AUTHORIZED DOCUMENTATION

Novell Apple* Filing Protocol for Linux* Administration Guide

Novell®
Open Enterprise Server

2 SP2

November, 2009

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide describes how to use the Novell® Apple Filing Protocol (AFP) service on a Novell Open Enterprise 2 SP 2 Linux Server to access and manage Macintosh* systems.

This guide is divided into the following sections:

Audience

The audience for this document is network administrators. This documentation is not intended for users of the network.

Documentation Updates

For the most recent version of the *Novell AFP Linux Administration Guide*, see the Novell Open Enterprise Server 2 SP2 Documentation (http://www.novell.com/documentation/oes2/).

Feedback

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

Additional Documentation

For information about AFP on NetWare®, see the *NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide*.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX *, should use forward slashes as required by your software.

Overview of AFP

1

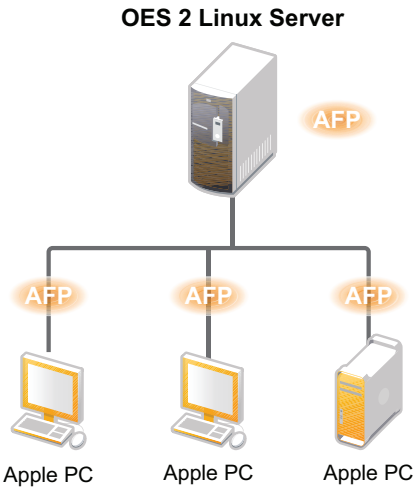
Novell® Open Enterprise Server (OES) 2 SP1 onwards provides the Novell Apple Filing Protocol (AFP) for Linux operating systems. AFP is a network protocol that offers file services for Mac* clients. OES 2 SP2 Linux currently supports AFP version 3.1.

1.1 Understanding AFP

Novell AFP (Apple Filing Protocol) lets Macintosh workstations access and store files on OES 2 SP2 Linux servers without installing any additional software. The AFP software is installed as part of OES 2 on the OES 2 SP2 Linux server and provides out-of-the-box network access. You can connect the network cable, start the Macintosh computer, and you have access to servers on your network.

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*



Enabling native protocols on a Linux server means that users can access files on the network, map network drives, and create shortcuts to the Linux servers by using the native methods available in their specific operating systems. 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 enables the users to seamlessly copy, delete, move, create, save, and open network files— just like they would if they were working locally.

AFP also provides integration with Novell 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.

1.2 AFP and Universal Password

Universal Password helps in management of password-based authentication schemes.The Universal password is not enabled by default. Each AFP user must be Universal Password enabled to be able to log in to the AFP server.

For details on Universal Password, see Novell Password Management (http://www.novell.com/documentation/password_management32/pwm_administration/index.html?page=/documentation/password_management32/pwm_administration/data/bookinfo.html)

1.3 AFP Features and Capabilities

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

- AFP parameter configuration and administration through iManager.
- Support for Mac OS* 10.3, 10.4, 10.5, and 10.6.
- Integration with Novell eDirectory.
- Migration capability from NetWare® to Linux.
- Cross-Protocol File Locking support between AFP, CIFS, and NCP™.
- Auditing support for File Access activities.
- Bonjour support for the AFP server discovery using the Bonjour protocol.
- Auditing and Monitoring support.
- Support for Unicode* filenames.
- Support for Universal Passwords longer than 8 characters.
- Clustering support for high availability.

1.4 What's Next

For information on new features in this release of AFP see, Chapter 2, "What's New," on page 13

What's New

2

This section describes additions to the Novell® Apple Filing Protocol (AFP) service for the Novell Open Enterprise Server 2 SP2 Linux platform and for maintaining feature parity with the existing solution on the NetWare® platform.

- **Bonjour Support:** This enables support for the AFP server discovery using the Bonjour protocol. It starts the avahi-daemon (similar to the slp daemon, it provides Bonjour™ discovery support). The AFP server uses the avahi-daemon to advertise its services.
- **Dynamic Volume Event Detection:** The AFP server now dynamically detects volume add/mount events, volume delete/umount events, and volume updates on the OES 2 server.A reload is not required when there is a change in the list of volumes mounted on the server
- **New Configuration Option:** EXPORT_ALL_VOLUMES is now a valid option in the afptcpd.conf file.
  - If the option is set to yes (the default value), the AFP Server exports all the available NSS volumes on the machine.
  - If the option is set to no, only the volumes listed in the afpvols.conf file are exported by the AFP Server.
- **Alias Names:** Specifying alias names for volumes in afpvols.conf file is mandatory in OES2 SP1. However, it is optional in OES2 SP2.
- **afpvols.conf Changes:** This file now acts as a resource for alias names and for the list of volumes to be exported.
- **Cluster Enabled Volumes Display:** When a MAC client connects to the physical IP of the AFP server, the local volumes and the cluster-enabled shared volumes are exported to the client. However, if the client connects to the cluster (virtual) IP, only the cluster-enabled shared volumes associated with the cluster IP are exported.
- **Alternate Guest Account Name:** This capability removes the restriction to have one preconfigured guest account. With OES2 SP2, any valid eDirectory™ user account name with appropriate privileges can be specified as a guest account name.
- **Cross-Protocol Lock Configuration Management Change:** Cross-protocol lock configuration is now managed centrally in the `ncpserv.conf` configuration file.
- Installation through YaST: Predefined system of installing the AFP service along with the associated dependencies.
- Secure authentication mechanism: DHX authentication provides a secure way to transport clear-text passwords of up to 64 characters to the server for further processing.
- Administering and Configuring parameters: Ability to administer and configure the AFP server through iManager.
- Auditing support: Helps you keep check on the authentication process and any changes that occur to the configuration parameters of the server.
- Monitoring support: Helps you assess the performance of the AFP server.
- Migrating to Linux platform: Ability to migrate the AFP service from NetWare to Linux.

Planning and implementing AFP

3

This section describes requirements and guidelines for using the Novell® Apple Filing Protocol (AFP) for Novell Open Enterprise Server (OES) 2 SP2 Linux servers.

3.1 Supported Platforms

Before installing AFP, ensure that your system meets the following requirements.

3.1.1 Server Requirements

- ❑ OES 2 SP1 Linux or later

3.1.2 Client Requirements

- ❑ Mac 10.3
- ❑ Mac 10.4
- ❑ Mac 10.5
- ❑ Mac 10.6

3.2 Requirements

- ❑ 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 (http://download.novell.com/Download?buildid=LYlbZMAom6k~).
- ❑ The AFP server requires at least one Read/Write replica in a tree with NMAS version 3.2 or later.

3.3 Antivirus Support

The Apple Filing Protocol (AFP) support for NSS files on OES 2 SP2 Linux is implemented via a technology that bypasses the real-time scanning employed by most OES 2 antivirus solutions. NSS files shared through an AFP connection might be protected by on-demand scanning on the OES 2 server or by real-time and on-demand scanning on the Apple client.

3.4 Unsupported Service Combinations

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

- Netatalk
- Novell Domain Services for Windows
- Xen* Virtual Machine Host Server

3.5 What's Next

To proceed with installation of AFP, see Chapter 4, "Installing and Setting Up AFP," on page 17

Installing and Setting Up AFP

4

This section describes how to install and configure the Novell® Apple Filing Protocol (AFP) on a Novell Open Enterprise Server (OES) 2 SP2 Linux server.

4.1 Installing AFP during the OES 2 SP 2 Installation

YaST uses a predefined system of installing components along with the associated dependencies. For a service to function properly, all the dependent products must be installed. Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

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 2 Linux installation process, see the *OES 2 SP2: 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)

     SMS helps back up file systems or applications on NetWare® and SUSE® Linux Enterprise Server (SLES) to removable tape media or other media for off-site storage.

   - Novell eDirectory

     eDirectory supports authentication of users.

   - Novell Linux User Management (LUM)

     LUM is a directory-enabled application that simplifies and unifies the management of user profiles on Linux-based platforms.

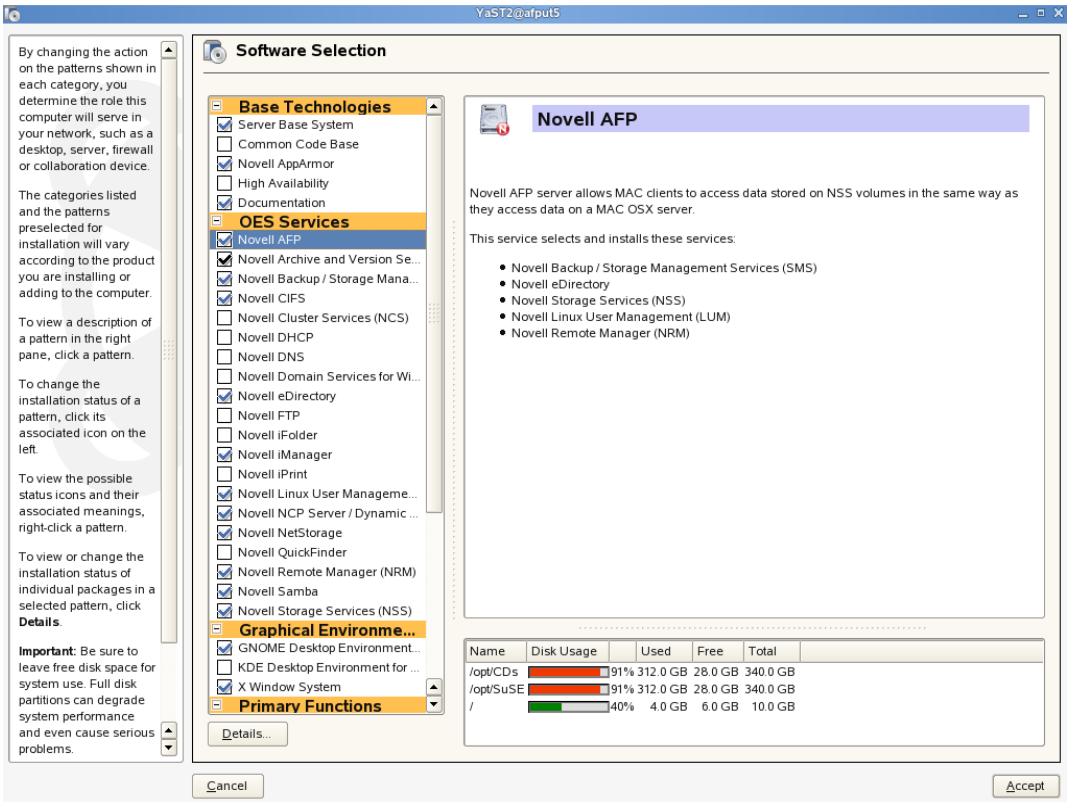
   - Novell Storage Services (NSS)

     Novell Storage Services™ helps you manage pools, and volumes on a Novell Open Enterprise Server 2 server.

     Novell AFP supports only Novell Storage Services (NSS) volumes.

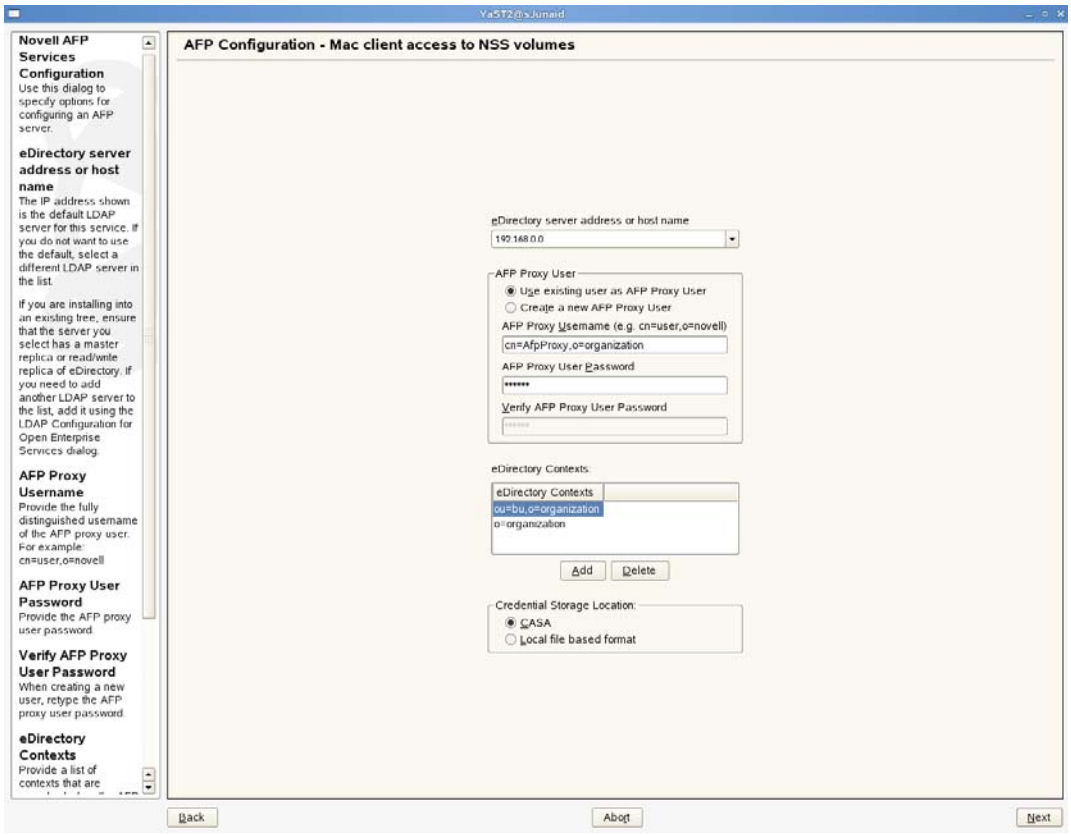
   - Novell Remote Manager (NRM)

     NRM for Linux is a browser-based utility that you can use to manage one or more Linux servers from a remote location.



3 To configure the AFP service, fill in the fields on the Configuration page.

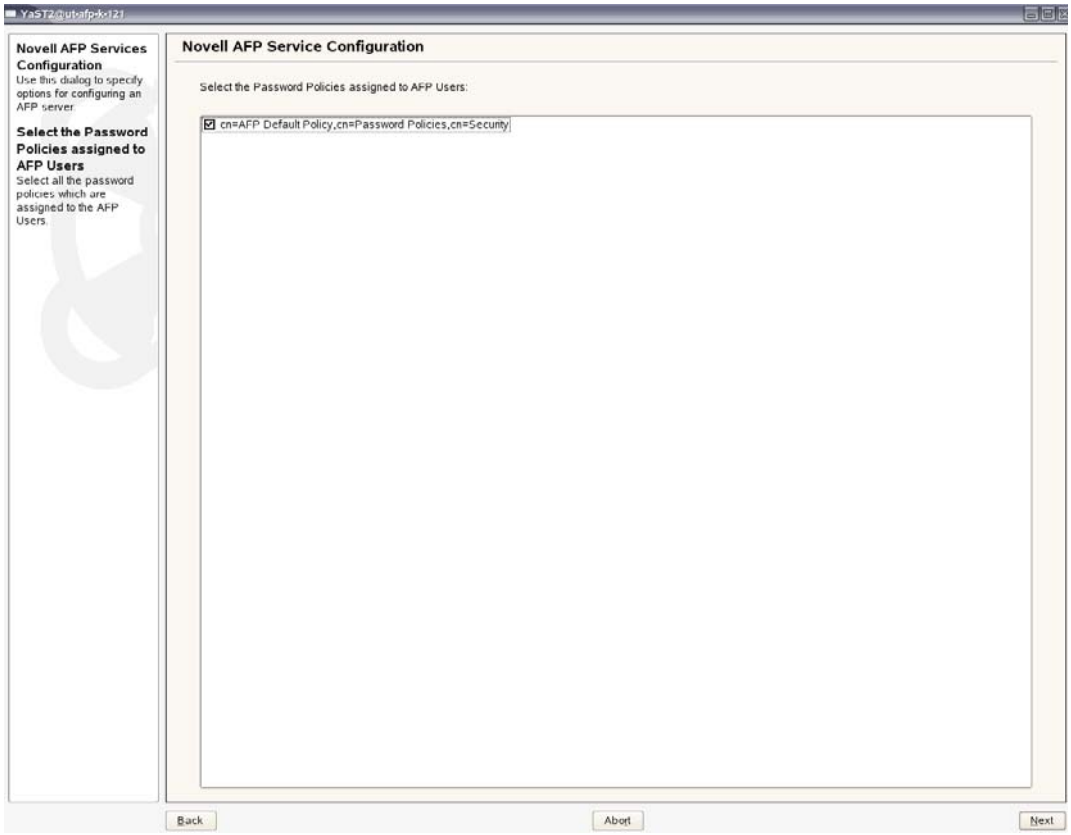
NOTE: AFP configuration fails when the container admin tries to add the proxy user as reader of passwords to the password policy. Configuration fails as the container admin does not have the write rights to the password policies in the security container. Provide the container admin create rights on the password policy container and rerun the configuration.



Configuration Parameter	Details
eDirectory server address or host name	Enter the IP Address in the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list.

Configuration Parameter	Details
AFP Proxy User	Select *Use existing user as AFP Proxy user* to use an existing proxy user to configure the AFP service.. Select *Create a new AFP Proxy user* to create a new proxy user to configure the AFP service. The AFP Proxy user: ◆ must be Universal Password enabled. ◆ must be added as a reader of passwords in the Universal Password policy. You can modify the proxy user details in CASA secret store using the casaforafp script. AFP proxy user requires rights to read the passwords of the AFP users in the AFP password policies. This cannot be performed by using casaforafp script only. When AFP proxy user information is modified, it is recommended that AFP should be reconfigured using `yast2 novell-afp` command. Else, the AFP administrator needs to manually grant the AFP proxy user rights to read passwords in password policies of AFP users through iManager.
AFP Proxy User Name	Specify the FQDN (fully qualified distinguished name) of the AFP proxy user. For example: cn=user, o=novell **NOTE:** This user is granted rights to read the passwords of any users, including non-AFP users, that are governed by any of the password policies you select in the Novell AFP Service Configuration page.
AFP Proxy User Password	Specify the password to authenticate to the AFP server. **NOTE:** User Credential Synchronization with eDirectory: If you need to change the AFP proxy user's name or password, you must use YaST and reconfigure AFP.
eDirectory Context	Specify the list of contexts to search for the AFP user, when the user enters the login credentials. 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.
Credential Storage Location	Specify where the user credentials of the AFP proxy server are to be stored. For security reasons, the default and recommended method of credential storage is CASA.

4 Click *Next* to continue with the AFP services installation.



NOTE: Installing novell-afptcpd also installs Audit and starts auditd.

4.2 Installing AFP after the OES 2 SP 2 Installation

If you did not install Novell AFP services during the OES 2 SP2 installation, you can install it later.

1 Invoke YaST Control Center. In left panel under *Groups* section click on *Open Enteprise Server* link. The OES Install and Configuration link opens the *Software Selection* page. Now select *Novell AFP*. Click *Accept*.

2 Installation starts.

After the install is finished, YaST displays a summary page indicating that AFP configuration is enabled. All the configured services are disabled in this page.

3 Select *AFP* to proceed with the configuration.

4 Specify the configuration details according to instructions in Step 3 on page 18

5 Click *Next* to continue.

4.3 Verifying the Installation

After the installation is done, you can verify that it succeeded using the following procedure:

1. Check for the following files in the `/etc/opt/novell/afptcpd` directory:
   - `afpdircxt.conf`
   - `afptcpd.conf`
   - `afpvols.conf`
2. Check the `afpdircxt.conf` file for the context added during installation.
3. (Conditional) If CASA is specified as the credential storage location, execute the `CASAcli` command at the console prompt to make sure that `afp-casa` is present in the CASA store.

   The output of the `CASAcli` command is as follows:

   ```
   # CASAcli -g -n afp-casa
   Getting afp-casa
   Name: afp-casa
   Key: Password (********)
   Key: CN (********)
   ```
4. (Conditional) If a local file is specified as the credential storage location, check for the `/etc/opt/novell/afptcpd/.afppwd.enc` file.
5. Check for the `/usr/share/mof/novell-afp-providers/AFPServices.mof` file.
6. Check for the following libraries under `/usr/lib/cmpi` on a 32-bit system and `/usr/lib64/cmpi` on a 64-bit system:

   ```
   libAFPConfigProvider.so
   libAFPConfigProvider.so.1
   libAFPConfigProvider.so.1.0.0

   libAFPContextProvider.so
   libAFPContextProvider.so.1
   libAFPContextProvider.so.1.0.0

   libAFPServicesProvider.so
   libAFPServicesProvider.so.1
   libAFPServicesProvider.so.1.0.0

   libAFPVolumeProvider.so
   libAFPVolumeProvider.so.1
   libAFPVolumeProvider.so.1.0.0
   ```

4.4 What's Next

For details on administering the AFP service, see "Administering the AFP Server" on page 23.

Administering the AFP Server

5

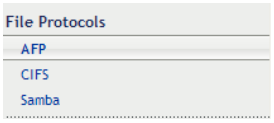
You can use Novell® iManager to change the configuration of your AFP server after AFP services have been installed on Novell Open Enterprise Server 2 (OES 2) SP2 Linux. The AFP configuration details are stored in a configuration file on the Linux server, and iManager provides an easy interface for changing the configuration details.

NOTE: Admin equivalent/container admin users should be LUM enabled to manage the AFP server through AFP iManager plug-in.

5.1 Selecting a Server to Manage

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 username 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 Novell 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 size of the data in the server.

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

Table 5-1 AFP Server Status

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* and *Reconnect Period*. Any change in these two parameters will require restarting of the AFP server. Reload doesn't affect the existing client connections to the AFP server.

5.2 Configuring General Parameters

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

1. Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username and password.
3. In the left column, select *File Protocols*, then click *AFP*.
4. Select the *General* tab.

   The following details are displayed:

- Section 5.2.1, “Security and Rights,” on page 24
- Section 5.2.2, “Threads and Connections,” on page 25
- Section 5.2.3, “Version and Logging,” on page 26
- Section 5.2.4, “Other Parameters,” on page 27

5.2.1 Security and Rights

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

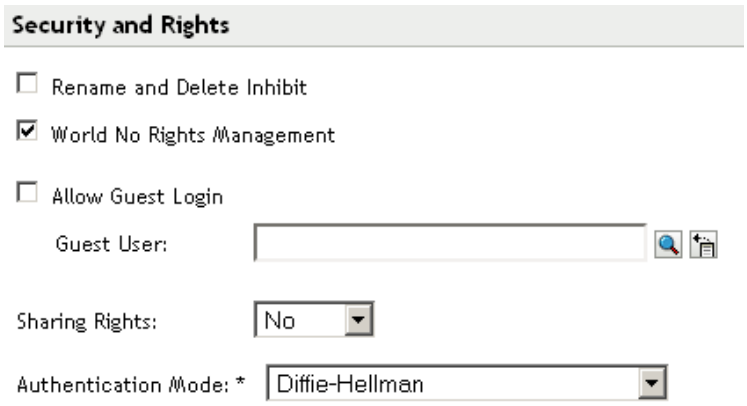


Table 5-2 *Security and Rights Configuration Parameters*

Setting	Description
Rename and Delete Inhibit	If this option is enabled, users are not permitted to rename or delete files from their home directories. To permit users to rename or delete files from their home directories, leave this option deselected.
Allow Guest Login	Select this option to allow users to log in as a guest.
World No Rights Management	Select this option to let users set permissions and give access to network directories and their contents to everyone (world). If this option is not selected, the AFP server ignores the Set Rights' requests coming from Macintosh clients, so the users cannot set permissions to give access to others.
Sharing Rights	Select this option to turn off fetching rights for the owner, groups, and everyone. Returns a set of default rights when queried.
Authentication Mode	Indicates the authentication mechanism to use. The supported methods are: ◆ Two-Way Random Key Exchange ◆ Cleartext ◆ Random Exchange ◆ Diffie Hellman

5.2.2 Threads and Connections

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

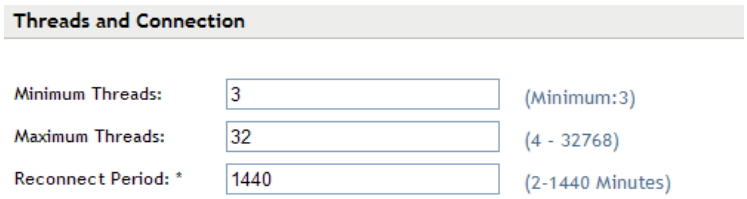
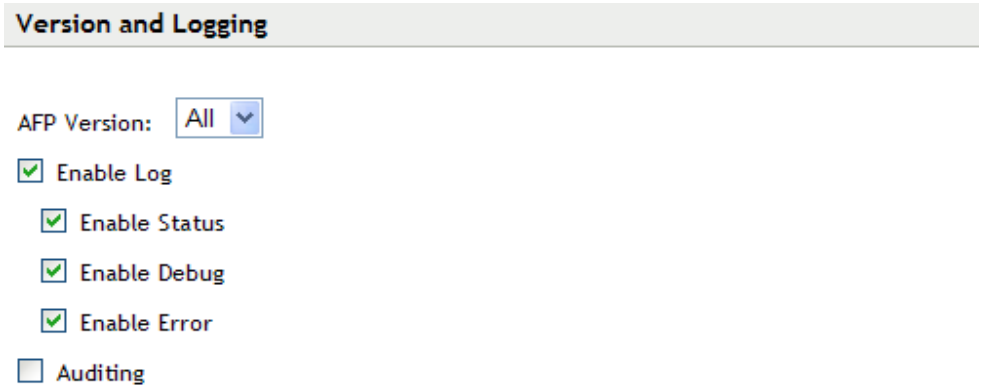


Table 5-3 *Threads and Connections Configuration Parameters*

Setting	Description
Minimum Threads	Indicates the minimum number of threads that should be set for the `afptcpd` daemon to start. The default value is 3. This value is set during installation.
Maximum Threads	Indicates the maximum number of threads that the AFP server can support. The maximum number of threads that can be supported is 32768.
Reconnect Period	Indicates the number of minutes the AFP server waits before attempting to reconnect. The minimum waiting time is 2 minutes and can extend up to 24 hours.

5.2.3 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 in the event of renaming the log file or changing the location of log file.

Table 5-4 *Version and Logging Configuration Parameters*

Setting	Description
AFP Version	Indicates the AFP versions that the AFP server can support. If you select *All*, AFP versions 2.2, 3.0 and 3.1 are supported.
Enable Log	Select this option to turn the logging feature on and add an entry to the log file. When logging is activated, AFP error messages are written to the `/var/log/afptcpd/afptcp.log` file.
Enable Status	Select this option if you want status messages to be recorded in the `/var/log/afptcpd/afptcp.log` file.
Enable Debug	Select this option if you want debug messages to be recorded in the `/var/log/afptcpd/afptcp.log` file.
Enable Error	Select this option if you want error messages to be recorded in the `/var/log/afptcpd/afptcp.log` file.
Auditing	Select this option, 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 `/var/log/audit/audit.log` file

5.2.4 Other Parameters

These parameters let you define the search parameters and unload behavior of the AFP server. Novell AFP supports only Novell Storage Services (NSS) volumes.

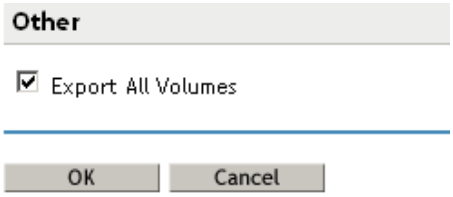


Table 5-5 *Other Parameters*

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 `afpvols.conf` 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, then the alternate name of the volume is displayed for export.

IMPORTANT: When OES2 SP1 AFP iManager plugin tries to manage a OES2 SP2 AFP server, configuration settings like *CROSS_PROTOCOL_LOCKS*, *NO_UNLOAD_TIME_CHECK*, *NO_COUNT_ON_OFFSPRING* cannot be managed as these options are removed from OES2 SP2 AFP Server. Similarly, the new settings *GUEST_USER* and *EXPORT_ALL_VOLUMES* added in OES2 SP2 AFP Server cannot be managed by OES2 SP1 AFP iManager plugin.

Specifying alias names for volumes in `afpvols.conf` file is mandatory in OES2 SP1. However, it is optional in OES2 SP2. Hence when an OES2 SP1 AFP iManager plugin tries to use the volume management feature of an OES2 SP2 AFP Server, it is mandatory to specify the alias name for the volumes.

5.3 Configuring Volume Details

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

Novell AFP supports only Novell Storage Services (NSS) volumes. NSS storage object names are case insensitive. Names such as AURORA, Aurora, and aurora are the same. Since NSS volume names are case insensitive, volumes which 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 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 lets the volumes mounted on clients have a clean unmount. Using the reload option for modification leads to irrecoverable issues and should be avoided.

Dynamic Detection of Volumes: The AFP server now dynamically detects adding/mounting a new NSS volume and deleting/unmounting an existing NSS volume. The AFP server updates itself with the current set of volumes on the OES 2 SP2 server. An explicit reload of the server is not required.

NOTE: The dynamic detection is applicable to standalone servers as well as cluster nodes.

Use the following tasks to administer AFP volume names:

5.3.1 Adding a New Volume Name

1. Start your browser (Internet* Explorer 5 or later, Firefox*, etc.) and specify 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 username 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.

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

5.3.2 Editing an Existing Volume Name

1. Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username 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*.

5.3.3 Deleting a Volume Name

1 Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username 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*.

5.3.4 Resetting the Desktop

1 Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username 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.

5.4 Configuring Context Details

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 username, the server searches through each context in the list until it finds the correct user object.

5.4.1 Adding a New Context

1. Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username 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. Use the *Object Selector* to select the server you want to modify.

   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.

5.4.2 Removing an Existing Context

1. Start your browser (Internet Explorer 5 or later, Firefox, etc.) and specify 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 username 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. Use the *Object Selector* to select the server you want to modify.

   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*.

5.5 Rights to a File or Folder

Returning rights to a file or a folder by AFP server is controlled through the rights configuration parameter. There are three options - *All*, *Default*, and *No*. If you do not wish to use the *All* parameter option, then set the option to *Default* or *No* option. The following lists the details for the configuration parameters:

- By setting the *Rights* parameter to *No*, rights returned by AFP server is set to returning the owner id for files or folders. AFP server does not calculate group and other rights for files and folders when *Rights* is set to *No*. In this case, AFP server returns default server id 0 (that is mapped to the username *Root*) for group and other rights.
- By setting *Rights* parameter to *Default*, AFP server turns off rights calculations for all the rights. AFP server returns AFP server id in this case which is set to 0 for owner, group, and other rights. This is because, after setting *Rights* configuration option to default, no rights calculations is performed for files and folders. Setting this option results in improved performance (compared to when *Rights* option is set to *All*) when files and folders have large number of trustees which requires more processing for calculating group rights.
- By setting *Rights* parameter to *All*, AFP server returns correct owner id that is set on a file/folder. For other IDs, AFP server finds the group or user trustee which has maximum rights on the file/folder. This group or user is then returned to other ID parameter when *Rights* option is set to *All*. For finding a group or user name with maximum rights, AFP server scans all the trustees assigned to a file/folder. This calculation takes more time when trustees assigned to a file/folder are large in numbers.

Migrating AFP from NetWare to OES 2 SP2 Linux

6

The Open Enterprise Server (OES) 2 SP2 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 an OES 2 SP2 Linux server 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 2 SP2: Migration Tool Administration Guide*.

For more information on migrating AFP, see "Migrating AFP from NetWare to OES 2 SP2 Linux "in the *OES 2 SP2: Migration Tool Administration Guide*.

Running AFP in a Virtualized Environment

7

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) 2 SP2 Linux, and require no special configuration or other changes.

To get started with virtualization, see "Introduction to Xen Virtualization (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_basics.html)" in the *Virtualization with Xen (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)* guide.

Configuring AFP with Novell Cluster Services for an NSS File System

8

Novell® Apple Filing Protocol can be used in a cluster environment with Novell Cluster Services™ on your Novell Open Enterprise Server 2 (OES 2) SP2 Linux server.

8.1 Benefits of Configuring AFP for High Availability

When you configure AFP in an OES 2 SP2 cluster, resources can be dynamically switched or moved to any server in the cluster. Resources can be configured to automatically switch or be moved in the event of 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 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*

8.2 Volumes in a Cluster

In a cluster setup, when a MAC client connects to the physical IP of the AFP server, both the local volumes as well as 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 serversrunning on nodes A & B. If the cluster resource is bound to A, a MAC client connecting to the physical IP of A can access both the local and the cluster enabled shared volumes.

If the client connects to the physical IP of B, then only local volumes on B are exported since the cluster resource is now on A.However, due to migration or failover, if the cluster resource is moves to B, then clients connecting to 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

- Section 8.2.1, "Volume Name Management in a Cluster," on page 38

8.2.1 Volume Name Management in a Cluster

Volume management is done in two ways in a cluster:

- Using iManager AFP Management Plugin:
  - The iManager AFP Management Plugin requires a volume to be locally mounted on the cluster node before adding it to the AFP configuration. Hence migrate the volume resource to each node and use iManager AFP Management Plugin to add the volume to the AFP configuration.
- By editing `/etc/opt/novell/afptcpd/afpvols.conf` on each cluster node. This is done without migrating the resource to each node. Enter the following syntax:

  ```
  ServerName.VolumeName      VolumeName
  ```

  Where ServerName is the host name of the local cluster node and VolumeName is the name of the shared, cluster-enabled volume.

8.3 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 8.3.1, "Identifying the Nodes to Host the AFP Service," on page 38
- Section 8.3.2, "Installing Novell Cluster Services," on page 38
- Section 8.3.3, "Creating Shared NSS Pools," on page 39
- Section 8.3.4, "Reviewing Load and Unload Scripts," on page 40

8.3.1 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 4, "Installing and Setting Up AFP," on page 17.
2. Restart the AFP server.
3. Continue with Section 8.3.2, "Installing Novell Cluster Services," on page 38.

8.3.2 Installing Novell Cluster Services

1. Install Novell Cluster Services 1.8.4 on the OES 2 SP2 Linux server. For details, see "Installing Novell Cluster Services on OES 2 Linux".
2. When you have finished installing Novell Cluster Services, continue with Section 8.3.3, "Creating Shared NSS Pools," on page 39.

8.3.3 Creating Shared NSS Pools

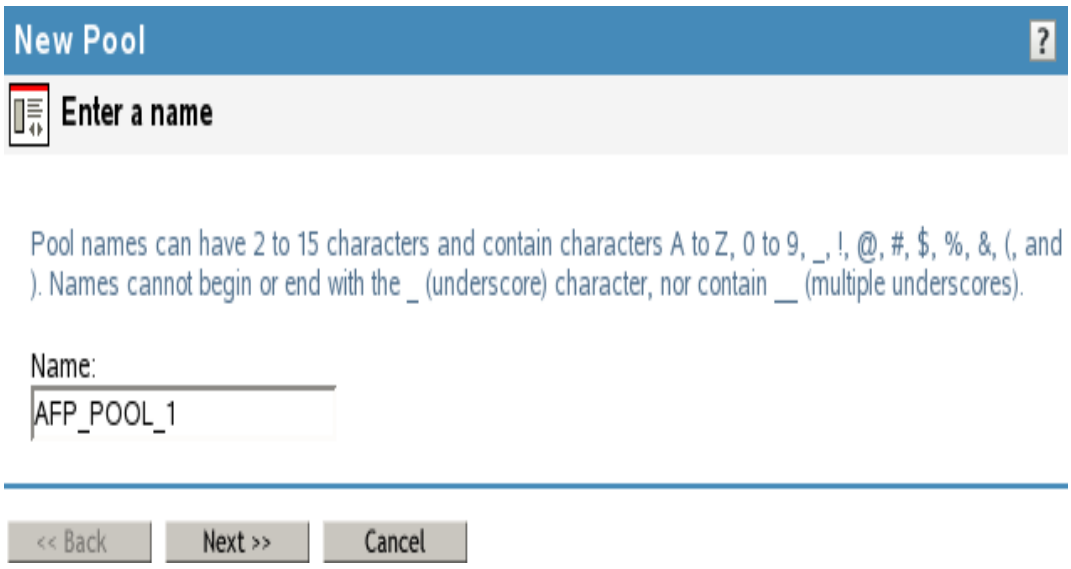
You can create a pool by using iManager or the NSSMU utility. The shared partition is automatically created when you create the pool.

- "Creating Shared Disk Partitions and Pools through iManager" on page 39
- "Creating Shared Disk Partitions and Pools through NSSMU" on page 39

Creating Shared Disk Partitions and Pools through iManager

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 username and password.
3. In the left pane, locate and select the *Storage* > *Volumes* task.
4. Specify a cluster server name or browse and select one, then click *New*.

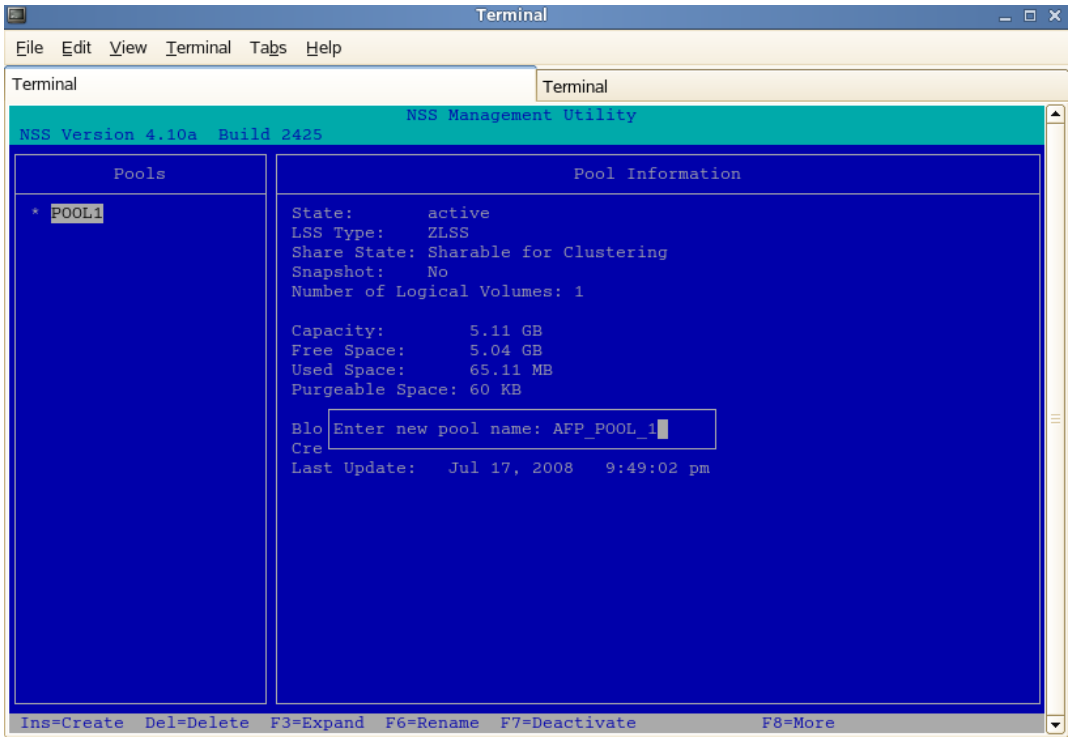


5. Specify the new pool name and click *Next*.
6. Allocate the size of the pool and click *Next*.
7. Specify an IP address for the virtual server.

   Make sure you select AFP as the advertising protocol. You should also make sure that NCP™ is selected. NCP is essential to activate the NCP protocol on the cluster.
8. Click *Finish* to complete configuration of the pool.
9. Continue with "Reviewing Load and Unload Scripts" on page 40.

Creating Shared Disk Partitions and Pools through NSSMU

1. From the NSSMU main menu, select *Pools*.



2 Select the device where you want the pool to be created.

3 Specify the name of the pool and the IP address of the virtual server.

Make sure you select AFP as the advertising protocol. You should also make sure that NCP is selected. NCP is essential to activate the NCP protocol on the cluster.

4 Click *Apply* to complete configuration of the pool.

5 Continue with Section 8.3.4, “Reviewing Load and Unload Scripts,” on page 40.

8.3.4 Reviewing Load and Unload Scripts

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

3 In the left pane, locate and select the *Cluster* > *Cluster Manager* task.

4 Select the cluster resource and click the *Scripts* tab. The Load and Unload scripts are displayed. Ensure that your load and unload scripts resemble the following examples:

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
exit_on_error nss /poolact=POOL1
exit_on_error ncpcon mount VOL2=253
exit_on_error ncpcon mount VOL1=254
exit_on_error add_secondary_ipaddress 192.168.0.0
exit_on_error ncpcon bind --ncpservername=CLUSTER1_POOL1_SERVER --
ipaddress=192.168.0.0
exit_on_error cluster_afp.sh add CLUSTER1_POOL1_SERVER 192.168.0.0
exit 0
```

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
ignore_error cluster_afp.sh del CLUSTER1_POOL1_SERVER 192.168.0.0
ignore_error ncpcon unbind --ncpservername=CLUSTER1_POOL1_SERVER --
ipaddress=192.168.0.0
ignore_error del_secondary_ipaddress 192.168.0.0
ignore_error nss /pooldeact=POOL1
exit 0
```

Working with Macintosh Computers

9

This section contains the following information:

9.1 Administrator Tasks for Macintosh

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

9.1.1 Configuring a Guest User Account

AFP lets you configure a guest user account through iManager.

1. In Novell® iManager, click the *Roles and Tasks* button. *Novell iManager 2.7.3 Administration Guide*.
2. Click *Users* > *Create User*.
3. Specify a username 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 as described in “Editing the Context Search File” on page 44.
9. Reload the AFP server to make the *Guest* button available on the login screen.

   To reload the AFP server through iManager, see Section 5.1, “Selecting a Server to Manage,” on page 23.

9.1.2 Editing the Volume File

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

To edit the `afpvols.conf` file to 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.sys System Volume
   server1.img Graphics
   ```

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

9.1.3 Editing the Context Search File

A context search file allows Macintosh users to log in to the network without specifying their full context. The context search file contains a list of contexts that are searched when no context is provided or the object cannot be found in the provided context. When the Macintosh user enters a username, the server searches through each context in the list until it finds the correct user object.

Macintosh allows only 31 characters for the username. If the full eDirectory context and username are longer than 31 characters, you must use a search list to provide access.

If User objects with the same name exist in different contexts, the first one in the context search list is used.

To edit the context search file:

1. Using any text editor, edit the `afpdirctx.conf` file stored in the `/etc/opt/novell/afptcpd/` directory of the AFP server.
2. On separate lines, enter the contexts to search.

   For example, if you had users with full eDirectory distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then enter the following contexts in the `afpdirctx.conf` file:

   ```
   ou=sales.o=acme
   ou=graphics.ou=marketing.o=acme
   ou=marketing.o=acme
   ```

3. After you have made the changes, save the file.

When a Macintosh user logs in with a username and password, the system finds the context corresponding to the user object in the `afpdirctx.conf` file.

9.1.4 Editing the Configuration File

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

Your configuration file resembles the following example:

```
# 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
```

9.2 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 9.2.1, "Accessing Network Files," on page 45
- Section 9.2.2, "Logging In to the Network As a Guest," on page 46
- Section 9.2.3, "Changing Passwords from a Macintosh Computer," on page 46
- Section 9.2.4, "Assigning Rights and Sharing Files from a Macintosh Computer," on page 46

9.2.1 Accessing Network Files

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

1. In Mac OS 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

   or

   In Mac OS X, click *Go* > *Connect to Server*.
2. Specify the IP address or DNS name of the OES 2 SP 2 Linux server, then click *Connect*.
3. Specify the username 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.

9.2.2 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 43, Macintosh users can log in to the network as a Guest.

1. In Mac OS 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

   or

   In Mac 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.

9.2.3 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 Mac OS 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

   or

   In Mac 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 username.
4. Click *Change Password*.
5. Type the old password and the new password, then click *OK*.

9.2.4 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

Using Chooser/Finder to access network files and folders is fairly 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

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 a 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 are not able to 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 means 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 has access control rights to the folder.

If the user has access control rights, then it 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.

Display only allows for 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.

Monitoring the AFP Server

10

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

10.1 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

10.2 Enabling Monitoring

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

```
afpstat
```

10.3 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 Novell® 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.

10.4 Understanding Performance Parameters

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

Table 10-1 *AFP Server Performance Parameters*

Parameter	Description
Active Threads	Indicates the number of threads that are presently active on the AFP server.
Load Ratio	Indicates the ratio of the total number of active threads to the total number of threads in the AFP server.
Availability	Indicates 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	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 5.2, “Configuring General Parameters,” on page 24. 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.
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.

Auditing the AFP Server

11

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

11.1 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 OES2 SP2.

However, if it is enabled, you can disable Audit configuration option in /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 following files:

  ```
  afptcpd.conf
  afpvols.conf
  afpdirctx.conf
  casaforafp.sh
  ```

11.2 Enabling Auditing

You can enable auditing either through the command line or through iManager.

11.2.1 Command Line

To enable auditing support through command line, use the following command:

```
afptcpd - a
```

11.2.2 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 Novell® 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 on 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.

IMPORTANT: When you manually make changes to the configuration parameters in the configuration files, the changes do not take effect until you restart the server.

11.3 Viewing Auditing Information

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

Your log file resembles 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

**********************************************************************
```

Troubleshooting AFP

12

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

For additional troubleshooting information, see the Novell Support Web site (http://support.novell.com)

12.1 AFP Login Issues

12.1.1 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.

12.1.2 AFP User Login to a Mac 10.5 Client Fails With a Connection Failed Error

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.

12.1.3 Invalid Username and Password Error

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.

12.2 Starting the AFP Server

12.2.1 Starting the AFP Daemon Failed

Action: If you are not able to start the AFP daemon, check the status of the `xregd` daemon to see if it is running. To do this, execute the following command at the prompt:

```
rcnovell-xregd status
```

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

12.3 File Creation

12.3.1 Failure to Create a File on a Mac 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.

12.4 Displaying Volumes

12.4.1 Volumes Tab on a Mac 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.

12.5 Log Messages

This section describes some commonly encountered log file messages and provides suggestions for resolving them.

12.5.1 nmasldap_get_password for user failed with error 1697

Cause: This error occurs because the eDirectory™ user is attempting to log in to an AFP server that is not part of any password policy or is not part of a password policy that is Universal Password enabled.

Action: To resolve this error, use the *Password* > *Password Policies* task to assign the user to a valid password policy.

12.5.2 nmas_ldap_get_password failed with error 1659

Cause: This error is logged when the eDirectory user attempting to log in to the AFP server is assigned to a policy that is enabled for Universal Password but its password is not synchronized with the NDS® password.

Action: To resolve this error, use one of the following methods:

- Log in to an iManager server with the NDS password. Use the *Password* > *Password Policies* task to select the option to set the Universal Password.
- As an administrator of the AFP server, set the default authentication mechanism to *Cleartext* or *Diffie Hellman*. The AFP server uses the passwords to do the synchronization as part of background processing.

For all the subsequent login attempts, the Universal Password is synchronized with the NDS Password.

12.5.3 NWDSResolveName failed to resolve supplied name <*user name*>

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

Action: To resolve this error, review the eDirectory contexts, using the details in "Configuring Context Details" on page 30.

12.5.4 zOpen on volume <VOLUME_NAME> failed

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

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

12.5.5 AFP proxy user authentication failed

Cause: This error occurs if the AFP proxy user entered during installation is an invalid user. It can also occur in cases where the AFP proxy user is valid but the password credentials entered during the installation do not match with the credentials stored in CASA or in a file.

Action: To resolve this error, reconfigure AFP according to the instructions in "Installing AFP after the OES 2 SP 2 Installation" on page 21 and provide correct proxy credentials.

12.5.6 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 command `ulimit -n <value>`) or close some of the open files ensuring that the number of open files does not exceed the ulimit value.

12.6 AFP Server Responds Slowly

Cause: This issue occurs in certain scenarios where the number of trustees on files / directories are high. This happens because the AFP server attempts to retrieve the rights of each trustee on the file / folder and return the trustee with the maximum rights as the owner / group of the file / folder.

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

12.7 Operation fails when a Mac client mounts an NSS volume and tries to open certain files

Cause: Mac 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.

Security Guidelines for AFP

13

This section describes security issues and recommendations for the Novell® Apple Filing Protocol (AFP) for a Novell Open Enterprise Server 2 SP2 Linux server. It 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.

13.1 Recommended Authentication Protocol

The recommended protocol for authentication is Diffie Hellman (DHX). It provides 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, if the eDirectory™ password is longer than 8 characters, any attempt to log in results in failure.

13.2 Storing Credentials

We recommend that you specify CASA as the credential storage location during configuration of the AFP service. This ensures that your credentials are safe.

13.3 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™.

13.4 Rights for the Proxy User

By default, the AFP proxy user does not have permission to read the passwords for users of a password policy. The AFP user can log in to the AFP server only when the AFP proxy user is granted rights to read the password in the password policy.

13.5 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 25.

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

Command Line Utilities for AFP

A

This section details the syntax and options for the following Novell® Apple Filing Protocol (AFP) utilities for Novell Open Enterprise Server 2 SP2 Linux.

A.1 afpdtreset

Resets the desktop database on a volume.

Syntax

```
afpdtreset
```

A.2 afpstat

Displays statistics for the afp daemon.

Syntax

```
afpstat
```

A.3 afptcpd

The daemon for the Novell AFP server.

Syntax

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

A.4 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.5 migafp

Migrates the AFP service from NetWare® to a Linux system.

Syntax

`migafp` -s <*IP address of the source server*> -u <*DN of the source server admin*> -w <*Password for the source server admin*> -b <*DN of the target server admin*> -x <*Password for the target server admin*> -q <*Port Number for the destination ldap server*> -t <*1 for ssl bind 0 for non-ssl bind*> -f <*full path of file containing the Password Policy DNS, each separated by a new line*>

Example

migafp -s 10.10.10.1 -u cn=sourceadmin.o=novell -w password -b cn=targetadmin.o=novell -x password -q 689 -t 1 -f /tmp/passwordpolicyfdn.ldf

A.6 casaforafp Script

`casaforafp` script is used by the AFP YaST install to configure AFP service. To execute it from the command line, run the `casaforafp` command without any arguments.

- This utility prompts you for the *proxy username* and *password* and stores these credentials in the CASA.
- Furthermore, it restarts the *cimom* daemon to ensure that the AFP iManager files are picked.
- It makes `novell-afptcpd` a boot daemon and enables the syslog service for AFP.
- It adds the Avahi (for bonjour support) as a boot daemon and starts the AFP service if not already running.

Comparing AFP on NetWare and AFP on Linux

B

This section compares features and capabilities of Novell® Apple Filing Protocol™ on the NetWare® and Linux platforms for Novell Open Enterprise Server 2 SP2 servers.

Feature Description	AFP for NetWare	AFP for Linux
Administering	Limited to starting and stopping the server. See "Enabling and Disabling AFP" in the *NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide*	Ability to configure AFP server parameters through iManager. "Administering the AFP Server" on page 23

File Names and Paths	`sys:\etc\ctxs.cfg`
	
	`sys:\etc\afpvol.cfg`
	
	`sys:\etc\afptcp.log`
		`/etc/opt/novell/afptcpd/afpdircxt.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 *NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide*	Installation through YaST along with associated dependencies. "Installing and Setting Up AFP" on page 17
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. "Migrating AFP from NetWare to OES 2 SP2 Linux" on page 33
Mac versions supported	Classic Mac, Mac OS 10.3, 10.4, 10.5, and 10.6	Mac OS 10.3, 10.4, 10.5, and 10.6.
Cross-Protocol Locking	Supported among AFP, CIFS, and NCP.	Supported between 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
Dynamic detection of volumes	Yes	Yes
Choosing volumes to be exported	Yes	Yes
Bonjour Support	No	Yes
Support for 64-bit architecture	No	Yes

Documentation Updates

C

C.1 January 2010

- The following note is added in Section 4.1, “Installing AFP during the OES 2 SP 2 Installation,” on page 17:

  NOTE: Installing novell-afptcpd also installs Audit and starts auditd.

C.2 November 2009

- The following is added in Section 5.2.4, “Other Parameters,” on page 27:

  When OES2 SP1 AFP iManager plugin tries to manage a OES2 SP2 AFP server, configuration settings like *CROSS_PROTOCOL_LOCKS*, *NO_UNLOAD_TIME_CHECK*, *NO_COUNT_ON_OFFSPRING* cannot be managed as these options are removed from OES2 SP2 AFP Server. Similarly, the new settings *GUEST_USER* and *EXPORT_ALL_VOLUMES* added in OES2 SP2 AFP Server cannot be managed by OES2 SP1 AFP iManager plugin.

  Specifying alias names for volumes in `afpvols.conf` file is mandatory in OES2 SP1. However, it is optional in OES2 SP2. Hence when an OES2 SP1 AFP iManager plugin tries to use the volume management feature of an OES2 SP2 AFP Server, it is mandatory to specify the alias name for the volumes.
- Section 8.2.1, “Volume Name Management in a Cluster,” on page 38 is added to Chapter 8, “Configuring AFP with Novell Cluster Services for an NSS File System,” on page 37.
- Section 12.6, “AFP Server Responds Slowly,” on page 56 is added to Chapter 12, “Troubleshooting AFP,” on page 53.
- In Section 5.2.4, “Other Parameters,” on page 27, Off Spring Count and Cross Protocol information is removed.
- Frontfile updated with the release date as November, 2009.
- The Load and Unload scripts are revised in Chapter 8, “Configuring AFP with Novell Cluster Services for an NSS File System,” on page 37.
- Section 12.5.6, “zAFPCountByScanDir: scandir failed,” on page 56 is added in Chapter 12, “Troubleshooting AFP,” on page 53.
- Section 3.3, “Antivirus Support,” on page 15 is added.
- Section 5.5, “Rights to a File or Folder,” on page 32 is added in the Chapter 5, “Administering the AFP Server,” on page 23.

- The following content is included in the Chapter 4, “Installing and Setting Up AFP,” on page 17:

  The AFP Proxy user:

  - must be a member of the Universal Password policy.
  - must be added as a reader of passwords in that policy.

- The following is included in the Chapter 5, “Administering the AFP Server,” on page 23:
  - The AFP volume share name supports all ASCII characters except NULL, colon(:), and forward slash(/).
- AFP now supports Bonjour. A new screenshot and a writeup is included in the “Installing AFP during the OES 2 SP 2 Installation” on page 17 in the Installing and Setting Up AFP chapter.
- The following note is included in “Administering the AFP Server” on page 23:

  NOTE: Admin equivalent/container admin users should be LUM enabled to manage the AFP server through AFP iManager plugin.

- *Cross Protocol Lock* and *Export All Volumes* are documented in the Section 5.2.4, “Other Parameters,” on page 27 in the Administering the AFP Server chapter.
- An important note is included in the Section 5.3, “Configuring Volume Details,” on page 28 as follows:

  IMPORTANT: Do not edit the afpvols.conf file for a volume that is already mounted and are already in use (mounted on AFP clients). However, if there is a need to modify the file, only restart of the server is recommended. This lets the volumes mounted on clients to have a clean unmount. Using the reload option for modification leads to irrecoverable issues and is recommended to avoid.

- The following description is included in the Section 5.3, “Configuring Volume Details,” on page 28:

  Dynamic Detection of Volumes: AFP server now dynamically detects adding/mounting a new NSS volume and deleting/unmounting an existing NSS volume. The AFP server updates itself with the current set of volumes on the OES 2 SP2 server. An explicit reload of the server is not required.

  NOTE: The dynamic detection is applicable to standalone servers as well as cluster nodes.

- A note is included in Installing AFP during the OES 2 SP 2 Installation section in Chapter 4, “Installing and Setting Up AFP,” on page 17 as follows:

  NOTE: AFP configuration fails when the container admin tries to add the proxy user as reader of passwords to the password policy. Configuration fails as the container admin does not have the write rights to the password policies in the security container. Provide the container admin create rights on the password policy container and rerun the configuration.

C.3 November 2008

- All chapters and sections are new additions to OES 2 SP1 release.