Novell
Advanced Audit Service

www.novell.com

INSTALLATION AND ADMINISTRATION GUIDE

Novell®

Legal Notices

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

www.novell.com

Novell Advanced Audit Service
March 2003

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 registered trademark of Novell, Inc. in the United States and other countries.
Novell 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

Third-Party Trademarks

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

Understanding Novell Advanced Audit Service

Novell® Advanced Audit Service (NAAS) lets you audit services running on the network. NAAS uses Novell eDirectory™ for storing policies and configuration information and for managing access to the audited data. By default, NAAS performs eDirectory and NetWare® Legacy File System (NWFS) and NSS auditing.

NAAS Components

NAAS 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 NAAS server

NAAS Server - Collects the audit records from the NAAS Agents and stores them in the database. The NAAS Server also services queries from the NAAS Utility for reading these audit records and performs the necessary access control.

NAAS Database - Stores the audit records.

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

NAAS Terminology

This section provides information on the commonly used NAAS terminologies.

NAAS Policies - Set of rules that govern the functioning of the NAAS frame work. The NAAS framework comprises NAAS policies that are stored in a NAAS container available just below the partition root in the eDirectory tree, and various components running in the network.

NAAS Agent Policy - Governs the functioning of the NAAS Agent.

NAAS Server Policy -Governs the functioning of the NAAS Server.

NAAS Event - Occurrence of an action on an object of interest (Target object).

Target Objects - Objects on which the events are generated.

NAAS Event Policy Template - Identity for the audited service in eDirectory. Every audited service should create its own Event Policy Template in eDirectory.This object contains some information specific to the service such as the service identifier, version, and list of events exposed by the service.

NAAS Event Policy - Is specific to an audited service and is created based on the Event Policy Template. This policy defines which events are to be audited and which are not. It specifies the action to be taken when an audit event occurs, and also how data policies should be evaluated for a particular event. The NAAS Agent filters the events generated by an audited service based on the event policy.

NAAS Data Policy - Every event has some data associated with it, such as who was the perpetrator of the event and on which machine the event occur on. Based on this data, NAAS Data policies define which events are to be audited and which are not. There are various types of data policies such as NAAS User Policy, NAAS Source Machine Policy, NAAS Target Machine Policy and NAAS File Policy. The NAAS Agent evaluates the data policies together with the event policy and accordingly decides if the event is to be audited or not.

NAAS Search Criteria Policy - A set of rules specifying how the NAAS Agent may search for a NAAS Policy for a particular audited object. Audit

Policies can be associated directly at an object, at a parent container, or at a group which the object belongs to.

Associated Policies - A NAAS policy can be associated directly to an object, to one of its parent containers, or one of the groups to which the object belongs to.

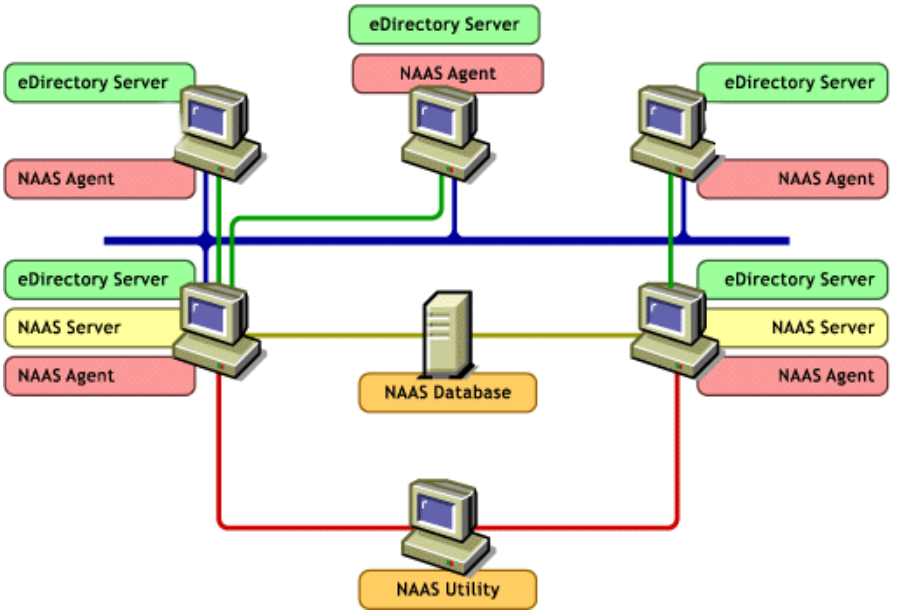
Effective Policy - When an Audited Service generates an event, the NAAS Agent processes it based on the effective policy set for that Agent and decides what is to be done with the event. When the NAAS framework searches for the policy applicable to an object, it must know the order in which to search the object, container and group for the policy.The search order and the level are provided by the Search Criteria policy.

NAAS Reports - NAAS reports provide the details of all the audited events that satisfy the criteria set based on target objects, filters, and dates.

Auditor - User responsible for viewing NAAS reports.

Filters - Filters can be used to filter the data stored in audit database for viewing the reports. The types of filters are filter sets, event filters and data filters.

(Figure Description) Describes the NAAS Framework



The above diagram depicts a sample setup of NAAS deployed in a network. Here, NAAS Agent is running on all servers, NAAS Server is running on two of the servers and both these servers are using the same database to store the audit records. The database can be any of the supported databases like MySQL*, Oracle*, and Pervasive* running on any platform. ConsoleOne can be used for running the NAAS utility on the Windows* client.

1 Installing Novell Advanced Audit Service

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

IMPORTANT: This chapter is a must read to perform overlay install. If the install is script-based, skip to System Requirements.

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

During the custom installation of NetWare 6, Novell Advanced Audit Service 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

- NAAS Agent - 3.37 MB
- NAAS Server - 1.45 MB
- NAAS 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

General Requirements

- Novell Certificate Server™ is installed and functional.

NAAS Agent

- NetWare 6 or later

NAAS Utility

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

NAAS Database

Requirements for Pervasive Database

Database engine	Pervasive.SQL 2000 or 2000i SP3 or above
JDBC driver	Pervasive JDBC driver. This can be downloaded from the Pervasive site (http://www.pervasive.com) **Recommendation:** For better performance, upgrade the Pervasive database engine running on the NetWare server from SP3 to SP4. After the upgrade, modify the database driver path in the st_srvr.ncf file present in the sys:\system directory, from **`envset JDBC_DRIVER_PATH=sys:\java\lib\pvjdbc2.jar`** to **`envset JDBC_DRIVER_PATH=sys:\audit\PervJar\pvjdbc2.jar`** In the server console, kill the NAAS Server by using the **`java-kill`** option and unload all the Java components using **`unload java`** command. Then, run st_srvr and restart the NAAS Server. For more information about upgrading to Pervasive SP4 on NetWare server, see Pervasive support site (http://support.pervasive.com/esupport/publisher.asp?id=ea2935c9-ed92-11d5-b263-00508b5d6b61&resource=&number=0&isExternal=0).
NAAS Server	Change the JDBC driver path setting in the st_srvr.ncf file to refer to the Pervasive JDBC driver. For example, the JDBC driver path setting can be envset JDBC_DRIVER_PATH=SYS:\JAVA\LIB\DRIVER.ZIP

NAAS configuration	Copy the driver in the specific location. For example, the JDBC driver can be placed in <consoleonehome>\ 1.2\lib\naas\driver.jar

Requirements for MySQL Database

Database engine	MySQL engine for NetWare 6.0. This can be downloaded from Novell site for MySQL (http://developer.novell.com/ndk/leadedge.htm#167).
JDBC driver	MySQL JDBC driver. this can be downloaded from Novell site for MySQL (http://mysql.provo.novell.com/downloads.html). For more information about the MySQL database see, the MySQL site (http://www.mysql.com)
NAAS Server	Change the JDBC driver path setting in the st_srvr.ncf file to refer to the MySQL JDBC driver. For example, the JDBC driver path setting can be envset JDBC_DRIVER_PATH=SYS:\JAVA\LIB\DRIVER.JAR
NAAS configuration	Copy the driver in the specific location. For example, the JDBC driver can be placed in <consoleonehome>\ 1.2\lib\naas\driver.jar

Requirements for Oracle Database

Database engine	Oracle 8i
JDBC driver	Oracle JDBC driver
NAAS Server	Change the JDBC driver path setting in the st_srvr.ncf file to refer to the Oracle JDBC driver. For example, the JDBC driver path setting can be: envset JDBC_DRIVER_PATH=sys:\java\lib\classes12.zip

NAAS configuration	Copy the driver in the specific location. For example, the JDBC driver can be placed in <consoleonehome>\ 1.2\lib\naas\driver.jar

NAAS Server

- ❑ NetWare 6 or later

NAAS Default Configuration Utility

- ❑ Windows 95, 98, 200, XP or NT Service Pack 4 or later
- ❑ ConsoleOne version 1.2d or higher
- ❑ Client NICI (Novell International Cryptography Infrastructure) version 2.0.2 or higher. This can be downloaded from the Novell download site (http://www.novell.com/download)
- ❑ For the Oracle database, copy the Oracle JDBC driver into the Novell\ConsoleOne\1.2\lib\naas directory.

NAAS Compatibility with Multiple Software

Software	Versions Tested with NAAS
Client operating systems	◆ Windows 95 ◆ Windows 98 ◆ Windows NT* Workstation 4.0 ◆ Windows 2000 with SP1 ◆ Windows XP ◆ Windows NT Server 4.0 SP4
ConsoleOne	ConsoleOne versions 1.2d and 1.3
Pervasive Database	Pervasive.SQL 2000/2000i SP3 or later

Installing the NAAS Utility and the Default Configuration Utility

NAAS snap-ins will be installed as part of ConsoleOne snap-ins taken from Client CD. NAAS snap-ins might not be installed if you don't have the latest client CD.

To verify if NAAS snap-ins are installed, click the tree name (or any object in the tree) in the ConsoleOne. NAAS is displayed as one of the menu items in the main menu if NAAS snap-ins are installed.

If NAAS snap-ins have not been installed as part of the ConsoleOne snap-ins, you can alternatively install the NAAS snap-ins by completing the following steps:

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 the ConsoleOne home directory is c:\novell\consoleone\1.2.

3. Continue with "Starting the Pervasive Database Server" on page 18.

Starting the Pervasive Database Server

Start the Pervasive database server before continuing with the post-installation steps.

1. To start the Database server, enter **`mgrstart`** at the server console.

2. Conditional. By default, two licenses are provided for Pervasive. To configure multiple NAAS Servers, the licenses should be incrementally increased.

   For unlimited licenses for 90 days, run the Pervasive utility by entering 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, enter the following command at the server console.

```
NWUCUTIL -g11
```

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.

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 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, then click OK.

   The following procedures provide details for configuring NAAS:

   - “Setting Up the NAAS Agent” on page 22
   - “Setting Up NAAS Server” on page 22
   - “Setting Up NAAS Database” on page 22
   - “Configuring NAAS Framework” on page 24

Setting Up the NAAS Agent

This utility should be run separately for configuring every NAAS Agent.

1. In the Select Configuration Task dialog box, select Set Up NAAS Agent and 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 configure the NAAS Agent on the server you selected.
4. Continue with "Setting Up NAAS Server" on page 22.

Setting Up NAAS Server

This utility should be run separately for configuring every NAAS 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, then click OK to display a dialog box where you can select the host server.
2. Browse and select the host server where you are setting up the NAAS server.
3. Click OK to configure the NAAS server on the server you selected.

Proceed to Setting Up NAAS Database.

Setting Up NAAS Database

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

During NAAS Database setup, DSN is created automatically in sys:_netware folder of specified server. A new database can be created using create database in different folder or volume using Pervasive Control Centre (PCC).

Manually Creating the DSN for NAAS Database

1. Install the Pervasive client on a Windows machine by running sys:\pvsw\clients\win\setup.exe, available on the NetWare 6 server.

   Installing the Pervasive client is optional. The Pervasive client is useful for database maintenance and for using other utilities offered by the Pervasive database.

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

2. From the client, start the Pervasive Control Center by clicking Start > Programs > Pervasive > Pervasive Control Center.
3. Right-click Pervasive.SQL 2000i Engine > click Register New Engine.
4. Enter the name of the server where the NAAS database is to be hosted.
5. Browse to the database folder.
6. Right-click Databases and click New Database.
7. In the New Database wizard, enter the following details.
   - Server Name
   - Interface - Select Engine as the interface type
   - User Name - The NDS or eDirectory administrator name in the format .admin.acme
   - Password - The password for the NDS or eDirectory administrator.
8. Click Next.
9. Enter NAASADMN as the database name and *Netware_server_name*\SYS:_*netware* as the directory and click Next.
10. Click Finish.

    A new database is created and an informational message is displayed.
11. Click OK.

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

Setting Up the Database

1. In the Select Configuration Task dialog box, select Set Up NAAS Database, then click OK to display a dialog box to enter details about the database.
2. Select Pervasive.SQL 2000* as the database type.
3. Enter the database (server) IP address.

4. Enter the fully distinguished name (FDN) and password of the eDirectory administrator. For example the FDN can be *.admin.acme*.
5. When you setup the NAAS Database, the system creates a user by name Master to manage the NAAS Database. Enter the password.
6. Re-enter the password.
7. Click OK to activate automatic configuration of the NAAS database.

Configuring 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, and click OK to display the Select Auditor dialog box.
2. Click Browse to select the user to be set as the Auditor and click OK to configure the NAAS framework.

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

   The configuration is completed and you can modify the default values for the various components, if required.

Refer "Deploying Novell Advanced Audit Service" on page 41 to know more about various scenarios in which NAAS can be deployed, after the default configuration.

By default, NAAS Default Configuration utility configures NAAS for a single partition. Complete the steps provided in "Configuring NAAS for Multipartition Auditing" on page 50, to configure NAAS for multiple partitions.

After configuring the NAAS Agent, NAAS Server, NAAS Database and NAAS framework, proceed with the following tasks:

- "Modifying NAAS Agent Policy" on page 25
- "Modifying NAAS Event Policy" on page 25

Modifying NAAS 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, then click Properties.
3. Go to the Policy Content tab.
4. Modify the commit period to speed up commit process.

   NOTE: The Commit Period must be greater than 30 seconds.

These changes are applicable to all agents in the partition.

An error message for restarting the NAAS modules is displayed. Ignore this error message.

Modifying NAAS Event Policy

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.
   - DSEventPolicyV2
   - FSEventPolicy
   - NSSEventPolicy
2. Right-click the object, then 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 agents in the partition.

   An error message for restarting the NAAS modules is displayed. Ignore this error message.

Configuring NAAS for Multipartition Auditing

The NAAS Default Configuration utility configures NAAS for a single partition. It creates a NAAS Agent for the selected eDirectory server. The Agent is capable of auditing all the partitions or replicas hosted on that server. It is must that all the objects (in partitions) have Event policies associated with them, for them to be audited. The Default configuration associates Event polices to the partition for which NAAS was configured only. All other hosted partitions on that server need to have Event policies associated for them to be audited.

To learn more about how to configure NAAS for multipartition auditing refer "Configuring NAAS for Multipartition Auditing" on page 50 for a few scenarios.

Deploying NAAS in a Mixed Environment with NetWare 6 and NetWare 6 Support Pack 1 or Later Servers

NOTE: If you are configuring and using NAAS for the first time after installing NetWare 6 with Support Pack 1 or later and do not have NAAS on any other NetWare 6 server, this issue isn't applicable to your setup.

Auditing eDirectory on NetWare 6 servers with Support Pack 1 or later installed uses a new eDirectory event template with Service Version 2.0, Service Identifier eDirectory, and a new eDirectory event policy. The new eDirectory event template and eDirectory event policy are created as part of the default configuration of NAAS on NetWare 6 Support Pack 1 or later.

Auditing eDirectory on NetWare 6 servers without Support Pack 1 or later continues to use the eDirectory template with Service Version 1.0, Service Identifier NDS, and the eDirectory event policy derived from it.

In order for eDirectory auditing to function on NetWare 6 Support Pack 1 or later servers, you must reconfigure the existing NAAS framework using the NAAS snap-ins that ship with Support Pack 1 or later.

IMPORTANT: Only the administrator can reconfigure the existing NAAS configurations, using the NAAS default configuration utility.

To successfully audit eDirectory after installing NetWare 6 Support Pack 1 or later, complete one of the following procedures.

If the Auditor has not created an eDirectory event policy template and an eDirectory event policy in the eDirectory partition manually (NAAS uses the DS Event policy template and DS Event Policy created by the NAAS default configuration utility on NetWare 6), complete the following steps:

1. Manually replicate the contents of the old eDirectory policy contents to the newly created eDirectory event policy.
2. Restart NetWare servers with Support Pack 1 or later after reconfiguring the NAAS framework.
3. To refresh templates and policies, restart ConsoleOne® after reconfiguring NAAS.

If the Auditor has created new eDirectory event policy template or eDirectory event policy in the eDirectory partition manually (by creating new ones in addition to the DS event policy template and DS event policy created by the default configuration utility on NetWare 6), complete the following steps:

1. For every eDirectory event template and eDirectory event policy in the partition, other than DSEventPolicyV2 and DSEventPolicyTemplateV2 created by default, manually create a new eDirectory event template using the EVENTS.TXT file located in the SYS:\AUDIT\naasEvents folder on all NetWare 6 Support Pack1 servers and a new eDirectory event policy respectively.
2. Manually replicate the contents of the old eDirectory policy contents to the newly created directory event policy.
3. Replicate associations to new event policies.

   For example, associate the new eDirectory event policies to wherever the old ones were associated.
4. After reconfiguring the NAAS framework, restart your NetWare 6 servers with Support Pack 1 or later.
5. To refresh templates and policies, restart ConsoleOne after reconfiguring NAAS.

Modifying Default Values

NAAS Agent Policy

To modify the default values set for the NAAS 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 and 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 Agent and Server" on page 33 instructions.

NAAS Server Policy

To modify the default values set for the NAAS 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 and 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 Agent and Server" on page 33.

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.
   - DSEventPolicyV2
   - FSEventPolicy
   - NSSEventPolicy
2. Right-click the object and 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 33 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 and select Trustees of this Object.
3. Select the Auditor from the trustee list and click Assigned Rights.
4. From the Property list, select naasTrail and check the Read right from the Rights list and 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, and click Add Trustee.
3. Browse to the Auditor user object, select the User object, and click OK.

4. Click Add Property.
5. Check Show all Properties.
6. Select the naasTrail attribute and click OK.
7. Check the Read right and click OK.
8. Apply the changes.

Starting the NAAS Server

1. Enter **ST_SRVR.NCF** at the server console to start the NAAS server.

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

   For example, the JDBC driver path setting can be

   envset JDBC_DRIVER_PATH=SYS:\JAVA\LIB\CLASSES12.ZIP

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

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

   The audit.server.SocketServer class should be displayed.

   2b Ensure that the ADSERVER.NLM module is loaded. Enter **m adserver** at the server console to verify this.

Starting the NAAS Agent

1. Enter ST_AGENT.NCF at the server console to start the NAAS Agent.
2. Check if the NAAS Agent is up:

   2a Enter **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. Enter **m adagent and m jadagent** at the server console to verify this.

Loading the Shims

FS Shim

Load FS Shim only after the agent is up.

1. Enter **`fsshim`** at the server console.
2. To check if the FS Shim is running, enter **`m fsshim`** at the server console.

NSS Shim

Load NSS Shim only after the agent is up.

1. Enter **`nssshim`** at the server console.
2. To check if the FS Shim is running, enter **`m nssshim`** at the server console.

DS Shim

Load DS Shim only after the agent is up.

1. Enter **`dsshim`** at the server console.
2. To check if the DS Shim is running, enter **`m dsshim`** at the server console.

Starting the NAAS Utility

Run ConsoleOne from the client machine to start the NAAS utility.

Stopping the NAAS Server

1. At server console, enter **`java -show`**. This will display the Classname and IDs for all the java classes running.
2. Find the corresponding ID for the class **audit.server.SocketServer**.

3 Stop the NAAS server application by entering **`java -kill`** command with the ID.

For example, if ID for *audit.server.SocketServe*r is 434, at the server console, enter **`java -kill434`**. This will stop the NAAS server.

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 all NAAS components can be viewed from NAASERR.LOG in the SYS:\ETC folder.

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 NAAS utility.

Prerequisites

Before configuring the NAAS agent and the NAAS server, the following procedures need to be completed.

- ❑ Setting Up NAAS Database (page 22)
- ❑ Setting Up the NAAS Agent (page 22)
- ❑ Setting Up NAAS Server (page 22)

Configuring Agent and Server

NAAS assumes partition-based auditing, where the domain for auditing is a Novell eDirectory™ partition. All the NAAS agents will audit only those objects that are in the same eDirectory partition as the agent. Also, the NAAS 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 NAAS Agent” on page 34

- "Configuring the NAAS Server" on page 35

The user can also configure the NAAS agent, NAAS server, and the policies by using the procedure provided in "NAAS Default Configuration Utility" on page 21.

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

Configuring the NAAS Agent

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

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

Configuring the NAAS 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 36 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 attributes 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 NAAS server.

Configuring the NAAS Server

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

The configuration information for an NAAS server is stored in eDirectory as a Server Policy object. The Server Policy object governs the functioning of the NAAS 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 NAAS server.

Configuring the NAAS 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 36 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 NAAS 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 in the same machine as the NAAS 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 are 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 36 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 eDirectory Auditing

If the NAAS Default Configuration Utility (page 21) has been run, Event Policy Templates for eDirectory auditing 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 eDirectory.

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

1b Enter the Service Identifier as NDS.

1c Enter the Service Version.

Enter version 2.0 if the template is being created using EVENTS.TXT on a NetWare 6 server wit Support Pack 1 or later.

Enter version 1.0 if the template is being created using EVENTS.TXT on a NetWare 6.0 server without Support Pack 1 or later.

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 eDirectory 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 36.

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

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

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

Continue with "Starting the NAAS Agent" on page 30.

Configuring Traditional File System Auditing

If the NAAS Default Configuration Utility (page 21) 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 Traditional File System.

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 36.

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

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

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

Continue with "Starting the NAAS Agent" on page 30.

Configuring NSS Auditing

If the NAAS Default Configuration Utility (page 21) 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.

NSSEVENTS.TXT is located in SYS:\AUDIT\NAASEVENTS.

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 36.

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

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

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

Continue with "Starting the NAAS Agent" on page 30.

4 Deploying Novell Advanced Audit Service

This section provides information about the NAAS default configuration and the setup in which Novell® Advanced Audit Service (NAAS) operates after default configuration. It also deals with the most common deployment scenarios that are different from the default setup of NAAS.

The configuration utility used for automatic configuration has be named as Post-install Configuration in the case of NAAS plug-ins for iManager and NAAS Default configuration Utility in the case of NAAS snap-ins for ConsoleOne. This particular term has been referred as NAAS Configuration utility in this chapter. Therefore, replace it with specific terms based on whether you are using iManager or ConsoleOne.

Setup Using NAAS Configuration Utility

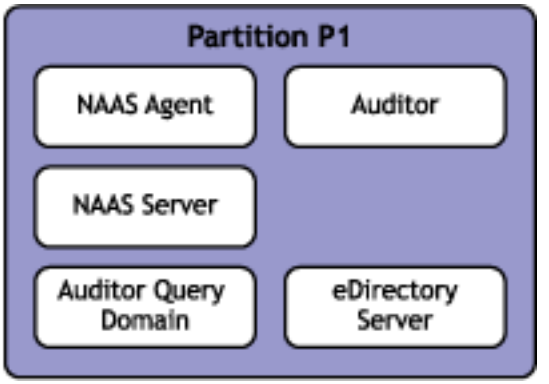
The configuration utility configures NAAS for one partition. NAAS assumes partition-based auditing, where the domain for auditing is a Novell eDirectory™ partition. The process of default configuration will result in creation of NAAS Agent, NAAS Server and NAAS Database, and will configure the NAAS framework and the three Event policies (eDirectory Auditing, NWFS auditing, and NSS auditing) with Event policy template and an Auditor Query domain. The NAAS Agent will be created and configured during the installation of NAAS.

The configuration utility also configures a user as an Auditor by giving all the required rights. All the objects are created in the NAAS container under the selected partition.

The configuration utility configures NAAS for a basic setup.

The following figure depicts the configuration setup after NAAS has been configured for the partition P1 using the default configuration. If you have a complex setup, you should perform the default configuration and then, perform a few additional steps to bring up NAAS for Auditing.

Figure 1 Configuration Setup



In the diagram, the NAAS Agent, NAAS Server, Auditor Query domain, Auditor and the eDirectory server are in the same partition.

Auditing

In the above setup, NAAS Agent will audit only those objects that are in the same partition as the eDirectory server hosting the NAAS Agent. Also, the NAAS Agent 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. The same association rule holds true for the NAAS Server.

Also, for a partition to be audited, a NAAS Agent and a NAAS Server should be configured for the partition containing the eDirectory server hosting the NAAS Agent and the NAAS Server in the same partition. If the partition is a parent partition for one or more child partitions, all the child partitions will also be audited. However, if the NAAS Agent, NAAS Server, and eDirectory server are in the child partition the parent partition will not be audited.

By default, NAAS searches only up to three levels up the tree to find a policy of any type for an object. If a policy is not found in the three levels, that object is not audited. If the depth of the partition is greater than three, specific NAAS Search Criteria policies should be associated with the objects with the search level equal to the partition depth.

Reporting

The configuration utility configures NAAS for a particular partition and configures an user as an Auditor. The configured user has to be present in the same partition to generate a report. By default, the NAAS Server generates reports only for the query domains in the same partition.

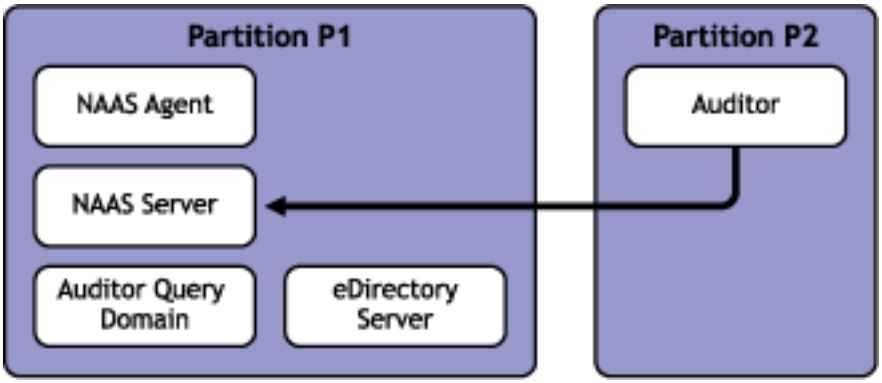
Deployment Scenarios

Scenario 1: Auditor Is Not a Part of the Partition in Which NAAS Is Configured

The following figure depicts a scenario in which the user who is configured as an auditor is not a part of the partition in which NAAS is configured.

Here, NAAS is configured in the Partition P1 and the auditor exists in the Partition P2.

Figure 2 Configuration Setup



Proceed with the following steps to bring up NAAS in this scenario:

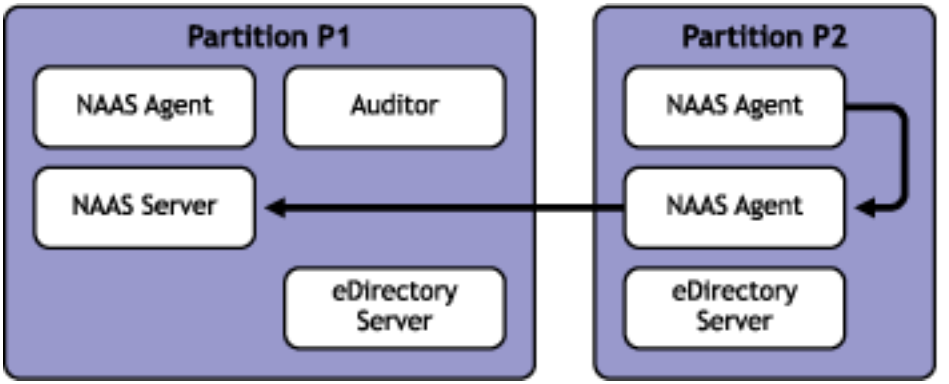
1. Grant the NAAS Server the Read right to the naasDomainList, and naasSelectedDomain attributes of the Auditor.
2. Grant the Auditor to the read right to naasserversList attributes of that Auditor.
3. Grant the NAAS Server the read right to all attributes of the Auditor Query domain for that Auditor.

Scenario 2: NAAS Agent Is Not a Part of the Partition in Which NAAS is Configured

The following figure depicts a scenario in which the NAAS Agent is not a part of the partition in which NAAS is configured.

Here, NAAS is configured in the Partition P1 and the NAAS Agent exists in the Partition P2.

Figure 3 Configuration Setup



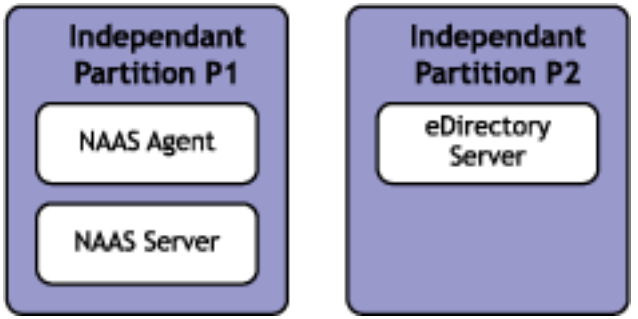
Scenario 3: NAAS Agent and NAAS Server Are Not Present in the Same Partition as the eDirectory server

Invalid Setups

NAAS auditing and reporting will not be performed for following scenarios:

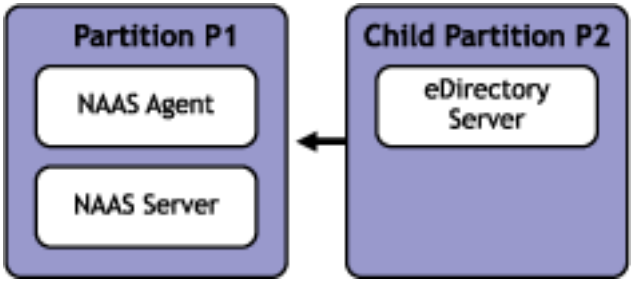
NAAS Agent, NAAS Server and eDirectory Server are in Independent Partitions

Figure 4 Invalid Configuration Setup



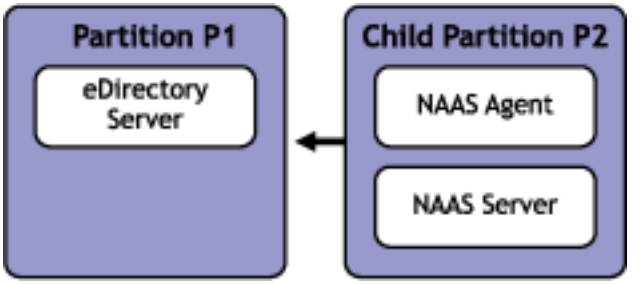
NAAS Agent and NAAS Server are in the partition P1 and eDirectory Server is in the child partition P2

Figure 5 Invalid Configuration Setup



eDirectory Server is in Parent Partition and NAAS Agent and NAAS Server are in Child Partition

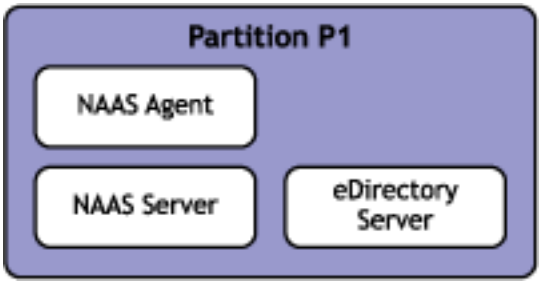
Figure 6 Invalid Configuration Setup



Valid Setup

Ensure that the NAAS Agent and the NAAS Server reside in the same partition in which the eDirectory server exists, as illustrated below.

Figure 7 Valid Configuration Setup - NAAS Agent, NAAS Server and eDirectory server are existing in the same partition



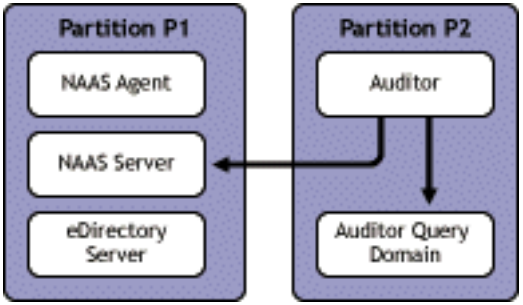
Scenario 4: The Auditor Query Domain and NAAS Server Are in Different Partitions

The following diagram depicts a scenario in which the Auditor Query domain set for the auditor and the NAAS Server are in two different partitions.

Here, the NAAS Server exists in Partition P1 and the Auditor Query Domain exists in the Partition P2.

Ensure that the NAAS Server has the read right to all the objects in the Auditor Query domain set for that Auditor.

Figure 8 Configuration Setup



5 Using Novell Advanced Audit Service

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

- "Setting Filters for Viewing Events" on page 72
- "Viewing the Audit Trail" on page 66
- "Generating Audit Reports" on page 76
- "Separating the Roles of the eDirectory Administrator and NAAS Auditor" on page 78

Installing NAAS

See "Installing Novell Advanced Audit Service" on page 13 for information about installing NAAS.

Configuring NAAS Components

You can run the NAAS default configuration utility to perform automatic default configuration of the NAAS agent, NAAS 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 21.

You can also configure NAAS manually by following the steps described in "Manually Configuring Novell Advanced Audit Service" on page 33.

Configuring NAAS for Multipartition Auditing

NAAS can perform multipartition auditing, based on the configuration done by the user.

The process of configuring NAAS for multi partition setup involves using the NAAS Default configuration Utility in combination with creation and association of few NAAS policies manually depending on the Auditing requirements.

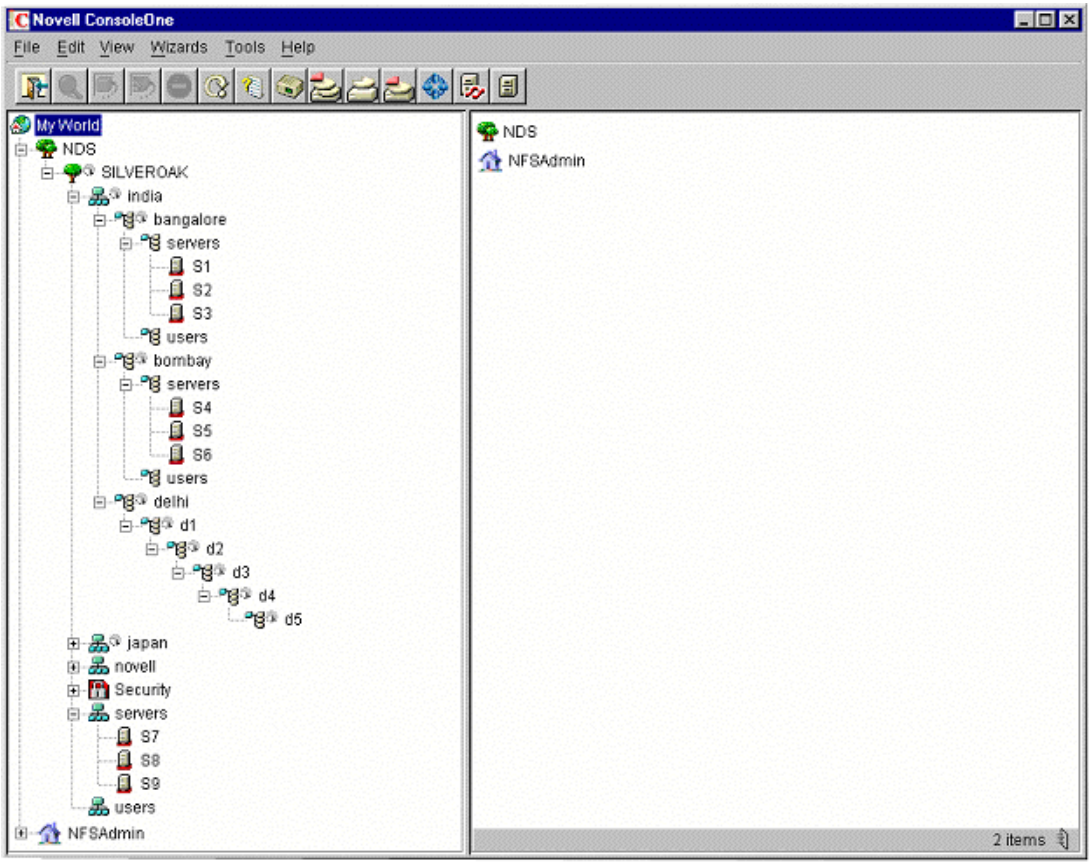
NAAS Default Configuration Utility configures NAAS for one partition. Auditing of a particular object in eDirectory depends on the Event Policies associated to it. During the Default Configuration an Agent is created for a selected eDirectory server. The Agent can Audit all the partitions / replicas hosted on that eDirectory server. It is must that ALL the objects (in Partitions)

have governing Event policies associated with them, for them to be audited. The Default configuration associates Event polices to the partition for which NAAS was configured only. All other partitions (residing on the eDirectory server) need to have Event policies associated for them to be audited. Depending on the setups it may or may not be necessary to associate Event policies manually, since NAAS searches up to three levels up the tree to find a NAAS policy of any type for an object.

Scenarios for Configuring NAAS for Multipartition Auditing.

This section describes a few scenarios. The following figure depicts a sample eDirectory Tree. For each scenario an abstract section of the tree is considered and the impact of NAAS configuration and auditing is explained.

(Figure Description) Network for Scenario Setups



Scenario 1

This scenario talks about configuring NAAS at eDirectory Tree root level. Read through it to get an idea of all steps which need to be performed for enabling multi partition auditing. But It is recommended to take this approach only if the number of objects in the tree is not very high. The rest of the scenarios cover various other scenarios of configuring at need basis.

To enable auditing for an entire eDirectory tree containing multiple partitions and servers, and comprising one NAAS Server, one central database, one Auditor, and multiple NAAS Agents:

1. Perform the NAAS default configuration at the root of the tree.

The policies are created and associated at root partition SILVEROAK.

2 Make these policies applicable to the entire tree to the lowest level.

2a Create a NAASSearchCriteriaPolicy with the following details.

Name: NAASSearchpolicy

Search Order: Object > Container > Group.

Search Level: 10. The search level should be set based on the current tree settings and should be greater than or equal to the depth of the tree.

2b Go to Properties page of the SILVEROAK > Associated NAAS Policies > Add NAASSearchPolicy, to associate it to the SILVEROAK.

3 Configure the NAAS Agent for the NCP servers that are to be audited.

Each agent can audit all the partitions hosted on that server.

4 The Agent needs to have the required rights to read the policies created during the NAAS Default configuration. By default only the agents in the Tree root partition are granted these rights.Perform the following steps to grant the rights to all agents which reside out side the Tree root partition if any.

4a Grant the Read right to the naasPolLink and naasSearchPolLink attributes for all the objects in the partition. This can be done even at the partition level.

4b Grant the Read right to the agent, so the event policies can be read.

5 Enable the NAASGloballyAuditable flag.

5a Right-click the partition Root object.

5b Go to Extensions and add an extension.

5c Select NAASGloballyAuditable and click OK.

5d Click OK in the message box

5e Enter a name for the flag.

5f Repeat the above steps for each partition that the agents are running on and for each respective partitions that agents are running.

6 Modify the properties of the Auditor Query Domain policy to set all the objects in the tree within the domain of the configured Auditor, so that the Auditor can get the audit data for the entire tree in the report.

6a Right-click the Auditor Query Domain policy.

6b Go to Properties and uncheck the Partition Boundary option.

7 Conditional. If the Auditor is not present in partition that the framework configuration is performed for, complete the following steps:

7a Grant the NAAS Server the Read rights to the naasRandomNonce, naasDomainList and naasSelectedDomain attributes of the Auditor.

7b Grant the Auditor the Write rights to the naasRandomNonce and the Read right to the *naasserversList* attributes of its own object.

7c Grant the NAAS Server the Read rights to all attributes of the naasAuditorQueryDomain object for that Auditor.

8 One or more NAAS Servers can be configured for a tree. The servers must be configured at the partition hosting the objects for the eDirectory server designated as the NAAS server. We recommend to have one NAAS Server for every geographical location. If the connectivity is fast, one NAAS Server can be configured for the whole tree.

Conditional. To create multiple NAAS Servers:

8a Create a NAAS Server using the Default Configuration Utility.

8b Right-click the NAAS Agent policy of the agent that contacts the server.

8c Go to Properties, enter the names of the Servers to be contacted and then click OK.

8d Grant the Read right to the naasPortNumber and the Host Device attribute for the NAAS Servers.

8e Grant the Read right to the Network Address attribute for the server objects hosting the NAAS Servers.

8f Grant the Read right to the Server policy of the NAAS Server.

8g Grant the Read right to the NAAS Database.

8h Grant the Read right to the naasPolLink, naasSearchPolLink and ACL attributes for all the objects in the partition.

8i Grant the Write right to its own naasPortNumber attribute.

8j Grant the NAAS Servers Read rights on this Auditor Query domain, and on the naasSelectedDomain, and *naasRandomNonce* attribute of the Auditor.

8k Grant the Auditor the Read right to the naasPortNumber and Host Device attributes of the NAAS Servers.

Scenario 2

This scenario talks about configuring NAAS for the eDirectory root partition SILVEROAK. The NAAS Agent is configured for the S7 eDirectory server hosting the following partitions:

- SILVEROAK
- BANGALORE
- BOMBAY
- DELHI
- JAPAN

Remarks

SILVEROAK is audited based on its default configuration.

BANGALORE, BOMBAY, DELHI, and JAPAN are audited based on the default configuration of SILVEROAK. For every object in these partitions, NAAS searches only three levels up to find the associated Event policy. If an effective policy is not obtained in up to three levels, then the object is not audited.

Therefore, Event policies should be associated, in order to perform multipartition auditing. This can be done by associating any new policy directly to the object or partition, or associating high-level search policy to the partition, so that the Event policies created using the default configuration of SILVEROAK are applicable to the current partition.

Scenario 3

This scenario talks about configuring NAAS for the eDirectory root partition SILVEROAK. The NAAS Agent is configured for the S7 eDirectory server hosting the following partitions:

- SILVEROAK
- D3

Remarks

SILVEROAK is audited based on its default configuration.

For every object in D3, NAAS searches only three levels up to find the associated Event policy. Therefore, D3 is not audited because the objects in D3 are not associated to any event policies.

Therefore, Event policies should be associated to D3, in order to perform multipartition auditing. This can be done by associating required event policies or associating a high-level search policy so that the configuration of SILVEROAK will be applicable to D3. If you have created and associated new Event policies, required rights should be provided based on the steps given in "Granting Rights to NAAS Agents" on page 60.

Scenario 4

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S1 eDirectory server hosting the following partitions:

- BANGALORE

Remarks

BANGALORE is audited based on its default configuration.

Scenario 5

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S1 eDirectory server hosting the following partitions:

- BANGALORE
- BOMBAY

Remarks

BANGALORE is audited based on its default configuration.

For every object in BOMBAY, NAAS searches only three levels up to find the associated Event policy. Therefore, BOMBAY is not audited because the objects in BOMBAY are not associated to any event policies.

Event policies should be associated to BOMBAY in order to audit it. This can be done by associating required event policies to BOMBAY. If you have created and associated new Event policies, required rights should be provided based on the steps given in “Granting Rights to NAAS Agents” on page 60.

Scenario 6

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S1 eDirectory server hosting the following partitions:

- BANGALORE
- BOMBAY
- DELHI

Remarks

BANGALORE is audited based on its default configuration.

For every object in BOMBAY and DELHI, NAAS searches only three levels up to find the associated Event policy. Therefore, BOMBAY and DELHI are not audited because the objects in these partitions are not associated to any event policies.

Event policies should be associated to BOMBAY and DELHI in order to get them audited. This can be done by associating required event policies to BOMBAY and DELHI. If you have created and associated new Event policies, required rights should be provided based on the steps given in “Granting Rights to NAAS Agents” on page 60.

D1, D2, D3 etc., cannot be audited in this setup.

Scenario 7

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S1 eDirectory server hosting the following partitions:

- BANGALORE
- JAPAN

Remarks

BANGALORE is audited based on its default configuration.

For every object in JAPAN, NAAS searches only three levels up to find the associated Event policy. Therefore, JAPAN is not audited because the objects are not associated to any event policies.

Event policies should be associated to Japan in order to audit it. This can be done by associating required event policies to JAPAN. If you have created and associated new Event policies, required rights should be provided based on the steps given in “Granting Rights to NAAS Agents” on page 60.

Scenario 8

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S2 eDirectory server hosting the following partitions:

- BANGALORE
- SILVEROAK

Remarks

BANGALORE is audited based on its default configuration.

For every object in ROOT, NAAS searches only three levels up to find the associated Event policy. Therefore, SILVEROAK is not audited because the objects are not associated to any event policies.

Event policies should be associated to SILVEROAK, in order to audit it. This can be done by associating required event policies to SILVEROAK. The policies associated to SILVEROAK will be effective to all the objects in that partition and policies associated to BANGALORE will be effective only to the objects in BANGALORE. If you have created and associated new Event policies, required rights should be provided based on the steps given in “Granting Rights to NAAS Agents” on page 60.

Scenario 9

This scenario talks about configuring NAAS for DELHI. The NAAS Agent is configured for the any eDirectory server under DELHI hosting the following partitions:

- DELHI
- D1

- D2
- D3
- D4

Remarks

DELHI is audited based on its default configuration.

D1, D2, D3, and D4 are audited depending on the setup. The objects in these partitions that are not associated to any event policies will not be audited. For every object in the partitions NAAS searches only three levels up to find the associated Event policy. If necessary, the user can change the search policy so that the search for an effective policy goes up higher than three levels.

Therefore, to audit D1, D2, D3, and D4 you need to either associate event policies to those partitions or set the search policy for these partitions at a suitable level so that it obtains a policy by searching upwards. If you have created and associated new Event policies, required rights should be provided based on the steps given in "Granting Rights to NAAS Agents" on page 60.

In the current setup, objects in D1, D2 and D3 can use the Event polices created by Default configuration of DELHI, since the default search level is 3.

Scenario 10

This scenario talks about configuring NAAS for INDIA. The NAAS Agent is configured for the any eDirectory server under INDIA hosting the following partitions:

- INDIA
- BOMBAY
- JAPAN

Remarks

INDIA is audited based on its default configuration.

For every object in JAPAN, NAAS searches only three levels up to find the associated Event policy. Therefore, JAPAN is not audited because the objects are not associated to any event policies.

Event policies should be associated to Japan, in order to audit it. This can be done by associating required event policies to JAPAN. If you have created and associated new Event policies, required rights should be provided based on the steps given in "Granting Rights to NAAS Agents" on page 60.

By default, BOMBAY is audited. For every object in the partitions NAAS searches only three levels up to find the associated Event policy and it will find the event Policies present in the partition INDIA. Therefore, those objects present in deep levels inside the partition INDIA might not have the Event policy associated. You might need to associate a high-level search policy or associate an Event policy directly. If you have created and associated new Event policies, required rights should be provided based on the steps given in "Granting Rights to NAAS Agents" on page 60.

Granting Rights to NAAS Agents

Assume that a NAAS Agent is Auditing Partition X and a NAAS Event policy is associated to the Partition X. The agent queries for the policies associated with the objects in the partition. The Agent needs the Read right to the naasPolLink and *naasSearchPolLink* attributes for all the objects in the partition. Also, when the agent finds an associated event policy, it should read its contents. Therefore, the agent must have Read access to the event policy

When the Default Configuration Utility is used to configure NAAS for a Partition, the above rights are provided by default. In case the Event policy is associated manually to any new partition, give the following rights:

- Read rights to the naasPolLink and naasSearchPolLink attributes for all the objects in the partition (Can be done at the partition level.)
- Read rights to the Event policy.

Reporting in Multipartition Auditing

The following conditions should be considered when using the Default Configuration utility regarding reporting.

- The user must be configured as an Auditor to obtain the report. The Default Configuration utility can be used to configure a user as an Auditor.
- By default, NAAS assumes that the user resides in the same partition for which NAAS is being configured.
- By default, the Auditor Query Domain is set as the partition root for which NAAS is configured. Therefore, the Auditor can view audit data with respect to that partition only.

Granting Rights

When configuring a NAAS Agent for a NAAS Server that hosts more than one partition, auditing is enabled for all the hosted partitions based on the policies associated. But a user is configured as an Auditor for only one partition. Therefore, the user would receive report only for that partition.

To receive the audit data of other partitions add the partitions to the Auditor Query Domain and grant the Auditor the Read right to the naasTrail attribute for the all partitions being added. For more information, refer to "Scenarios for Reporting in Multipartition Auditing" on page 61.

Partition Boundary

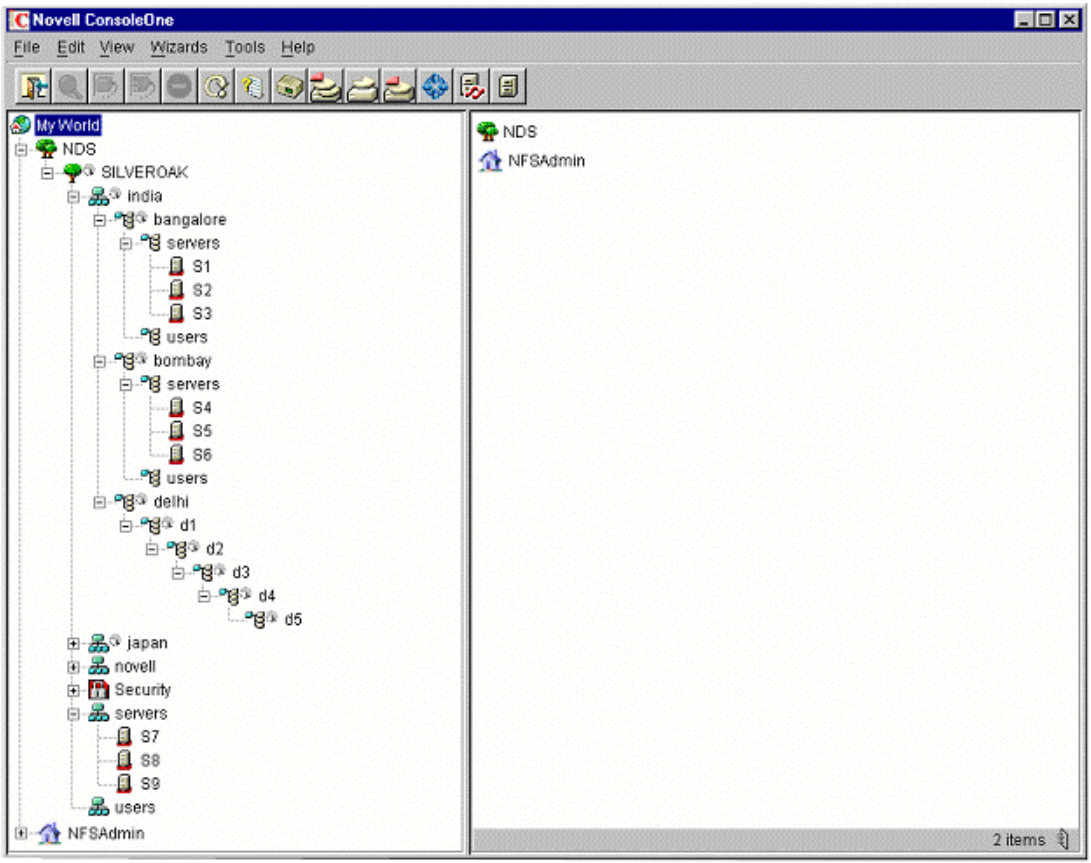
The Auditor Query Domain has an attribute called Partition Boundary.

On the Properties page of the Auditor Query Domain, a list of domain roots and a check box for Partition boundary are provided. The lists of objects in the domain are calculated based on these attributes. If Partition Boundary is checked, then the scope will limit itself to the respective partition boundaries of the domain roots. If the Partition Boundary is unchecked, then the scope includes all objects under the domain roots and all the child partitions hierarchically under the listed domain roots.

Scenarios for Reporting in Multipartition Auditing

This section describes a few scenarios. The following figure depicts a sample eDirectory Tree. For each scenario an abstract section of the tree is considered and the impact of NAAS configuration and auditing is explained.

(Figure Description) Network for Scenario Setup



Scenario 1

This scenario talks about configuring NAAS for BANGALORE. The NAAS Agent is configured for the S1 eDirectory server hosting the following partitions:

- BANGALORE
- BOMBAY

Remarks

If the Event polices are associated to BOMBAY, then auditing is enabled for both BOMBAY and BANGALORE. Because the Auditor Query Domain

associated to the Auditor by default has only the partition BANGALORE, the Auditor can view only BANGALORE related data.

To view BOMBAY-related data, perform the following steps.

1. Add the partition BOMBAY to the Auditor Query Domain.
2. Grant the Auditor the Read rights to the naasTrail attribute for the entire partition.

Scenario 2

This scenario talks about configuring NAAS for DELHI. The NAAS Agent is configured for the DELHI eDirectory server hosting the following partitions.

- DELHI
- D1
- D2
- D3
- D4

Remarks

If appropriate Event policies are associated to D1, D2, D3, and D4 and auditing is enabled for all these partitions, then by default, the Audit Query Domain is set for DELHI. Therefore, the Auditor would receive Audit data only for DELHI. To also receive audit data for all the Partitions D1, D2, D3 and D4 do either of the following:

- Uncheck the Partition Boundary option. This extends the scope beyond DELHI.
- Add D1, D2, D3, and D4 can be added to the Query Domain List in the properties of the Auditor Query Domain.

Recommendations

- Associate the individual policies at every partition root. This will improve the search speed.

- It is better to manage the policies from one single place, after the initial configuration. Therefore, store all NAAS policies at central location and associate accordingly.

Setting Up NAAS Database

Place the JDBC driver at CONSOLEONE_HOME/1.2/LIB/NAAS directory.

Setting Up Pervasive Database

Ensure the JDBC driver of the database in SYS:\JAVA\LIB directory.

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 as Pervasive.SQL 2000*.
3. Specify the Database (server) IP address.
4. Specify a new password for the NAAS Super User.

   NAAS Super User is the administrator of the NAAS database.

   For Pervasive database Master will be the NAAS Super user.
5. Re-enter the password.
6. Enter the fully distinguished name (FDN) and password of the eDirectory administrator.For example, *.admin.novell*
7. Click OK to activate automatic configuration of the NAAS database.

Setting Up MySQL Database

1. In the Select Configuration Task dialog box, select Set Up NAAS Database and click OK to display a dialog box to enter details about the database.
2. Select the database type as MySQL.
3. Specify the database (server) IP address.
4. Enter the DBA name (default = root), enter the DBA password (default = blank password).

5 Click OK to activate automatic configuration of the NAAS database.

Proceed to Configuring NAAS framework.

Setting Up Oracle 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 as Oracle.

3 Specify the Database (server) IP address.

4 Specify a new password for the NAAS Super User.

NAAS Super User is the administrator of the NAAS database.

For Oracle database NAASADMN will be the NAAS Super user.

5 Re-enter the password.

6 Enter the DBA name > enter the DBA password. For example DBA name system and the DBA password manager.

7 Click OK.

Auditing eDirectory

Audit eDirectory by following the steps described in “Configuring eDirectory Auditing” on page 37.

Auditing NWFS

Audit NWFS (NetWare Legacy File System) by following the steps described in “Configuring Traditional File System Auditing” on page 38.

Auditing NSS

Audit NSS (Novell Storage Services™) by following the steps described in “Configuring NSS Auditing” on page 39.

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 36.

Creating and Modifying Audit Policies

Creating an Audit Policy

1. In ConsoleOne™, right-click the desired container and click New > Object.
2. Select the policy to be created and 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 and 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.

   An Auditor Query domain is essentially a subset of the eDirectory tree. When the Auditor connects to an NAAS 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 NAAS Server should query objects.

1a In ConsoleOne, right-click the desired container then, click New > Object.

1b Select the NAASQueryDomain then, click OK.

1c Enter the name of the Auditor Query Domain.

1d Enter eDirectory context of the tree where NAAS is installed.

1e Add a list distinguished name (DN) that are roots of the subtrees that make up the domain.

1f (Optional). To bind each subtree in the domain by the partition boundary of the eDirectory partition containing the subtree root, check Partition Boundary.

1g (Optional). To restrict the number of tree levels where the domain can extend below the subtree roots, check Depth.

Maximum Depth will be enabled only if Depth is checked. Type the maximum number of tree levels for extending the associated domain below the subtree roots.

1h (Optional). To limit the domain at specific objects, check this Specific Objects. If one of the specified DN is present in a subtree, then that DN and the subtrees below it are excluded from the domain.

2 Right-click the User object.

3 Click 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 NAAS Servers that the Auditor can contact.

The servers configured here must have the Read right to the NaasSelectedDomain attribute of this user. Also, the servers must have the Read right for the Auditor query domains configured in Step 4.

7 Grant the Auditor the Read right to the naasPortNumber, naasKMO and HostDevice attributes of the NAAS Server objects to be contacted.

8 Grant the Auditor the Read right to the NetworkAddress attribute of the NetWare server objects hosting the NAAS Servers to be contacted.

9. Grant the user the Read and Write rights to the naasDomainList, naasSelectedDomain and naasServersList attributes on the user object set as the auditor.
10. Assign the Read right to Auditor for naasTrail attribute on the NAAS Server object.

Granting Rights for Generating NAAS Reports

The NAAS 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.

Auditor Query Domains

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

Name: Name of the Auditor Query Domain.

Context: eDirectory context of the tree in which NAAS is installed.

Domain Roots: Adds a list distinguished name (DN) that are roots of the subtrees that make up the domain.

Partition Boundary: Optional. Binds each subtree in the domain to the partition boundary of the eDirectory partition containing the sub tree root.

Depth: Optional. Restricts the number of tree levels where the domain can extend below the subtree roots.

Maximum Depth: The maximum number of tree levels for extending the associated domain below the sub tree roots. This can be enabled only if Depth is enabled.

Specific Objects: Optional. Limits the domain at specific objects. If one of the specified DN is present in a subtree, then that DN and the subtrees below it are excluded from the domain.

IMPORTANT: Only those NAAS 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 and click Define Additional Properties > 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 NAAS 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 NAAS 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 NAAS 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 36.

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 72
- “Event Filters” on page 72
- “Data Filters” on page 72

IMPORTANT: You must be an Auditor to create and use filters. See “Setting the User as Auditor” on page 66 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: Filter 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 and 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 and click OK to apply the filter and generate the report. For more details on report generation, see "Generating Audit Reports" on page 76.

   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. ◆ **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 must be an Auditor to generate reports. See “Setting the User as Auditor” on page 66 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 76
- “Executing Queries” on page 77

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 in “Apply Filters during Report Generation” on page 75.

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.

Generating Reports in non-English Languages

When generating reports in some non-English language environments with Oracle 8i on NetWare 5.1 as the NAAS database, some character sets might not be clear.

To resolve this problem, complete the following at the database server.

IMPORTANT: Before proceeding, back up the database.

1. If the database is running, stop it using ORASTOP and ORAUNLD at the Netware 5.1 server console.
2. Start the database by using ORALOAD and ORASTART at the Netware 5.1 server console
3. Enter **SVRMGR31** at the Netware 5.1 server console.
4. Enter **SYSTEM** and enter the password.

   By default, the password is *manager*.
5. Execute the following SQL commands:

```
SQL> ALTER SYSTEM ENABLE RESTRICTED SESSION;
SQL> ALTER SYSTEM SET JOB_QUEUE_PROCESSES=0;
SQL> ALTER DATABASE OPEN;
SQL> ALTER DATABASE CHARACTER SET UTF8;
```

6. Restart the Oracle database server.

Executing Queries

1. From the NAAS menu, click Query.

   The query screen is displayed.
2. Type the SQL condition for the statement SELECT * FROM NAASADMN.TRAIL WHERE (*condition*).

   The auditor can provide a condition based on the following fields

   - VERSION

- SERVICE_ID
- SERVICE_VERSION
- EVENT_ID
- EVENT_NAME
- TIMESTAMP
- TO_NAME
- USER_NAME
- SOURCE_IP
- TARGET_IP
- ACTION_TAKEN
- PROCESS_ID
- SUCCESS_CODE

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

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

  SOURCE_IP LIKE *'IP ADDRESS%'*

- To filter based on MAC address, enter the *condition* as

  SOURCE_IP LIKE *'%MAC ADDRESS'*

IMPORTANT: The FDNs in the condition 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 the 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, click Add Trustee, and 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, and 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.

6 NAAS Troubleshooting

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

NAAS Server

This section provides the troubleshooting scenarios encountered when using the NAAS Server.

Unable to start Audit server

Source: NAAS server.

Problem: The NAAS server is unable to start because of unsuccessful or incomplete operations performed during startup. Report requests will not be serviced by the NAAS server.

Action: See error codes "7100" on page 95 and "7101" on page 96 for information on actions for resolving the problem.

Server start up failed. Unable to log in to Novell eDirectory.

Source: NAAS Server.

Problem: The NAAS Server is unable to log in to Novell eDirectory. The Server will fail to come up and auditing cannot be done

Action: See error codes "7332" on page 104 and "-669" on page 112, for information on actions for resolving the problem.

Unable to register Real Time Server Plug-in

Source: NAAS server.

Problem: NAAS was unable to register the Real Time Server plug-in because it could not successfully obtain the configuration parameters. Real Time Alert will be unavailable to the system in this state.

Action: See error codes "7102" on page 96, "7103" on page 96, "7104" on page 96, "7105" on page 97, "7106" on page 97, and "7107" on page 97 for information on actions for resolving the problem.

Unable to Log in to NDS

Source: NAAS server.

Explanation: All configurable information is stored in Novell eDirectory™. Failure to log into Novell eDirectory indicates the failure in all operations, which have dependency of Novell eDirectory to obtain information.

Action: See error codes "7110" on page 98, "-634" on page 112, "-1416 / -669" on page 112, "-601 or -610" on page 110 and "- 663" on page 112 for information on actions for resolving the problem.

Unable to Establish a Secure / SSL Channel

Source: NAAS server.

Problem: Communication failure between the NAAS server and NAAS utility.

Action: See error codes "7108" on page 97, "7109" on page 97 and "7203" on page 102 for information on actions for resolving the problem.

Unable to Obtain / Set Database Initialization Parameters

Source: NAAS server.

Problem: Failure of all database operations. The database, which holds all the audit trail data, is not ready for operation.

Action: See error codes “7111” on page 98 and “7112” on page 98 for information on actions for resolving the problem.

Authentication Process Failed

Source: NAAS server.

Problem: Failure in the authentication process occurs when the authentication protocol fails between NAAS Server and Auditor.The user will not be able to obtain information, such as reports, from the system.

Action: See error codes “7114” on page 98, “7115” on page 99, “7116” on page 99, and“7124” on page 101 for information on actions for resolving the problem.

Communication Error

Source: NAAS server.

Problem: Results in no communication between components.

Action: See error code “7113” on page 98 for information on action for resolving the problem.

Database Operation Failed

Source: NAAS server.

Problem: The database is the central store for the Audit trail, so a failure in operations on the database will lead to a failure in obtaining reports.

Action: See error codes “7117” on page 99, “7118” on page 99, “7121” on page 100, “7122” on page 100, and “7127” on page 101 for information on actions for resolving the problem.

System Error

Source: Database.

Problem: An internal error within the system.

Action: See error codes “7119” on page 100, “7120” on page 100, and “7126” on page 101 for information on actions for resolving the problem.

Real Time Server Error

Source: Real Time Plug-in.

Problem: Unable to receive request because of data corruption.

Action: See error code “7123” on page 101 for information on actions for resolving the problem.

Problem: Invalid address

Action: See error code “7200” on page 101 for information on actions for resolving the problem.

Problem: Mail could not be delivered

Action: See error code “7201” on page 102 for information on actions for resolving the problem.

NAAS Configuration Utility

This section provides the troubleshooting scenarios encountered when using the configuration utility.

Configuration Error

Source: The error message appears on the Audit utility screen.

Problem: Failure of configuration of the framework. Auditing will not take place.

Action: See error code “7600” on page 110 for information on actions for resolving the problem.

NAAS Agent Setup failed. Com.novell.admin.ns.NamespaceException

Explanation: Occurs when creating NAAS objects using NAAS default configuration utility.

Possible Cause: The NAAS schema for NDS is not extended successfully. NAAS could not locate any NDS 8.*x* replicas.

Action: Copy SYS:\SYSTEM\SCH_EXT.NLM from any of the NetWare® 6 servers with NAAS installed to any of NetWare servers with NDS 8.*x* having a read-write replica. At the system console of the same NetWare server with NDS 8.*x* having read-write replica, enter the following:

```
Sys:\system\sch_ext FQDN_of_ admin admin_password
```

NAAS Server setup failed. com.novell.admin.ns.NamespaceException

Explanation: Occurs when creating NAAS objects using NAAS default configuration utility.

Possible Cause: The NAAS schema for NDS is not extended successfully. NAAS could not locate any NDS 8.*x* replicas.

Action: At the system console of any NetWare server with NDS 8.*x* having read-write replica, enter the following:

```
Sys:\system\sch_ext FQDN of admin admin password
```

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 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.

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: NAAS 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 utility displays this error message even after successful completion of the NAAS framework.

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.

The Pervasive license and key files are not updated

Source: NetWare upgrade process.

Explanation: 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 the 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

Unable to Connect to Server

Possible Cause: Occurs when configuring NAAS Database using the default configuration utility.

Action: Check the connectivity problems using Pervasive System Analyzer (PSA).

1. Click Start > Pervasive > Pervasive.SQL 2000i > Utilities > Pervasive System Analyzer > Next.
2. Select Test Network Communication > enter the path to the file for storing the test log > Next.
3. Enter or browse to the location of the Pervasive engine (for example, \\SERVER_NAME\SYS:\PVSW) and click Next.

   The PSA performs the connectivity test and logs the errors in the test log.

4. Click Next to view the log file.

The latest standalone version of the PSA available for Pervasive.SQl 2000

SP3 can be downloaded from the Pervasive support site (http://www.pervasive.com/support/updates/psa_update.asp). For information about using PSA, refer to the Webinar archive (http://www.pervasive.com/training/webinar_arch.asp)

Action: Resolve and verify the IP address of the NetWare server, since Pervasive.SQL 2000 SP3 uses either the DNS or eDirectory name of the NetWare server to resolve the IP address.

To resolve the IP address of the NetWare server based on its eDirectory name, the following conditions should be satisfied.

- Novell client should be installed on the work station.
- NetWare 5.0 or above should be installed in the server.

To verify whether the IP address of the machine has been resolved, refer to the connection test log generated by the PSA.

To check whether the IP address can be resolved using the DNS name of the server, PING the server using the server name. If this is successful, then the Pervasive.SQL 2000 SP3 client will resolve the IP address.

Action: Configure the Pervasive client such that only TCP/IP is used as the communication protocol. Ensure that both the Btrieve* and the Pervasive.SQL 2000 clients are configured for TCP/IP protocol.

To configure the Pervasive client:

1. In the client, go to the Pervasive Control Center (PCC) and click Configuration > Client > Communications Protocol.
2. Set Supported Protocols to Microsoft* TCP/IP Only.

To configure the Pervasive server:

1. Go to the PCC and register the server.
2. Click Configuration > Server and set supported protocols and ODBC supported protocols to Novell TCP/IP.

Restart the PCC and the server.

Action: If the server has multiple IP addresses, the IP address used for the client communication should be checked.

If the server has both public and private IP address, ping the server using the private IP addresss.

HINT: If you are unable to ping the server using the server name or its IP address, then check the network connectivity.

Action: If the server has multiple IP addresses, the DNS query will return only the public IP address. To connect the client through the firewall, open the ports 1583 and 3351 (Decimal).

All the errors generated during the process of establishing the server connection are logged in the log file PVSW.LOG. This file is located in SYS:\SYSTEM directory in the server or C:\WINNT directory in Windows NT or 2000 client.

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

Source: NAAS utility.

Explanation: This error message appears 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.

Cannot create database name. You do not have sufficient access rights for the operation, or the destination directory does not exist.

Possible Cause: When upgrading from NetWare 5.1 to NetWare 6, the Pervasive BTI.CFG configuration file is not updated.

Action: Manually edit BTI.CFG and add the following section:

Database Names

DBNamesDirectory = SYS:SYSTEM

NAAS Agent

This section provides the troubleshooting scenarios encountered when using the NAAS Agent.

Unable to start the Audit Agent

Source: NAAS Agent.

Problem: The NAAS Agent will not come up. Auditing cannot be done for this server.

Action: See error codes “7320” on page 103 and “7322” on page 103 for information on actions for resolving the problem.

Agent start up failed. Unable to log in to Novell eDirectory.

Source: NAAS Agent.

Problem: The NAAS Agent is unable to log in to Novell eDirectory. The Agent will fail to come up and auditing cannot be done for this server.

Action: See error codes "7332" on page 104, "-669" on page 112, and "-602 or -603" on page 111 for information on actions for resolving the problem.

Agent start up failed. Unable to read the agent policy

Source: NAAS Agent

Problem: The NAAS Agent is unable to read the associated agent policy. The Agent will fail to come up and auditing cannot be done for this server.

Action: See error codes "-602 or -603" on page 111 and "7338" on page 105 for information on actions for resolving the problem.

Unable to start auditing for the service.

Source: NAAS Agent.

Problem: The Audited Service registration with NAAS agent fails. As a result, the service will not be audited. If loading the service is dependent on auditing, the service might not come up.

Possible Cause: The problem may be because of one of the following problems:

- "Service initialization failed. Unable to find event policy." on page 90
- "Agent start up failed. Unable to read the agent policy" on page 90
- "Unable to read the data policy." on page 91
- "Unable to read the search policy." on page 91

Service initialization failed. Unable to find event policy.

Source: NAAS Agent.

Problem: The Agent could not find the naasEventPolicy for the service being audited. The service will not be audited. The service might not come up.

Action: See error code "7322" on page 103 for information on actions for resolving the problem.

Service initialization failed. Unable to read the event policy.

Source: NAAS Agent.

Problem: The Agent could not read the associated naasEventPolicy for the service getting audited. The service will not be audited. The service might not come up.

Action: See error codes "7337" on page 105, "7338" on page 105, and "-602 or -603" on page 111 for information on actions for resolving the problem.

Unable to read the data policy.

Source: NAAS Agent.

Problem: The Agent could not read the associated naasDataPolicy for the service being audited. The service will not be audited. The service might not come up.

Action: See error codes "7338" on page 105 and "-601 or -610" on page 110 for information on actions for resolving the problem.

Unable to read the search policy.

Source: NAAS Agent.

Problem: The Agent could not read the associated naasSearchCriteriaPolicy. The affected module might not come up.

Action: See error codes "-602 or -603" on page 111, and "7338" on page 105 for information on actions for resolving the problem.

Unable to write to the cache file.

Source: NAAS Agent.

Problem: The NAAS Agent was unable to write the event record to the cache file. The event will not be logged and an error will be returned to the audited service. The service may reject the event.

Action: See error codes "7309" on page 102, "7321" on page 103, and "File system error" on page 110 for information on actions for resolving the problem.

Failed to raise real time alert.

Source: NAAS Agent.

Problem: The NAAS Agent was unable to raise a real-time alert for the event. The alert will not be raised but the data is logged in the NAAS audit trail.

Action: See error codes “7400” on page 106, “7325” on page 103, “7326” on page 104, and “BSD socket error codes” on page 110 for information on actions for resolving the problem.

Unable to commit the cache file. The file is corrupted and will be deleted

Source: NAAS Agent.

Problem: The audit cache file was corrupted. The file will be deleted and all data in it will be lost.

Action: See error code “7400” on page 106 for information on actions for resolving the problem.

Unable to commit audit data.

Source: NAAS Agent.

Problem: The NAAS Agent is unable to commit the audit cache file to the NAAS server. The file will be committed during the next commit period.

Action: See error codes “7401” on page 106, “7402” on page 106, “7403” on page 106, “7404” on page 107, “7405” on page 107, and “7406” on page 107 for information on actions for resolving the problem.

NAAS Utility

This section provides the troubleshooting scenarios encountered when using the NAAS utility.

There was an error getting filter list from the database.

Source: NAAS utility.

Problem: The NAAS utility is unable to create, update, or delete the filters. This could be because either the NAAS utility is unable to communicate with the NAAS server or some database operation failed.

Action: See error codes “7503” on page 108, “7504” on page 108, “7505” on page 108 and “7508” on page 108 for information on actions for resolving the problem.

There was an error generating the report.

Source: NAAS utility.

Problem: The NAAS utility is unable to generate the report because some database operations have failed or the NAAS utility is unable to communicate with the NAAS server.

Action: See error codes “7503” on page 108, “7504” on page 108, “7505” on page 108 and “7508” on page 108 for information on actions for resolving the problem.

There was an error in displaying the query results.

Source: NAAS utility.

Problem: The NAAS utility is unable to generate the report because some database operations have failed or the NAAS utility is unable to communicate with the NAAS server.

Action: See error codes “7503” on page 108, “7504” on page 108, “7505” on page 108 and “7508” on page 108 for information on actions for resolving the problem.

Authentication to the Audit Server failed.

Source: NAAS utility.

Problem: The NAAS utility is unable to communicate with the NAAS server either because the user is a non-auditor or there is some problem with SSL.

Action: See error codes “7502” on page 107 for information on actions for resolving the problem.

Miscellaneous

This section provides miscellaneous troubleshooting scenarios encountered when using NAAS.

NAAS components fail to come up on a non eDirectory replica server.

Action: Load the NAAS Agent on the non- replica server by entering the following on the server console:

```
adagtset -nr username password
```

where the *username* is the dot- delimited FDN for a user with supervisor rights on the partition with the server.

Action: Load the NAAS server on the non- replica server by entering the following on the server console:

```
adsrvset -nr username password
```

where *username* is the dot-delimited FDN for a user with supervisor rights on the partition with the server.

The NAAS components can now be loaded following the normal procedure.

NAAS reports are not generated and audit trail is not getting committed to the database.

Possible Cause: A mismatch exists in the NICI key strengths of the NAAS Utility and NAAS Server machines

Action: Reconfigure the NAAS database with the required NICI key strength.

One or more NAAS modules fail to come up after reconfiguring NAAS

Explanation: On a NetWare 6 server, after applying Support Pack 1 or later and re-configuring NAAS one or more NAAS modules may fail to come up.

Possible Cause: eDirectory synchronization may not have happened after NAAS reconfiguration

Action: Force eDirectory synchronization among all replicas and load the NAAS modules using ST_SRVR.NCF and ST_AGENT.NCF.

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 server.

Error message and error code -625 are logged

Problem: The NAAS agent fails to load.

Possible Cause: The communication channel between components is broken.

Action: Restart the NetWare server.

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.

NAAS Error Codes

This section provides the error codes that you could use to manage your servers when NAAS error conditions exist.

The error codes are categorized as follows:

- NAAS Error Codes

  The error codes 7*xxx* represent the problems with NAAS in general.

- NAAS Server Error Codes

  The error codes 71*xx* to 72*xx* represent the problems specific to the NAAS server.

- NAAS Agent Error Codes

  The error codes 73*xx* to 74*xx* represent the problems specific to the NAAS Agent.

- NAAS Utility Error Codes

  The error codes 75*xx* to 76*xx* represent the problems specific to the NAAS utilities, such as the Audit and Configuration utilities.

7100

Problem: "Unable to start Audit server" on page 81.

Possible Cause: Unable to load or locate ADSERVER.NLM (NetWare) or NAASSERVER.SO (UNIX).

Action: Ensure that the files are located in the specified path. The ADSERVER.NLM must be located in the SYS:\SYSTEM\ directory before startup. Also ensure that the file level privileges have been provided.

7101

Problem: “Unable to start Audit server” on page 81.

Possible Cause: The server configuration file is missing or the content is corrupted.

Action: Ensure that the server configuration file is present in the specified location. The file must be located at SYS:_NETWARE\SRCONFIG.CFG.

Also ensure the contents are correct. The correct format is:

```
.Treename.+.
naas server object name
```

7102

Problem: “Unable to register Real Time Server Plug-in” on page 82.

Possible Cause: The contents of the Real Time Server configuration file are corrupted or the contents might not be in the specified format.

Action: Ensure that the contents of the Real Time Server configuration file are in the required format. The file is located at SYS:\AUDIT\MAILALERT.CFG.

The correct format is: RTAS-CLASSNAME = Plugin Classname

7103

Problem: “Unable to register Real Time Server Plug-in” on page 82.

Possible Cause: Unable to find Real Time Server plug-in configuration file.

Action: Ensure that the Real Time Server plug-in configuration file is placed in the required location. The file must be located at SYS:\AUDIT\RTS.CFG.

7104

Problem: “Unable to register Real Time Server Plug-in” on page 82.

Possible Cause: Security or access violation while accessing the Real Time Server plug-in configuration file. The file is located at SYS:\AUDIT\RTS.CFG.

Action: Ensure that the required access control is provided for the specific file/directory.

7105

Problem: "Unable to register Real Time Server Plug-in" on page 82.

Possible Cause: Communication or I/O problem while reading the Real Time Server plug-in configuration file.

Action: Restart the NAAS server.

7106

Problem: "Unable to register Real Time Server Plug-in" on page 82.

Possible Cause: The Real Time Server plug-in could not be loaded.

Action: Ensure that the plug-in name (class name) is specified correctly in the Real Time Server plug-in configuration file. Also ensure that the class exists in the classpath.

7107

Problem: "Unable to register Real Time Server Plug-in" on page 82.

Possible Cause: Internal error in registering the Real Time Server plug-in.

Action: Restart the NAAS server.

7108

Problem: "Unable to Establish a Secure / SSL Channel" on page 82.

Possible Cause: Socket/server-socket factory is not available to create secure server sockets.

Action: Ensure that the socket/server-socket factory implementation is present in the classpath. Confirm if SPI is present. By default, NAAS uses NSSL1.2_EXP.JAR as its SSL implementation.

7109

Problem: "Unable to Establish a Secure / SSL Channel" on page 82.

Possible Cause: The security option could not be set for creating sockets.

Action: Ensure that there are sufficient privileges to create sockets on the server port.

7110

Problem: "Unable to Log in to NDS" on page 82.

Possible Cause: The NAAS Server object or the NAAS Server Policy object in eDirectory might be corrupted.

Action: Reconfigure the NAAS framework.

7111

Problem: "Unable to Obtain / Set Database Initialization Parameters" on page 83.

Possible Cause: The Database object might be corrupted in eDirectory. Information represented by the Database object is corrupted.

Action: Re-create the Database object and reconfigure the NAAS framework.

7112

Problem: "Unable to Obtain / Set Database Initialization Parameters" on page 83.

Possible Cause: Unable to locate or load the JDBC driver.

Action: Ensure that the latest JDBC driver is present in the required location. The default location is SYS:\JAVA\LIB. To find out more about JDBC driver required for the system, refer "Software Requirements" on page 14.

7113

Problem: "Communication Error" on page 83.

Possible Cause: I/O or communication components failure.

Explanation: This occurs because of exceptions at the socket communication level or because of the data corruption during data transfer.

Action: Restart the affected components, usually the NAAS server and NAAS utility.

7114

Problem: "Authentication Process Failed" on page 83.

Possible Cause: The Auditor failed to perform the necessary prerequisites for authentication. The authentication has failed because the Auditor has not performed the necessary operations for self-authentication.

Action: If this error occurs with valid Auditors, ensure that the user has necessary rights and extensions of an Auditor.

7115

Problem: "Authentication Process Failed" on page 83.

Possible Cause: Invalid credentials or the authentication information from the Auditor is incorrect.

Explanation: This typically occurs when the authentication fails because the user is not an authorized user or because invalid data has been given as parameters for the authentication process.

Action: Ensure that the user has sufficient rights. Restart the NAAS server and try again.

7116

Problem: "Authentication Process Failed" on page 83.

Possible Cause: Unable to register the Auditor with the system.

Explanation: Two auditors with the same name have logged in and are using the system. This is an invalid state.

Action: One Auditor needs to log out of the system.

7117

Problem: "Database Operation Failed" on page 83.

Possible Cause: The database is down.

Action: Start the database.

7118

Problem: "Database Operation Failed" on page 83.

Possible Cause: Invalid request or user credentials unresolved.

Explanation: This state occurs when the system ceases to service requests because of a failure in the internal encryption process, or because the database is not initialized.

Action: Make sure NICI is properly installed and configured on the server side. Refer to the NICI Documentation (http://www.novell.com/documentation) for

details. Also ensure that related objects and policies in the database are not corrupted. Restart the NAAS server.

7119

Problem: "System Error" on page 83.

Possible Cause: Unable to deregister the Auditor with the system because of an internal error.

Action: Restart the NAAS server.

7120

Problem: "System Error" on page 83.

Possible Cause: Unable to receive a request because of data corruption.

Explanation: This occurs when the data has been sent in the right format, but the data has been corrupted during transfer. The system will usually behave as if an I/O problem has occurred, and the communication will no longer exist between modules.

Action: Restart the NAAS server.

7121

Problem: "Database Operation Failed" on page 83.

Possible Cause: Insufficient rights.

Explanation: The user does not have enough privileges to perform the operation.

Action: Reconfigure the framework with the user as an Auditor and try again.

7122

Problem: "Database Operation Failed" on page 83.

Possible Cause: Invalid parameters received during database operation.

Action: Database operation has failed because of invalid data either received or supplied from the database. Ensure that the data is not corrupted in the request or in the database.

7123

Problem: “Real Time Server Error” on page 84.

Possible Cause: Unable to receive request because of data corruption.

Explanation: This occurs when the data has been sent in the right format, but the data has been corrupted during transfer. The system will usually behave as if an I/O problem has occurred and the real time alerts will no longer function.

Action: Restart the NAAS Server and try again.

7124

Problem: “Authentication Process Failed” on page 83.

Possible Cause: The user is not an Auditor.

Explanation: The user must have the Auditor extension to perform operations of an Auditor.

Action: Configure the user as an Auditor.

7126

Severity: High

Problem: “System Error” on page 83.

Possible Cause: An error in writing audit data to the secure local storage.

Explanation: The server cache file is corrupted.

Action: To resume operation, delete the cache file, restart the NAAS server, and continue. The cache file is located at SYS:_NETWARE\SECFILE.

7127

Problem: “Database Operation Failed” on page 83.

Possible Cause: The SQL syntax is incorrect.

Action: Correct the SQL Syntax and try again.

7200

Problem: “Real Time Server Error” on page 84.

Possible Cause: Invalid Address. The mailing address specified in SYS:\AUDIT\MAILALERT.CFG is invalid.

Action: Ensure that a valid mailing address is in SYS:\AUDIT\MAILALERT.CFG.

7201

Problem: “Real Time Server Error” on page 84.

Possible Cause: Valid address but mail could not be delivered. The database server might be down.

Action: Ensure that the SMTP server specified in SYS:\AUDIT\MAILALERT.CFG is up and running.

Possible Cause: Invalid addresses specified in SYS:\AUDIT\MAILALERT.CFG

Action: Ensure that all the addresses specified in SYS:\AUDIT\MAILALERT.CFG are valid.

7202

Problem: “There was an error generating the report.” on page 93

Problem: “There was an error getting filter list from the database.” on page 92

Problem: “There was an error in displaying the query results.” on page 93

Possible Cause: Auditor has insufficient rights.

Action: Assign read rights for the NAAS audit trail in the NAAS Server. Restart ConsoleOne and try again.

7203

Problem: “Unable to Establish a Secure / SSL Channel” on page 82

Possible Cause: The key material object (NAASKMO) specified in the NAAS Server object is invalid.

Action: Ensure that certificates in the KMO specified in the NAAS Server object are valid. This can be checked using the PKI snap-ins for ConsoleOne.

7309

Problem: “Unable to write to the cache file.” on page 91.

Possible Cause: The audit cache file has exceeded the value given in the naasAgentPolicy.

Action: Increase the cache file size or reduce the commit period in the naasAgentPolicy and restart the server.

7320

Problem: "Unable to start the Audit Agent" on page 89.

Possible Cause: The NAAS Agent cache file is locked by another process.

Action: Restart the NetWare server hosting the NAAS Agent. This will release all file locks.

7321

Problem: "Unable to write to the cache file." on page 91.

Possible Cause: There was some problem in writing the record to the cache file.

Action: Restart the server if the problem persists.

7322

Problem: "Unable to start the Audit Agent" on page 89.

Possible Cause: There is no applicable naasAgentPolicy for this agent object. This agent object does not have read rights to the naasPolLink attribute for the eDirectory sub-tree hosting it.

Action: If the Agent was created using the NAAS default configuration utility, reconfigure the system by completing the steps in "Configuring NAAS Framework" on page 24. If the naasAgent object for the server was created manually, configure the object by completing the steps in "Manually Configuring Novell Advanced Audit Service" on page 33.

Problem: "Service initialization failed. Unable to find event policy." on page 90.

Possible Cause: The naasEventPolicy object for the audited service has not been created in eDirectory or the agent does not have appropriate rights to read the policy object.

Action: For NAAS Shims, run the Default Configuration Utility with the Configure NAAS Framework option. For other audited services, create the appropriate naasEventPolicy object and grant the agent appropriate rights as described in "Configuring eDirectory Auditing" on page 37.

7325

Problem: "Failed to raise real time alert." on page 91.

Possible Cause: The NAAS Agent was unable to open socket connection to the NAAS Server.

Action: Check if the NAAS Server is up and the network connectivity is correct.

7326

Problem: "Failed to raise real time alert." on page 91.

Possible Cause: The NAAS Agent was unable to write the data on the socket.

Action: Check if the NAAS Server is up and the network connectivity is correct. Restart the NAAS components, if required.

7332

Problem: "Agent start up failed. Unable to log in to Novell eDirectory." on page 90.

Possible Cause: The NAAS Agent is unable to read the password file. The file might be missing.

Action: Load the ADAGTSET.NLM from the server console. The NLM is located in the SYS:\SYTEM or SYS:\AUDIT directory. This will create the password file.

Possible Cause: The agent is unable to read the password file. The file may be locked by some other process.

Action: Restart the NetWare server hosting the NAAS Agent. This will release all file locks.

Problem: "Server start up failed. Unable to log in to Novell eDirectory." on page 82.

Possible Cause: The NAAS Server is unable to read the password file. The file might be missing.

Action: Load the ADSRVSET.NLM from the server console. The NLM is located in the SYS:\SYTEM or SYS:\AUDIT directory. This will create the password file.

Possible Cause: The NAAS Server is unable to read the password file. The file may be locked by some other process.

Action: Restart the NetWare server hosting the NAAS Server. This will release all file locks.

7337

Problem: “Service initialization failed. Unable to read the event policy.” on page 91.

Possible Cause: The naasEventPolicy object for the audited service has not been created in eDirectory or the agent does not have appropriate rights to read the policy object.

Action: For NAAS Shims, run the default configuration utility with the Configure NAAS Framework option. For other audited services, create the appropriate naasEventPolicy object and grant the agent appropriate rights.

7338

Problem: “Agent start up failed. Unable to read the agent policy” on page 90.

Possible Cause: The attributes of the associated naasAgentPolicy contain invalid values.

Action: Modify the existing naasAgentPolicy object with attribute values.

Problem: “Service initialization failed. Unable to read the event policy.” on page 91.

Possible Cause: The naasEventPolicy object for the audited service is corrupted with some attribute having out of range values.

Action: Modify the naasEventPolicy object with appropriate attribute values.

Problem: “Unable to read the data policy.” on page 91.

Possible Cause: The IP address or the DNS name entered for a naasSourceMachinePolicy or a naasTargetMachinePolicy is invalid.

Action: Modify the policy to enter a valid IP address or host DNS name.

Possible Cause: NETDB.NLM is not loaded on the server.

Action: Load NETDB.NLM from the server console.

Possible Cause: The naasActionFlag attribute for the policy is out of range.

Action: Modify the policy to enter appropriate values for the naasActionFlag attribute.

Problem: “Unable to read the search policy.” on page 91.

Possible Cause: An attribute in the policy has out of range value.

Action: Modify the policy to provide proper attribute values.

7400

Problem: “Failed to raise real time alert.” on page 91.

Possible Cause: There was some problem in the initialization of the NAAS agent.

Action: The NAAS Agent should recover to raise the alerts. Restart the server if the problem persists.

Problem: “Unable to commit the cache file. The file is corrupted and will be deleted” on page 92.

Possible Cause: The audit records in the cache file got mixed up.

Action: The agent should recover by the next commit period.

7401

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: There was an error accessing the cache files. Some other application may have locked the file.

Action: The agent should recover by the next commit period. Restart the server if the problem persists.

7402

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: The NAAS server is down.

Action: Bring up the NAAS server.

Possible Cause: There is an error accessing the socket connection to the NAAS server.

Action: The agent should recover by the next commit period. Restart the server if the problem persists.

7403

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: The naasKMO attribute is not set for the NAAS server.

Action: Check if the attribute is set for the server and set it with a proper value.

Possible Cause: The NAAS agent does not have rights to read the naasKMO attribute for the NAAS server.

Action: Grant the NAAS agent object appropriate rights.

Possible Cause: There was a problem initializing the SSL connection.

Action: Restart the server if the problem persists.

7404

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: All the NAAS servers are down.

Action: Bring up the NAAS servers.

Possible Cause: The network connectivity between the NAAS agent and server is lost.

Action: Check the network connectivity and take the action required to continue.

7405

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: There was an internal error.

Action: Restart the NAAS agent.

7406

Problem: “Unable to commit audit data.” on page 92.

Possible Cause: There was an internal error.

Action: Restart the NAAS agent.

7502

Problem: “Authentication to the Audit Server failed.” on page 93.

Possible Cause: User does not have Auditor rights and therefore is not a valid Auditor.

Action: Ensure that the user is configured as an Auditor. Check whether the Auditor has the Read right for NAASKMO and naasTrail attributes on the NAAS Server object. Assign the right and restart ConsoleOne and try again.

7503

Problem: “There was an error generating the report.” on page 93.

Problem: “There was an error getting filter list from the database.” on page 92.

Problem: “There was an error in displaying the query results.” on page 93.

Possible Cause: Unable to establish a secure channel of communication with the NAAS server.:

Action: Ensure that NAAS Server is up. Restart ConsoleOne and try again.

7504

Problem: “There was an error generating the report.” on page 93

Problem: “There was an error getting filter list from the database.” on page 92

Problem: “There was an error in displaying the query results.” on page 93

Possible Cause: Unable to read the NAAS Server certificate from the eDirectory for authenticating the NAAS Server.

Action: Ensure that the NAAS Server is up, restart ConsoleOne then, try again.

Action: Check whether the Auditor is assigned with the read rights for the NAASKMO and NAAS trail on the NAAS Server. Assign the rights if not assigned, restart the ConsoleOne then, try again.

7505

Problem: “There was an error generating the report.” on page 93.

Problem: “There was an error getting filter list from the database.” on page 92.

Problem: “There was an error in displaying the query results.” on page 93.

Possible Cause: NAAS server may be down or NAAS server disconnected the utility connection due to some communication problem.

Action: Ensure that the NAAS Server is up. Restart ConsoleOne and try again.

7508

Problem: “There was an error generating the report.” on page 93.

Problem: “There was an error getting filter list from the database.” on page 92.

Problem: “There was an error in displaying the query results.” on page 93.

Possible Cause: eDirectory has returned an error in the process of establishing a communication with NAAS Server.

Action: Ensure that the NAAS Server is up. Restart ConsoleOne and try again.

NOTE: For eDirectory error codes, Novell eDirectory Error Code Documentation (http://www.novell.com/documentation)

7510

Problem: “There was an error generating the report.” on page 93

Problem: “There was an error getting filter list from the database.” on page 92

Problem: “There was an error in displaying the query results.” on page 93

Possible Cause: Unable to read the NAAS Server parameters.

Action: For ConsoleOne: Check whether the Auditor is assigned with the read rights for the naasPortNumber, HostDevice, NAASKMO and naasTrail on the NAAS Server. Assign the rights if not assigned, restart the ConsoleOne and then try again.

7511

Problem: “There was an error generating the report.” on page 93

Problem: “There was an error getting filter list from the database.” on page 92

Problem: “There was an error in displaying the query results.” on page 93

Possible Cause: eDirectory has returned error while authenticating the auditor.

Possible Cause: Incorrect username and password.

Action: Re-enter the correct username and password and try again.

7512

Problem: “There was an error generating the report.” on page 93

Problem: “There was an error getting filter list from the database.” on page 92

Problem: “There was an error in displaying the query results.” on page 93

Possible Cause: Internal error.

Action: Restart the NAAS Server and client and try again.

7600

Problem: “Configuration Error” on page 84.

Possible Cause: JCRYPTOR.DLL was not successfully loaded.

Action: Ensure that the required library is placed in the appropriate path, CONSOLEONEHOME\1.2\BIN. Also ensure that NICI 2.*x* is installed.

Miscellaneous Error Codes

File system error

Problem: “Unable to write to the cache file.” on page 91.

Action: Refer file system error code description for more information.

BSD socket error codes

Problem: “Failed to raise real time alert.” on page 91.

Action: Refer the BSD socket error code documentation.

-601 or -610

Source: eDirectory

Problem: “Unable to Log in to NDS” on page 82.

Possible Cause: Unable to find the specified object in eDirectory. The NAAS server object specified in the server configuration file might be incorrect.

Action: Run SYS:\AUDIT\ADSRVSET.NLM to re-enter the NAAS Server object name in the configuration file, or manually enter the correct NAAS Server object name in the file and then restart the NAAS server.

The server configuration file is located at SYS:_NETWARE\SRCONFIG.CFG.

Problem: “Unable to read the data policy.” on page 91.

Possible Cause: The user name entered in a naasUserPolicy is not a valid eDirectory user name.

Action: Modify the policy to enter valid user names.

-602 or -603

Problem: "Agent start up failed. Unable to log in to Novell eDirectory." on page 90.

Possible Cause: The eDirectory replicas are not synchronized.

Action: Check the replica synchronization. If required, force synchronization and restart the agent by entering **`st_agent`** at the server console.

For more details, refer the Novell eDirectory Error Code Documentation (http://www.novell.com/documentation).

Problem: "Agent start up failed. Unable to read the agent policy" on page 90.

Possible Cause: The naasAgent object for this server does not have sufficient rights to read the policy object.

Action: If the Agent was created using NAAS default configuration utility, reconfigure the system by completing the steps in "Configuring NAAS Framework" on page 24. If the naasAgent object for the server is created manually, grant the object appropriate rights.

Possible Cause: The Agent Policy object is corrupted with some mandatory attributes missing.

Action: Modify the existing naasAgentPolicy object to add the mandatory attributes.

Problem: "Service initialization failed. Unable to read the event policy." on page 91.

Possible Cause: The naasAgent object for this server does not have the required rights to read the Policy object.

Action: If the Agent was created using NAAS default configuration utility, reconfigure the system by using the Configure NAAS Framework option in the default configuration utility. If the naasAgent object for the server or the naasEventPolicy objects was created manually, grant the object appropriate rights.

Possible Cause: The naasEventPolicy object is corrupted and some mandatory attributes are missing.

Action: Modify the existing naasEventPolicy object to add the mandatory attributes.

Problem: "Unable to read the search policy." on page 91.

Possible Cause: A mandatory attribute is missing in the naasSearchCriteriaPolicy, or the naasAgent object does not have rights to the attributes.

Action: Modify the policy to add all the mandatory attributes and grant the naasAgent object appropriate rights.

-634

Source: eDirectory

Problem: “Unable to Log in to NDS” on page 82.

Possible Cause: Unable to find the specified tree name in eDirectory. The tree name, which is present in SRCONFIG.CFG, might be corrupted.

Action: Run SYS:\AUDIT\ADSRVSET.NLM to re-enter the tree name in the configuration file, or manually enter the correct tree name in the file and then restart the NAAS server.

The Server Configuration file is located at SYS:\NETWARE\SRCONFIG.CFG.

- 663

Source: eDirectory

Problem: “Unable to Log in to NDS” on page 82.

Possible Cause: Unable to access eDirectory because it might be locked.

Action: Load eDirectory by loading DS.NLM.

-1416 / -669

Source: eDirectory

Problem: “Unable to Log in to NDS” on page 82.

Possible Cause: Invalid user name or password provided by NAAS server while logging to eDirectory.

Action: Run SYS:\AUDIT\ADSRVSET.NLM and then restart the NAAS server.

-669

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

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.
Problem:	“Agent start up failed. Unable to log in to Novell eDirectory.” on page 90.
Possible Cause:	The password file is corrupted and contains the wrong password.
Action:	Load the ADAGTSET.NLM from the server console. The NLM is located in SYS:\SYTEM or SYS:\AUDIT directory. This will create the password file.