Novell Advanced Audit Service

www.novell.com

ADMINISTRATION GUIDE

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Advanced Audit Service
October 2001
103-000165-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a trademark of Novell, Inc.
eDirectory is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
NLM is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Storage Services is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

Understanding Novell Advanced Audit Service

Novell® Advanced Audit Service (NAAS) enables you to audit services running on the network. NAAS uses Novell eDirectory™ for storing policies and configuration information, and for managing access to the audited data. The main components of NAAS are:

Audit Utility - Provides a user interface for communicating with the audit framework. Using this utility, you can configure and view the Audit policies, and view the audit data stored in the Audit database.

Audit Agent - Resides on each machine that is hosting the services you want to audit. The agent performs the following tasks:

- Collects audit events from the audited services based on the policy.
- Stores the audit records locally, and periodically forwards them to the Audit server.

Audit Server - Collects the audit records from the Audit agents and stores them in the database. The Audit server also services queries from the Audit utility for reading these audit records and performs the necessary access control.

Audit Database - Stores the audit records.

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.

1 Installing Novell Advanced Audit Service

This section contains the system requirements for Novell® Advanced Audit Service (NAAS), and the procedure for installing the Audit utility and the default configuration utility. The basic configuration details are also given here.

During the express installation of NetWare® 6, NAAS will be installed by default.

During the custom installation of NetWare 6, NAAS is displayed in the list of products. Select NAAS to install it with NetWare 6.

If NAAS is not selected during NetWare 6 installation it can be installed as an add-on product using the source Netware 6 installation CD. To install as an add-on product:

1. Load the NetWare 6 source CD in the CD drive.
2. At the server console, type **`Startx`**.
3. From the NetWare interface, click Install.

   A list displays, showing products that have been installed.
4. Click Add.
5. Click the Browse icon and select the path of the source CD.

For example, the path can be SOURCE DIRECTORY/SERVER/PRODUCT.NI.

A list of products with the size and description of each component that can be installed is displayed.

6 Select NAAS and proceed with the installation.

System Requirements

The system must meet the following hardware and software requirements for installing NAAS.

Hardware Requirements

- Audit Agent - 3.37 MB
- Audit Server - 1.45 MB
- Audit Utility - 6.68 MB
- Default Configuration Utility - 1.41 MB
- Memory requirements are the same as ConsoleOne™ 1.2d on Windows* and NetWare 6.

Software Requirements

Audit Agent

- ❑ NetWare 6

Audit Utility

- ❑ Windows* 95, 98, 2000, or NT Service Pack 4 or later
- ❑ ConsoleOne version 1.2d

Audit Server

- ❑ NetWare 6
- ❑ Pervasive.SQL* 2000 and Pervasive JDBC driver or Oracle* 8i on NetWare and the Oracle JDBC driver

  The Pervasive SQL.2000 will be installed as a part of NetWare 6. The Pervasive JDBC driver and The Oracle JDBC driver will be installed as part of the NAAS Audit server.

- Windows 95, 98, 2000, or NT Service Pack 4 or later
- ConsoleOne version 1.2d
- Client NICI (Novell International Cryptography Infrastructure) 128-bit version 1.5.7 or higher. This can be downloaded from the Novell download site (http://www.novell.com/download)

  NOTE: You need to install Client NICI 1.5.7 or higher even if Client NICI 128-bit version 2.0.2 is already installed. Client NICI of version 1.5.7 and 2.0.2 can co-exist.

Installing the NAAS Utility and Default Configuration Utility

1. Run the N_Snapin.exe available in SYS:\AUDIT folder. This file was copied as part of NAAS components installed on the server.
2. Enter the path to the ConsoleOne home directory. The default path to ConsoleOne is C:\NOVELL\CONSOLEONE\1.2.
3. Continue with "Post-Installation Steps If You Are Using the Pervasive Database" on page 11.

Post-Installation Steps If You Are Using the Pervasive Database

1. The Pervasive database server should be started before continuing with the post-installation steps. To start the server, type **`mgrstart`** at the server console.
2. Execute the command **`psregsvr sys:\system\mkc.nlm`** at the server console.
3. By default, two licenses are provided for Pervasive. For unlimited licenses for 90 days, run the Pervasive utility by typing the following command at the server console.

   `NWUCINIT -C11 -Q sys:\pvsw\license2`

   SYS:\PVSW refers to the directory in which Pervasive is installed.

   To view the installed licenses, type the following command at the server console.

   `NWUCUTIL -g11`

4. Install the Pervasive client on a Windows machine by running SYS:\PVSW\CLIENTS\WIN\SETUP.EXE, available on the NetWare 6 server.

   For information on Pervasive 2000i client compatibility with different versions of the Windows operating system, refer to the Pervasive 2000i Readme file.

5. From the client, start the Pervasive Control Center by clicking Start > Programs > Pervasive > Pervasive Control Center.

6. Right-click Pervasive.SQL 2000i Engine > click Register New Engine.

7. Enter the name of the server where the Audit database is to be hosted.

8. Browse to the database folder.

9. Right-click Databases > click New Database.

10. In the New Database wizard, enter the following details.

    - Server Name
    - Interface - Select Engine as the interface type
    - User Name - The server administrator name in the format .admin.novell
    - Password for the server administrator.

11. Click Next.

12. Enter NAASADMN as the database name and \\Netware_server_name\sys:_netware as the directory > click Next.

13. Click Finish.

    A new database is created and an informational message is displayed. .

14. Click OK

    The NAASADMN entry will appear below Databases in the left pane.

After you complete the post-installation tasks, NAAS must be configured before you can use the components. You can run the NAAS default configuration utility to do this, or you can do the configuration manually. For information on the default configuration utility, see “NAAS Default Configuration Utility” on page 13. For information on manual configuration, see “Manually Configuring Novell Advanced Audit Service” on page 23.

2 NAAS Default Configuration Utility

The Novell® Advanced Audit Service (NAAS) default configuration utility performs automatic default configuration of the system. This utility must be used only after installing NAAS and completing the Post-Installation Steps If You Are Using the Pervasive Database (page 11).

Default Configuration of NAAS

NAAS is configured on a per-partition basis.

To automatically configure NAAS:

1. In ConsoleOne™, select a partition root object for configuration.
2. Click Tools > Configure NAAS. A new dialog box to select a configuration task is displayed.

   NOTE: The configuration utility can also be run by right-clicking the selected partition root object and selecting Configure NAAS.
3. In the Select Configuration Task dialog box, select one of the following tasks > click OK.

   NOTE: The following tasks should be performed in the same sequence as they are listed below.

   - “Setting Up the NAAS Database” on page 14
   - “Setting Up the NAAS Agent” on page 14
   - “Setting Up the NAAS Server” on page 15
   - “Configuring the NAAS Framework” on page 15

Setting Up the NAAS Database

This utility should be run separately for configuring every database. Typically, one database should be configured for each partition.

NOTE: Make sure you have completed the post-installation tasks (see "Post-Installation Steps If You Are Using the Pervasive Database" on page 11 for details) before you set up the NAAS database.

1. In the Select Configuration Task dialog box, select Set Up NAAS Database > click OK to display a dialog box to enter details about the database.
2. Select the database type. NAAS supports both Oracle and Pervasive.SQL 2000.
3. Specify the database (server) IP address.
4. Specify a new password for the NAAS Super User.
5. Re-enter the password.
6. If the selected database type is Oracle, enter the database administrator name (DBA name) and the password (DBA password).

   Any Oracle* database will have the valid DBA name system and the password manager that is created during the database installation. You can use these values if necessary.
7. Click OK to activate automatic configuration of the NAAS database.
8. Continue with "Setting Up the NAAS Agent" on page 14.

Setting Up the NAAS Agent

This utility should be run separately for configuring every Audit agent.

1. In the Select Configuration Task dialog box, select Set Up NAAS Agent > click OK to display a dialog box where you can select the host server.
2. Click Browse > select the host server where you are setting up the agent.
3. Click OK to activate automatic configuration of the NAAS Agent on the server you selected.
4. Continue with "Setting Up the NAAS Server" on page 15.

Setting Up the NAAS Server

This utility should be run separately for configuring every Audit server. Typically, one or two servers should be configured for each partition.

1. In the Select Configuration Task dialog box, select Set Up NAAS Server > click OK to display a dialog box where you can select the host server.
2. Click Browse > select the host server where you are setting up the NAAS server.
3. Click OK to activate automatic configuration of the NAAS server on the server you selected.
4. Continue with "Configuring the NAAS Framework" on page 15.

Configuring the NAAS Framework

This procedure creates all policies, objects, and related templates with default values. These values should be modified based on the auditing requirements.

1. In the Select Configuration Task dialog box, select Configure NAAS Framework > click OK to display the Select Auditor dialog box.
2. Click Browse to select the user who will have Audit rights > click OK to configure the NAAS framework.

   The configuration is completed and you can modify the default values for the various components, if required (see "Modifying Default Values" on page 18).

Default Configuration Performed by the Utility

The Agent policy governs the functioning of the Audit agent. It contains various parameters that are used by the Audit agent to configure itself.

A single Agent policy is configured for all the NAAS agents in the partition.

The default values for the parameters of the Agent policy are given in the following table.

Parameters	Default Values
Commit Period - Sets the time interval (in seconds) for periodic commits of the Audit agent's cache to the database.	3600
Commit Fragment Size - Specifies the fragment size (in bytes) of the commit. The commit data is divided into manageable blocks called fragments to send to the Audit server.	2 KB
Commit Compression - Select ON to compress the commit data before it is sent to the Audit server.	ON
Cache Size - Specifies the maximum size (in bytes) of the Audit agent cache. If the cache cannot be committed and reaches the cache size, no more data will be stored in the cache, and auditing will be suspended until data in the cache is committed.	10 KB
Cache Threshold - Specifies the threshold cache size (percentage of the cache size). If the Audit agent cache is utilized up to this threshold before the specified commit period, the Audit data will be committed automatically.	90%

These default values can be modified later using the modification procedure provided for “Audit Agent Policy” on page 18.

After the automatic configuration of the Audit agent, the default configuration utility proceeds with the configuration of Audit server.

The Server policy governs the functioning of the Audit server. It contains various parameters that are used by the Audit server to configure itself.

A single Server policy is configured for all the NAAS servers in the partition.

The default values for the parameters in the Server policy are given in the following table.

Parameters	Default Values
Auditor Rights Recalculation Period - Specifies the time interval (in seconds) for recalculating audit trail rights of the Auditors connected to the Audit server. The Audit trail rights are calculated by the Audit server based on the eDirectory rights of the Auditor. The rights are recalculated periodically when the auditor is connected to the server for a long period of time.	3600
Database polling Period - Specifies the time interval (in seconds) for polling the database. If the database is down, the audit data is stored locally on the Audit server. Periodic polling of the database ensures that the data on the local machine is transferred to the database, once the database is up.	900

These default values can be modified later using the modification procedure provided for "Audit Server Policy" on page 19.

After the configuration of the Audit server, the default configuration utility proceeds with the configuration of audited services.

A default configuration is done for three audited services: eDirectory, NWFS (NetWare legacy file system), and NSS (Novell Storage Services™).

NAAS Event Policy Template objects are created for each of these services in the NAAS Container. This container will be present just below the partition root object. The names of the template objects are DSEventPolicyTemplate, FSEventPolicyTemplate, and NSSEventPolicyTemplate.

IMPORTANT: These objects should not be modified manually.

An Event Policy object is also created in the NAAS container for each audited service. The names of these policies are DSEventPolicy, FSEventPolicy, and NSSEventPolicy. In these policies, the action flag for all the events is set to IGNORE by default, which implies that no event is being audited. These policies are made applicable to all the objects in the partition.

Auditing for some events can be activated using the modification procedure provided for “Audited Services” on page 19.

For more details about the various event policies and event policy templates, refer to “Using Novell Advanced Audit Service” on page 31.

After the configuration of the audited services, the default configuration utility proceeds with the configuration of the Auditor.

The NAAS Auditor is an entity that views the audit trail.

The selected user is given the necessary rights for connecting to an Audit server and viewing the audit data for all the audited objects in the partition.

These rights provided to the Auditor can be modified later using the procedure provided for the “Auditor Rights” on page 20.

Modifying Default Values

Audit Agent Policy

To modify the default values set for the Audit agent policy:

1. In ConsoleOne, locate the NAASAgentPolicy object in the NAAS container. The container will be just below the partition root object.
2. Right-click the object > click Properties.
3. Go to the Policy Content tab.
4. Modify the values there according to your requirements.

   NOTE: The Commit Period must be greater than 30 seconds. The Commit Fragment Size should be greater than 300 bytes. The Cache Size should be greater than 1 KB.

   These changes are applicable to all agents in the partition. If you want to configure different policies for different agents, refer to “Configuring the Agent and the Server” on page 23 instructions.

Audit Server Policy

To modify the default values set for the Audit server policy:

1. In ConsoleOne, locate the NAASServerPolicy object in the NAAS container. The container will be just below the partition root object.
2. Right-click the object > click Properties.
3. Go to the Policy Content tab.
4. Modify the values there according to your requirements.

   These changes are applicable to all servers in the partition. If you want to configure different policies for different servers, refer to "Configuring the Agent and the Server" on page 23 instructions.

Audited Services

By default, no events are audited.

To activate auditing for specific events and services:

1. In ConsoleOne, select the specific Event Policy object from the following Event Policy objects. These objects are in the NAAS container just below the partition root.
   - DSEventPolicy
   - FSEventPolicy
   - NSSEventPolicy
2. Right-click the object > click Properties
3. Go to the Policy Content tab.
4. Modify the action flag and filtering condition for the events, according to your requirements.

   These changes are applicable to all audited objects in the partition. If you want to configure different policies for different audited objects, refer to "Manually Configuring Novell Advanced Audit Service" on page 23 chapter.

Auditor Rights

A user's rights to the audit data are controlled by the rights to the naasTrail attribute in eDirectory. The default configuration utility grants the Auditor rights to view the audit data for the entire partition.

To enable auditor rights:

1. In ConsoleOne, select the partition root object.
2. Right-click the object > select Trustees of this Object.
3. Select the Auditor from the trustee list > click Assigned Rights.
4. From the Property list, select naasTrail and check the Read right from the Rights list > click OK.

To grant an Auditor rights to the audit trail for a particular object:

1. In ConsoleOne, select the required object.
2. Right-click the object > select Trustees of this Object > click Add Trustee.
3. Browse to the Auditor user object, select the User object > click OK.
4. Click Add Property.
5. Check Show all Properties.
6. Select the naasTrail attribute > click OK.
7. Check the Read right > click OK.
8. Apply the changes.

Starting the Audit Server

The Audit server should be started before you start the Audit agent.

1. Type **ST_SRVR.NCF** at the server console to start the Audit server.

   NOTE: If the database is Oracle, the JDBC driver path setting in the ST_SRVR.NCF file should be changed to refer to the Oracle JDBC driver.

   For example, the JDBC driver path setting can be

   envset JDBC_DRIVER_PATH=sys:\audit\classes111.zip.

2. Check to see if the Audit server is up and running.

   2a. Type **java -show** at the server console.

   The audit.server.SocketServer class should be displayed.

   2b. Ensure that the adserver.nlm module is loaded. Type **m adserver** at the server console to verify this.

Starting the Audit Agent

The Audit server should be started before you start the Audit agent.

1. Type ST_AGENT.NCF at the server console to start the Audit agent.
2. Check if the NAAS agent is up:

   2a. Type **java -show** at the server console. This should display the audit.client.tester class.

   2b. Ensure that the adagent.nlm and jadagent.nlm modules are loaded. Type **m adserver** at the server console to verify this.

Loading the Shims

DS Shim

Load DS Shim only after the agent is up.

1. Type **dsshim** at the server console.
2. To check if the DS Shim is running, type **m dsshim** at the server console.

FS Shim

Load FS Shim only after the agent is up.

1. Type **fsshim** at the server console.
2. To check if the FS Shim is running, type **m fsshim** at the server console.

NSS Shim

Load NSS Shim only after the agent is up.

1. Type **nssshim** at the server console.
2. To check if the FS Shim is running, type **m nssshim** at the server console.

Starting the Audit Utility

Run ConsoleOne from client machine to start the Audit utility.

Stopping the Audit Server

1. Unload Java*.
2. Unload ADSERVER.NLM.

Viewing NAAS Error Logs

In case of an error during execution, NAAS server-side components log the error messages in error logs. The error logs for the components can be viewed from the following files.

Component	Log files
Audit agent	SYS:\ETC\ADAGERR.LOG and SYS:\ETC\AGENT.ERR
Audit server	SYS:\ETC\SERVER.ERR

3 Manually Configuring Novell Advanced Audit Service

This chapter contains configuration details for all the components of Novell® Advanced Audit Service (NAAS). The configuration is done using the Audit utility.

Prerequisites

Before configuring the Agent and the Server, the following procedures need to be completed.

- ❑ Setting Up the NAAS Database (page 14)
- ❑ Setting Up the NAAS Agent (page 14)
- ❑ Setting Up the NAAS Server (page 15)

Configuring the Agent and the Server

NAAS assumes partition-based auditing, where the domain for auditing is a Novell eDirectory™ partition. All the Audit agents will audit only those objects that are in the same eDirectory partition as the agent. Also, the Audit agents will read only those policies that are in the same partition. All policies outside the partition are ignored, even if they are associated with one of the objects within the partition. Refer to the following sections for performing manual configuration.

- "Configuring the Audit Agent" on page 24
- "Configuring the Audit Server" on page 25

The user can also configure the Audit agent, Audit server, and the policies by using the procedure provided in “NAAS Default Configuration Utility” on page 13.

WARNING: All the objects created and configured manually should be deleted before running the default configuration utility.

Configuring the Audit Agent

The Audit agent collects audit data and sends it to the Audit server. It resides on the same machine where the audited service is hosted.

The configuration information for an Audit agent is stored in eDirectory as an Agent policy. The Agent policy governs the functioning of the Audit agent and contains information such as the size of the Audit agent cache, the time interval for periodic commits of the Audit agent's cache to the database, and the Audit servers that can be contacted to commit the data.

Configuring the Audit Agent

1. In ConsoleOne™, right-click the desired container > click New > Object > naasAgentPolicy.
2. Set the desired values for all the configuration parameters.

   NOTE: The Commit Period must be greater than 30 seconds. The Commit Fragment Size should be greater than 300 bytes. The Cache Size should be greater than 1 KB.
3. Follow the steps detailed in “Associating the Policy” on page 26 to associate the policy to the Agent object.
4. Grant the Agent object Read rights to this policy object using the normal eDirectory rights mechanism.
5. Grant the Agent object Read rights to the naasPolLink and naasSearchPolLink attributes for the entire tree.
6. Grant the Agent object Read rights to the naasPortNumber and HostDevice attribute of the server objects to be contacted.
7. Grant the Agent object Read rights to the Network Address attribute of the NetWare® server object hosting the audit server.

Configuring the Audit Server

The Audit server stores and manages audit trails and gives real-time notification of events.

The configuration information for an Audit server is stored in eDirectory as a Server Policy object. The Server Policy object governs the functioning of the Audit server and contains information such as the name of the database to store audit data, the time interval for polling the database, and the time interval for recalculating the audit trail rights of the auditors connected to the Audit server.

Configuring the Audit Server

1. In ConsoleOne, right-click a Container object > click New > Object > naasServerPolicy.
2. Set the desired values for all the configuration parameters > click OK.
3. Follow the steps detailed in "Associating the Policy" on page 26 to associate the policy to the specified Server object.
4. Grant the Server object Read rights to this policy object using the normal eDirectory rights mechanism.
5. Grant the Server object Read rights to the database object for the database to be used, using the normal eDirectory rights mechanism.
6. Grant the Server object Read rights to the naasPolLink, naasSearchPolLink, and ACL attribute for the entire tree.
7. Grant the Server object Read rights to the naasRandomNance attribute and naasSelectedDomain attributes for the entire tree.
8. Grant the Server object Write rights to its own naasPortNumber attribute.

Configuring the Audit Server for Real-Time Alert Notification

1. Open the SYS:\AUDIT\MAILALERT.CFG configuration file for real-time alert notification. This file will be installed along with the NAAS components in the server.
2. Enter the name of the mail server (SMTP server) to be contacted for real-time alerts as the first line in the configuration file.
3. Enter the list of recipients' e-mail IDs, separated by a comma or space, in the second line of the configuration file. All these recipients will receive the real-time alert notification.

   IMPORTANT: The real-time alert configuration file should be on the same machine as the Audit server.

Associating an Audit Policy to an Object

An Audit policy can either be associated directly to an object, to one of its parent containers, or to one of the groups to which the object belongs. When the NAAS framework searches for the policy applicable to an object, it must know the order in which to search for the policy. The three possible places for the search are at the object, at the container, and at the group. The search order and the level is provided by the Search Criteria policy.

The Search Criteria policy can either be associated directly to the object, or to one of its parent containers. The NAAS framework begins the search for the effective Search Criteria policy at the object (O) and then at each parent container (C). The first policy that is located is set as the effective Search Criteria policy for the object. If no policy is found, the default Search Criteria policy is assumed as the effective policy (object > group > container). Once the effective Search Criteria policy for an object is determined, the same policy is used to evaluate the effective policy of any other type for that object.

If the default Search Criteria policy is suitable, you do not need to create a customized Search Criteria policy. If it is not, the policy should be created with the desired parameters and associated with the object or with its parent containers, as applicable.

NOTE: Grant the Agent objects Read rights on all configured policies.

Creating the Search Criteria Policy

1. In ConsoleOne, right-click a Container object > click New > naasSearchCriteriaPolicy.
2. Set the desired values for all the configuration parameters > click OK.
3. Follow the steps in “Associating the Policy” on page 26 to associate the policy to the required object or to its parent container.

Associating the Policy

You can associate the policy by using either of the following methods:

1. Select an object.
2. Go to the properties page of that object.
3. Click Associated NAAS Policies > click Add.
4. Select the policy to be associated > click OK.

or

1. Select a policy object.
2. Go to the properties page of that policy object.
3. Click Associated Objects > click Add.
4. Select the object to be associated > click OK.

Finding the Effective Audit Policy for an Object

1. In ConsoleOne, right-click the object for which the effective policies are to be retrieved.
2. Click Properties > Associated NAAS Policies > Get Effective Policy.
3. Select the type of policy > click OK. (For event policies, the Service ID and Service Version also need to be specified).

   The name of the applicable policy is displayed.

Configuring DS Auditing

If the NAAS Default Configuration Utility has been run, Event Policy Templates for Directory Services (DS) will already be present and should be used for creating more policies. Additional templates for the same service should not be created. If the default automatic configuration utility is run, start with Step 2.

1. Create an Event Policy Template for DS.
   - **1a** Select a container > New > Object > naasEventPolicyTemplate.
   - **1b** Enter the Service Identifier as eDirectory.
   - **1c** Enter the Service Version as 1.0.
   - **1d** Select the applicable data policy types. The applicable data policies are naasUserPolicy, naasSourceMachinePolicy, and naasTargetMachinePolicy.
   - **1e** Check Associable to All Object Types in the Schema.
   - **1f** To generate the event list, click Read From File > type EVENTS.TXT, which is the name of the file containing the list of DS events.

     The EVENTS.TXT file is located in the SYS:\AUDIT\NAASEVENTS directory.

2 Create one or more DS Event Policies.

2a Select a container > New > Object > naasEventPolicy.

2b Select an existing DS Event Policy Template.

3 Configure the policies based on the requirements.

4 Associate the policy to the objects that are to be audited. For more details see "Associating an Audit Policy to an Object" on page 26.

5 Grant the specific Audit agent Read rights to these policies.

6 Load the DS Shim from the server console by using the following command:

```
Load sys:\system\dsshim
```

7 Move on to "Starting the Audit Agent" on page 21.

Configuring FS Auditing

If the NAAS Default Configuration Utility has been run, Event Policy Templates for File System (FS) will already be present and should be used for creating more policies. Additional templates for the same service should not be created. If the Default Configuration utility has been run, skip to Step 2.

1 Create an Event Policy Template for FS.

1a Select a container > New > Object > naasEventPolicyTemplate

1b Enter the Service Identifier as NWFS.

1c Enter the Service Version as 1.0.

1d Select the applicable data policy types. The applicable data policies are naasUserPolicy, naasSourceMachinePolicy, naasFilePolicy, and naasTargetMachinePolicy.

1e Select Volume as the Associable Object Type.

1f To generate the event list, click Read From File > type FSEVENTS.TXT, which is the name of the file containing the list of FS events.

The FSEVENTS.TXT file is located in the SYS:\AUDIT\NAASEVENTS directory

2 Create one or more FS Event Policies.

2a Select a container > New > Object > naasEventPolicy.

2b Select an existing FS Event Policy Template.

3 Configure the policies based on the requirements.

4 Associate the policy to the file volumes that are to be audited. For more details, see “Associating an Audit Policy to an Object” on page 26.

5 Grant the specific Audit agent Read rights to these policies.

6 Load the FS Shim from the server console by using the following command:

```
Load sys:\system\fsshim
```

7 Move on to “Starting the Audit Agent” on page 21.

Configuring NSS Auditing

If the NAAS Default Configuration Utility has been run, Event Policy Templates for Novell Storage Services™ (NSS) have already been created. If this is the case, skip Step 1 and begin with Step 2.

1 Create an Event Policy Template for NSS.

1a Select a container > New > Object > naasEventPolicyTemplate.

1b Enter the Service Identifier as NSS.

1c Enter the Service Version as 1.0.

1d Select the applicable data policy types. The applicable data policies are naasUserPolicy, naasSourceMachinePolicy, naasFilePolicy, and naasTargetMachinePolicy.

1e Select Volume as the associable object type.

1f To generate the event list, click Read From File > type NSSEVENTS.TXT, which is the name of the file containing the list of NSS events.

The NSSEVENTS.TXT file is located in the SYS:\AUDIT\NAASEVENTS directory.

2 Create one or more NSS Event Policies.

2a Select a container > New > Object > naasEventPolicy.

2b Select an existing NSS Event Policy Template.

3 Configure the policies according to the requirements.

4 Associate the policy to the file volumes that are to be audited. For more details see “Associating an Audit Policy to an Object” on page 26.

5 Grant the specific Audit agent Read rights to these policies.

6 Load the NSS Shim from the server console by using the following command:

```
Load sys:\system\nssshim
```

7 Move on to “Starting the Audit Agent” on page 21.

4 Using Novell Advanced Audit Service

This section provides basic details for installing, configuring, and using Novell® Advanced Audit Service (NAAS).

Installing NAAS

See “Installing Novell Advanced Audit Service” on page 9 for information about installing NAAS.

Configuring NAAS Components

You can run the NAAS default configuration utility to perform automatic default configuration of the Audit agent, Audit server, audited services, and the Auditor. The default values created during this configuration can be modified later. For more information, see “NAAS Default Configuration Utility” on page 13.

You can also configure NAAS manually by following the steps described in “Manually Configuring Novell Advanced Audit Service” on page 23.

Auditing NDS

Audit Novell eDirectory™ by following the steps described in “Configuring DS Auditing” on page 27.

Auditing NWFS

Audit NWFS (NetWare Legacy File System) by following the steps described in “Configuring FS Auditing” on page 28.

Auditing NSS

Audit NSS (Novell Storage Services™) by following the steps described in “Configuring NSS Auditing” on page 29.

Associating Policies

Policies can be associated to the objects, groups or containers. For more details, see “Associating an Audit Policy to an Object” on page 26.

Creating and Modifying Audit Policies

Creating an Audit Policy

1. In ConsoleOne™, right-click the desired container > click New > Object.
2. Select the policy to be created > click OK. The corresponding policy creation screen will appear.

Modifying an Audit Policy

1. Select the policy for which the properties are to be modified.
2. Click Properties from the File menu in the ConsoleOne. The property page of that corresponding policy will appear. You can also double-click the policy to invoke its property page.
3. Modify the required parameters > click Apply > OK.

Viewing the Audit Trail

For viewing the audit trail, the user should be set as the Auditor with rights to view the audit trail. See the steps below for more information.

Setting the User As Auditor

1. Create one or more Auditor domains (see “Auditor Query Domains” on page 34 for more information).

   In ConsoleOne, right-click the desired container > click New > Object > NAASAuditorQueryDomain.
2. Right-click the User object.
3. Select Extensions > Add Extension > NAASAuditor.
4. Add one or more Auditor query domains.
5. Set one of the configured Auditor query domains as the preferred domain.

   This step is mandatory. This setting can be modified later in the Properties page of the Auditor.
6. Configure one or more Audit servers that the auditor can contact.

The servers configured here must have Read rights to the NaasRamdomNance and NaasSelectedDomain attributes of this user. Also, the servers must have Read rights for the Auditor query domains configured in step 4.

7. Grant the Auditor Read rights to the naasPortNumber and HostDevice attributes of the Audit server objects to be contacted.
8. Grant the Auditor Read rights to the NetworkAddressattribute of the NetWare server objects hosting the audit servers to be contacted.

Granting Rights for Viewing the Audit Trail

The Audit server supports fine-grained access control to the Audit data based on eDirectory rights. Every audit record contains a Target Object Name that corresponds to the name of the object in eDirectory, on which the audited event was generated.To view the audit records, a user must have Audit rights to the eDirectory object that is set as the target object. Having Audit rights to an object means having Read rights to the naasTrail attribute on that object.

The normal eDirectory Rights granting mechanism can be used for this purpose. All the normal rules of rights flowing down the tree are applicable here.

Also for connecting to the audit server, the auditor should have Read rights to the LDAP Server attribute and the LDAP:keyMaterialName attribute for the entire partition.

Auditor Query Domains

A domain is essentially a subset of the eDirectory tree. When the Auditor connects to an Audit server, the server queries all objects in the Auditor's domain and builds a list of objects to which the Auditor has Audit rights. An Auditor Query domain specifies the boundaries within which the Audit server should query objects.

IMPORTANT: Only those Audit reports that belong to the object in the preferred domain will be displayed to the Auditor. To retrieve reports of objects that are outside the preferred domain, the Auditor must reset the preference to the domain to be queried.

Auditing Events Generated by Specific Users

Events generated by specific users can be audited by using the User policy containing that user. This policy contains a list of users and an action flag for each user. The action for the event generated by the specific user will be executed based on the corresponding action flag.

To create and associate a User policy:

1. Select a container.
2. Click New > Object > New naasUserpolicy.
3. Specify a name for the new policy > click Define Additional Properties > click OK.

   The Properties page is displayed.
4. Add the users whose actions are to be audited, with an appropriate action flag for each user.
5. Make this policy applicable to appropriate audited objects.
6. Grant the appropriate Audit agent objects Read rights to this policy.

NOTE: For auditing events generated by specific users, an Event policy must also be present. In the Event policy, if the filter condition for any event is set to DON'T CARE or the action flag is set to IGNORE, the User policy will not be applied for that event. In this case, the event will be audited irrespective of the user who generated it. The filtering condition should be set to either AND or OR for the event to be audited based on the corresponding user.

Auditing Events Generated on Specific Files

Events generated on specific files can be audited using the File policy containing the specific file name. This policy holds a set of file names and the corresponding action flags. This policy is specific to the file system and is applicable only to volume objects. Action flags indicate the action to be taken for events involving the file.

To create and associate a File policy:

1. Select a container.
2. Click New > Object > New naasFilePolicy.
3. Add the files that are to be audited, with the appropriate action flag for each file. For example, \system\test.txt (do not include the volume).

4. Make this policy applicable to appropriate audited volumes.
5. Grant the appropriate Audit agent objects Read rights to this policy.

NOTE: For auditing events generated on specific files, an Event policy must also be present. In the Event policy, if the filter condition for any event is set to DON'T CARE or the action flag is set to IGNORE, the File policy will not be applied for that event. In this case, the event will be audited irrespective of the file on which it was generated. The filtering condition should be set to either AND or OR for the event to be audited based on the corresponding file.

Auditing Events Generated from Specific Source Machines

Events generated from a specific source machine can be audited using the Source Machine policy. This policy contains a set of DNS names or IP addresses of the source machines, and an action flag for each machine. The action for the event generated from the specific source machine will be executed based on the corresponding action flag.

To create and associate a Source Machine policy:

1. Select a container.
2. Click New > Object > New naasSourceMachinepolicy.
3. Add the DNS names or IP addresses of the source machine whose actions are to be audited with the appropriate action flag for each machine.
4. Make this policy applicable to appropriate audited objects.
5. Grant the appropriate Audit agent objects Read rights to this policy.

NOTE: For auditing events generated from specific source machines, an Event policy must also be present. In the Event policy, if the filter condition for any event is set to DON'T CARE or the action flag is set to IGNORE. The Source Machine policy will not be applied for that event, and the event will be audited irrespective of the source machine from which it was generated. The filtering condition should be set to either AND or OR for the event to be audited based on the corresponding source machine.

Auditing Events Generated on Specific Target Machines

Events generated on a specific target machine can be audited using the Target Machine policy. This policy contains a set of DNS names or IP addresses of the target machines, and an action flag for each machine. The action for the event generated on the specific target machine will be executed based on the corresponding action flag.

To create and associate a Target Machine policy:

1. Select a container.
2. Click New > Object > New naasTargetMachinePolicy.
3. Add the DNS names or IP addresses of the target machines whose actions are to be audited with the appropriate action flag for each machine.
4. Make this policy applicable to appropriate audited objects.
5. Grant the appropriate Audit agent objects Read rights to this policy.

NOTE: For auditing events generated on specific target machines, an Event policy must also be present. In the Event policy, if the filter condition for any event is set to DON'T CARE or the action flag is set to IGNORE. The Target Machine policy will not be applied for that event, and the event will be audited irrespective of the target machine from which it was generated. The filtering condition should be set to either AND or OR for the event to be audited based on the corresponding target machine.

Setting Search Criteria for Policies

The search criteria for the policies can be set using the Search Criteria policy.

For more information on setting the search criteria, see "Associating an Audit Policy to an Object" on page 26.

Setting Filters for Viewing Events

Filters are used for filtering the data logged in the audit trail. Users can control what audit data is displayed to them by configuring and applying filters. The types of filters are:

- "Filter Sets" on page 38
- "Event Filters" on page 38
- "Data Filters" on page 38

IMPORTANT: You need to be an auditor to create and use filters. See "Setting the User As Auditor" on page 33 for details.

Filter Sets

Filter sets allow the user to group event filters and data filters together.

Event Filters

Event filters filter the audit data based on the event name. Each event filter corresponds to an audited service.While creating a new event filter, you must specify the name of the Event Policy template that corresponds to the audited service.

Data Filters

Data filters filter the audit data based on the contents of the event data fields, such as the name of the user who generated the event, the machine on which the event was generated, the action taken by NAAS for an event, and the success code of the event. The types of data filters are:

- Username filters
- Source IP filters
- Target IP filters
- Action taken filters
- Success code filters

Username Filters: Filter the audit data based on the name of the user who perpetrated the event.

Source IP Filters: Filter the audit data based on the IP address of the machine from where the event was generated.

Target IP Filters: Filter the audit data based on the IP address of the machine on which the event was generated.

Action Taken Filters: Filter the audit data based on the action taken by NAAS for an event. The actions can be:

- Log - Records the event in the audit database.
- Raise Alert - Raises a real-time alert when the event occurs.

This filter must be specified numerically. Action = 1 means the event is logged and Action = 2 means the event was logged and a real-time alert was also raised.

Success Code Filters: Filters the audit data based on the success code of the event. The success code for an event provides details on whether the event went through successfully or failed with some error code.

Creating Filters

1. Select Filter from the NAAS menu. This will display a list of existing filters.
2. Click New to create a new filter.
3. Type the name of the filter.
4. Select the filter type.
5. If the filter type is Event Filter, browse or type the name of the event policy template that corresponds to an audited service.
6. Click OK. An empty filter is created in the database and a new screen to set the properties for this filter is displayed.

Editing Filters

1. Select Filter from NAAS menu. This will display a list of existing filters.
2. Select the filter to be edited > click Edit.
3. Based on the type of filter, follow the steps below:

   Edit Filter Sets: Add or delete names of existing filters that are to be grouped together in the specific filter set.

   Editing Event Filters: Each event filter corresponds to some audited service. The edit screen displays the list of events exposed by that audited service. Turn on the events that are to be included in the audit report. For those events that are turned on, an appropriate filter condition should also be specified. The filter conditions are:

   - DON'T CARE - The event will be included in the report irrespective of whether the data filters have been satisfied.
   - AND - The event will be included in the report only if all the selected data filters are satisfied.
   - OR - The event will be included in the report even if any one of the selected data filters is satisfied.

   The data filters will be applied to the particular event during audit report generation.

Edit Data Filters: The properties of a data filter can be modified by changing the contents of the event data field corresponding to the data filter type.

- For User name filter - Add or delete the FDNs of users based on your requirements.

  IMPORTANT: The FDNs should be in lowercase.

- For Source IP filters - Add or delete the IP addresses of the machine, based on requirements. Note that the DNS name of the machine cannot be specified here.
- For Target IP filters - Add or delete the IP addresses of the machine, based on requirements. Note that the DNS name of the machine cannot be specified here.
- For Action Taken filters - Add or delete action values based on requirements.
- For Success codes - Add or delete success code values.

Apply Filters during Report Generation

1. From the NAAS menu, click Reports.
2. In the Filters panel, select the filters required for generating the report. Multiple filters can be selected by pressing the Ctrl key.
3. Click Enable Filters.
4. Set all the other required conditions > click OK to apply the filter and generate the report. For more details on report generation, see “Generating Audit Reports” on page 41.

   If multiple filters are selected for report generation, they are applied as follows:

Filter Type	Description
One or more event filters	Each event filter is applied independently of other event filters; that is, an audit record will be included in the report if it satisfies any one of the specified event filters.
One or more data filters along with event filters	Data filters are applied to each event based on the filtering condition set for that event in the event filter.

Filter Type	Description
	IGNORE: Ignores data filters
	AND: The Audit record is included only if all the data filters are satisfied.
	OR: The Audit record is included even if any one of the data filters is satisfied.
Only data filters without event filters	The Audit record is included in the report only if all the data filters are satisfied.
A set of filters	The filters contained in the set are extracted and applied appropriately as described above, depending on whether they are event filters or data filters.

Generating Audit Reports

You need to be an auditor to generate reports. See "Setting the User As Auditor" on page 33 for details.

Audit reports provide the details of all the audited events that satisfy the various filtering criteria specified in the parameters. Reports can be generated using one of the following methods:

- "Generating Reports" on page 41
- "Executing Queries" on page 42

Generating Reports

Audit reports provide data of all the audited events. The audit data can be filtered using the criteria set based on target objects, filters, and dates. The objects on which the events are generated are called target objects.

1. From the NAAS menu, click Reports.

   The Reports screen with options to enter target objects, filters, and dates is displayed.

2. To filter audit data based on the target objects:

   2a. Check Enable Filtering on Target Objects.

   2b. Add the target objects required for report generation.

3 To filter audit data based on filters, follow the steps given in "Apply Filters during Report Generation" on page 40.

4 To filter audit data based on the dates:

4a To get the audit data corresponding to the events on a specific date, check Enable Filtering on Start Date. Type the start date in the format yyyy-mm-dd hh:mm:ss.

4b To get the audit data corresponding to the events generated till a specific date, Check Enable Filtering on End Date. Type the end date in the format yyyy-mm-dd hh:mm:ss.

5 Click OK to filter the audit data based on the set criteria and generate the report.

After the report is generated, it can be saved as a .CSV file. This enables you to open the file in a spreadsheet application like Microsoft* Excel.

Executing Queries

1 From the NAAS menu, click Query.

The query screen is displayed.

2 Type the SQL sub-clause for the statement SELECT * FROM NAAS_ADMIN.TRAIL WHERE (*sub_clause*).

To generate reports based on IP address or MAC address of source machine, use the following query:

- To filter based on IP address, enter the sub_clause as:

  SOURCE_IP LIKE *'IP ADDRESS%'*

- To filter based on MAC address enter the *sub_clause* as

  SOURCE_IP LIKE *'%MAC ADDRESS'*

IMPORTANT: The FDNs in the sub-clause should be entered in lowercase.

3 Click OK to filter the audit data based on the specified query and generate the audit report.

After the report is generated, it can be saved as a .CSV file. This enables you to open the file in a spreadsheet application like Microsoft* Excel.

Separating the Roles of eDirectory Administrator and NAAS Auditor

For network auditing to be secure, it is desirable to separate the roles of the network administrator and that of the auditor. Novell Advanced Audit Service can achieve this by utilizing the eDirectory rights of the administrator.

To separate the roles of the administrator and the auditor, the following tasks need to be completed.

The administrator needs to perform the following tasks:

1. Run the default configuration utility to do the basic configuration for NAAS. For NAAS Database configuration, it is the auditor and not the administrator who should enter the database.
2. Browse to the NAAS container > right-click Trustees of This object > Add Trustee. Add the auditor's name to the Trustee list and grant the auditor rights to All Attributes Rights and to Entry Rights. Check the Inheritable flag.

   The Administrator has now granted supervisor rights over the NAAS container to the auditor.

The auditor needs to perform the following tasks:

1. Browse to the NAAS container > right-click Trustees of This object > Add Trustee > add the administrator's name to the trustee list.
2. Remove all administrator rights by browsing to the Assigned Rights > uncheck all rights for All Attributes Right and Entry Rights > Check the Inheritable flag. This is to ensure that the administrator cannot modify the policies.

   The Auditor has now removed the administrator's rights to the NAAS container.

   NOTE: If the auditor has manually created the policies, steps 1 and 2 should be repeated for all the Policy objects created.
3. Configure the policies.

5 Troubleshooting

This section provides solutions to problems you might encounter when using Novell® Advanced Audit Service (NAAS).

Troubleshooting NAAS

There was an error initializing the Audit Utility

Explanation:	Occurs when NAAS objects in eDirectory™ are deleted and you are trying to reconfigure the NAAS framework.
Possible Cause:	Before reconfiguring the NAAS framework using the NAAS default configuration utility, the naasAuditor extension has not been removed for one or more NAAS auditors.
Action:	Remove the naasAuditor extension for all NAAS auditors, and then reconfigure the NAAS framework using the NAAS default configuration utility.
Possible Cause:	Before re-creating the NAAS Database object to use Pervasive 2000i, database cleanup was not properly completed.
Action:	Before re-creating the NAAS Database object to use Pervasive 2000i, delete the *.MKD and *.DDF files from the SYS:_NETWARE folder on the NetWare® server.

Unable to Create the Database Object. Database Security Option Could Not be Set

Explanation:	Occurs while creating the NAAS Database object in eDirectory using the NAAS default configuration utility.
Possible Cause:	DSN is not created in Pervasive 2000i.
Action:	Ensure that DSN is created in Pervasive 2000i before creating the NAAS Database object in eDirectory.
Possible Cause:	DSN is created in Pervasive 2000i, but Pervasive is not started.
Action:	Before creating the NAAS Database object in eDirectory, start Pervasive using the mgrstart command on the server console.
Possible Cause:	The security option for the new DSN created is set to ON. By default it should be set to OFF.

Action: From the Pervasive Control Centre, perform the following steps:

1. Right-click the database's namespace node (NAASADMN) and select Properties.
2. Select the Security tab in the Database Properties dialog box.
3. Check the Disable Database Security check box > click OK.

java.lang.NoClassDefFoundError

Source: An error message displays when loading the NAAS server.

Problem: The NAAS server fails to load.

Action: Restart the NetWare server and then start the NAAS Audit server.

DSN Could Not Be Created in Pervasive 2000i

Possible Cause: A DSN is already created at the specified directory.

Action: Drop the database from Pervasive 2000i, and delete the *.DDF and *.MKD files created earlier under the SYS:_NETWARE folder, or specify a different directory to create DSN.

com.novell.admin.common.exceptions.UniqueSPIException: -678

Source: Error message from the Audit utility.

Explanation: Occurs when some of the NAAS objects in eDirectory are re-created and the NAAS framework is reconfigured using the NAAS default configuration utility.

Possible Cause: The naasAuditor extension is not removed before reconfiguring the NAAS framework.

Action: This error message can be ignored. The NAAS Audit utility displays this error message even after successful completion of the NAAS framework.

Error code -669 is logged

Source: The error message is logged in SERVER.ERR file under SYS:\ETC folder on the NetWare server.

Problem: The NAAS server fails to load.

Action: Run ADSRVSET.NLM from SYS:\AUDIT folder and start the NAAS Server using ST_SRVR.NCF. If the problem still persists, restart the NetWare server.

Unable to start NAAS Agent. Error code = -669

Source: The error message is logged in the ADAGERR.LOG file under the SYS:\ETC folder on the NetWare server.

Problem: The NAAS agent fails to load.

Action: Run ADAGTSET.NLM from the SYS:\AUDIT folder and start the NAAS Agent by using ST_AGENT.NCF. If the problem still persists, restart the NetWare server.

Unable to start the Audit Agent. Error code: -602

Source: The error message is logged in the ADAGERR.LOG file under the SYS:\ETC folder on the NetWare server.

Problem: The NAAS agent fails to load.

Action: Restart the NetWare server and start the NAAS Agent.

"Failed to plug-in security" is logged, and the Error Code -602 displays

Source: The error message is logged in the SERVER.ERR file under the SYS:\ETC folder on the NetWare server, and an error code -602 is displayed on the NAAS server screen.

Problem: The NAAS server fails to load.

Action: Restart the NetWare server and start the NAAS server.

Error message and error code -625 are logged

Source: The error message and error code are logged in the ADAGERR.LOG file under the SYS:\ETC folder on the NetWare server.

Problem: The NAAS agent fails to load.

Possible Cause: The communication channel between components is broken.

Action: Restart the NetWare server.

Error message and error code -625 are logged.

Source: The error message and error code are logged in the SERVER.ERR file under the SYS:\ETC folder on the NetWare server.

Problem: The NAAS server fails to load.

Possible Cause: The communication channel between components is broken.

Action: Restart the NetWare server.

There was an error generating the report. Database has returned an error

Source: The error message displays when generating an audit report from ConsoleOne™.

Possible Cause: The database is down.

Action: Start the database and try generating the report from ConsoleOne.

Possible Cause: Database licenses for Pervasive have expired.

Action: Increase the database licenses to Unlimited for Pervasive.

Possible Cause: The NAAS server is not committing audited data to the database.

Action: Delete the SECFILE from the SYS:_NETWARE folder on the NetWare server hosting NAAS server, and restart the NAAS server.

There was an error in getting the filter list from database. The database has returned an error

Source: The error message displays when generating an audit report from ConsoleOne.

Possible Cause: The database is down.

Action: Start the database and try generating the report again.

NAAS Database set-up failed: -1460

Problem: NAAS Database object creation fails.

Explanation: The error message occurs while creating the NAAS Database object in eDirectory using the NAAS default configuration utility.

Action: Ensure that Client NICI versions 1.5.7 and 2.0.2 are installed on the machine used to configure NAAS.

There was an error in getting the filter list from database. NDS has returned an error.

Source: The error message displays when generating audit report from ConsoleOne.

Possible Cause: Either the database, NAAS server, or both database and NAAS server are down.

Action: Ensure that both the database and NAAS server are up, and then try generating the report again.

There was an error in displaying query result. The database has returned an error.

Source: The error message displays when generating a report using an SQL query.

Possible Cause: SQL query syntax may not be correct.

Action: Ensure the correctness of the SQL query while generating the report.

Security plug-in failed

Source: The error message is logged in the SERVER.ERR file under the SYS: \ETC folder on the NetWare server.

Problem: The NAAS server fails to load.

Action: Restart the NetWare server and start the NAAS server components using ST_SRVR.NCF.

Cursor remains as hour glass even after getting report or creating filter

Source: The NAAS screen, when generating a report or creating filters.

Action: Click anywhere outside the NAAS screen on ConsoleOne to set the cursor back to the default.

Some of the NAAS snap-ins for ConsoleOne Fail to Work

Possible Cause: PKI snap-ins for ConsoleOne are interfering with functionality of NAAS snap-ins.

Action: After creating NAASKMO, rename the PKI.JAR file under *CONSOLEONE_HOME*\1.2\SNAPINS\SECURITY to a different name.

The pervasive license and key files are not updated

Source: When an existing NetWare server is upgraded to NetWare 6.0.

Action: Overwrite the Pervasive and key files with the files bundled with NetWare 6.0 build to which you have upgraded. To do this, execute the following steps:

1. Restart NetWare server with the -na option.

   ```
   restart server -na
   ```

2. Copy the following NLM™ software from NetWare 6.0 CD to the SYSTEM folder on the server.

   - NWUCINIT.NLM
   - NWUCMGR.NLM
   - NWUCUTIL.NLM

3. Upgrade the licenses by executing the following command from the system console:

   ```
   nwucinit -C11 -Q sys:\pvsw\license2
   ```

4. Verify the available licenses by executing the following command from the system console:

   ```
   nwucutil -g11
   ```

com.novell.admin.common.exceptions.UniqueSPIException: -609

Source: This is an error message from the Audit utility when the NAAS framework is being configured by using the NAAS default configuration utility.

Action: Remove the naasAuditor extension for all NAAS auditors and re-configure the NAAS framework by using the NAAS default configuration utility.