Novell Nsure™ Audit

1.0.3

www.novell.com

INSTALLATION GUIDE

February 25, 2005

Novell®

Legal Notices

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

www.novell.com

Novell Nsure Audit Installation Guide
February 25, 2005

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

Novell Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.
SUSE is a registered trademark of SUSE AG, a Novell business.

Third-Party Materials

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

Contents

1 Overview

This section provides an overview of the Novell® Nsure™ Audit Report auditing system and reviews auditing fundamentals.

Product Overview

Novell Nsure Audit is a centralized, cross-platform auditing service. It collects event data from multiple applications across multiple platforms and writes the data to a single, non-repudiable data store. Nsure Audit is also capable of creating filtered data stores. Based on criteria you define, Nsure Audit captures specific types of events and writes those events to secondary data stores.

After you have collected the data, the next challenge is making sense of it. Using the query and report generating tools included with Nsure Audit Report, you can evaluate the information in your data stores to determine resource access, usage patterns, and overall compliance with organizational policies and regulations.

Although queries and reports are invaluable in reviewing system activity, sometimes you need to know what is happening on your system as it happens. Therefore, Nsure Audit provides real-time notifications and real-time monitoring so you can assess and act on events as they occur.

To some extent, Nsure Audit can even automate the process of responding to events in real time. The Critical Value Reset (CVR) channel allows you to flag Directory attributes with reset policies. If the value of a given attribute is changed, the CVR channel resets the value as per the policy defined in the CVR Channel object. For example, if your organization has a policy prohibiting security equivalence, you can create a CVR Channel object that automatically resets the Security Equals attribute to a null value if it is ever reset by an administrator.

We understand that security standards are becoming increasingly rigorous. In order to manage liability and protect assets, organizations need to be able to provide a record of all their electronic proceedings and to identify when business policies are being violated. With real-time monitoring, notifications, and historical reporting capabilities, Novell Nsure Audit can give you the facts you need to make informed decisions and ensure the safety of your most valuable corporate asset—its information.

Auditing Background and Fundamentals

Novell Nsure Audit provides the tools you need to audit your organization's compliance with internal and external policies and regulations; however, the use of secure logging technology such as Novell Nsure Audit does not, in itself, provide a complete auditing solution. Auditing is actually a human-driven process and Novell Nsure Audit is simply a tool to facilitate that process.

Therefore, a complete auditing strategy requires that you:

1. Define your organization's security and usage policies. That is, determine what resources your users are allowed to access, what rights they have to those resources, and so forth.
2. Log the events relevant to those policies.
3. Configure Notification Filters to notify you in real time when a policy violation occurs. You can also use Notification Filters to route the events to the Critical Value Reset (CVR) channel to trigger an automated response to the violation.
4. Perform regular compliance audits. This entails querying the data store for events relevant to your policies and then manually reviewing those events to determine if there are any violations of your corporate policies, when the violations occurred, and who was responsible.

After you have implemented your auditing strategy, Novell Nsure Audit provides the information you need to assess overall compliance with organizational policies and to respond to policy violations in a timely manner.

For example, in a secure environment, you might have a policy that prohibits assigning user rights using the Security Equals attribute because it makes it difficult to track and manage user rights. To audit this policy, you first configure Novell Nsure Audit to log the Change Security Equals event.

To facilitate a timely response to policy violations, you configure a Notification Filter to send a message to your mailbox any time the Change Security Equals event occurs. You also have the Notification Filter route the event to the CVR channel, which is configured to automatically reset the Security Equals attribute on User objects to a null value.

You can monitor your organization's compliance with this policy by using iManager or Nsure Audit Report to query the data store for Change Security Equals events. You then review the query results to determine when violations occurred and who was responsible.

2 System Architecture

As a system administrator, you need a clear understanding of Novell® Nsure™ Audit architecture and functionality so you can better design, configure, and maintain your auditing system. This section provides a basic explanation of the components that make up Novell Nsure Audit.

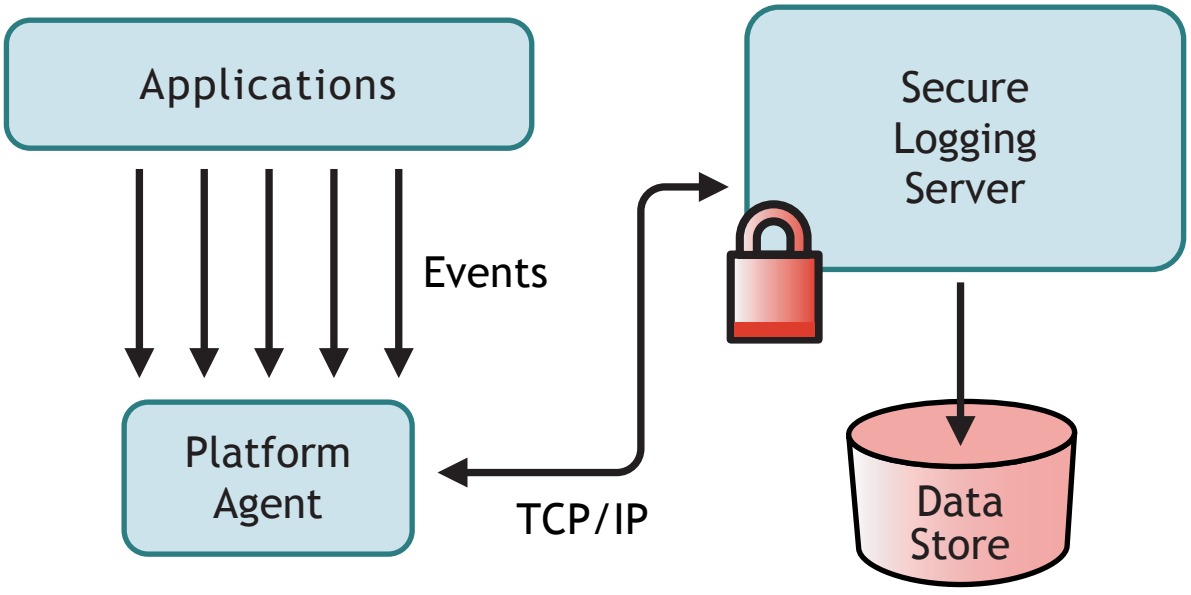
Nsure Audit System Components

Novell Nsure Audit has a highly modular architecture. Product functions are strategically divided among several different components to protect data integrity, optimize system performance, and provide maximum flexibility. Depending on usage and system resources, these components can be located on a single server or distributed across multiple servers.

The full auditing system consists of the following components:

- Platform Agent
- Secure Logging Server
- Data Store
- Reporting Applications

The Platform Agent, Secure Logging Server, and data store are the central components in this structure. To log events from system applications to the data store, Novell Nsure Audit uses a client/server model. The Platform Agent, as the client piece, receives all log data from the system applications. It securely transmits this data to the Secure Logging Server, which then writes the information to the data store.



Separating the Platform Agent from the actual logging function provides the following advantages:

- You can run Platform Agents on multiple servers throughout the network while still maintaining a single data store.
- Applications are not slowed down trying to commit an event to disk. Applications simply relay their log events to the Platform Agent, which then transmits the information the Logging Service. The Secure Logging Server assumes the full load of writing events to disk.
- You can off-load the system's logging overhead by running the Secure Logging Server on a dedicated server.

The remaining Nsure Audit component includes two reporting applications: iManager and Nsure Audit Report. These supplementary tools allow you, as the administrator, to tap vital data from the system.

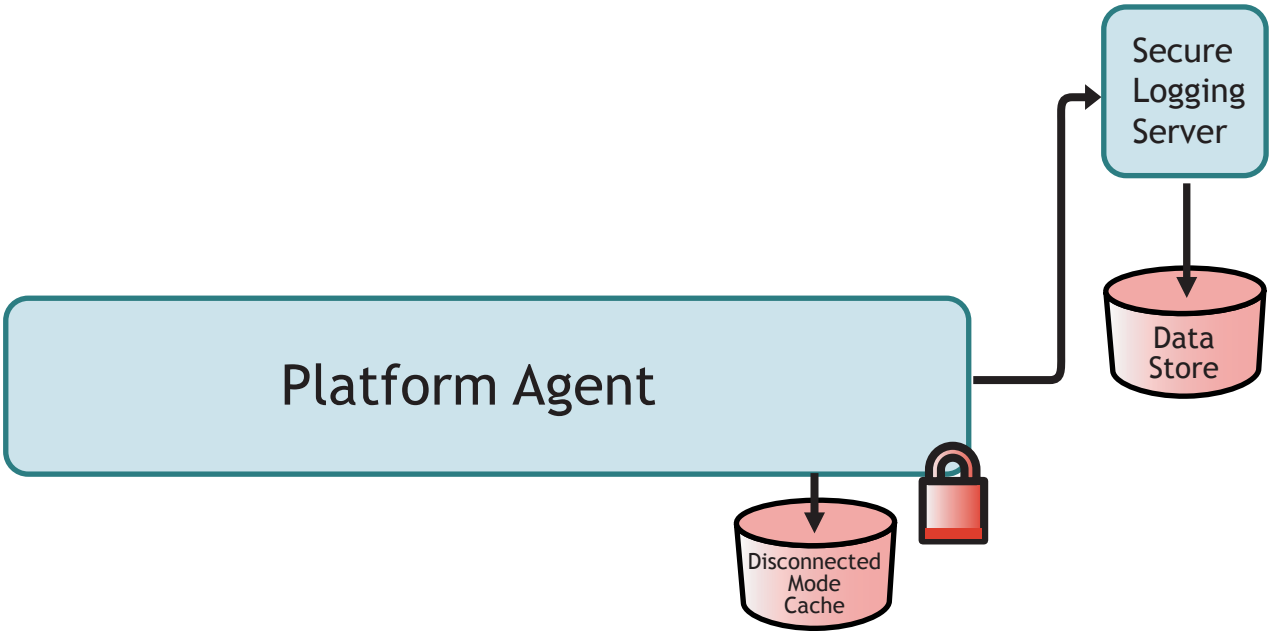
The following sections provide a discussion of each component in the Nsure Audit architecture.

- "Platform Agent" on page 10
- "Secure Logging Server" on page 14
- "Data Store" on page 19
- "Reporting Applications" on page 20

Platform Agent

The Platform Agent (logevent) is the client portion of the Nsure auditing system. The Platform Agent receives logging information and system requests from authenticated applications and transmits the information to the Secure Logging Server.

If the connection between the Platform Agent and the Secure Logging Server fails, applications continue to log events to the local Platform Agent, just as they always do. The Platform Agent simply switches into Disconnected Cache Mode and the Cache Module writes all logged events to the local cache until the connection is restored. The switch into Disconnected Cache Mode is completely transparent to the logging applications.

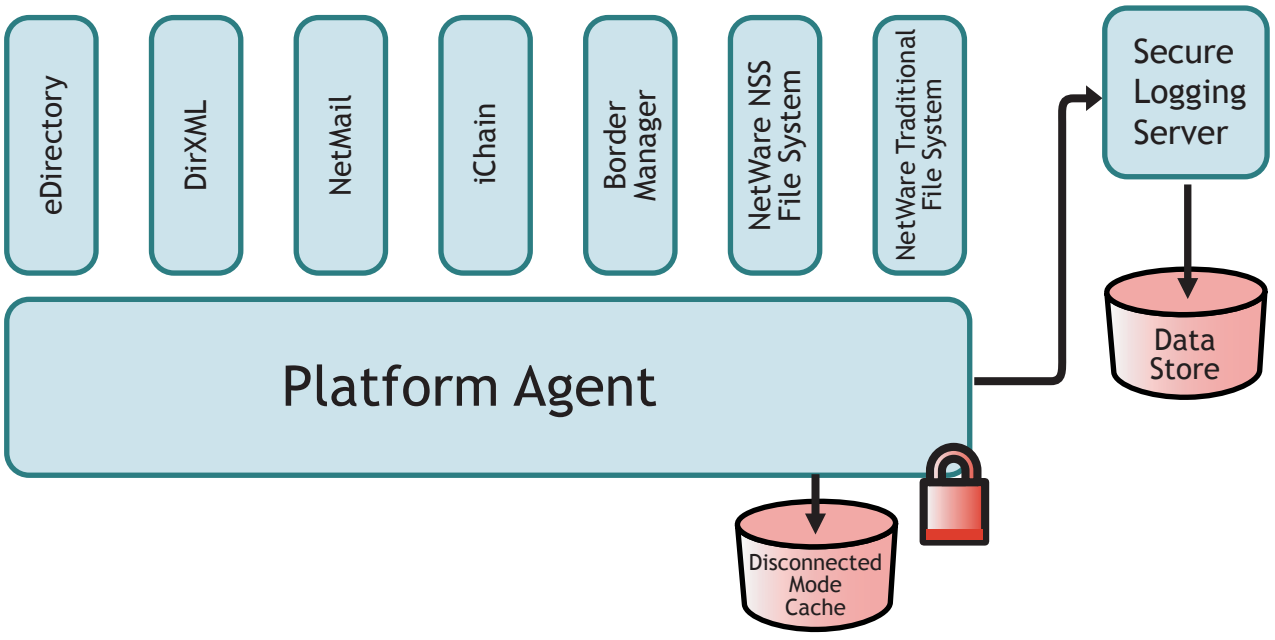


Supported Applications

Currently, the Platform Agent can receive log events from the following:

- Novell eDirectory™ 6.0 and higher
- Nsure™ Identity Manager 2.0
- NetMail™ 3.5 and higher
- iChain® 2.2 SP1
- BorderManager® 3.8
- NetWare® NSS File System
- NetWare Traditional File System

NOTE: Before an application can log events to Novell Nsure Audit, it must be able to authenticate with the system and report events in the auditing system's required format. For more information on the authentication process, see "Authenticating Logging Applications". For more information on event structure, see "Event Structure".

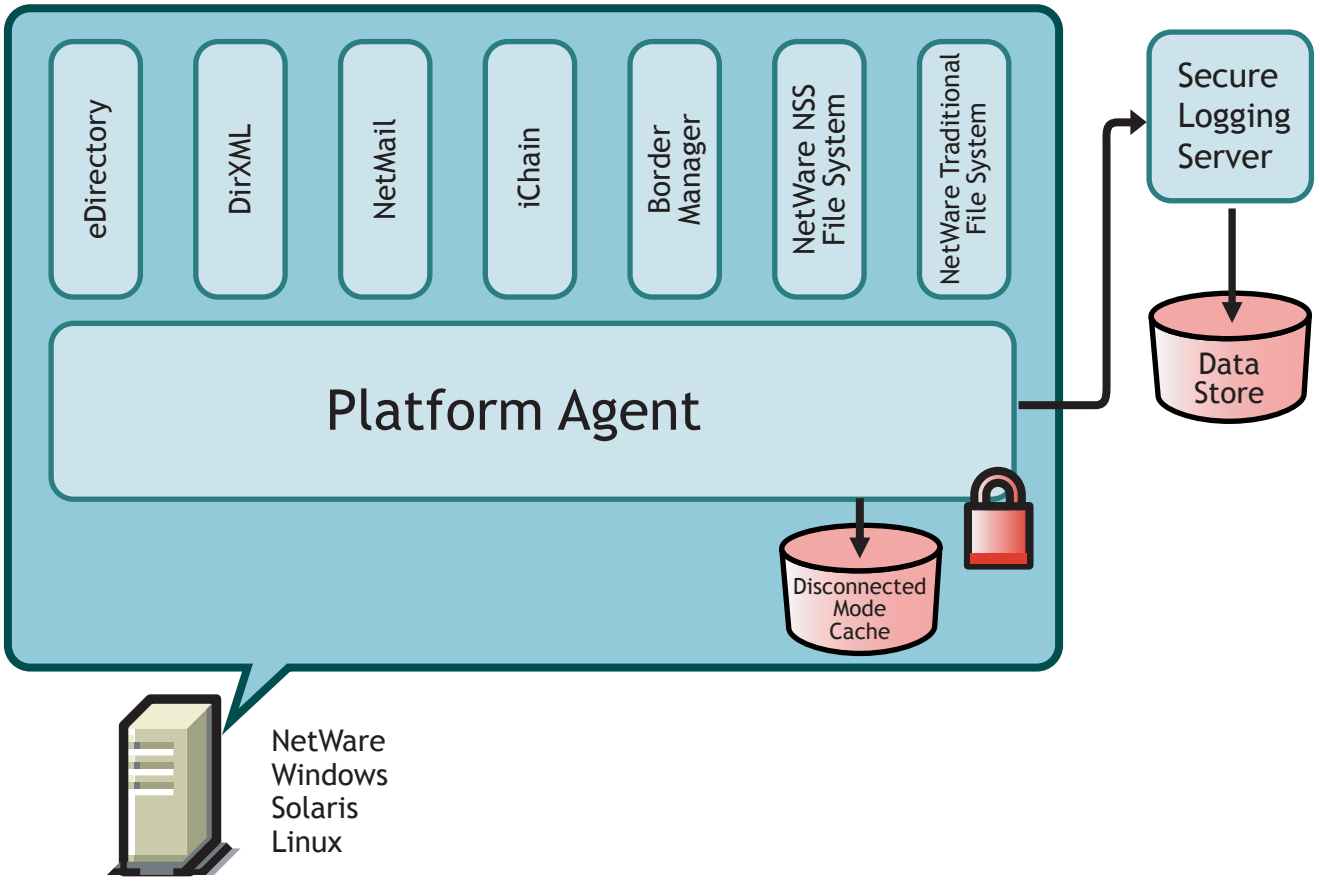


Supported Platforms

The Nsure Audit architecture requires that the Platform Agent be locally installed on every server or workstation running applications that log events to Nsure Audit.

This design ensures secure, uninterrupted logging because the logging applications are insulated from external communication failures. The Platform Agent is supported on the following platforms:

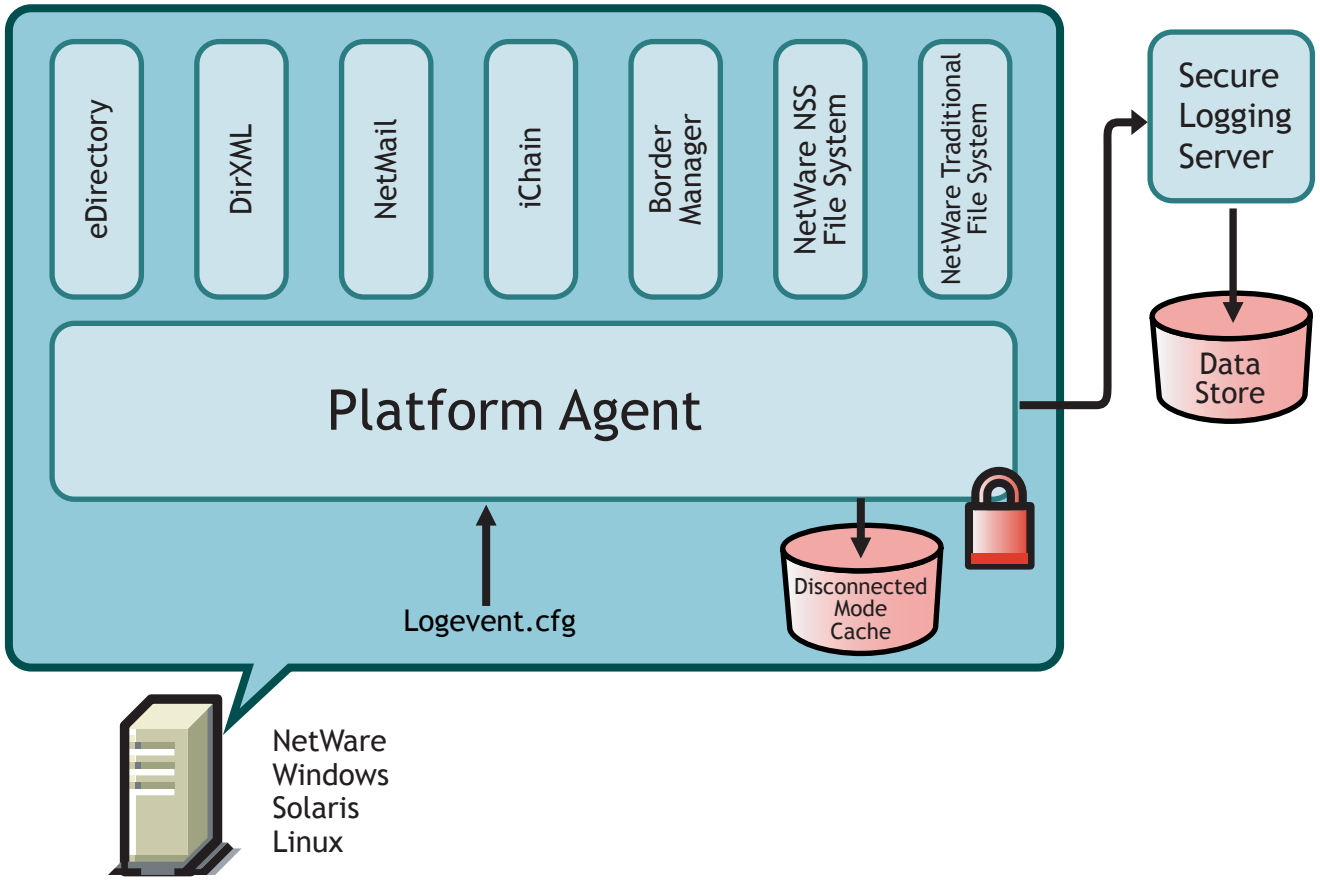
- NetWare 4.2 or later
- Windows* NT, Windows 2000 and Windows 2000 Server, Window XP, Windows 2003 Server.
- SUSE® Linux* Enterprise Server 8
- Solaris 8 and 9
- RedHat* Linux 7.3, 8, AS, and ES 2.1



Platform Agent Configuration

The Platform Agent is not configured through eDirectory. Instead, the Platform Agent's configuration settings are stored in a simple, text-based configuration file (logevent). This makes the Platform Agent small, unobtrusive, and self-contained—that is, it has no external dependencies so it is always available to receive logged events. Storing the Platform Agent's configuration in a text-based file also allows the Platform Agent to eventually run on platforms that do not have eDirectory support.

The logevent file stores the host name or IP address of the logging server, the Disconnected Mode Cache directory, port assignments, and other related information. For more information on Platform Agent configuration settings, including a sample logevent file, see "Logevent".



Secure Logging Server

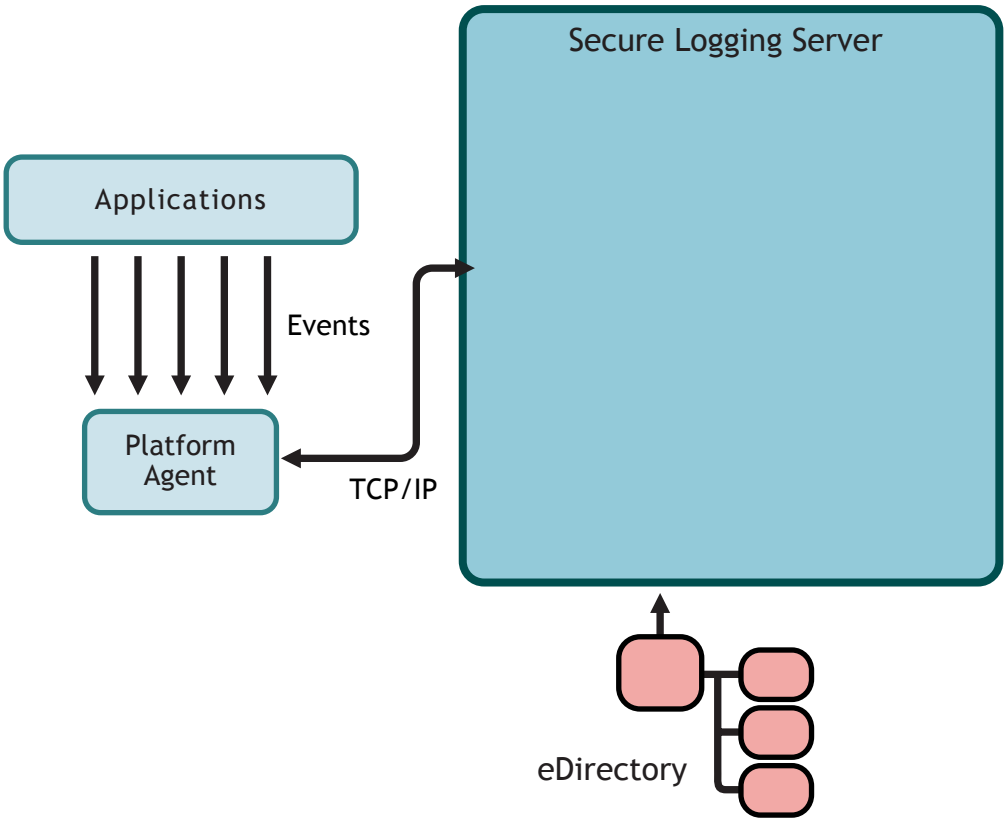
The Secure Logging Server (lengine) is the server component in the Nsure auditing system.The Secure Logging Server manages the flow of information to and from the Nsure auditing system—that is, it receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. It can also be configured to automatically reset critical system attributes according to a specified policy.

The Secure Logging Server supports the following platforms:

- NetWare 6.5
- NetWare 6.0 SP3 or later
- NetWare® 5.1 SP6 or later
- Windows 2003 Server
- Windows 2000 Server SP4 or later
- Solaris 8 and 9
- SUSE Linux Enterprise Server 8
- Red Hat Linux AS and ES 2.1

The Secure Logging Server is configured through eDirectory. The Logging Server object contains all the configuration settings for the Secure Logging Server. Consequently, the logging server must have access to eDirectory and the Logging Server object before it can launch the Secure Logging Server. For more information, see “Configuring the Logging System”.

NOTE: To minimize server reaction time and ensure high system performance, you should create a local replica of the Logging Server object and its associated objects on the logging server.



The Secure Logging Server provides the following services:

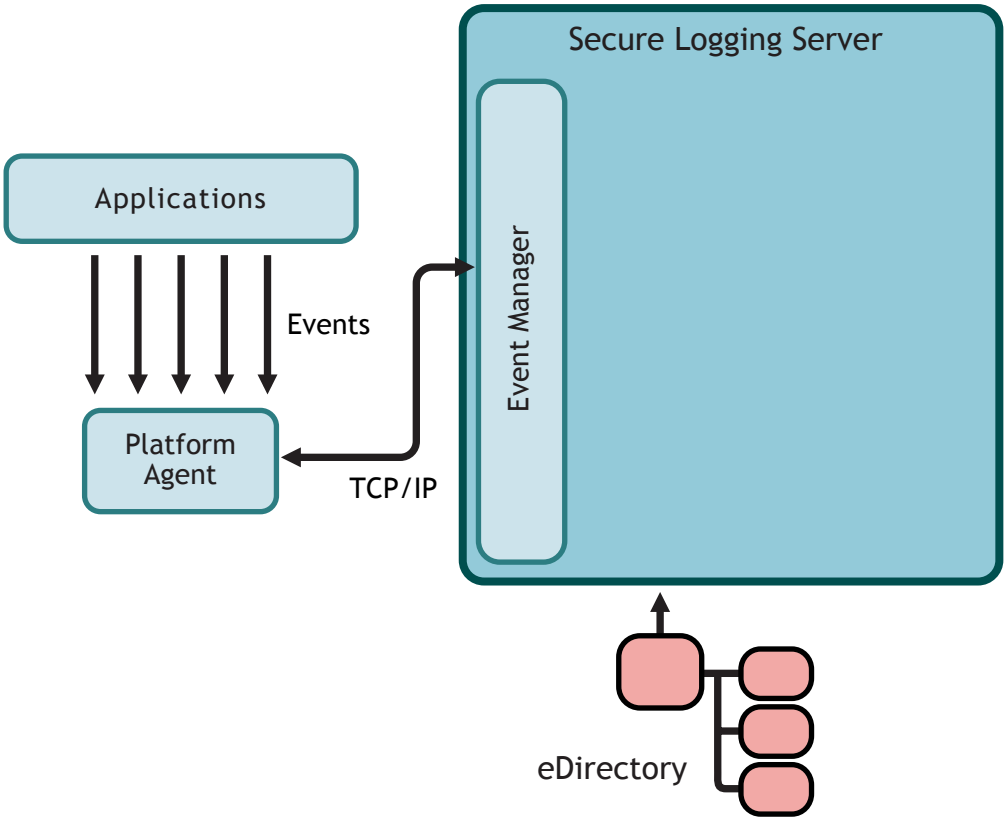
- Event Management
- Logging and Notification Channels
- Logging Service
- Notification Service

A description of each service follows.

Event Management

The Event Manager receives all incoming data from the Platform Agents and directs the information to the appropriate service. It also routes outgoing information from the logging server to the appropriate Platform Agent.

This mode of operation is very efficient. Indeed, the Event Manager service is designed to maximize system efficiency and performance. Depending on the Secure Logging Server's cache settings, the Event Manager can handle more than 60,000 events per second. For information on configuring the Secure Logging Server's cache, see "Logging Server Objects ".



Logging and Notification Channels

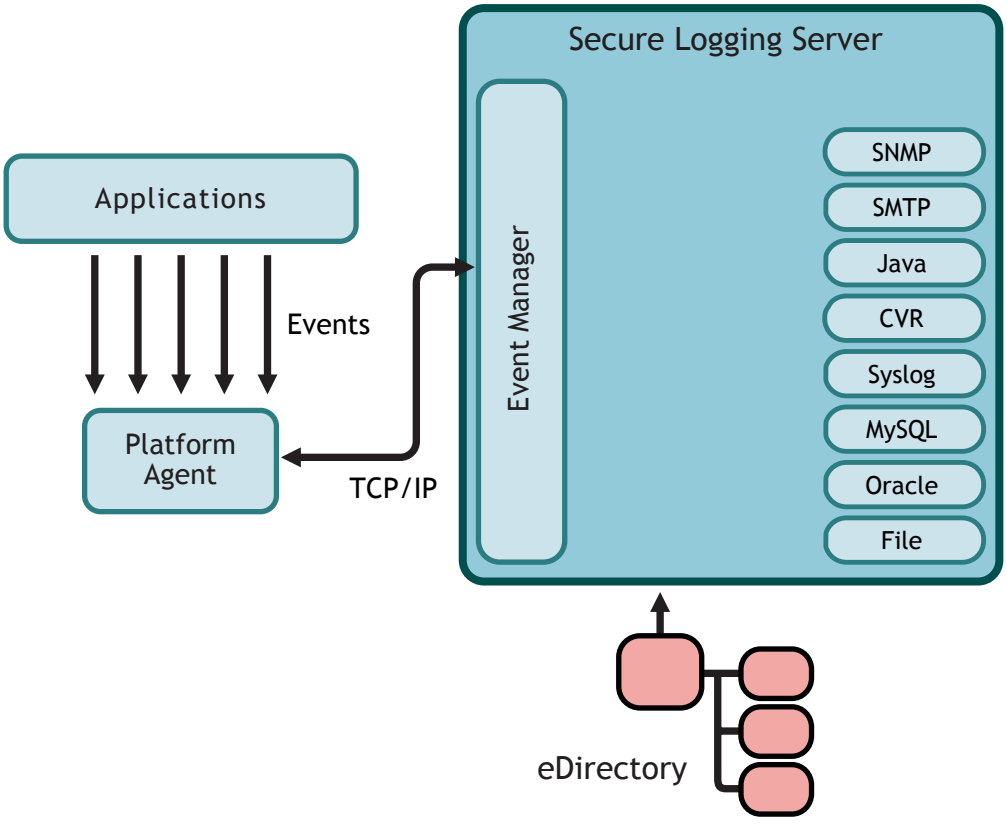
The Secure Logging Server uses channels to log events and provide event notification. For example, to e-mail events, the logging server uses the SMTP channel; to log events to an Oracle* database, the logging server uses the Oracle channel; and so forth.

Nsure Audit currently supports the following channels:

SMTP	Oracle (Available on NetWare using the Java JDBC channel driver.)
SNMP	File
Java	Syslog
MySQL	CVR (Critical Value Reset)
JDBC	Microsoft* SQL Server

Third-party channels can be easily incorporated into this structure. For more information, see the Novell Nsure Audit SDK (http://developer.novell.com/ndk/naudit.htm).

Channels are configured in eDirectory using Channel objects. Each Channel object stores the information the logging server needs to use its associated channel. For further information, see “Channel Objects” on page 23.

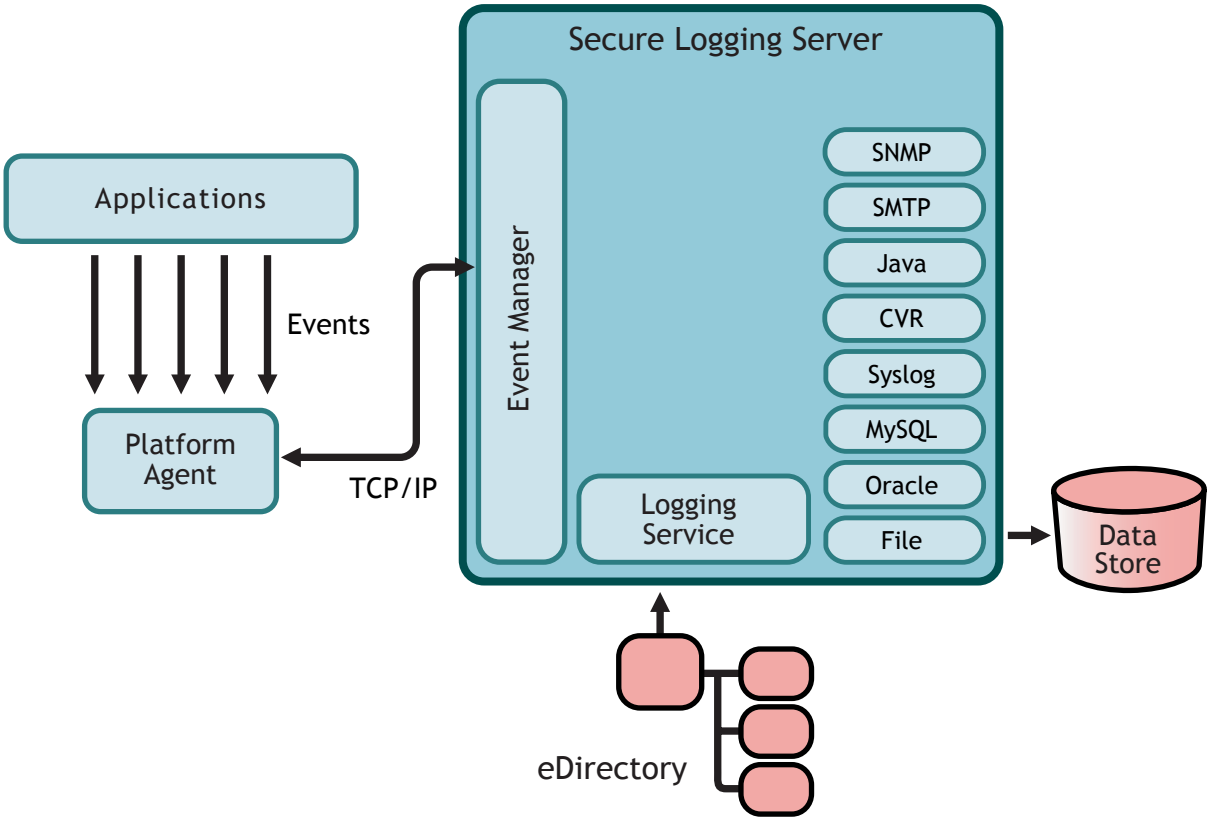


Logging Service

The Logging Service is the only Nsure Audit component that can write to the data store. This design protects log data from unauthorized record modification, insertion, or deletion.

To ensure that the auditing system maintains accurate records, the Event Manager delivers all incoming data directly to the Logging Service. All events and requests must be recorded in the data store before the Event Manager sends them to the Monitoring or Notification services.

Write times vary per storage option. On a P4 Xeon class server, the Logging Service can write approximately 60,000 events per second to a flat file in a file system or 3,000 events per second to a MySQL* database.



Using the logging server's channels, the Logging Service can write events to the following storage devices:

- Flat file in the file system
- MySQL database
- Oracle database
- Syslog database
- Microsoft* SQL Server database

NOTE: Although you can use any channel to log events, for performance reasons we recommend that you only log to the Syslog, MySQL, Oracle, Microsoft SQL Server, or File channels.

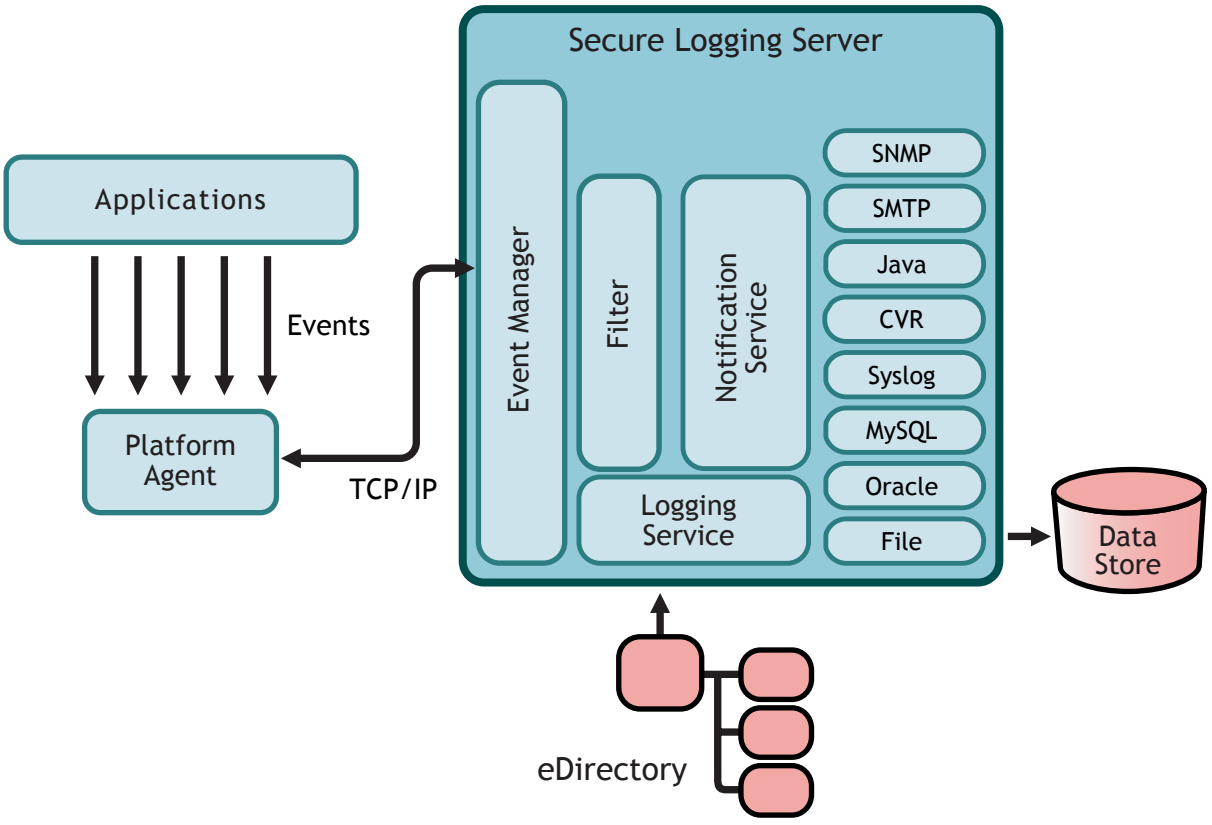
For more information on configuring these channels, see "Configuring System Channels".

Notification Service

The Notification Service provides two kinds of notification: filtered and heartbeat. Filtered notification tells you when a specific event has occured; heartbeat notification tells you when an event has not occured.

In both cases, the Notification Service identifies the event and routes it to specific channels. For example, the Notification Service can send a notification event to a system administrator's mailbox or cell phone using the SMTP channel, route the event to the network management system as an SNMP trap, or write the event to a flat file in the file system or to a Syslog, MySQL, Oracle, or SQL Server database.

Both filtered and heartbeat notifications are configured in eDirectory using Notification Filter and Heartbeat objects. These objects define event criteria and designate which Channel objects are used to provide event notification. For more information, see “Notification Objects” on page 24.



Data Store

Using its available channel drivers, Nsure Audit can log events to the following storage devices:

- Flat file in the file system
- MySQL database
- Oracle database
- Microsoft SQL Server database
- Syslog database

Nsure Audit protects log data from record modification, insertion, or deletion by allowing only one program component, the Logging Service, to write events to the data store. Nsure Audit also limits read access to log data by controlling which applications can request log information through the auditing system. However, the security of the data store itself is up to you and the security mechanisms provided by the database. Although Nsure Audit maintains an internal security perimeter around the data store, it is possible for individuals or applications to directly access the data store outside the boundaries of the auditing system. Therefore, file system rights, directory rights, and the database’s internal security features must be carefully configured to secure your log data.

For further information, see “Configuring the Data Store ”.

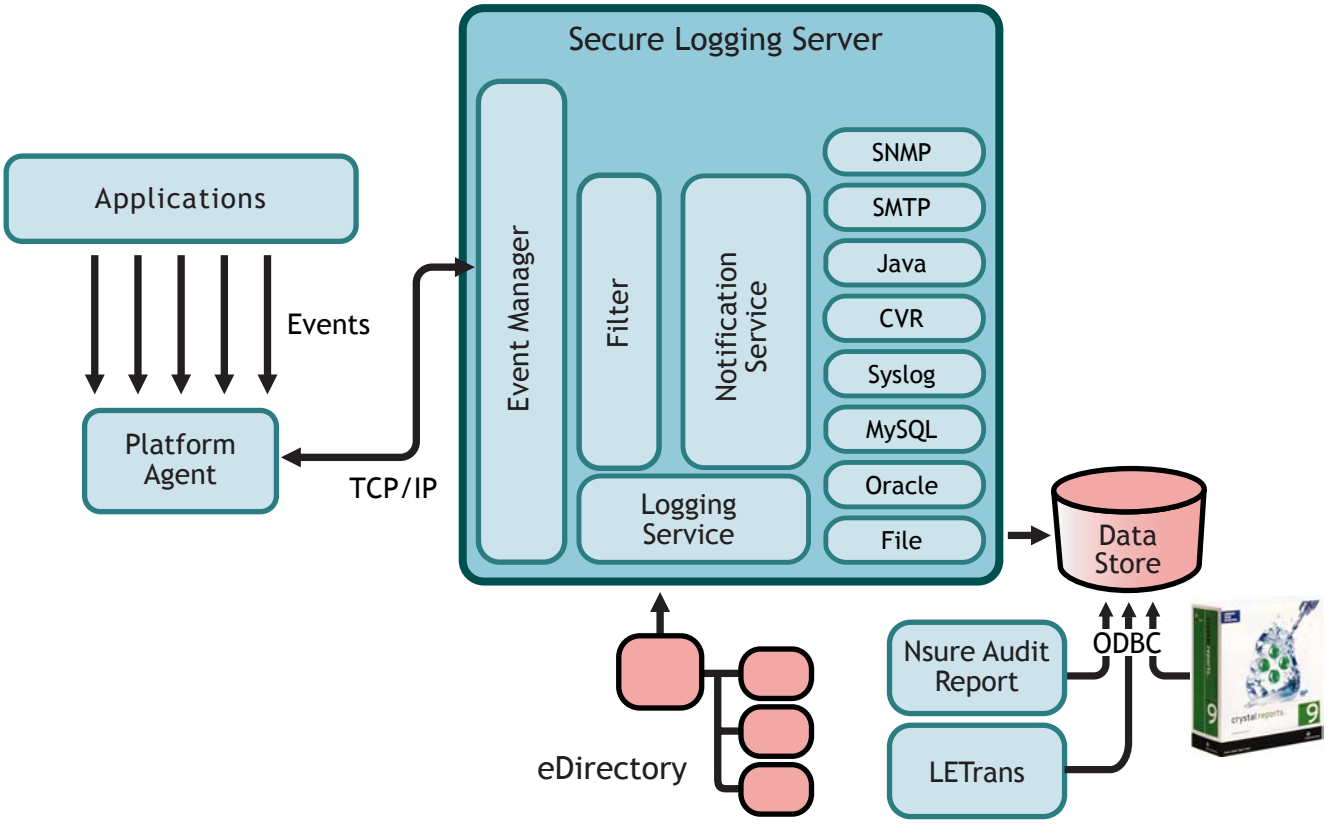
Reporting Applications

Nsure Audit provides two tools that can be used to generate reports from MySQL, Microsoft SQL Server, and Oracle data stores.

NOTE: Any standardized syslog reporting tool can be used to generate reports from syslog data stores.

- Nsure Audit Report is a Windows-based, ODBC-compliant application that can generate reports from Oracle and MySQL data stores. It includes predefined reports and can be integrated with Crystal Reports* to provide full custom reporting capabilities.
- iManager is a browser-based, JDBC*-compliant application that can generate reports from MySQL data stores.

For more information on generating reports with these tools, see "Generating Queries and Reports". Any standardized syslog reporting tool can be used to generate reports from syslog data stores.



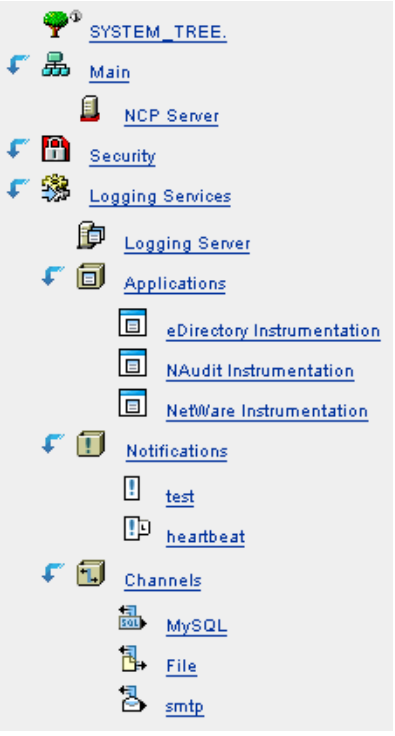
Configuration Objects

When you install the Secure Logging Server, the installation program extends the eDirectory schema to include the following objects:

- Logging Services Container (page 21)
- Logging Server Object (page 21)
- Nsure Audit Attributes on the NCP Server Object (page 22)
- Application Objects (page 22)

- Channel Objects (page 23)
- Notification Objects (page 24)

Nsure Audit uses these objects to store and look up system configuration parameters.



IMPORTANT: The Platform Agent is not configured through eDirectory. Instead, the Platform Agent's configuration settings are stored in a simple, text-based configuration file (logevent). For more information, see "Logevent".

Logging Services Container

During your initial installation, Nsure Audit extends the eDirectory schema and creates the Logging Services container at the root of your directory tree. Because it is part of Nsure Audit, there can only be one Logging Services container per tree and, as the logging system container, it only contains Nsure Audit component objects.

Locating all logging system components in the Logging Services container is ideal for organizations that need a simple, easy-to-manage logging system. It also suits organizations that are implementing Nsure Audit as an auditing solution and, for security reasons, want to centrally manage their system. To facilitate distributed administration, however, Nsure Audit components can also be created and managed outside the Logging Services container.

If the Logging Services container is deleted, it can only be re-created by re-running AuditExt. For more information, see "AuditExt".

Logging Server Object

In eDirectory, the Logging Server object represents the physical server where you installed the Secure Logging Server. However, because the Logging Server object is specific to Nsure Audit, it does not replace the NCP Server object. Instead, each Logging Server object is associated with an NCP Server object.

The Logging Server object is represented as a container with server attributes; it can contain Nsure Audit objects and it stores all the properties and attributes for the Secure Logging Server. For information on creating and configuring the Logging Server object, see "Configuring the Secure Logging Server".

Nsure Audit Attributes on the NCP Server Object

During installation, Nsure Audit extends the definition of the NCP Server object to include the log settings for eDirectory, NetWare, traditional file system, and NSS events. These settings are found under the NCP Server object's Nsure Audit tab.

The Nsure Audit screen has separate menus for NetWare, Filesystem, and eDirectory events. Each menu lists the events that fall in its respective category. To configure NetWare, Filesystem, or eDirectory instrumentation to log a particular type of event, simply mark the event's check box and click Apply. The instrumentation automatically begins logging the marked events to the Secure Logging Server.

NOTE: You do not need to restart the logging server to effect changes to NSure Audit attributes in the NCP Server object.

For more information on configuring the NCP Server object's Nsure Audit attributes, see "Logging eDirectory, NetWare, and File System Events".

Application Objects

Application objects are associated with applications that log to or request information from Nsure Audit. These objects store the information required by the logging server to authenticate logging applications. They also identify which users have rights to monitor the applications' events and they store the applications' log schemas.

NOTE: The log schema catalogs the events that can be logged for a given application. For more information, see "Log Schema Files".

Application objects are usually created automatically when either Nsure Audit or the logging application is installed. If necessary, they can also be manually added to the tree using iManager.

During installation, Novell Nsure Audit automatically creates Application objects for itself (the Naudit Instrumentation), the eDirectory Instrumentation, and the NetWare Instrumentation.The Naudit Instrumentation allows Nsure Audit to audit its own events such as creating Channel or Notification objects. The eDirectory Instrumentation manages logging of eDirectory events and the NetWare Instrumentation provides logging for NetWare and file system events.

NOTE: The NetWare Instrumentation is only installed on NetWare versions.

Application objects can be created only within Application containers. Novell Nsure Audit creates the Application objects for the Naudit, eDirectory, and NetWare Instrumentations in the Application container under Logging Services.

For more information on creating and configuring Application objects, see "Managing Applications that Log to Nsure Audit".

Application Containers

Application containers provide a reference point through which the logging server can locate Application objects. At startup, the logging server scans its list of Application containers and loads the included Application object configurations in memory where it can quickly access the information when authenticating applications. For information on configuring the Application Container property on the logging server, see "Logging Server Objects ".

IMPORTANT: The logging server scans its list of Application containers only at startup. Therefore, if you create or modify an Application object, you must restart the logging server. For information on restarting the logging server, see "Secure Logging Server Startup Commands".

The Application container under Logging Services is automatically created during installation; however, additional Application containers can be created anywhere in the tree.

Channel Objects

Channel objects store the information the logging server needs to use channel drivers. For example, a MySQL Channel object contains the IP address or host name of the MySQL database server; a username and password for connecting to the server, the name of the database and table, and any other relevant information. An SMTP Channel object, on the other hand, includes the address of the SMTP server; a username and password; and the recipient, sender, subject, and body of the log message.

Nsure Audit is designed so you can create multiple Channel objects for any given channel. This means you can apply different channel configurations to different functions or events. For instance, you can configure the logging server to use one MySQL Channel object to add events to the central data store and configure a Notification Filter to use another MySQL Channel object to create a filtered log.

The available types of Channel objects are:

 SMTP

 SNMP

 Java

 MySQL

 JDBC

 Oracle (Only available on NetWare using the JDBC Java channel.)

 File

 Syslog

 CVR

 Microsoft SQL Server

Additional Channel objects can be easily incorporated in this model. For more information, see the Nsure Audit SDK (http://developer.novell.com/ndk/naudit.htm).

Of particular note is the Critical Value Reset (CVR) Channel object. In configuring a CVR Channel object, you can flag an attribute in eDirectory with a reset policy. If the value of that

specific attribute is changed, the CVR channel automatically resets the value as per the policy defined in the CVR Channel object.

The logging server looks for Channel objects only in Channel containers; therefore, Channel objects can only be created within Channel containers. For information on creating and configuring Channel objects, see “Configuring System Channels”.

Channel Containers

Channel containers provide a reference point through which the logging server can locate Channel objects. At startup, the logging server scans its list of Channel containers and loads the included Channel object configurations and their drivers. The drivers and Channel object configurations are then available to provide event notification and to log events. Note that the logging server only loads those drivers that have Channel objects in supported Channel containers. For information on configuring the Channel Container property on the logging server, see “Logging Server Objects ”.

IMPORTANT: The logging server scans its list of Channel containers only at startup. Therefore, if you create or modify a Channel object, you must restart the logging server. For information on restarting the logging server, see “Secure Logging Server Startup Commands”.

The Channel container under Logging Services is automatically created during installation; however, Channel containers can be created anywhere in the tree.

Notification Objects

Nsure Audit provides two kinds of event notification:

- Filtered Notification
- Heartbeat Notification

Filtered notification tells you when a specific event has occured; heartbeat notification tells you when an event has not occured. The following sections discuss the objects associated with each notification.

Notification Filter Objects

Notification Filter objects store the criteria the logging server uses to filter system events. They also designate which Channel objects the logging server uses to provide event notification.

When you define a Notification Filter, you specify a value for a given event field. To narrow the results, you can define values for multiple event fields. Using standard “and,” “or,” and “not” operators, you can define up to 15 event conditions. For more information on the event fields, see “Event Structure”.

After you define the filter criteria, you must select the object’s notification channel. Notification channels are simply the Channel objects the logging server uses to provide event notification. For example, if you want to e-mail filtered events to your mailbox, you must select an SMTP Channel object that is configured to relay events to your e-mail address. Similarly, if you want to log filtered events to a MySQL database, you must select a MySQL Channel object that is configured to write events to the correct database and table. You can define multiple notification channels for any given Notification Filter.

The logging server looks for Notification Filter objects only in Notification containers; therefore, Notification Filter objects can be created only within Notification containers. For information on creating and configuring Notification Filter objects, see “Configuring Filters and Event Notifications”.

Heartbeat Objects

Heartbeat objects define which Event IDs the logging server looks for and the interval at which those events must occur. If an event does not occur within the designated interval, the logging server generates a heartbeat event.

The heartbeat event is automatically logged to the central data store; however, if you want to receive notification that a specific event has not occurred, you must create a Notification Filter for the corresponding heartbeat event.

The logging server looks for Heartbeat objects only in Notification containers; therefore, Heartbeat objects can be created only within Notification containers. For information on creating and configuring Heartbeat objects, see “Configuring Filters and Event Notifications”.

Notification Containers

Notification containers provide a reference point through which the logging server can locate Notification objects. At startup, the logging server scans its list of Notification containers and loads the included Notification object configurations in memory where it can quickly access the information to filter or monitor events. For information on configuring the Notification Container property on the logging server, see “Logging Server Objects ”.

IMPORTANT: The logging server scans its list of Notification containers only at startup. Therefore, if you create or modify a Notification object, you must restart the logging server. For information on restarting the logging server, see “Secure Logging Server Startup Commands”.

The Notification container under Logging Services is automatically created during installation; however, Notification containers can be created anywhere in the tree.

3 Preparing for Installation

The remaining sections of this guide walk you through installing and configuring Nsure Audit.

Installing and configuring Nsure Audit is an eight-step process:

1. Meet the Nsure Audit prerequisites and requirements.
   - “Prerequisites and Requirements” on page 28
2. Configure MySQL* or another supported application as the event repository.
   - “Configuring an Event Repository” on page 31
3. Install or update the Secure Logging Server component of Nsure Audit on a single server in your tree.
   - “Upgrading Novell Nsure Audit” on page 35
   - “Installing Novell Nsure Audit” on page 39
4. Install or update the Nsure Audit iManager plug-in on your iManager server.
   - “Installing the Nsure Audit 1.0.3 iManager Plug-in” on page 49
5. Use the Nsure Audit iManager plug-in to create the Channel Driver object used by your Secure Logging Server to connect to the event repository you established in step 2. Additionally, you can set up additional channels or notifications at this time.
   - “Configuring the Secure Logging Server” on page 50
6. Install the Platform Agent component and instrumentation on each system on a supported platform that will report events, then configure the Platform Agent on each client to connect to your newly-established Secure Logging Server.
   - “Installing Instrumentation on Additional Servers” on page 53
7. Select the events you want reported by each NetWare and eDirectory™ server you have configured. If necessary, install and configure any additional products instrumented for Nsure Audit, following the instructions provided by each product.
   - “Selecting Events Reported by NetWare and eDirectory” on page 56
8. Test your installation to ensure that your Nsure Audit environment is set up and functioning correctly.
   - “Verifying the Installation” on page 57

NTS Nsure Audit Installation TID

Novell Technical Support provides a detailed walk through of the Nsure Audit installation process on NetWare, in TID 10091433 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091433.htm). This TID contains instructions on setting up MySQL and the other components of Nsure Audit, and is very useful even if your server is not hosted on NetWare.

Prerequisites and Requirements

This section contains Nsure Audit prerequisites and requirements. The following must be set up in order to use Nsure Audit:

- "NICI 2.6.5" on page 28
- "eDirectory 8.5 or Later" on page 28
- "iManager 2.01 or Later" on page 28
- "Bouncy Castle Java Cryptographic Package" on page 28
- "Server Requirements" on page 28
- "Platform Requirements" on page 29

After you have met the requirements in this section, proceed to "Configuring an Event Repository" on page 31 to configure MySQL or other supported application as the event repository.

NICI 2.6.5

Any NetWare server that will report eDirectory events must be updated with the NICI 2.6.5 or later. This udpate is available at download.novell.com.

eDirectory 8.5 or Later

eDirectory 8.5 or later must be installed and configured in your environment. Nsure Audit uses eDirectory to store product configuration, and requires eDirectory schema extensions specific to Nsure Audit. In order to extend the schema and create the necessary objects, you must have admin rights to the root of the tree where you plan to install Nsure Audit.

Additionally, make sure the tree is synchronized and error free. For detailed information on eDirectory Health Check procedures, see "Keeping eDirectory Healthy" in the eDirectory 8.7 Administration Guide (http://www.novell.com/documentation/lg/edir87/edir87/data/a5ziqam.html).

iManager 2.01 or Later

Nsure Audit is configured using the Nsure Audit iManager plug-in, which requires iManager 2.01 or later.

Bouncy Castle Java Cryptographic Package

In order to use event verification in iManager, you must obtain and install the Bouncy Castle Java* Cryptographic Package. This JAR package, bcprov*.jar, is located in the add_ons/java_libraries folder of the *Nsure Audit 1.0.3 Installation* CD, or can be downloaded from http://www.bouncycastle.org/latest_releases.html (http://www.bouncycastle.org/latest_releases.html).

This JAR package must be copied to the tomcat\4\common\lib folder of your iManager server.

Server Requirements

In order to install Nsure Audit, you must have a server which meets the following requirements:

- Pentium* II or equivalent 400 Mhz

- 512 MB RAM
- At least 40 MB of available disk space on the system volume.
- A supported server platform. See “Platform Requirements” on page 29.

Platform Requirements

The server hosting the Secure Logging Server component must be running one of the following platforms:

- Open Enterprise Server
- NetWare 6.5, NetWare 6.0 SP3 or later, NetWare 5.1 SP6 or later
- SUSE® Linux Enterprise Server 8 or 9, or RedHat* Linux* AS or ES 2.1, or AS 3
- Windows 2000 Server SP3 or later, or Windows 2003 Server
- SPARC* server running Solaris 8 or 9

Servers or clients hosting the Platform Agent and instrumentation components must be running one of the following platforms:

- Open Enterprise Server
- NetWare 5.1 or later
- SUSE® Linux Enterprise Server 8 or 9, or RedHat* Linux* AS or ES 2.1, or AS 3
- Windows 2000 Server SP3 or later, or Windows 2003 Server
- SPARC* server running Solaris 8 or 9

4 Configuring an Event Repository

The Secure Logging Server manages the flow of information to and from the Nsure auditing system. It receives incoming events, monitors system events, and provides filtering and notification services.

By default, events are logged in delimited format on the file system where your Secure Logging Server is installed. This works for some installations, but the majority of users require a more robust event repository that enables more advanced querying and reporting.

In most circumstances, the Secure Logging Server is connected to a separate database, notification service, or other custom application to store event data.

The MySQL database is a powerful open database that provides the flexibility and platform support most users require, and is a good choice as the event repository in a majority of environments.

The Secure Logging Server can also use several additional applications and interfaces to log events, including Oracle*, Microsoft* SQL Server, Java, JDBC*, SNMP, SMTP, and syslog.

Before you install Nsure Audit, you should set up and configure this repository. Instructions on using MySQL as this event repository are included in the next section, "MySQL as the Event Repository" on page 31. Instructions on the other available repositories are included in the *Nsure Audit 1.0.3 Administration Guide*.

MySQL as the Event Repository

This installation guide provides basic information on installing and configuring MySQL* for use as a Novell Nsure Audit event repository. Additional information is contained in the *Novell Nsure Audit 1.0.3 Administration Guide* on the Nsure Audit Documentation Web site (http://www.novell.com/documentation/nsureaudit/index.html).

Installing MySQL

The following instructions provide detailed information on installing MySQL on all supported platforms:

- **NetWare 6 and 6.5:** Installing MySQL on NetWare (http://dev.mysql.com/doc/mysql/en/NetWare_installation.html)
- **Windows 2000 Server and Windows 2003 Server:** Installing MySQL on Windows (http://dev.mysql.com/doc/mysql/en/Windows_installation.html)
- **Linux:** Installing MySQL on Linux (http://dev.mysql.com/doc/mysql/en/Linux-RPM.html)
- **Solaris:** Installing MySQL on Other Unix-Like Systems (http://dev.mysql.com/doc/mysql/en/Installing_binary.html)

After you have completed the MySQL installation for your platform, start MySQL and complete the tasks in "Creating an Nsure Audit Database and User" on page 32.

Creating an Nsure Audit Database and User

After your MySQL database is installed and running, You must create an Nsure Audit database and user with the necessary privileges. The required table in this database is created automatically the first time the Secure Logging Server connects.

To Create a database and user:

1. launch MySQL Monitor.

   MySQL Monitor is launched by running **`mysql -u username -p`** from the NetWare terminal or from the mysql folder, depending on the platform. If this is a new installation of MySQL, use the default user, root.

2. Enter the following command in MySQL Monitor to create the Nsure Audit database:

   ```
   CREATE DATABASE naudit;
   ```

3. Enter the following command in MySQL Monitor to create the Nsure Audit user:

   ```
   GRANT ALL PRIVILEGES ON naudit.* TO auditusr@'%' IDENTIFIED BY 'auditpwd'
   WITH GRANT OPTION;
   ```

   NOTE: The @'%' after the username enables remote access for this account. You can omit this if the MySQL database is located on the same server as the Secure Logging Server. The default password is auditpwd, though we strongly suggest changing this password from the default in a production environment.

4. Enter the following command in MySQL Monitor to flush the MySQL privileges:

   ```
   FLUSH PRIVILEGES;
   ```

5. Record the following information:

   - IP address or DNS name of your MySQL server.
   - Nsure Audit database name.
   - Nsure Audit username and password.

   This information is required to configure the log channel object in eDirectory used by the Secure Logging Server to connect to your MySQL server.

6. Exit MySQL Monitor.

Troubleshooting

The following Technical Information Documents contain MySQL troubleshooting information relating to MySQL:

- How to troubleshoot the Nsure Audit MySQL channel - TID10088985 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088985.htm)
- Is Nsure Audit actually capturing any data to the MySQL channel? - TID10092777 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092777.htm)
- Nsure Audit Report Error 145 or 127 querying the MySQL database - TID10091360 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091360.htm)

- Error: Could not find the Driver Class: com.mysql.jdbc.Driver - TID10091351 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091351.htm)

5 Upgrading Novell Nsure Audit

This section contains information on upgrading from a previous version of Nsure Audit. To upgrade, complete the instructions for your Secure Logging Server platform:

Upgrading on NetWare

If you are upgrading from a previous version of Nsure Audit, the previous version does not need to be uninstalled. To upgrade, follow the instructions in "Installing on NetWare" on page 42 with the following considerations:

- If any applications that log events to Nsure Audit are running during the install, the new Platform Agent cannot be updated until your server is restarted. To avoid restarting your server after the installation, shut down any applications dependent on Logevent.nlm (for example, NetMail®, or BorderManager®) before you install.
- If an existing logevent.cfg file is found during install, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- If you upgrade your existing eDirectory instrumentation, it could take up to 5 minutes before the updated instrumentation is automatically loaded after install. To load the updated instrumentation faster, manually stop and restart the instrumentation using the following commands:

  ```
  unload auditds
  load auditds
  ```

- Replace your Nsure Audit iManager plug-in with the version included with Nsure Audit 1.0.3, as detailed in "Installing the Nsure Audit 1.0.3 iManager Plug-in" on page 49.

Upgrading on Linux

If you are upgrading from a previous version of Nsure Audit, the previous version does not need to be uninstalled. To upgrade, follow the instructions in "Installing on Linux" on page 43 with the following considerations:

- If an existing logevent.cfg file is found during install, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.

- Replace your Nsure Audit iManager plug-in with the version included with Nsure Audit 1.0.3, as detailed in “Installing the Nsure Audit 1.0.3 iManager Plug-in” on page 49.
- If you upgrade your existing eDirectory instrumentation, it could take up to 5 minutes before the updated instrumentation is automatically loaded after install. To load the updated instrumentation faster, manually stop and restart the instrumentation using the following commands:

```
start ndstrace -c "unload auditds"
start ndstrace -c "load auditds"
```

- After the upgrade is complete, you might need to manually start the Secure Logging Server using the following command:

```
/etc/init.d/novell-naudit start
```

Upgrading on Solaris

If you are upgrading from a previous version of Nsure Audit, the previous version does not need to be uninstalled. To upgrade, follow the instructions in “Installing on Solaris” on page 45 with the following considerations:

- If an existing logevent.cfg file is found during install, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- Replace your Nsure Audit iManager plug-in with the version included with Nsure Audit 1.0.3, as detailed in “Installing the Nsure Audit 1.0.3 iManager Plug-in” on page 49.
- If you upgrade your existing eDirectory instrumentation, it could take up to 5 minutes before the updated instrumentation is automatically loaded after install. To load the updated instrumentation faster, manually stop and restart the instrumentation using the following commands:

```
start ndstrace -c "unload auditds"
start ndstrace -c "load auditds"
```

- After the upgrade is complete, you might need to manually start the Secure Logging Server using the following command:

```
/etc/init.d/naudit start
```

Upgrading on Windows

If you are upgrading from a previous version of Nsure Audit, the previous version does not need to be removed. To upgrade, follow the instructions in “Installing on Windows” on page 46 with the following considerations:

- If an existing logevent.cfg file is found during install, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your platform agent to revert to the default settings.
- Replace your Nsure Audit iManager plug-in with the version included with Nsure Audit 1.0.3, as detailed in “Installing the Nsure Audit 1.0.3 iManager Plug-in” on page 49.
- If you upgrade your existing eDirectory instrumentation, it could take up to 5 minutes before the updated instrumentation is automatically loaded after install. To load the updated instrumentation faster, manually stop and restart the instrumentation using the following

commands. See Starting and Stopping the eDirectory Instrumentation on Windows (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/am38ahy.html#am38ai0) for instructions.

6 Installing Novell Nsure Audit

This section contains instructions for installing Nsure Audit on each supported platform. To install, complete the instructions for your Secure Logging Server platform:

Installing with Open Enterprise Server

1. Start the Open Enterprise Server (OES) installation.
2. In the Choose a Pattern window, select the Novell Nsure Audit Starter Pack.
   - Select Pre-Configured Server > Novell Nsure Audit Starter Pack.

     or
   - Select Customized NetWare Server and mark the following components:
     - Apache Web Server and Tomcat Servlet Container
     - MySQL (if you want to configure the MySQL data store during installation)
     - Novell Nsure Audit Starter Pack
     - iManager
3. In the Summary window, review the products to be installed, then click Copy Files.
4. When the installation program displays the Component Selection window for the Novell Nsure Audit Starter Pack, select the program components you want to install.
   - **Install Secure Logging Server:** Installs the Secure Logging Server (lengine.nlm), the Multiple Directory Database (mdb.nlm), and the channel drivers (lgd*.nlm) to the current server. It also creates a Logging Server object in the Logging Services container.

     You need at least one Secure Logging Server in your network.
     - **Autoconfigure MySQL:** creates the MySQL Channel object in the Logging Services' Channel container and configures the Secure Logging Server to log events to the MySQL database. If you select this option, you must install MySQL with the OES install. (See Step 2.)

       WARNING: The MySQL Channel object is created with a default Expiration script that runs every night at midnight and automatically deletes every record older than 12 hours. This was

done because the default events logged by the NetWare and eDirectory instrumentations quickly fill the database. To remove this setting, simply delete the script from the SQL Expiration Commands property in the MySQL Channel object and restart the Secure Logging Server. For more information, see "MySQL Channel Object" in the *Novell Nsure Audit 1.0.3 Administration Guide*.

- **Install Platform Agent** installs and configures the Platform Agent (logevent.nlm), the Caching Module (lcache.nlm), and the NetWare and eDirectory instrumentations (auditNW.nlm and auditDS.nlm respectively).

  You must install the Platform Agent on every workstation or server that is running an application that logs events to Novell Nsure Audit. To enable NetWare and file system logging, the NetWare instrumentation must be installed and loaded on every server on which you want to log NetWare and file system events. To log eDirectory events, auditDS must be installed and loaded on one server per DS Replica.

  - **Secure Logging Server Address** is the IP address or host name of the Secure Logging Server that the Platform Agent connects to.

5. If you selected the Autoconfigure MySQL option, the installation program displays the Database Options window so you can define your MySQL data store.
   - **MySQL Database Host:** The IP Address or host name of the MySQL database server.
   - **Port:** Defines the port at which the Secure Logging Server connects to the database server. If this field is left blank, the Secure Logging Server uses the default MySQL port assignment, 3306.
   - **DB Username:** User account the Secure Logging Server uses to log in to the database. This account has all privileges to the default database and can log in from any IP address. The default username for the OES data store is "auditusr."
   - **DB User Password:** Password the logging server uses to authenticate with the database. You must confirm this password. The default password for the OES data store is "auditpwd."
   - **Database Name:** Name of the database to which the logging server writes events. The default database name is "naudit."
   - **Table Name:** Database table to which the logging server writes events. The default table is "log."
6. Follow the prompts to complete the rest of the OES install.

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see "Commands and Utilities" in the *Novell Nsure Audit 1.0.3 Administration Guide*.

Installing with NetWare 6.5

When installing Novell Nsure Audit on NetWare 6.5, we recommended that you follow these instructions to first install Nsure Audit 1.0 from your NetWare 6.5 Installation CD, then run the Nsure Audit 1.0.3 installation to upgrade to version 1.0.3 using the instructions in "Installing on NetWare" on page 42.

1. Start the NetWare 6.5 installation.
2. In the Choose a Pattern window, select the Novell Nsure Audit Starter Pack.
   - Select Pre-Configured Server > Novell Nsure Audit Starter Pack.

or

- Select Customized NetWare Server and mark the following components:
  - Apache2 Web Server and Tomcat4 Servlet Container
  - MySQL (if you want to configure the MySQL data store during installation)
  - Novell Nsure Audit Starter Pack
  - iManager 2.0

3. In the Summary window, review the products to be installed, then click Copy Files.
4. When the installation program displays the Component Selection window for the Novell Nsure Audit Starter Pack, select the program components you want to install.
   - **Install Secure Logging Server:** Installs the Secure Logging Server (lengine.nlm), the Multiple Directory Database (mdb.nlm), and the channel drivers (lgd*.nlm) to the current server. It also creates a Logging Server object in the Logging Services container.

     You need at least one Secure Logging Server in your network.
     - **Autoconfigure MySQL:** creates the MySQL Channel object in the Logging Services' Channel container and configures the Secure Logging Server to log events to the MySQL database. If you select this option, you must install MySQL with the NetWare 6.5 install. (See Step 2.)

       WARNING: The MySQL Channel object is created with a default Expiration script that runs every night at midnight and automatically deletes every record older than 12 hours. This was done because the default events logged by the NetWare and eDirectory instrumentations quickly fill the database. To remove this setting, simply delete the script from the SQL Expiration Commands property in the MySQL Channel object and restart the Secure Logging Server. For more information, see "MySQL Channel Object" in the *Novell Nsure Audit 1.0.3 Administration Guide*.
   - **Install Platform Agent** installs and configures the Platform Agent (logevent.nlm), the Caching Module (lcache.nlm), and the NetWare and eDirectory instrumentations (auditNW.nlm and auditDS.nlm respectively).

     You must install the Platform Agent on every workstation or server that is running an application that logs events to Novell Nsure Audit. To enable NetWare and file system logging, the NetWare instrumentation must be installed and loaded on every server on which you want to log NetWare and file system events. To log eDirectory events, auditDS must be installed and loaded on one server per DS Replica.
     - **Secure Logging Server Address** is the IP address or host name of the Secure Logging Server that the Platform Agent connects to.
5. If you selected the Autoconfigure MySQL option, the installation program displays the Database Options window so you can define your MySQL data store.
   - **MySQL Database Host:** The IP Address or host name of the MySQL database server.
   - **Port:** Defines the port at which the Secure Logging Server connects to the database server. If this field is left blank, the Secure Logging Server uses the default MySQL port assignment, 3306.
   - **DB Username:** User account the Secure Logging Server uses to log in to the database. This account has all privileges to the default database and can log in from any IP address. The default username for the NetWare 6.5 data store is "auditusr."

- **DB User Password:** Password the logging server uses to authenticate with the database. You must confirm this password. The default password for the NetWare 6.5 data store is "auditpwd."
- **Database Name:** Name of the database to which the logging server writes events. The default database name is "naudit."
- **Table Name:** Database table to which the logging server writes events. The default table is "log."

6 Follow the prompts to complete the rest of the NetWare 6.5 install. For more information, see the NetWare 6.5 Overview and Installation Guide (http://www.novell.com/documentation/lg/nw65/install/data/hz8pck9v.html).

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see "Commands and Utilities" in the *Novell Nsure Audit 1.0.3 Administration Guide*.

Installing on NetWare

1 On the NetWare server, insert, and if necessary, mount the Nsure Audit 1.0.3 installation CD, then launch NWConfig.

- On NetWare 5.x or later, load nwconfig.nlm at the server console.
- On NetWare 4.2, enter **`load install`** at the server console. Only the instrumentation and Platform Agent can be installed on NetWare 4.2.

2 In NWConfig, Select Product Options > Install a Product Not Listed.

3 Press F3 (F4 if you're using RCONSOLE) and specify the path to the directory where the installation program can find the base.ips file, which is located in the NetWare directory on the installation CD.

4 Select your install options. Each option is outlined in the following table. The third and fourth columns contain the recommended settings for a new installation and upgrade.

Option	Description	New Install	Upgrade
First-time Directory Install	Extends the Directory schema for Novell Nsure Audit version 1.0.3.	Yes	No
Configure Server for Nsure Audit	Creates the Secure Logging Server object in Logging Services. It also creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel.	Yes	No
Nsure Audit Log Server Files	Installs the Novell Nsure Audit Secure Logging Server (lengine.nlm). The Secure Logging Server securely receives reported events, and is installed on only one server in your tree.	Yes	Yes

Option	Description	New Install	Upgrade
Nsure Audit Instrumentation Files	Installs the NetWare Instrumentation (auditNW.nlm) and the eDirectory Instrumentation (auditDS.nlm). This instrumentation must be installed on any NetWare server that will report events.	Yes	Yes
Nsure Audit Platform Agent Files	Installs the Novell Nsure Audit Platform Agent (logevent.nlm). The Platform Agent must be present on any NetWare server that will report events. If you are certain another instrumented application has previously installed the Nsure Audit 1.0.3 Platform Agent on this server, you can leave this unselected.	Yes	Yes
Backup Files from Previous Versions	Makes a backup of existing Nsure Audit files to enable rollback.	No	Yes
Directory Schema Update	Updates the Directory schema for Novell Nsure Audit version 1.0.3. **NOTE:** You must scroll to see this option in nwconfig.	No	Yes

5 Press F10 to continue, then follow the on-screen instructions until you have completed the installation program.

If you selected First-time Directory Install or Directory Schema Update, enter the Directory administrator's login name and password to update the schema. This account must have admin rights to the root of the tree. If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example,.Admin.Accounts.Finance.YourCo).

If you selected Configure Server for Nsure Audit, you are prompted to provide a name for the Secure Logging Server object.

Upon completing the installation, you must restart the server or manually launch the installed components. For the program startup commands, see "Commands and Utilities" in the *Novell Nsure Audit 1.0.3 Administration Guide*.

Installing on Linux

1 Log in as root on the host.

2 Enter the following command from the Linux console:

On SUSE, **`mount /media/cdrom`**

On RedHat, **`mount /mnt/cdrom`**

3 Enter the following command from the Linux console:

On SUSE, **`cd /media/cdrom/Linux`**

On RedHat, **cd /mnt/cdrom/Linux**

4. You are now in the setup directory for the Nsure Audit Linux install. Enter the following command from the Linux console to begin the installation:

   ./pinstall.lin

   The pinstall.lin script performs the following actions:

   - Verifies that eDirectory for Linux has been installed.
   - Copies the Novell Nsure Audit files to the installation directory.
   - Starts the auditext.sh script.

   If you receive a Permission Denied error when attempting to execute the install script, you might need to grant execute rights to pinstall.lin by running **chmod 755 pinstall.lin**.

5. When prompted, accept the license agreement.
6. Select your install options.
   - Platform Agent: Installs the Novell Nsure Audit Platform Agent.
   - eDirectory Instrumentation Files and Platform Agent: Installs the eDirectory Instrumentation and Platform Agent.
   - Secure Logging Server and Platform Agent: Installs the Novell Nsure Audit Secure Logging Server.
   - All: Installs the Secure Logging Server, Platform Agent, and the eDirectory instrumentation.
7. After the Nsure Audit components are installed, the auditext utility is automatically launched to extend your eDirectory schema, and configure the default Nsure Audit objects.

   In auditext, run Add Schema Extensions if you are performing a new install or an upgrade, then run Configure Server if you are performing a new install.

   If prompted, enter the Directory administrator's login name and password to update the schema.

   IMPORTANT: This account must have admin rights to the root of the tree.

   If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example, .Admin.Accounts.Finance.YourCo).
8. If prompted, enter a name for the Secure Logging Server object.
9. Continue to follow the installation instructions on the screen until you have exited the Novell Nsure Audit installation program.

When the installation is complete, the Secure Logging Server automatically launches, and the following command is added to /usr/lib/nds-modules/ndsmodules.conf to automatically load the eDirectory instrumentation with eDirectory:

```
auditds auto #NSure Audit Platform Agent
```

Remove this command if you do not want the eDirectory instrumentation to automatically load.

To manually start the eDirectory instrumentation, enter:

start ndstrace -c "load auditds"

Installing on Solaris

1. Log in as root on the host.
2. If necessary, mount the *Nsure Audit 1.0.3 Installation* CD, then browse to the Solaris directory from the Solaris console.
3. You are now in the setup directory for the Nsure Audit Solaris install. Enter the following command from the Solaris console to begin the installation:

   `./pinstall.sol`

   The pinstall.sol script performs the following actions:

   - Verifies that eDirectory for Solaris has been installed.
   - Copies the Novell Nsure Audit files to the installation directory.
   - Starts the auditext.sh script.

   If you receive a permission denied error when attempting to execute the install script, you might need to grant execute rights to pinstall.lin by running **`chmod 755 pinstall.lin`**
4. When prompted, accept the license agreement.
5. Select your install options.
   - Platform Agent: Installs the Novell Nsure Audit Platform Agent.
   - eDirectory Instrumentation Files and Platform Agent: Installs the eDirectory Instrumentation and Platform Agent.
   - Secure Logging Server and Platform Agent: Installs the Novell Nsure Audit Secure Logging Server.
   - All: Installs the Secure Logging Server, Platform Agent, and the eDirectory instrumentation.
6. After the Nsure Audit components are installed, the auditext utility is launched automatically to extend your eDirectory schema, and configure the default Nsure Audit objects.

   In auditext, run Add Schema Extensions if performing a new install or an upgrade, then run Configure Server if you are performing a new install.

   If prompted, enter the Directory administrator's login name and password to update the schema.

   IMPORTANT: This account must have admin rights to the root of the tree.

   If the admin object is not in the same context as the current server, you must enter the object's fully distinguished name (for example, .Admin.Accounts.Finance.YourCo).
7. If prompted, enter a name for the Secure Logging Server object.
8. Continue to follow the installation instructions on the screen until you have exited the Novell Nsure Audit installation program.

When the installation is complete, the Secure Logging Server automatically launches, and the following command is added to /etc/init.d/naudit to automatically load the eDirectory instrumentation with eDirectory:

```
ndstrace -c "load auditds"
```

Remove this command if you do not want the eDirectory instrumentation to automatically load.

To manually start the eDirectory instrumentation, run the following command from the Solaris console:

```
ndstrace -c "load auditds"
```

Installing on Windows

1. At the Windows server, log in as Administrator or as a user with administrative privileges.
2. Run naudit_win32 from the Windows setup directory on the *Nsure Audit 1.0.3 Installation* CD.
3. Follow the on-screen instructions in the Novell Nsure Audit Installation Wizard to view and accept the license agreement.
4. Provide your customer information.
5. Specify the destination directory, then click Next.

   The default directory is \program files\novell\nsure audit.
6. Select the type of installation you want to perform on the current server, then click Next.
   - Custom: Allows you to individually select which program components to install.
   - Full installation: Installs the Secure Logging Server (lengine.exe), the channel drivers (lgd*.dll), the Platform Agent (logevent.dll), the eDirectory instrumentation (auditDS.dlm), and Nsure Audit Report (lreport.exe).
   - instrumentation: Installs the Platform Agent and the eDirectory instrumentation.
   - Reporting Application: Installs Nsure Audit Report.
   - Server: Installs the Secure Logging Server, and the channel drivers.

   The Custom, Full Installation, and Server options create the Secure Logging Server object in Logging Services. They also create a File Channel object in the Logging Services Channel container and they configure the logging server to log events to the File channel.
7. If you are installing the instrumentation, specify the IP address of the Secure Logging Server.
8. Confirm your settings, then click Next.
9. If you are installing the Secure Logging Server, provide the following information when prompted:
   - Specify the Directory administrator's login name and password to update the schema.

     IMPORTANT: This account must have admin rights to the root of the tree.
   - Specify a name for the Secure Logging Server object.
10. Click OK to confirm the installation.
11. Click Finish to complete the Novell Nsure Audit installation.

When the installation is complete, the Secure Logging Server automatically launches; however, you must manually load the eDirectory instrumentation.

To manually load or unload the eDirectory instrumentation:

1. Load ndscons.exe.

   NOTE: ndscons.exe is usually in the \novell\nds directory.
2. In the list of installed services, select Novell Nsure Audit Component.

3 Click Start or Stop.

To configure the eDirectory instrumentation to load each time the server restarts:

1 Load ndscons.exe.

2 In the list of installed services, select Novell Nsure Audit Component.

3 Click Startup.

4 Mark the Automatic startup type and click OK.

7 Configuring Nsure Audit

This section contains tasks you must perform after the Nsure Audit installation. To configure Nsure Audit, complete the tasks contained in the following sections:

- “Installing the Nsure Audit 1.0.3 iManager Plug-in” on page 49
- “Configuring the Secure Logging Server” on page 50

Installing the Nsure Audit 1.0.3 iManager Plug-in

The Nsure Audit iManager plug-in package file is contained in the add_ons\iManager_plugins folder in the *Nsure Audit 1.0.3 Installation* CD. Additionally, if an installation of iManager is found during install, the package file was copied to the iManager packages folder on your server.

To install or upgrade the iManager plug-in, complete one of the following task:

- “Install or Upgrade the iManager Plug-in” on page 49
- “Install or Upgrade the iManager Plug-in in Assigned Mode with Role-Based Services” on page 50

Install or Upgrade the iManager Plug-in

1. Log in to iManager.
2. Click the Configure icon  .
3. Under Module Configuration click Install Module Package.
4. Browse to the naudit.npm file, then click the Install button.

   The naudit.npm module package is located in the add_ons\iManager_plugins directory on the *Nsure Audit 1.0.3 installation* CD. The installation process takes a few minutes. You should then see a message indicating that the module was saved successfully.
5. Click OK.
6. The Modules dialog box displays the new module. You can now close iManager.
7. Restart Tomcat 4.
   - On NetWare, enter TC4STOP at the NetWare prompt. Wait at least 1 minute, then enter TOMCAT4 to start the service again.
   - On Windows, Linux, or Solaris, run the shutdown script contained in your tomcat folder. Wait at least 1 minute, then run the startup script contained in your tomcat folder.

   Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log into iManager.
8. When you log in to iManager, the Nsure Audit role is displayed.

Install or Upgrade the iManager Plug-in in Assigned Mode with Role-Based Services

If you are running iManager in Assigned Mode and have RBS configured, complete the following steps to install or update the Nsure Audit iManager plug-in:

1. Log into iManager as a Collection Owner.
2. Click the Configure icon  .
3. Under Module Configuration, click Install Module Package.
4. Browse to the naudit.npm file, then click the Install button.

   The naudit.npm module package is located in the add_ons\iManager_plugins directory on the *Nsure Audit 1.0.3 installation* CD. The installation process takes a few minutes. You should then see a message indicating that the module was saved successfully.
5. Click OK.
6. The Modules dialog box displays the new module. You can now close iManager.
7. Restart Tomcat 4.
   - On NetWare, enter TC4STOP at the NetWare prompt. Wait at least 1 minute, then enter TOMCAT4 to start the service again.
   - On Windows, Linux, or Solaris, run the shutdown script contained in your tomcat folder. Wait at least 1 minute, then run the startup script contained in your tomcat folder.

   Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log into iManager.
8. Log into iManager, then click Configure again.
9. Under RBS Configuration, select Configure iManager.
10. Select Upgrade Collections, then click Next.
11. Verify that the correct collection is selected, then click Next. The new Nsure Audit plug-is displayed under Modules To Be Installed.
12. Select the Nsure Audit plug-in, assign a scope, then click Start.
13. Wait for the Completed message, then click Close. The new role appears on the Roles and Tasks page.

Configuring the Secure Logging Server

The Secure Logging Server is configured with the Nsure Audit iManager plug-in. If you are performing an upgrade, configuring the Secure Logging Server is optional, because your Nsure Audit environment continues to operate with your previous configuration.

To configure the Secure Logging Server:

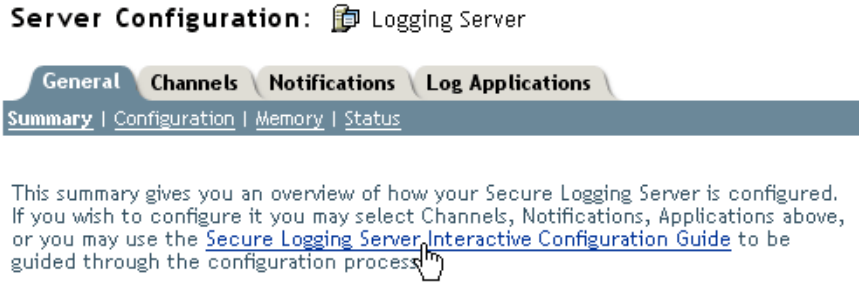
1. Log in to iManager.
2. Click the Roles and Tasks button  on the iManager toolbar.
3. In the Roles and Tasks view, expand the Nsure Audit role, then select the Server Configuration task.
4. Select the Secure Logging Server object, then click OK. By default, this object is installed in the Logging Services Organizational Unit at the root of your tree.

- Click the Object History button to see a list of Logging Server objects that have been selected during this iManager session.

  or

- Click the Object Selector button to locate the object in the directory tree. To move up or down in the tree, click the navigation arrows. You can also search the tree by typing the object name and context in the Search frame.

5 Run the configuration wizard by clicking the Secure Logging Server Interactive Configuration Guide link on the summary screen. This configuration guide provides on-screen information to guide you in setting up your Secure Logging Server.



6 After you have completed the Interactive Configuration guide, restart your Secure Logging Server using the following commands:

```
/etc/init.d/novell-naudit stop
/etc/init.d/novell-naudit start
```

8 Installing Instrumentation on Additional Servers

This section contains instructions on installing and configuring the Platform Agent and instrumentation components on all additional servers that will report events to your Secure Logging Server. Complete the following instructions to configure these servers:

- “Installing the NetWare and eDirectory Instrumentation on Other NetWare Servers” on page 53
- “Installing the eDirectory Instrumentation on Other Linux Servers” on page 54
- “Installing the eDirectory Instrumentation on Other Solaris Servers” on page 54
- “Installing the eDirectory Instrumentation on Other Windows Servers” on page 54

Additionally, complete the following configuration for each server you install:

- “Configuring the Platform Agent” on page 55
- “Selecting Events Reported by NetWare and eDirectory” on page 56

Installing the NetWare and eDirectory Instrumentation on Other NetWare Servers

In order to report events to Nsure Audit, the Platform Agent and the NetWare and eDirectory instrumentation must be installed on each NetWare server that will report events. Run the Nsure Audit 1.0.3 installation on each server, selecting only the following components:

- Nsure Audit Instrumentation Files: Installs the NetWare Instrumentation (auditNW.nlm) and the eDirectory Instrumentation (auditDS.nlm). This instrumentation must be installed on any NetWare server that will report events.

  WARNING: Before you install the eDirectory instrumentation on NetWare, your server must be updated with the latest version of NICI. See “NICI 2.6.5” on page 28 for details.

- Nsure Audit Platform Agent Files: Installs the Novell Nsure Audit Platform Agent (logevent.nlm). The Platform Agent must be present on any NetWare server that will report events. If you are certain another instrumented application has previously installed the Nsure Audit 1.0.3 Platform Agent on this server, you can leave this unselected.
- If an existing logevent.cfg file is found during install, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- If you are installing the eDirectory instrumentation on a server located in a different tree than your Secure Logging Server, select the First Time eDirectory Install; or if a previous version of Nsure Audit has been installed on that tree, select Directory Schema Update instead. (If the eDirectory sever is located in the same tree as your Secure Logging Server, your schema was already extended during that installation.)

After the installation is complete, configure the Platform Agent on each server as explained in "Configuring the Platform Agent" on page 55.

Installing the eDirectory Instrumentation on Other Linux Servers

In order to report eDirectory events to Nsure Audit, the eDirectory instrumentation and Platform Agent must be installed on each Linux server hosting an installation of eDirectory that will report events. Follow the instructions in "Installing on Linux" on page 43, selecting only the following component:

- eDirectory Instrumentation Files and Platform Agent: Installs the Platform Agent and the eDirectory instrumentation.
- If an existing logevent.cfg file is found during installation, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- If you are installing the eDirectory instrumentation on a server located in a different tree than your Secure Logging Server, select the Add Schema Extensions option in auditext. (If the eDirectory sever is located in the same tree as your Secure Logging Server, your schema was already extended during that installation.)

After the installation is complete, configure Platform Agent parameters as explained in "Configuring the Platform Agent" on page 55.

Installing the eDirectory Instrumentation on Other Solaris Servers

In order to report eDirectory events to Nsure Audit, the eDirectory instrumentation and Platform Agent must be installed on each Solaris server hosting an installation of eDirectory that will report events. Run the Nsure Audit 1.0.3 installation on each server, selecting only the following components:

- **eDirectory Instrumentation Files and Platform Agent:** Installs the Platform Agent and the eDirectory instrumentation.
- If an existing logevent.cfg file is found during installation, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- If you are installing the eDirectory instrumentation on a server located in a different tree than your Secure Logging Server, select the Add Schema Extensions option in auditext. (If the eDirectory sever is located in the same tree as your Secure Logging Server, your schema was already extended during that installation.)

After the installation is complete, configure Platform Agent parameters as explained in "Configuring the Platform Agent" on page 55.

Installing the eDirectory Instrumentation on Other Windows Servers

In order to report eDirectory events to Nsure Audit, the eDirectory instrumentation and Platform Agent must be installed on each Windows server hosting an installation of eDirectory that will report events. Run the Nsure Audit 1.0.3 installation on each server, selecting only the following components:

- **Instrumentation:** Installs the Platform Agent and the eDirectory instrumentation.
- If an existing logevent.cfg file is found during installation, you are prompted whether or not you want to overwrite this file. Do not overwrite your existing logevent.cfg unless you want your Platform Agent to revert to the default settings.
- Your eDirectory schema is extended automatically during the instrumentation install.

When prompted, specify the IP address or DNS name of your newly-established Secure Logging Server. After the installation is complete, you can optionally configure additional Platform Agent parameters as explained in "Configuring the Platform Agent" on page 55.

Configuring the Platform Agent

The Platform Agent is required on any client reporting events to Nsure Audit. The Platform Agent is configured using a text-format configuration file located on each server. The default location of this file is as follows:

Netware /etc/logevent.cfg
Windows /<WindowsDir>/logevent.cfg (Usually c:\windows)
Linux /etc/logevent.conf
Solaris /etc/logevent.conf

At a minimum, you must provide the IP address or DNS name of the Secure Logging Server in the *LogHost* parameter.

The configuration settings are not case sensitive, and you must restart the Platform Agent any time you make a change to the configuration. The following table contains the Platform Agent configuration options:

Option	Description
LogHost=<dns name>	Name or IP address of the Secure Logging Server the Platform Agent should use. Set to 127.0.0.1 (localhost) by default during initial install.
LogCacheDir=<path>	The directory where the Platform Agent should store the cached event information if the Primary or Secondary Secure Logging Server becomes unavailable.
LogEnginePort=<port>	Port used by the Secure Logging Server to accept data from Platform Agents.
LogCachePort=<port>	Port used by the Platform Agent caching mechanism.
LogCacheUnload=<Y|N>	Set to N if lcache should not allow unloading.
LogCacheSecure=<Y|N>	If the local cache file should be encrypted, this option must be set to Y.
LogReconnectInterval=<s>	Interval, in seconds, indicating how often the Platform Agent and the Platform Agent Cache try to reconnect to the Secure Logging Server after the connection was lost.

Option	Description
LogDebug=<Never|Always|Server>	Set to Never to never log debug events. Set to Always to always log debug events. Leave out or set to Server to use the default setting provided by the Secure Logging Server.
LogSigned=<Never|Always|Server>	Set to Never to never sign events. Set to Always to always log events with signature. Leave out, or set to Server to use the default setting provided by the Secure Logging Server.
LogMaxBigData=<bytes>	Set this value to allow the data field in the event to be larger than the default (3072 bytes). This should be set to the maximum number of bytes that this client will allow. Larger data is truncated, or not sent if the application doesn't allow truncated events to be logged.
LogMaxCacheSize=<bytes>	Set to the maximum size in bytes that a cache file will hold.
LogCacheLimitAction=<stop logging|drop cache>	The action that you want the cache module to take when it has reached the maximum cache size limit. Set to 'stop logging' if you want to stop collecting new events. Set to 'drop cache' if you want to delete the cache and start over with any new events that are generated.

Selecting Events Reported by NetWare and eDirectory

On each server where you have installed the NetWare or eDirectory instrumentation, you should select the events you want reported. Click the Server | NetWare | Filesystem | eDirectory links on the Nsure Audit tab of your NetWare or eDirectory NCP Server Object in iManager to select events:

9 Verifying the Installation

This section contains instructions to verify that your Nsure Audit installation was successful. Complete the instructions for your selected platform to verify your Nsure Audit installation:

Linux

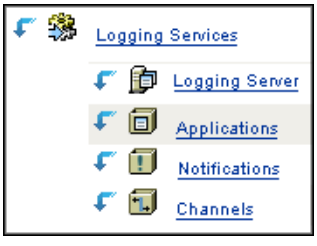
After you have completed the instructions in this installation guide, the following should be established in your environment:

- A Secure Logging Server running on a supported platform. This server is configured to log events to your event repository, and send notifications to any additional channels you have configured.
- One or more additional systems on a supported platform running the Platform Agent and various instrumentations. The Platform Agent on each system should be configured to report events to your Secure Logging Server, and each system should be configured to report the events you want to monitor.

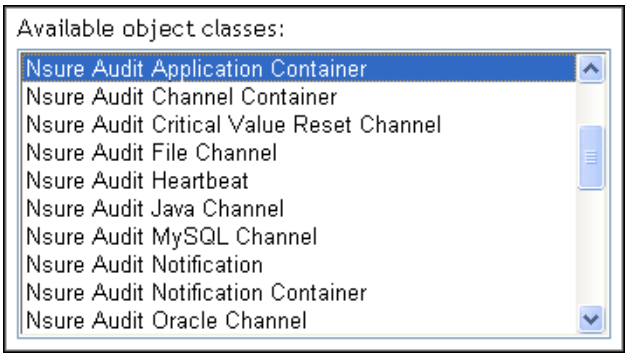
This section contains basic procedures and information to make sure these Nsure Audit components are installed and working correctly. See the Troubleshooting section in the *Nsure Audit 1.0.3 Administration Guide* for more information.

eDirectory Objects

In eDirectory, verify that you have a Logging Services container at the root of your tree, containing a Secure Logging Server object, and Applications, Notifications, and Channels container objects (these are placed in ou=Channels,ou=Logging Services by default):



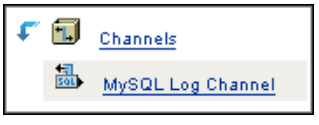
If any of these objects are missing, verify that the Nsure Audit schema extensions are installed. This can be accomplished in iManager using the Schema role > Class Info task, and verifying the presence of several classes beginning with Nsure Audit:



If these schema extensions are missing, run opt/novell/naudit/auditext, and select the Add Schema Extensions option.

If the schema has been extended correctly, but you do not have a Logging Services container or Secure Logging Server object, run opt/novell/naudit/auditext and select the Configure Server option.

Additionally, if you are using MySQL or another event repository, you should have created a MySQL Channel object or other object representing your repository in the Channels container:



If you have not done this, follow the instructions in "Configuring the Secure Logging Server" on page 50.

Event Repository

Make sure that your event repository is running and accessible to the Secure Logging Server.

If you are using a MySQL database on Linux, you can verify that database is running with the following command:

```
ps -ef |grep mysql
```

Secure Logging Server

The Nsure Audit Secure Logging Server should be running on your Linux server.

You can verify that the Secure Logging Server is running using the following command:

```
ps -ef |grep lengine
```

If the Secure Logging Server is not running, start it using the following command:

```
/etc/init.d/novell-naudit start
```

Platform Agents

The LogHost parameter in the Platform Agent configuration file on each server must be updated to contain the IP address or DNS name of your Secure Logging Server.

You can view all clients connected to the Secure Logging Server by starting the Nsure Audit Secure Logging Server using the -d option to view the console.

TIP: Clients connect to the Secure Logging Server only when they have an event to report. If you are running more clients than are listed, ensure that an operation has been performed that would trigger an event on each client.

Verifying Event Logging

The final step in testing is verifying that your event repository is receiving the events reported to the Secure Logging Server. The audit console displays the number of events that have been stored; verify that the events reported to your Secure Logging Server are in your event repository by running queries in iManager or Nsure Audit Report (LReport).

NetWare

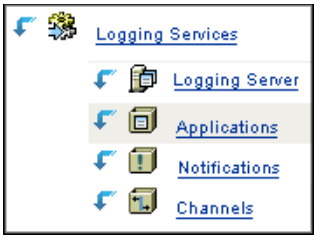
After you have completed the instructions in this installation guide, the following should be established in your environment:

- A Secure Logging Server running on a supported platform. This server is configured to log events to your event repository, and send notifications to any additional channels you have configured.
- One or more additional systems on a supported platform running the Platform Agent and various instrumentations. The Platform Agent on each system should be configured to report events to your Secure Logging Server, and each system should be configured to report the events you want to monitor.

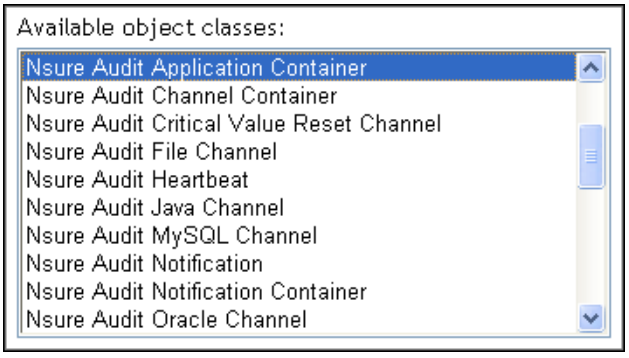
This section contains basic procedures and information to make sure these Nsure Audit components are installed and working correctly. See the Troubleshooting section in the *Nsure Audit 1.0.3 Administration Guide* for more information.

eDirectory Objects

In eDirectory, verify that you have a Logging Services container at the root of your tree, containing a Secure Logging Server object, and Applications, Notifications, and Channels container objects (these are placed in ou=Channels,ou=Logging Services by default):



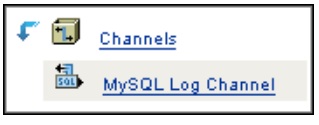
If any of these objects are missing, verify that the Nsure Audit schema extensions are installed. This can be accomplished in iManager using the Schema role > Class Info task, and verifying the presence of several classes beginning with Nsure Audit:



If these schema extensions are missing, rerun the installation and select the First-time Directory Install option if performing a new install, or select Directory Schema Update if you are performing an upgrade.

If the schema has been extended correctly, but you do not have a Logging Services container or Secure Logging Server object, rerun the installation and select the Configure Server for Nsure Audit option.

Additionally, if you are using MySQL or another event repository, you should have created a MySQL Channel object or other object representing your repository in the Channels container:



If you have not done this, follow the instructions in "Configuring the Secure Logging Server" on page 50.

Event Repository

Make sure that your event repository is running and accessible to the Secure Logging Server.

Secure Logging Server

Lengine.nlm should be running on the server hosting the Secure Logging Server. This is configured to load automatically at startup during install.

To determine if lengine.nlm is loaded, enter **`m lengine`** at the NetWare command prompt. If lengine is not loaded, reload it and check the NetWare logger screen for any messages.

```
SDF1:m lengine
LENGINE.NLM
  Loaded from [SYS:\SYSTEM\]
  (Address Space = OS)
  Nsure Audit Secure Logging Server (DEBUG)
  Version 1.00.02 June 10, 2004
```

Platform Agents

Logevent.nlm should be running on any NetWare server that reports events. This is configured to load automatically at startup during install.

To determine if logevent.nlm is loaded, enter **`m logevent`** at the NetWare command prompt:

```
SDF1:m logevent
LOGEVENT.NLM
  Loaded from [SYS:\SYSTEM\]
  (Address Space = OS)
  Nsure Audit Platform Agent (DEBUG)
  Version 1.00.02 June 16, 2004
```

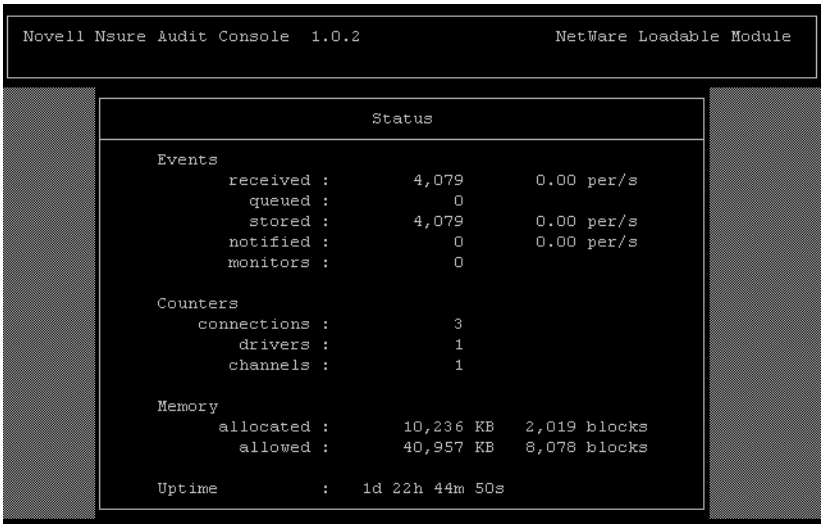
If logevent is not loaded, reload it and check the NetWare logger screen for any messages.

The LogHost parameter in the Platform Agent configuration file on each server must be updated to contain the IP address or DNS name of your Secure Logging Server.

Nsure Audit Console

The Nsure Audit Console displays details about the events received, and clients connected to your Secure Logging Server.

The Nsure Audit Console is loaded using the -d option when loading the Secure Logging Server (lengine.nlm):



The events section displays the number of events received, queued, and stored, as well as the number of clients connected to your Secure Logging Server.

TIP: Clients connect to the Secure Logging Server only when they have an event to report. If you are running more clients than are listed, ensure that an operation has been performed that would trigger an event on each client.

If Nsure Audit is configured to load automatically, you can add the -d option in sys:\system\auditsvr.ncf:

```
load lengine.nlm -d
```

Verifying Event Logging

The final step in testing is verifying that your event repository is receiving the events reported to the Secure Logging Server. The audit console displays the number of events which have been

stored, verify that the events reported to your Secure Logging Server are in your event repository by running queries in iManager or Nsure Audit Report (LReport).

Solaris

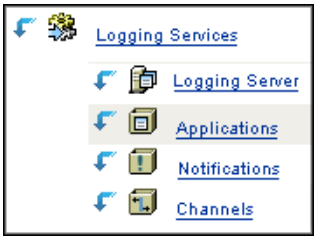
After you have completed the instructions in this installation guide, the following should be established in your environment:

- A Secure Logging Server running on a supported platform. This server is configured to log events to your event repository, and send notifications to any additional channels you have configured.
- One or more additional systems on a supported platform running the Platform Agent and various instrumentations. The Platform Agent on each system should be configured to report events to your Secure Logging Server, and each system should be configured to report the events you want to monitor.

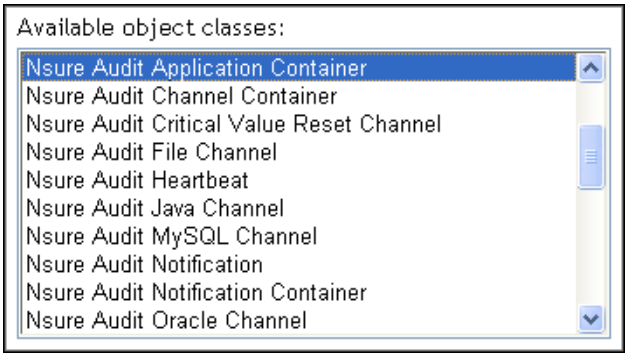
This section contains basic procedures and information to make sure these Nsure Audit components are installed and working correctly. See the Troubleshooting section in the *Nsure Audit 1.0.3 Administration Guide* for more information.

eDirectory Objects

In eDirectory, verify that you have a Logging Services container at the root of your tree, containing a Secure Logging Server object, and Applications, Notifications, and Channels container objects (these are placed in ou=Channels,ou=Logging Services by default):



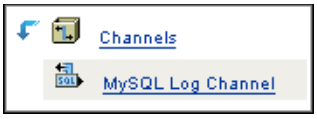
If any of these objects are missing, verify that the Nsure Audit schema extensions are installed. This can be accomplished in iManager using the Schema role > Class Info task, and verifying the presence of several classes beginning with Nsure Audit:



If these schema extensions are missing, run opt/NOVLnaudit/auditext and select the Add Schema Extensions option.

If the schema has been extended correctly, but you do not have a Logging Services container or Secure Logging Server object, run opt/NOVLnaudit/auditext and select the Configure Server option.

Additionally, if you are using MySQL or another event repository, you should have created a MySQL Channel object or other object representing your repository in the Channels container:



If you have not done this, follow the instructions in "Configuring the Secure Logging Server" on page 50.

Event Repository

Make sure that your event repository is running and accessible to the Secure Logging Server.

Secure Logging Server

The Nsure Audit Secure Logging Server should be running on your Solaris server. If it is not running, you can start it with the following command:

```
/etc/init.d/naudit start
```

Platform Agents

The LogHost parameter in the Platform Agent configuration file on each server must be updated to contain the IP address or DNS name of your Secure Logging Server.

You can view all clients connected to the Secure Logging Server by starting the Nsure Audit Secure Logging Server using the -d option to view the console.

TIP: Clients connect to the Secure Logging Server only when they have an event to report. If you are running more clients than are listed, ensure that an operation has been performed that would trigger an event on each client.

Verifying Event Logging

The final step in testing is verifying that your event repository is receiving the events reported to the Secure Logging Server. The audit console displays the number of events which have been stored, verify that the events reported to your Secure Logging Server are in your event repository by running queries in iManager or Nsure Audit Report (LReport).

Windows

After you have completed the instructions in this installation guide, the following should be established in your environment:

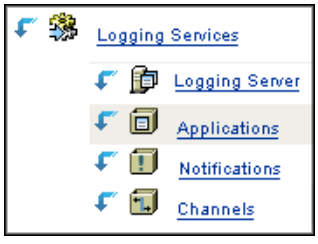
- A Secure Logging Server running on a supported platform. This server is configured to log events to your event repository, and send notifications to any additional channels you have configured.

- One or more additional systems on a supported platform running the Platform Agent and various instrumentations. The Platform Agent on each system should be configured to report events to your Secure Logging Server, and each system should be configured to report the events you want to monitor.

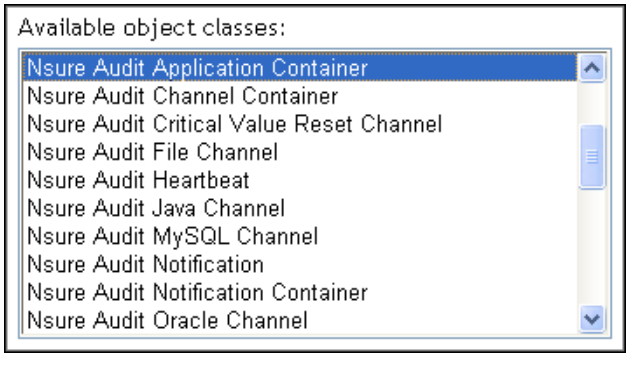
This section contains basic procedures and information to make sure these Nsure Audit components are installed and working correctly. See the Troubleshooting section in the *Nsure Audit 1.0.3 Administration Guide* for more information.

eDirectory Objects

In eDirectory, verify that you have a Logging Services container at the root of your tree, containing a Secure Logging Server object, and Applications, Notifications, and Channels container objects (these are placed in ou=Channels,ou=Logging Services by default):



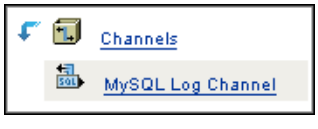
If any of these objects are missing, verify that the Nsure Audit schema extensions are installed. This can be accomplished in iManager using the Schema role > Class Info task, and verifying the presence of several classes beginning with Nsure Audit:



If these schema extensions are missing, rerun the installation and select the Custom, Full Installation, or Server option.

If the schema has been extended correctly, but you do not have a Logging Services container or Secure Logging Server object, rerun the installation and select the Custom, Full Installation, or Server option.

Additionally, if you are using MySQL or another event repository, you should have created a MySQL Channel object or other object representing your repository in the Channels container:



If you have not done this, follow the instructions in "Configuring the Secure Logging Server" on page 50.

Event Repository

Make sure that your event repository is running and accessible to the Secure Logging Server.

Secure Logging Server

The Novell Nsure Audit Manager service should be running on the server hosting the Secure Logging Server.

To determine if the Novell Nsure Audit Manager service is running, open the Services applet from Control Panel > Administrative Tools.

Platform Agents

The Platform Agent should be running on any server that will report events.

To determine if the eDirectory instrumentation is running on Windows, make sure the Novell Nsure Audit Component is started in NDS® console.

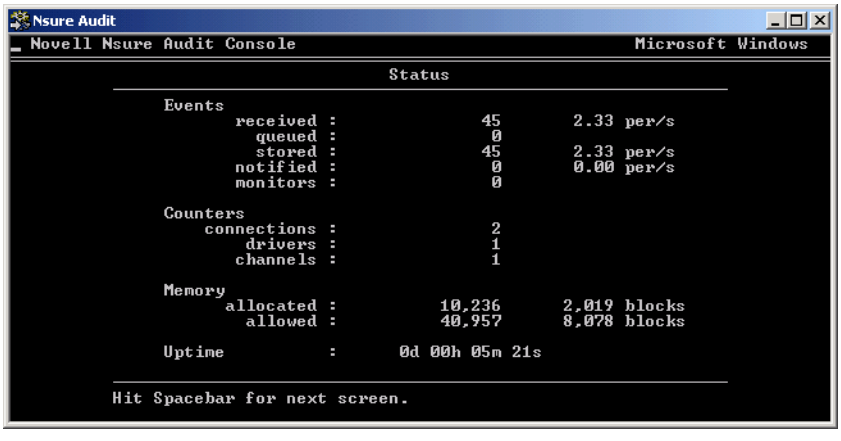
The LogHost parameter in the Platform Agent configuration file on each server must be updated to contain the IP address or DNS name of your Secure Logging Server.

Nsure Audit Console

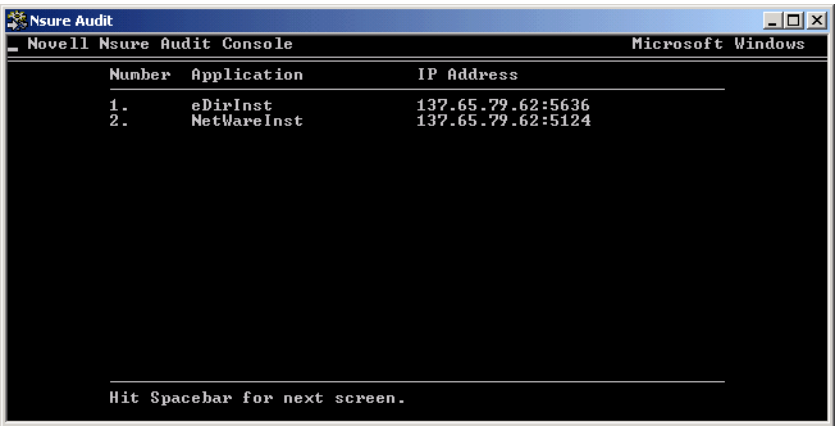
The Nsure Audit Console displays details about the events received, and clients connected to your Secure Logging Server.

The Nsure Audit Console is loaded by right-clicking the Nsure Audit services icon and selecting console:

The events section displays the number of events received, queued, and stored, as well as the number of clients connected to your Secure Logging Server:



Press the Spacebar to view details about each connected client:



TIP: Clients connect to the Secure Logging Server only when they have an event to report. If you are running more clients than what are listed, ensure that an operation has been performed that would trigger an event on each client.

Verifying Event Logging

The final step in testing is verifying that your event repository is receiving the events reported to the Secure Logging Server. The audit console displays the number of events that have been stored; verify that the events reported to your Secure Logging Server are in your event repository by running queries in iManager or Nsure Audit Report (LReport).