934049.914:5):

audit_backlog_limit=256 old=64 by auid=4294967295
type=DAEMON_END msg=audit(1186036669.479:4313) auditd normal halt, sending auid=0
pid=6208 subj=86036669.479:6): audit_enabled=0 old=0

type=DAEMON_START msg=audit(1186036762.687:1615) auditd start, ver=1.2.9,
format=raw, auid=4294967295 pid=3020 res=success, auditd pid=30

type=CONFIG_CHANGE msg=audit(1186036762.784:4): audit_enabled=0 old=0 by
auid=4294967295

*****
```

13 Troubleshooting AFP

This section describes some issues you might experience with the Novell Apple Filing Protocol (AFP) and provides suggestions for resolving or avoiding them.

- [Section 13.1, “Known Issues,” on page 57](#)
- [Section 13.2, “AFP Login Issues,” on page 59](#)
- [Section 13.3, “Starting the AFP Server,” on page 60](#)
- [Section 13.4, “File Creation,” on page 60](#)
- [Section 13.5, “Displaying Volumes,” on page 61](#)
- [Section 13.6, “Log Messages,” on page 61](#)
- [Section 13.7, “AFP Server Responds Slowly,” on page 61](#)
- [Section 13.8, “Operation Fails When a Macintosh Client Mounts an NSS Volume and Opens Files,” on page 62](#)
- [Section 13.9, “Hard Links are Broken When Files Are Accessed from an AFP Mount Point,” on page 62](#)
- [Section 13.10, “AFP Subtree Search Fails,” on page 62](#)
- [Section 13.11, “Cannot Access an AFP Share by Using an Alias,” on page 62](#)

For additional troubleshooting information, see the [Micro Focus Support Web site](#).

13.1 Known Issues

- [Section 13.1.1, “AFP Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured,” on page 57](#)
- [Section 13.1.2, “AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit,” on page 58](#)
- [Section 13.1.3, “Owner’s Name Not Displayed in the Macintosh Client,” on page 58](#)
- [Section 13.1.4, “File Level Trustees Are Deleted When a File is Modified,” on page 58](#)
- [Section 13.1.5, “AFP Does Not Support DST Shadow Volumes,” on page 59](#)

13.1.1 AFP Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured

AFP service configured with service proxy fails to come up after upgrading to OES 2018 or later. This is because the service proxy users are not migrated to OES Credential Store (OCS). To resolve this issue, perform the following:

- 1 Login as root user.
- 2 Run `yast2 novell-afp` and then enter eDirectory user password.
- 3 Specify the AFP proxy user password.
- 4 Click **Next** and continue with AFP configuration.

- 5 Verify the AFP service is up and running by using the following command:

```
systemctl status novell-afpcpd.service
```

- 6 Verify the service entry is present in OES Credential Store by using the following command:

```
oescredstore -l
```

13.1.2 AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit

On Mac, when you access the NSS volumes with ZID value greater than the 32-bit limit, AFP users might experience abnormal behavior while performing the file operations on that volume.

- ♦ If the ZID value for NSS volume is less than the 32-bit limit, AFP users can access and perform any file operation on this volume. Therefore, it is recommended to set `zid32` to restrict the ZID from crossing the 32-bit limit.
 - ♦ For local volumes, add `zid32` in the mount option for the volume in `/etc/fstab`.
 - ♦ For shared volumes, add `zid32` to the volume's `/opt` in the resource load script.

For more information on how to set ZID mode in local and shared volumes, see [Setting and Viewing the ZID Mode for a Volume](#) in the [OES 2018 SP1: NSS File System Administration Guide for Linux](#).

- ♦ If the ZID value for NSS volume has already crossed the 32-bit limit, it is recommended to use CIFS or NCP protocol to access this volume.

Also, you can configure AFP users to access only those volumes with ZID value less than the 32-bit limit by using the iManager AFP Management plug-in.

- ♦ For local volumes, disable the **Export All Volumes** setting and add only those volumes with ZID value less than the 32-bit limit. For more information on **Export All Volumes** setting, see [Section 6.3.4, “Other,” on page 31](#).
- ♦ For shared volumes, see [Section 9.2.1, “Volume Name Management in a Cluster,” on page 42](#).

13.1.3 Owner's Name Not Displayed in the Macintosh Client

The owner's name is not displayed when you right-click a folder.

Micro Focus has no current plans to fix this.

13.1.4 File Level Trustees Are Deleted When a File is Modified

File level trustees might be deleted when a file is modified, depending on how the application works with files it opens for writing. Some third-party applications record changes in a temporary file in order to save internal memory or as a safety net to prevent data loss due to a power failure, system crash, or human error. When a user saves the changes, the application deletes the original file, and saves the temporary file with same name as the original file. In response to the deletion instruction, the file system deletes the original file as well as any file level trustees set on the file. The file system is not application aware; that is, it does not track the ultimate intent of the applications that you might use.

For more information, see [“File-Level Trustees”](#) in the [OES 2018: File Systems Management Guide](#).

13.1.5 AFP Does Not Support DST Shadow Volumes

AFP does not support Dynamic Storage Technology Shadow volumes. The AFP users are able to see only the data that is on the primary volume. Primary or secondary volumes that are used in a DST shadow volume should not be exposed through AFP.

13.2 AFP Login Issues

- [Section 13.2.1, “Cannot See the Login Dialog Box,” on page 59](#)
- [Section 13.2.2, “AFP User Login to a Macintosh 10.5 Client Fails With a “Connection Failed” Error,” on page 59](#)
- [Section 13.2.3, “Invalid Username and Password Error,” on page 59](#)
- [Section 13.2.4, “Cleartext Authentication Fails on Mac Clients,” on page 59](#)
- [Section 13.2.5, “One-Way or Two-Way Random Exchange Authentication Fails on Mac Clients,” on page 60](#)
- [Section 13.2.6, “Enabling Authentication Mechanisms for a Mac 10.7 Client,” on page 60](#)

13.2.1 Cannot See the Login Dialog Box

Cause: This error is displayed when the firewall is enabled on the AFP server.

Action: To resolve this problem, use `YaST` to stop the firewall or set the firewall to allow connections from the client on TCP port 548.

13.2.2 AFP User Login to a Macintosh 10.5 Client Fails With a “Connection Failed” Error

Cause: The AFP user needs access permission to at least one of the volumes exported from the AFP server to resolve this issue.

Action: This problem can be resolved by assigning appropriate access rights to the AFP user.

13.2.3 Invalid Username and Password Error

Cause: Incorrect credentials

Action: If the credentials you have entered are correct, verify whether the `afpdircxt.conf` file has the context information for AFP users. The AFP server requires valid context information to resolve the typeless name user login.

13.2.4 Cleartext Authentication Fails on Mac Clients

Cause: This error occurs if you attempt to connect to an AFP server from a Mac client by using the Cleartext method. The Cleartext authentication method is by default disabled on Mac clients.

Action: To resolve this issue, execute the following commands:

For Mac OS 10.5.X versions:

```
defaults write com.Apple.AppleShareClient afp_cleartext_allow -bool YES
```

For Mac 10.6.x versions:

```
/usr/bin/plutil -convert xml1  
  
/Users/<user-name>/Library/Preferences/com.Apple.AppleShareClient.plist  
defaults write com.Apple.AppleShareClient afp_cleartext_allow -bool YES  
  
/usr/bin/plutil -convert binary1  
  
/Users/<user-name>/Library/Preferences/com.Apple.AppleShareClient.plist
```

For more information about enabling authentication methods in the Mac 10.7 client, see [Section 13.2.6, “Enabling Authentication Mechanisms for a Mac 10.7 Client,” on page 60](#)

13.2.5 One-Way or Two-Way Random Exchange Authentication Fails on Mac Clients

Cause: This error occurs if you attempt to connect to an AFP server from a Mac client by using the One-way Random Exchange or Two-Way Random Exchange authentication methods. Both of these authentication methods are deprecated on Mac clients.

Action: Ensure that you use the DHX or DHX2 method of authentication.

13.2.6 Enabling Authentication Mechanisms for a Mac 10.7 Client

By default, only the DHX2 authentication mechanism is enabled in Mac 10.7 and later clients. To use other authentication mechanisms to connect to the OES server, see the [Apple Knowledge base](#).

13.3 Starting the AFP Server

- ♦ [Section 13.3.1, “Starting the AFP Daemon Failed,” on page 60](#)

13.3.1 Starting the AFP Daemon Failed

Action: If you cannot start the AFP daemon, check the status of the `xregd` daemon and NSS daemon to see if it is running. To do this, execute the following commands at the prompt:

```
rcnovell-xregd status
```

If the daemon is not up, execute the `rcnovell-xregd start` command to start the daemon.

13.4 File Creation

- ♦ [Section 13.4.1, “Failure to Create a File on a Macintosh Client,” on page 60](#)

13.4.1 Failure to Create a File on a Macintosh Client

Cause: This error is displayed when the server volume quota has exceeded its limits and a partially created file cannot be deleted.

Action: To resolve this problem, terminate the AFP client by unmounting the volume where the partial file resides.

13.5 Displaying Volumes

- ♦ [Section 13.5.1, “Volumes Tab on a Macintosh 10.4 Client Displays an Empty Volume List,” on page 61](#)

13.5.1 Volumes Tab on a Macintosh 10.4 Client Displays an Empty Volume List

Action: This problem can be resolved by assigning appropriate access rights to the AFP user. The AFP user needs access permission to at least one of the volumes exported from the AFP server to resolve this issue.

13.6 Log Messages

- ♦ [Section 13.6.1, “NWDSResolveName failed to resolve supplied name <user name>,” on page 61](#)
- ♦ [Section 13.6.2, “zOpen on volume <VOLUME_NAME> failed,” on page 61](#)
- ♦ [Section 13.6.3, “zAFPCountByScanDir: scandir failed,” on page 61](#)

13.6.1 NWDSResolveName failed to resolve supplied name <user name>

Cause: During login, the AFP server requires an eDirectory context to build an FQDN for the user name. This error message is logged when there is no matching context for the user name.

Action: To resolve this error, review the eDirectory contexts, using the details in [“Configuring Context Details” on page 36](#).

13.6.2 zOpen on volume <VOLUME_NAME> failed

Cause: This error message is seen when you attempt to log in to a Macintosh 10.5 machine without appropriate rights to the volumes.

Action: To resolve this error, use iManager to set rights for the volumes.

13.6.3 zAFPCountByScanDir: scandir failed

Cause: This error occurs if the number of open files limit exceeds the ulimit maximum for open files.

Action: To resolve this error, either increase the ulimit for open files (using the `ulimit -n <value>` command) or close some of the open files to ensure that the number of open files does not exceed the ulimit value.

13.7 AFP Server Responds Slowly

Cause: This issue can occur when files or directories have a large number of trustees. This happens because the AFP server attempts to retrieve the rights of each trustee on the file or folder and return the trustee with the maximum rights as the owner or group of the file or folder.

Action: To disable this, go to the **General** tab of iManager AFP plug-in and update the **Sharing** rights to **NO**.

13.8 Operation Fails When a Macintosh Client Mounts an NSS Volume and Opens Files

Cause: Macintosh stores metadata in certain files beginning with a (.) dot character. These files exist on Mac volumes but are not stored on NSS.

Action: The error log message for these files can be ignored.

13.9 Hard Links are Broken When Files Are Accessed from an AFP Mount Point

Macintosh specifications do not support this action.

13.10 AFP Subtree Search Fails

Cause: The AFP Proxy user is probably not added as a trustee of the search contexts.

Action: Check eDirectory to determine if the AFP Proxy user has been added as a trustee of all the search contexts mentioned in the `afpdirxt.conf` file.

13.11 Cannot Access an AFP Share by Using an Alias

Cause: Rights have not been assigned to the containers where the user and user alias exist.

Action: If you are using an alias for a user, make sure you assign rights to Proxy user for the container where the actual user and user alias exist.

14 Security Guidelines for AFP

This section describes security issues and recommendations for the Novell Apple Filing Protocol (AFP) for an Open Enterprise Server 2018 or later server.

The information is intended for security administrators or anyone who is using AFP for Linux and is responsible for the security of the system. It requires a basic understanding of AFP protocol. It also requires the organizational authorization and the administrative rights to carry out the configuration recommendations.

- ♦ [Section 14.1, “Recommended Authentication Protocol,” on page 63](#)
- ♦ [Section 14.2, “Storing Credentials,” on page 63](#)
- ♦ [Section 14.3, “Intruder Detection,” on page 63](#)
- ♦ [Section 14.4, “Timeout Values,” on page 64](#)

14.1 Recommended Authentication Protocol

The recommended protocol for authentication is Diffie Hellman(DHX) or Diffie Hellman 2(DHX2). They provide a secure way to transport clear-text passwords of up to 64 characters to the server for further processing.

Other authentication modes like Cleartext, Random Number Exchange, and the Two-Way Random Key Exchange protocol support only 8-character passwords. With these modes, any attempt to log in fails if the eDirectory password is longer than 8 characters.

14.2 Storing Credentials

We recommend that you specify OES Credential Store as the credential storage location during configuration of the AFP service.

This ensures that your credentials are safe.

14.3 Intruder Detection

Intruder detection limits the number of unsuccessful login attempts.

The AFP server does not support intruder detection, so if the AFP user does not log in successfully, the user is not locked out even if you have set intruder detection to ON in NMAS.

14.4 Timeout Values

The timeout values for the AFP server range from 2 minutes to 24 hours. The default timeout value is 24 hours. This default value can be reconfigured by setting the `RECONNECT_PERIOD` value in the `afptcpd.conf` file or by setting the **Reconnect period** option through iManager.

For more information on how to set the reconnect period value through iManager, see [“Threads and Connections” on page 29](#).

To configure this value through CLI, start the AFP daemon by using the `-r` option. For example:
`afptcpd -r <reconnect period>` or `afptcpd --reconnect-period =<reconnect period>`

A

Command Line Utilities for AFP

This section details the syntax and options for the following Novell Apple Filing Protocol (AFP) utilities for an Open Enterprise Server 2018 or later server.

- ♦ [Section A.1, “novaftp,” on page 65](#)
- ♦ [Section A.2, “afpdtrreset,” on page 65](#)
- ♦ [Section A.3, “afpstat,” on page 66](#)
- ♦ [Section A.4, “afptcpd,” on page 66](#)
- ♦ [Section A.5, “afpbind,” on page 66](#)
- ♦ [Section A.6, “afpnames,” on page 66](#)
- ♦ [Section A.7, “migafp,” on page 67](#)

A.1 novaftp

A command line utility to configure, monitor, and manage the AFP service (afptcpd daemon).

Syntax

```
novaftp
```

Usage

```
novaftp [options]
```

For more information, see [Chapter 3, “AFP Monitoring and Management,” on page 15](#).

A.2 afpdtrreset

Resets the desktop database on a volume.

Syntax

```
afpdtrreset
```

Usage

```
afpdtrreset [AFP Volume Name]
```

Example A-1 Example:

```
afpdtrreset acme.new volume
```

A.3 afpstat

Displays statistics for the afp daemon.

Syntax

```
afpstat
```

A.4 afptcpd

The daemon for the Novell AFP server.

Syntax

```
afptcpd [options <parameters>]
```

To start the daemon:

```
rcnovell-afptcpd start
```

This command reads the configuration parameters from the `afptcpd.conf` file and starts the daemon. However, you can start the daemon by overriding configuration parameters specified in the conf file. To start the daemon by overriding configuration parameters, refer to the `afptcpd` man page.

To stop the daemon:

```
rcnovell-afptcpd stop
```

To check the status:

```
rcnovell-afptcpd status
```

To restart the daemon:

```
rcnovell-afptcpd restart
```

A.5 afpbind

Allows cluster pool names and virtual IP addresses to be advertised through the AFP server.

Syntax

```
afpbind [add] <cluster pool name> <virtual IP address>
```

```
afpbind [del] <cluster pool name> <virtual IP address>
```

A.6 afpnames

This command notifies the AFP server to operate a particular volume or all volumes in case-sensitive or case-insensitive mode. By default, new volumes or existing volumes operate in case-sensitive mode.

Syntax

`afpnames<case-sensitive | case-insensitive> <all | volume-name>`

A.7 migafp

Migrates the AFP service from NetWare to an OES system.

Syntax

`migafp -s <IP address of the source server> -u <DN of the source server admin> -w <Password for the source server admin> -h<Prints summary of the migration process>`

Example A-2 Example:

```
migafp -s 10.10.10.1 -u cn=sourceadmin.o=novell -w password
```


B Comparing AFP on NetWare and AFP on Linux

This section compares features and capabilities of Novell Apple Filing Protocol on the NetWare and Linux platforms for a Open Enterprise Server 2018 or later server.

Feature Description	AFP for NetWare	AFP for Linux
Administration	Limited to starting and stopping the server.	Ability to configure AFP server parameters through iManager. “Administering the AFP Server” on page 27
File names and paths	sys:\etc\ctxs.cfg sys:\etc\afpvols.cfg sys:\etc\afptcp.log	/etc/opt/novell/afptcpd/afpdirxtd.conf /etc/opt/novell/afptcpd/afpvols.conf /etc/opt/novell/afptcpd/afptcpd.conf /var/log/afptcpd/afptcp.log
Installation	Customized installation during installation of NetWare 6.5. See, “Installing Novell Native File Access Protocols on a NetWare 6.5 Server” in the <i>NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide</i>	Installation through YaST along with associated dependencies. “Installing and Setting Up AFP” on page 21
Simple password support	Yes	No
Universal Password	Yes. Limited to 8 characters.	Yes. More than 8 characters.
Migration support	Not Applicable	Support to migrate from NetWare to Linux. Support to migrate from Linux to Linux. “Migrating AFP to OES 2018 SP1” on page 37
Mac versions supported	Classic Mac, Mac OS 10.3, 10.4, 10.5, and 10.6	Mac OS 10.12 or later.
Cross-protocol locking	Supported for AFP, CIFS, and NCP.	Supported for AFP, CIFS, and NCP.

Feature Description	AFP for NetWare	AFP for Linux
Authentication methods	Cleartext	Cleartext
	Two-Way Random Key Exchange	Two-Way Random Key Exchange
	Random Exchange	Random Exchange
		Diffie Hellman Exchange
		Diffie Hellman Exchange 2
Dynamic detection of volumes	Yes	Yes
Choosing volumes to be exported	Yes	Yes
SLP and Bonjour support	Supports only SLP	Supports both SLP and Bonjour
Support for 64-bit architecture	No	Yes
Guest user support	Yes	Yes