

Novell Audit

2.0

June 1, 2006

INSTALLATION GUIDE

www.novell.com



Novell®

Legal Notices

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

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

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

Copyright © 2006 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

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

Novell Trademarks

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

eDirectory is a trademark of Novell, Inc.

NCP is a trademark of Novell, Inc.

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

NetWare is a registered trademark of Novell, inc., in the United States and other countries.

NLM is a trademark of Novell Inc.

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

Novell Application Launcher is a trademark of Novell, Inc.

Nsure Audit is a trademark of Novell, Inc.

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

Third-Party Materials

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

Contents

| | |
|---|-----------|
| About This Guide | 7 |
| 1 Installation Overview | 9 |
| 2 System Requirements and Prerequisites | 11 |
| 2.1 System Requirements | 11 |
| 2.1.1 Secure Logging Server | 11 |
| 2.1.2 Platform Agent | 12 |
| 2.1.3 eDirectory Instrumentation | 12 |
| 2.1.4 NetWare Instrumentation | 13 |
| 2.1.5 Windows Instrumentation | 13 |
| 2.1.6 Log Parser Instrumentation | 13 |
| 2.2 Prerequisites | 13 |
| 2.2.1 NICI | 13 |
| 2.2.2 eDirectory | 13 |
| 2.2.3 iManager | 14 |
| 3 Configuring the Data Store | 15 |
| 3.1 File Data Store | 16 |
| 3.2 MySQL Data Store | 17 |
| 3.3 Microsoft SQL Server Data Store | 18 |
| 3.4 Oracle Data Store | 19 |
| 3.5 Syslog Data Store | 19 |
| 3.6 JDBC Data Store | 20 |
| 4 Upgrading Novell Audit | 21 |
| 5 Installing and Activating Novell Audit | 23 |
| 5.1 Installing on NetWare | 23 |
| 5.2 Installing on Linux | 26 |
| 5.3 Installing on Solaris | 29 |
| 5.4 Installing on Windows | 32 |
| 5.5 Activating Novell Audit | 34 |
| 5.6 Activating Novell Audit Report | 35 |
| 6 Installing the Novell Audit iManager Plug-In | 37 |
| 6.1 Install or Upgrade the iManager Plug-In | 37 |
| 6.2 Install or Upgrade the iManager Plug-In in Assigned Mode with Role-Based Services | 38 |
| 7 Configuring the Secure Logging Server | 39 |
| 7.1 Configuring the Secure Logging Server | 39 |
| 7.2 Configuring Multiple Secure Logging Servers | 40 |
| 7.3 Configuring a Secure Logging Server with More Than One IP Address | 41 |

| | | |
|----------|--|-----------|
| 8 | Configuring the Platform Agent and Logging Instrumentations | 43 |
| 8.1 | Installing the Logging Components | 43 |
| 8.2 | Configuring the Platform Agent | 44 |
| 8.3 | Selecting Logged Events | 45 |
| 8.3.1 | Configuring eDirectory Events | 45 |
| 8.3.2 | Configuring NetWare and File System Events | 46 |
| 8.3.3 | Configuring Novell Audit Events | 47 |
| 8.3.4 | Configuring Windows Events | 47 |
| | | |
| 9 | Verifying the Installation | 49 |
| 9.1 | eDirectory Objects | 49 |
| 9.2 | Data Store | 50 |
| 9.3 | Secure Logging Server | 50 |
| 9.4 | Platform Agent and Logging Instrumentations | 52 |
| 9.4.1 | Platform Agent | 52 |
| 9.4.2 | NetWare and eDirectory Instrumentations | 53 |
| 9.4.3 | Windows Instrumentation | 55 |
| 9.4.4 | Novell Audit Instrumentation | 56 |
| 9.4.5 | Log Parser Instrumentation | 56 |
| 9.5 | Verifying Event Logging | 57 |
| 9.6 | Server and System Statistics | 58 |

About This Guide

Welcome to Novell® Audit. This guide provides the information required to install Novell Audit.

- “Audience” on page 7
- “Feedback” on page 7
- “Documentation Updates” on page 7
- “Additional Documentation” on page 7
- “Documentation Conventions” on page 7

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual. Please use the Feedback option at the bottom of each page of the Novell Audit online documentation.

Documentation Updates

For the most recent version of the *Novell Audit 2.0 Installation Guide*, see the [Novell Documentation Web site](http://www.novell.com/documentation/novellaudit20/index.html), (<http://www.novell.com/documentation/novellaudit20/index.html>).

Additional Documentation

For information on managing Novell Audit, see the *Novell Audit 2.0 Administration Guide*.

Documentation Conventions

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

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark. When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

Installation Overview

1

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

- 1 Meet the Novell Audit prerequisites and requirements. For more information, see [“System Requirements and Prerequisites” on page 11](#).
- 2 Configure MySQL* or another supported application as the data store. For more information, see [“Configuring the Data Store” on page 15](#).
- 3 Install or update the Secure Logging Server component of Novell Audit on a single server in your tree. Depending on whether this is a first-time install or an upgrade, see the following:
 - [“Installing and Activating Novell Audit” on page 23](#)
 - [“Upgrading Novell Audit” on page 21](#)

If you want to configure multiple Secure Logging Server in the tree, see [Section 7.2, “Configuring Multiple Secure Logging Servers,” on page 40](#).

- 4 Install or update the Novell Audit iManager plug-in on your iManager server. For more information, see [“Installing the Novell Audit iManager Plug-In” on page 37](#).
- 5 Use the Novell Audit iManager plug-in to configure your Secure Logging Server. This includes creating the Channel object required to connect to the data store you created in [Step 2](#) as well as any other logging channels or notifications you want to activate on your logging system. For more information, see [“Configuring the Secure Logging Server” on page 39](#).
- 6 Install and configure the Platform Agent on every server that you want to report events. You must also install the Instrumentation for each logging application that you want to report events. For example, if you have NetWare® and eDirectory™ running on a server, you must install the Platform Agent, the NetWare Instrumentation, and the eDirectory Instrumentation for that server to report NetWare and eDirectory events. For more information, see [Chapter 8, “Configuring the Platform Agent and Logging Instrumentations,” on page 43](#).
- 7 (Optional) If you are running NetWare or eDirectory, select which events you want to report. For more information, see [“Selecting Logged Events” on page 45](#).
- 8 Test your installation to ensure that your Novell Audit environment is set up and functioning correctly. For more information, see [“Verifying the Installation” on page 49](#).

System Requirements and Prerequisites

2

This section contains Novell® Audit prerequisites and requirements.

- [Section 2.1, “System Requirements,” on page 11](#)
- [Section 2.2, “Prerequisites,” on page 13](#)

After you have met the requirements in this section, proceed to [“Configuring the Data Store” on page 15](#) to configure MySQL or another supported application as the data store.

2.1 System Requirements

The following sections outline the system requirements for each Novell Audit component.

- [Section 2.1.1, “Secure Logging Server,” on page 11](#)
- [Section 2.1.2, “Platform Agent,” on page 12](#)
- [Section 2.1.3, “eDirectory Instrumentation,” on page 12](#)
- [Section 2.1.4, “NetWare Instrumentation,” on page 13](#)

2.1.1 Secure Logging Server

The Secure Logging Server is the server component in the Novell auditing system. It is installed on the server where you want to manage the flow of information to and from the auditing system.

The server where you install the Secure Logging Server must meet the following requirements:

| Requirement | Description |
|------------------|--|
| Operating System | Open Enterprise Server 1.0 SP1 (NetWare® and Linux*) NetWare 6.5 Windows* 2003 Server Windows 2000 Server SP4 or later SUSE® Linux Enterprise Server 9 Red Hat* Linux 3 AS and ES Solaris* 8, 9, and 10 IMPORTANT: Solaris 8 requires GCC 3.3 and zlib 1.2.3 to function as a Secure Logging Server. Without GCC3.3, applications fail to authenticate to the logging server. The resulting error in <code>nproduct.log</code> is, <code>Failed SSL Handshake</code> . |
| eDirectory™ | Novell eDirectory version 8.7 or 8.8 must be installed on the server where the Secure Logging Server is located. |

| Requirement | Description |
|-------------|---|
| Processor | A single processor, server-class PC with a Pentium* II 400 Mhz |
| Disk Space | At least 40 MB The space you need for your data store depends on a number of factors that include, but are not limited to, how many events per second you are storing and how long you want to keep the data. For MySQL, a system that generates around 80 events per second with an average event size of 80 bytes consumes approximately 500 MB of disk space for the database table and 150 MB for the index in a 24-hour period. |
| RAM | 512 MB |

2.1.2 Platform Agent

The Platform Agent is the client portion of the Novell auditing system. It is a shared library that is used by instrumented applications to log events to Novell Audit. It does not have any system requirements other than disk space for the Disconnected Mode Cache. (eDirectory is not required.)

The Platform Agent must be installed on every server running applications that log events to Novell Audit. The Platform Agent supports the following platforms:

- Open Enterprise Server 1.0 SP1 (NetWare and Linux)
- NetWare 6.5
- Windows 2000
- Windows 2000 Server SP4 or later
- Windows XP Professional and Home Editions
- Windows 2003 Server
- SUSE Linux Enterprise Server 9
- Red Hat 3 AS and ES
- Solaris 8, 9, and 10

2.1.3 eDirectory Instrumentation

The eDirectory Instrumentation enables Novell Audit to log eDirectory events. To avoid receiving duplicate entries for eDirectory events, select the *Do not send replicated events* option in the *Novell Audit* tab of the NCP Server object.

To log non-replicated eDirectory events (such as logins), the eDirectory Instrumentation and Platform Agent must be installed on each server where you want to log non-replicated events.

The eDirectory Instrumentation supports the following versions of the Directory:

- eDirectory 8.7 (NetWare, Windows, Linux, and Solaris)
- eDirectory 8.8 (NetWare, Windows, Linux, and Solaris)

2.1.4 NetWare Instrumentation

The NetWare Instrumentation allows Novell Audit to log NetWare and file system events. The NetWare Instrumentation and Platform Agent must be loaded on every server where you want to log NetWare and file system events.

The NetWare Instrumentation supports the following versions of NetWare:

- NetWare 6.5
- OES NetWare

2.1.5 Windows Instrumentation

The Novell Audit Windows instrumentation collects events from the Event Viewer and sends them to the Secure Logging Server for processing by Novell Audit.

The Novell Audit Windows Instrumentation runs as a service on the following Windows platforms:

- Windows 2000
- Windows 2000 Server SP4 or later
- Windows XP Professional and Home Editions
- Windows 2003 Server

2.1.6 Log Parser Instrumentation

The Log Parser Instrumentation harvests events from text-based log files such as Syslog, Apache error logs, and Novell Application Launcher™ logs on all supported platforms.

Events are parsed one line at a time and formatted into the Novell Audit event structure. Parsing text-based log files allows Novell Audit to process and log events from applications that are not currently instrumented for Novell Audit.

2.2 Prerequisites

The following must be set up to use Novell Audit:

- [Section 2.2.1, “NICI,” on page 13](#)
- [Section 2.2.2, “eDirectory,” on page 13](#)
- [Section 2.2.3, “iManager,” on page 14](#)

2.2.1 NICI

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

2.2.2 eDirectory

eDirectory 8.7 or 8.8 must be installed and configured in your environment. Novell Audit uses eDirectory to store product configuration, and requires eDirectory schema extensions specific to Novell Audit.

Make sure the tree is synchronized and error free. For detailed information on eDirectory Health Check procedures, see “[Keeping eDirectory Healthy](http://www.novell.com/documentation/lg/edir87/edir87/data/a5ziqam.html)” in the *eDirectory 8.7 Administration Guide* (<http://www.novell.com/documentation/lg/edir87/edir87/data/a5ziqam.html>).

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 Novell Audit. You must provide the administrator username and password during installation so the installation program can extend the schema.

2.2.3 iManager

Novell Audit is configured using the Novell Audit iManager plug-in, which requires iManager 2.5 or 2.6 (2.6 is preferred).

Configuring the Data Store

3

Using its available channel drivers, Novell Audit can log events to the following applications and interfaces:

- Flat file in the file system
- MySQL database
- Oracle* database
- Microsoft* SQL Server database
- Java*
- JDBC*
- JMS
- SNMP
- SMTP
- Syslog database

Before selecting a storage device for your data store, you need to consider your system's logging traffic. On the high end, the File driver can process over 30,000 events per second on a P4 Xeon* class server. Databases, on the other hand, are, much slower (the MySQL driver can handle about 5,000 events per second on a P4 Xeon class server); however, they provide advanced querying and reporting.

Novell Audit is designed to handle occasional peaks that exceed a given database's limitations; however, if you expect to consistently exceed the database driver's capacity, you must plan your setup accordingly, either by using multiple Secure Logging Servers or by using the File driver. For information on configuring multiple logging servers, see “[Configuring Multiple Secure Logging Servers](#)” in the *Novell Audit 2.0 Administration Guide*.

IMPORTANT: In planning your system setup, you should perform your own throughput test in your environment and not rely solely on the numbers provided in this document.

After configuring a Novell Audit data store, you must create a Channel object. Each Channel object defines the parameters associated with its corresponding storage device. For example, MySQL Channel objects include the IP address or host name of the MySQL database server, a username and password for connecting with the server, the database and table names, and fields for SQL table create and expiration commands. For more information on creating and configuring Channel objects, see “[Configuring System Channels](#)” in the *Novell Audit 2.0 Administration Guide*.

After creating the Channel object, you must configure the logging server to log events to that channel. The Log Driver property in the Logging Server object determines which Channel object the server uses to create the data store. For more information on the Log Driver property, see “[Logging Server Object Attributes](#)” in the *Novell Audit 2.0 Administration Guide*.

After the Channel and Logging Server objects are configured, you must restart the logging server to load the Channel object configuration and the channel driver. In most cases, the channel driver automatically creates the necessary file or database table for the data store.

IMPORTANT: Novell Audit does not secure the data store. Therefore, you must manage data store security at the database for MySQL and Oracle data stores, or through the file system for file data stores.

The data store structure for common storage devices is discussed in the following sections:

- [Section 3.1, “File Data Store,” on page 16](#)
- [Section 3.2, “MySQL Data Store,” on page 17](#)
- [Section 3.3, “Microsoft SQL Server Data Store,” on page 18](#)
- [Section 3.4, “Oracle Data Store,” on page 19](#)
- [Section 3.5, “Syslog Data Store,” on page 19](#)
- [Section 3.6, “JDBC Data Store,” on page 20](#)

3.1 File Data Store

Depending on the File Channel object configuration, the File channel driver (`lgdfile`) can log events in raw format, or it can translate the event data into a human-readable log. By default, file data stores are named `auditlog; however;` however, you can specify the log filename in the File Channel object configuration.

Raw files simply contain the event data; consequently, they are not in a human-readable format. However, because they maintain a consistent field structure across events, they can be imported into spreadsheet programs like Microsoft Excel.

The following is a sample from a raw log file:

```
16777343,1051924636,1051924647,eDirInst\Object,721699,7,0,.OntarioTest
Data.Channels.Logging
Services,,0,0,0,LlNhdHVybiBMb2dnaW5nIFNlcnZlci5Mb2dnaW5nIFNlcnZpY2Vz
16777343,1051924636,1051924647,eDirInst\Object,721690,7,0,.eDirectoryI
nstrumentation.Applications.Logging
Services,,0,0,0,LlNhdHVybiBMb2dnaW5nIFNlcnZlci5Mb2dnaW5nIFNlcnZpY2Vz
16777343,1051926065,1051926065,eDirInst\Object,720897,7,0,.BillBob.SIM
,,0,0,1,LmFkbWluLlNJTQ=
```

NOTE: Novell Audit includes a utility, called `LETrans`, that can translate raw log files into human-readable format. See “[LETrans](#)” in the *Novell Audit 2.0 Administration Guide*.

Translated log files, on the other hand, can be visually scanned for content; however, it is difficult to generate reports from these files because there is no consistent field structure—they contain only the event descriptions.

The following is a sample from a translated log file:

```
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A read operation was
performed on object .OntarioTestData.Channels.Logging Services by
.Saturn Logging Server.Logging Services
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A list Subordinate
Entires operation has been performed on container .eDirectory
Instrumentation.Applications.Logging Services by .Saturn Logging
Server.Logging Services
```


[Sat, 03 May 2003 01:39:41 +0000] eDirInst\Object: A new eDirectory object called .BillBob.SIM (Class:User) was created by .admin.SIM

In addition to providing different log formats, the File channel is capable of creating localized logs. If the logging applications have localized Log Schema (LSC) files, the File channel can write translated log files in the language designated in the File Channel object.

NOTE: LSC files catalog the events that can be logged for a given application. They can also indicate what kind of data is stored in the event fields and provide descriptive information on the event itself. For more information, see “[Log Schema Files](#)” in the *Novell Audit 2.0 Administration Guide*.

For more information on the File channel, see “[File](#)” in the *Novell Audit 2.0 Administration Guide*.

3.2 MySQL Data Store

When the logging server loads the MySQL Channel object configuration, the MySQL channel driver, `lgdmsql`, automatically creates the data store’s table using the following table structure:

| Field | Type | Null | Key | Default | Extra |
|-------------------|--------------|------|-----|---------|-------|
| SourceIP | int(11) | YES | | | |
| ◆ ClientTimestamp | int(11) | YES | MUL | | |
| ClientMS | int(11) | YES | | | |
| ServerTimestamp | int(11) | YES | | | |
| SessionID | int(11) | YES | | | |
| Component | varchar(255) | YES | | | |
| ◆ EventID | int(11) | YES | MUL | | |
| Severity | int(11) | YES | | | |
| Grouping | int(11) | YES | | | |
| Originator | varchar(255) | YES | | | |
| OriginatorType | int(11) | YES | | | |
| Target | varchar(255) | YES | | | |
| TargetType | int(11) | YES | | | |
| SubTarget | varchar(255) | YES | | | |
| Text1 | varchar(255) | YES | | | |
| Text2 | varchar(255) | YES | | | |
| Text3 | varchar(255) | YES | | | |
| Value1 | int(11) | YES | | | |
| Value2 | int(11) | YES | | | |
| Value3 | int(11) | YES | | | |
| MIMEType | int(11) | YES | | | |
| DataSize | int(11) | YES | | | |
| Data | mediumblob | YES | | | |
| Signature | varchar(255) | YES | | | |

The table name is defined in the MySQL Channel object configuration page. The default table name is NAUDITLOG. For more information, see “[MySQL Channel Object](#)” in the *Novell Audit 2.0 Administration Guide*.

The MySQL Channel uses MyIsam as its database engine; therefore, the default maximum table size using MySQL 4.1 is 4 GB. MySQL 5.0 limits table sizes to 65,536 TB. Table size may be further constrained by the maximum file size your operating system can manage.

IMPORTANT: If the SQL server data volume runs out of disk space, any clients logging events will freeze and need to be restarted.

If you need larger tables, use the `max_rows` and `avg_row_length` commands in the MySQL Channel object's Create Table Options property.

For more information on the MySQL channel, see “**MySQL**” and “**Using MySQL with Novell Audit**” in the *Novell Audit 2.0 Administration Guide*.

3.3 Microsoft SQL Server Data Store

When the SQL Server Channel object configuration is loaded in the logging server's memory, the SQL Server channel driver, `lgdmssql`, automatically creates the following table structure for the SQL Server data store:

| Column Name | Data Type | Length | Allow Nulls |
|-----------------|-----------|--------|-------------|
| SourceIP | int | 4 | ✓ |
| ClientTimeStamp | int | 4 | ✓ |
| ClientMS | int | 4 | ✓ |
| ServerTimeStamp | int | 4 | ✓ |
| SessionID | int | 4 | ✓ |
| Component | varchar | 255 | ✓ |
| EventID | int | 4 | ✓ |
| Severity | int | 4 | ✓ |
| Grouping | int | 4 | ✓ |
| Originator | varchar | 255 | ✓ |
| OriginatorType | int | 4 | ✓ |
| Target | varchar | 255 | ✓ |
| TargetType | int | 4 | ✓ |
| SubTarget | varchar | 255 | ✓ |
| Text1 | varchar | 255 | ✓ |
| Text2 | varchar | 255 | ✓ |
| Text3 | varchar | 255 | ✓ |
| Value1 | int | 4 | ✓ |
| Value2 | int | 4 | ✓ |
| Value3 | int | 4 | ✓ |
| MIMEType | int | 4 | ✓ |
| DataSize | int | 4 | ✓ |
| Data | image | 16 | ✓ |
| Signature | varchar | 255 | ✓ |

The table name is defined in the Microsoft SQL Channel object configuration page. The default table name is `NAUDITLOG`. For more information, see “**Microsoft SQL Server Channel Object**” in the *Novell Audit 2.0 Administration Guide*.

For more information on the Microsoft SQL Server channel, see “**Microsoft SQL Server**” and “**Using Microsoft SQL Server with Novell Audit**” in the *Novell Audit 2.0 Administration Guide*.

3.4 Oracle Data Store

When the Oracle Channel object configuration is loaded in the logging server's memory, the Oracle channel driver, `lgdora`, automatically creates the following table structure for the Oracle data store:

| Name | Datatype | Size | Scale | Nulls? |
|-----------------|----------|------|-------|--------|
| SOURCEIP | NUMBER | | 0 | |
| CLIENTTIMESTAMP | NUMBER | | 0 | |
| CLIENTMS | NUMBER | | 0 | |
| SERVERTIMESTAMP | NUMBER | | 0 | |
| SESSIONID | NUMBER | | 0 | |
| COMPONENT | VARCHAR2 | 255 | | |
| EVENTID | NUMBER | | 0 | |
| SEVERITY | NUMBER | | 0 | |
| GROUPING | NUMBER | | 0 | |
| ORIGINATOR | VARCHAR2 | 255 | | ✓ |
| ORIGINORTYPE | NUMBER | | 0 | |
| TARGET | VARCHAR2 | 255 | | ✓ |
| TARGETTYPE | NUMBER | | 0 | |
| SUBTARGET | VARCHAR2 | 255 | | ✓ |
| TEXT1 | VARCHAR2 | 255 | | ✓ |
| TEXT2 | VARCHAR2 | 255 | | ✓ |
| TEXT3 | VARCHAR2 | 255 | | ✓ |
| VALUE1 | NUMBER | | 0 | |
| VALUE2 | NUMBER | | 0 | |
| VALUE3 | NUMBER | | 0 | |
| MIMETYPE | NUMBER | | 0 | |
| DATASIZE | NUMBER | | 0 | |
| DATA | LONG RAW | | | ✓ |
| SIGNATURE | VARCHAR2 | 255 | | ✓ |

The table name is defined in the Oracle Channel object configuration page. The default table name is `NAUDITLOG`. For more information, see “[Oracle Channel Object](#)” in the *Novell Audit 2.0 Administration Guide*.

For more information on the Oracle channel, see “[Oracle](#)” and “[Using Oracle with Novell Audit](#)” in the *Novell Audit 2.0 Administration Guide*.

This channel driver is used only on platforms where Oracle can run natively; when running the Secure Logging Server on NetWare, create a JDBC channel to connect to the Oracle server.

3.5 Syslog Data Store

The Syslog channel driver, `lgdsyslg`, allows the logging server to log events to a specific syslog facility on any syslog host.

It is also capable of creating localized logs. If the logging applications have localized LSC files, the Syslog channel can write the log files in the language designated in the Syslog Channel object.

For more information on the Syslog channel, see “**Syslog**” in the *Novell Audit 2.0 Administration Guide*.

3.6 JDBC Data Store

The JDBC channel allows the logging server to output filtered events to any JDBC-enabled data store. For performance reasons, we recommend using only the File or database channels discussed in this section as the primary log channel. You should use JDBC data stores only for notifications.

WARNING: The JDBC channel does not work on NetWare 5.x. The JDBC channel requires JVM* 1.4.2, which is not compatible with NetWare 5.x. Attempting to run the JDBC channel on NetWare 5.x abends the server.

For more information on the JDBC channel, see “**JDBC**” and “**Using JDBC Data Stores with Novell Audit**” in the *Novell Audit 2.0 Administration Guide*.

Upgrading Novell Audit

4

When upgrading from a previous version of Novell® Audit, please consider the following:

- You do not need to uninstall the previous version of Nsure™ Audit. To upgrade, simply follow the 2.0 product installation instructions for your respective platform. If the 2.0 product installer detects a previous version, it automatically removes and upgrades the Novell Audit components as necessary.
- If an existing Platform Agent configuration file (`logevent.cfg` or `logevent.conf`) is found during the upgrade, the installation asks if you want to overwrite the Platform Agent configuration file. Do not overwrite the existing file unless you want your Platform Agent to revert to the default configuration settings.
- During an upgrade or install, if iManager 2.0 or newer is found on the system, the Novell Audit 2.0 plug-in is copied to the appropriate iManager directory. To complete the upgrade of the iManager plug-in, please follow the instructions as detailed in [Chapter 6, “Installing the Novell Audit iManager Plug-In,” on page 37](#).
- If you upgrade an existing eDirectory™ Instrumentation, it could take up to five minutes before the updated Instrumentation reloads. To expedite the loading of the eDirectory Instrumentation Agent, you can manually stop and restart it using the following commands:

Table 4-1 eDirectory Instrumentation Commands

| Operating System | command |
|------------------|--|
| NetWare® | <code>unload auditds</code> <code>load auditds</code> |
| Windows | <p>To manually load or unload the eDirectory instrumentation:</p> <ol style="list-style-type: none">1. Load <code>ndscons.exe</code>. <hr/> <p>NOTE: <code>ndscons.exe</code> is usually in the <code>\novell\nds</code> directory.</p> <ol style="list-style-type: none">2. In the list of installed services, select <i>Novell Audit Component</i>.3. Click <i>Start</i> or <i>Stop</i>. <p>To configure the eDirectory instrumentation to load each time the server restarts:</p> <ol style="list-style-type: none">1. Load <code>ndscons.exe</code>.2. In the list of installed services, select <i>Novell Audit Component</i>.3. Click <i>Startup</i>.4. Select the <i>Automatic</i> startup type and click <i>OK</i>. |
| Linux | <code>ndstrace -c "unload auditDS"</code> <code>ndstrace -c "load auditDS"</code> |
| Solaris | <code>ndstrace -c "unload auditDS"</code> <code>ndstrace -c "load auditDS"</code> |

- On NetWare, if you upgrade an existing NetWare Instrumentation, it could take up to five minutes before the updated Instrumentation reloads. To expedite the loading of the NetWare Instrumentation, you can manually stop and restart it using the following commands:

```
unload auditnw
```

```
load auditnw
```

- On NetWare, if any applications that log events to Novell Audit are executing during the upgrade, the new Platform Agent cannot be updated until your server restarts. To avoid restarting your server after the upgrade completes, shut down any applications dependent on `logevent.nlm` (such as NetMail® or BorderManager®) before you attempt the Novell Audit upgrade.

Installing and Activating Novell Audit

5

This section contains instructions for installing and activating Novell Audit on each supported platform.

- [Section 5.1, “Installing on NetWare,” on page 23](#)
- [Section 5.2, “Installing on Linux,” on page 26](#)
- [Section 5.3, “Installing on Solaris,” on page 29](#)
- [Section 5.4, “Installing on Windows,” on page 32](#)
- [Section 5.5, “Activating Novell Audit,” on page 34](#)
- [Section 5.6, “Activating Novell Audit Report,” on page 35](#)

5.1 Installing on NetWare

Novell Audit can be installed on NetWare® 6.5 SP3 or OES 1.0 SP1 (NetWare kernel).

To install Novell Audit on NetWare:

- 1 On the NetWare server, insert, and if necessary, mount the Novell Audit installation CD.
- 2 Load `nwconfig.nlm` at the server console.
- 3 In NWConfig, select *Product Options > Install a Product Not Listed*.
- 4 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.
- 5 Select your install options.

Unlike previous versions of Novell Audit, the installation options are not specific to new or upgrade installations. For a complete first-time or upgrade installation, we recommend you select all the options.

The installation options are outlined in the following table.

| Option | Description |
|---|--|
| Install Novell Audit Instrumentation Agents | <p>Installs the NetWare Instrumentation (<code>auditNW.nlm</code>) and the eDirectory™ Instrumentation (<code>auditDS.nlm</code>).</p> <p>These instrumentations must be installed on any NetWare server that you want to report eDirectory, file system, or NetWare events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.</p> |
| Install Novell Audit Platform Agent | <p>Installs the Novell Audit Platform Agent (<code>logevent.nlm</code>) and adds <code>auditagt.ncf</code> to the <code>autoexec.ncf</code> file.</p> <p>The Platform Agent must be installed on any NetWare server that you want to report events.</p> |

| Option | Description |
|------------------------------------|---|
| Novell Audit Secure Logging Server | <p>Installs the Novell Audit Secure Logging Server (<code>lengine.nlm</code>), the Novell Audit Instrumentation Agents (<code>auditNW.nlm</code> and <code>auditDS.nlm</code>), the Platform Agent (<code>logevent.nlm</code>), the Log Parser (<code>logparse.nlm</code>), and adds the Novell Audit 2.0 schema extensions to eDirectory. It also adds <code>auditsvr.ncf</code> and <code>auditagt.ncf</code> to the <code>autoexec.ncf</code> file.</p> <p>The Secure Logging Server securely receives reported events.</p> <p>NOTE: If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects. For more information, see Section 7.2, "Configuring Multiple Secure Logging Servers," on page 40.</p> |
| Add Schema Extensions | <p>Adds the Novell Audit schema extensions to eDirectory.</p> <p>NOTE: If you select only this option, you are automatically exited from the installer after the eDirectory schema is extended.</p> |

6 Press F10 to continue.

7 Accept the License Agreement.

8 To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.

If the admin object is not in the same context as the current server, you must use the object's fully distinguished name (for example, `.Admin.Accounts.Finance.YourCo`).

9 After logging in to AuditExt, select from the following options:

| AuditExt Options | Action |
|--------------------------|---|
| Add Schema Extensions | <p>Adds the Novell Audit 2.0 schema objects.</p> <p>IMPORTANT: This does not destroy or overwrite any objects in your current eDirectory tree.</p> |
| Remove Schema Extensions | <p>Removes all Novell Audit schema extensions from the eDirectory tree.</p> <p>This option is required to uninstall Novell Audit.</p> <p>WARNING: This option deletes all existing Novell Audit objects from eDirectory.</p> |

| AuditExt Options | Action |
|-----------------------|---|
| Configure This Server | <p>Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions:</p> <ul style="list-style-type: none"> For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. <p>If you choose to configure the Secure Logging Server, you are prompted as follows:</p> <ol style="list-style-type: none"> AuditExt automatically creates the Secure Logging Server name as "<i>server_name</i> Logging Server." Choose if you want to create all Novell Audit objects in the Logging Services container. <hr/> <p>NOTE: Logging Services is the default container for all Novell Audit objects in eDirectory.</p> <hr/> <p>If you select <i>No</i>, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects.</p> <ol style="list-style-type: none"> When you're finished, press Esc, then click <i>Yes</i>. <p>For additional configuration information, see Chapter 7, "Configuring the Secure Logging Server," on page 39.</p> |
| Exit AuditExt | Closes the AuditExt utility. |

10 When finished, select *Exit AuditExt*, then click *Yes*.

11 Choose if you want to start the Secure Logging Server now.

If you select *Yes*, the installer loads the Secure Logging Server. It does not reboot the server.

To manually load the Secure Logging Server, enter

```
load lengine
```

or

```
load auditsvr.ncf
```

If you want to prevent the Secure Logging Server from being unloaded by users with access to the server console, you can append the `-n` switch to the server startup script. (For example, `load lengine -n`.)

12 Choose if you want to start logging eDirectory and NetWare events now.

If you select *Yes*, the installer loads the instrumentations and the Platform Agent.

To manually start the NetWare or eDirectory Instrumentation on NetWare, enter

```
load auditnw
```

or

```
load auditDS
```

To load both the NetWare and eDirectory Instrumentations, enter

```
load auditagt.ncf
```

Auditnw.nlm, audit.ds, and auditagt.ncf are located in the sys:\system directory.

- 13 Press Enter to complete the installation.
- 14 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it. For instructions on installing the plug-in, see [Chapter 6, “Installing the Novell Audit iManager Plug-In,”](#) on page 37.

5.2 Installing on Linux

Novell Audit 2.0 can be installed on SUSE® Linux Enterprise Server 9 or Red Hat Linux AS and ES (3 and 4).

To install Novell Audit on Linux:

- 1 Log in as root on the host.
- 2 Enter the following commands at the Linux console to mount the Novell Audit installation CD and go to the setup directory for the Novell Audit Linux install:

| Operating System | Commands |
|------------------|-----------------------|
| SUSE | mount /media/cdrom |
| | cd /media/cdrom/Linux |
| Red Hat | mount /mnt/cdrom |
| | cd /mnt/cdrom/Linux |

- 3 From the setup directory for the Novell Audit Linux install, enter the following command at the Linux console to begin the installation:

```
./pinstall.lin
```

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 Accept the license agreement.
- 5 Select your install options.

| Option | Description |
|----------------|--|
| Platform Agent | Installs the Novell Audit Platform Agent (<code>liblogevent.so</code>) and the Log Parser (<code>logparse</code>). The Platform Agent must be installed on any server that you want to report events. |

| Option | Description |
|--|--|
| eDirectory Instrumentation Files with Platform Agent | <p>Installs the eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), and the Log Parser (<code>logparse</code>).</p> <p>The eDirectory instrumentation must be installed on any server that you want to report eDirectory events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.</p> |
| Extend Schema | <p>Adds the Novell Audit schema extensions to eDirectory.</p> <hr/> <p>NOTE: If you select only this option, you are returned to the Linux console after the eDirectory schema is extended.</p> |
| Novell Audit Secure Logging Server | <p>Installs the Novell Audit Secure Logging Server (<code>lengine</code>), the Novell Audit eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), the Log Parser (<code>logparse</code>), and adds the Novell Audit 2.0 schema extensions to eDirectory.</p> <p>The Secure Logging Server securely receives reported events.</p> <hr/> <p>NOTE: If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects. For more information, see Section 7.2, "Configuring Multiple Secure Logging Servers," on page 40.</p> |

- 6** To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.

NOTE: If the admin object is not in the same context as the current server, you must use the object's fully distinguished name (for example, `.Admin.Accounts.Finance.YourCo`).

- 7** After logging in to AuditExt, select from the following options:

| AuditExt Options | Action |
|--------------------------|---|
| Add Schema Extensions | <p>Adds the Novell Audit 2.0 schema objects.</p> <hr/> <p>IMPORTANT: This does not destroy or overwrite any objects in your current eDirectory tree.</p> |
| Remove Schema Extensions | <p>Removes all Novell Audit schema extensions from the eDirectory tree.</p> <p>This option is required to uninstall Novell Audit.</p> <hr/> <p>WARNING: This option deletes all existing Novell Audit objects from eDirectory.</p> |

| AuditExt Options | Action |
|-----------------------|--|
| Configure This Server | <p>Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions:</p> <ul style="list-style-type: none"> For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. <p>If you choose to configure the Secure Logging Server, you are prompted as follows:</p> <ol style="list-style-type: none"> AuditExt automatically creates the Secure Logging Server name as "server_name Logging Server." Choose if you want to create all Novell Audit objects in the Logging Services container. <hr/> <p>NOTE: Logging Services is the default container for all Novell Audit objects in eDirectory.</p> <hr/> <p>If you select <i>No</i>, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects.</p> <ol style="list-style-type: none"> When you're finished, press Esc, then click <i>Yes</i>. <p>For additional configuration information, see Chapter 7, "Configuring the Secure Logging Server," on page 39.</p> |
| Exit AuditExt | Closes the AuditExt utility. |

8 When finished, select *Exit AuditExt*.

9 When the installation is complete, the Secure Logging Server automatically launches.

10 Choose if you want to load the Platform Agent.

11 If you select *Yes*, you are asked if you want to overwrite the pre-existing Platform Agent configuration file (`logevent.conf`).

For more information on `logevent.conf`, see "[Logevent](#)" in the *Novell Audit 2.0 Administration Guide*.

12 Choose if you want to load the eDirectory Instrumentation.

Novell Audit adds the following command to the `ndsmodules.conf` file to automatically load the eDirectory Instrumentation with eDirectory:

```
auditDS auto #NSure Audit Platform Agent
```

NOTE: On eDirectory 8.7, the path to the `ndsmodules.conf` file is `/usr/lib/nds-modules/ndsmodules.conf`. On eDirectory 8.8, the path is `/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf`.

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

To manually start the eDirectory instrumentation, enter:

```
ndstrace -c "load auditDS"
```

- 13 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it. For instructions on installing the plug-in, see [Chapter 6, “Installing the Novell Audit iManager Plug-In,”](#) on page 37.

5.3 Installing on Solaris

Novell Audit 2.0 can be installed on Solaris 8, 9, and 10.

IMPORTANT: Solaris 8 requires GCC 3.3 and zlib 1.2.3 to function as a Secure Logging Server. Without GCC3.3, applications fail to authenticate to the logging server. The resulting error in `nproduct.log` is `Failed SSL Handshake`.

To install Novell Audit on Solaris:

- 1 Log in as root on the host.

- 2 Insert the CD into the drive.

If the Volume Manager (`vold`) is running on your system, the CD is automatically mounted as `/cdrom/CDROM`.

- 3 (Optional) If the Volume Manager is not running on your system, complete the following steps to mount the CD:

- 3a Determine the name of the device by entering the following command:

```
ls -al /dev/sr* |awk '{print "/" $11}'
```

- 3b Enter the following commands to mount the CD-ROM:

```
mkdir -p /cdrom/CDROM
mount -F hsfs -o ro device_name /cdrom/CDROM
```

- 4 Enter the following command to go to the directory for the Novell Audit Solaris install:

```
cd /cdrom/CDROM/Solaris
```

- 5 From the setup directory for the Novell Audit Solaris install, enter the following command at the Solaris console to begin the installation:

```
./pinstall.sol
```

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.sol`.

- 6 Accept the license agreement.

- 7 Select your install options.

| Option | Description |
|----------------|--|
| Platform Agent | Installs the Novell Audit Platform Agent (<code>liblogevent.so</code>) and the Log Parser (<code>logparse</code>). The Platform Agent must be installed on any server that you want to report events. |

| Option | Description |
|--|--|
| eDirectory Instrumentation Files with Platform Agent | <p>Installs the eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), and the Log Parser (<code>logparse</code>).</p> <p>The eDirectory instrumentation must be installed on any server that you want to report eDirectory events. This option automatically installs the Platform Agent, regardless of whether the Platform Agent option is selected.</p> |
| Extend Schema | <p>Adds the Novell Audit schema extensions to eDirectory.</p> <hr/> <p>NOTE: If you select only this option, you are returned to the Linux console after the eDirectory schema is extended.</p> |
| Novell Audit Secure Logging Server | <p>Installs the Novell Audit Secure Logging Server (<code>lengine</code>), the Novell Audit eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), the Log Parser (<code>logparse</code>), and adds the Novell Audit 2.0 schema extensions to eDirectory.</p> <p>The Secure Logging Server securely receives reported events.</p> <hr/> <p>NOTE: If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration objects. For more information, see Section 7.2, "Configuring Multiple Secure Logging Servers," on page 40.</p> |

- 8 To add the Novell Audit schema extensions, enter the user name and password of an administrator with rights to the root of the eDirectory tree. This logs you into the AuditExt utility.
 If the admin object is not in the same context as the current server, you must use the object's fully distinguished name (for example, `.Admin.Accounts.Finance.YourCo`).
- 9 After logging in to AuditExt, select from the following options:

| AuditExt Options | Action |
|--------------------------|---|
| Add Schema Extensions | <p>Adds the Novell Audit 2.0 schema objects.</p> <hr/> <p>IMPORTANT: This does not destroy or overwrite any objects in your current eDirectory tree.</p> |
| Remove Schema Extensions | <p>Removes all Novell Audit schema extensions from the eDirectory tree.</p> <p>This option is required to uninstall Novell Audit.</p> <hr/> <p>WARNING: This option deletes all existing Novell Audit objects from eDirectory.</p> |

| AuditExt Options | Action |
|-----------------------|--|
| Configure This Server | <p>Configures the Secure Logging Server. Depending on the installation, it performs one of the following actions:</p> <ul style="list-style-type: none"> For a new installation, it creates the Secure Logging Server object in Logging Services, creates a File Channel object in the Logging Services Channel container, and configures the Secure Logging Server to log events to the File channel. It also creates a Monitor channel for iManager. For an upgrade installation, it upgrades the Novell Audit 1.0.3 objects to the Novell Audit 2.0 schema. <p>If you choose to configure the Secure Logging Server, you are prompted as follows:</p> <ol style="list-style-type: none"> AuditExt automatically creates the Secure Logging Server name as "server_name Logging Server." Choose if you want to create all Novell Audit objects in the Logging Services container. <hr/> <p>NOTE: Logging Services is the default container for all Novell Audit objects in eDirectory.</p> <hr/> <p>If you select <i>No</i>, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects.</p> <ol style="list-style-type: none"> When you're finished, press Esc, then click <i>Yes</i>. <p>For additional configuration information, see Chapter 7, "Configuring the Secure Logging Server," on page 39.</p> |
| Exit AuditExt | Closes the AuditExt utility. |

10 When finished, select *Exit AuditExt*.

11 When the installation is complete, the Secure Logging Server automatically launches.

12 Choose if you want to load the Platform Agent.

13 If you select *Yes*, you are asked if you want to overwrite the pre-existing Platform Agent configuration file (`logevent.conf`).

For more information on `logevent.conf`, see "[Logevent](#)" in the *Novell Audit 2.0 Administration Guide*.

14 Choose if you want to load the eDirectory Instrumentation.

Novell Audit adds the following command to the `ndsm_modules.conf` file to automatically load the eDirectory Instrumentation with eDirectory:

```
auditDS auto #NSure Audit Platform Agent
```

NOTE: On eDirectory 8.7, the path to the `ndsm_modules.conf` file is `/usr/lib/nds-modules/ndsm_modules.conf`. On eDirectory 8.8, the path is `/etc/opt/novell/eDirectory/nds-modules/ndsm_modules.conf`.

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

To manually start the eDirectory instrumentation, enter:

```
ndstrace -c "load auditDS"
```

- 15 After you install Novell Audit, iManager 2.0 or above detects that you have a new plug-in and prompts you to install it. For instructions on installing the plug-in, see [Chapter 6, "Installing the Novell Audit iManager Plug-In,"](#) on page 37.

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"
```

5.4 Installing on Windows

The Novell Audit Secure Logging Server can be installed on Windows 2000 and 2003 Server. The Platform Agent and instrumentations can be installed on Windows 2000 and Windows 2000 Server, Windows XP Professional and Home Editions, and Windows 2003 Server.

- 1 At the Windows server, log in as Administrator or a user with administrative privileges.
- 2 Insert the Novell Audit installation CD.
The auto install launches.
- 3 Accept the license agreements.
- 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*.

| Installation Option | Description |
|---------------------|---|
| Custom | Allows you to individually select which program components to install. When you select individual program components, the installer automatically selects your dependencies. IMPORTANT: For upgrades, the installer automatically installs all channels; you cannot install only specific channels. |
| Extend Schema | Adds the Novell Audit 2.0 schema objects. IMPORTANT: This does not destroy or overwrite any objects in your current eDirectory tree. |

| Installation Option | Description |
|-----------------------|--|
| Full Installation | Installs the Secure Logging Server (<code>lengine.exe</code>), all channel drivers (<code>lgd*.dll</code>), the Platform Agent (<code>logevent.dll</code>), the eDirectory instrumentation (<code>auditDS.dlm</code>), the Windows Instrumentation (<code>nauditwin.exe</code>), Novell Audit Report (<code>lreport.exe</code>), and the Log Parser (<code>logparse.exe</code>). |
| Instrumentation | Installs the Platform Agent, the eDirectory and Windows instrumentations, and the Log Parser (<code>logparse.exe</code>). |
| Platform Agent | Installs only the Platform Agent (<code>logevent.dll</code>). |
| Reporting Application | Installs Novell Audit Report (<code>lreport.exe</code>). |
| Server | Installs the Secure Logging Server (<code>lengine.exe</code>), all channel drivers (<code>lgd*.dll</code>), the Platform Agent (<code>logevent.dll</code>), the eDirectory instrumentation (<code>auditDS.dlm</code>), the Windows Instrumentation (<code>nauditwin.exe</code>), and the Log Parser (<code>logparse.exe</code>). |

The Custom, Full Installation, and Server options create the Secure Logging Server object in the Logging Services container. 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.

For additional configuration information, see [Chapter 7, “Configuring the Secure Logging Server,”](#) on page 39.

NOTE: If you want more than one Secure Logging Server in the tree, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server’s configuration objects. For more information, see [Section 7.2, “Configuring Multiple Secure Logging Servers,”](#) on page 40.

- 7 (Optional) If you are installing the Platform Agent, specify the IP address of the Secure Logging Server.
- 8 Confirm your settings, then click *Next*.
- 9 Verify the location of eDirectory.
The default location is `drive:\novell\nds`.
- 10 (Optional) If you are installing the Secure Logging Server, provide the following information when prompted:
 - 10a 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.
 - 10b Specify a name for the Secure Logging Server object.
 - 10c Select *Yes* or *No* to create all Novell Audit objects in the Logging Services container.
 Logging Services is the default container for all Novell Audit objects in eDirectory.
 If you select *No*, you must provide the name of an existing organizational unit in which AuditExt can create the Secure Logging Server and its associated objects.
- 11 Click *OK* to complete the installation.
- 12 Select *Yes* or *No* to reboot the server now.
You must reboot the server to load Novell Audit.

13 Click *Finish*.

When the server reboots, the Secure Logging Server automatically launches (the Startup Type for the Secure Logging Server Service is Automatic); however, you must manually load the eDirectory Instrumentation.

To load the Windows Instrumentation:

- 1** Go to *Control Panel > Administrative Tools > Services*.
- 2** Select the Novell Audit Windows Instrumentation.
- 3** Right-click and select *Properties*.
- 4** In the Properties dialog box, start the Novell Audit Windows Instrumentation Service:
 - 4a** To automatically load the Novell Audit Windows Instrumentation each time the server restarts, select *Automatic* in the *Startup type* drop-down list.
 - 4b** To manually load the Novell Audit Windows Instrumentation, click *Start*.
- 5** When finished, click *OK*.

To manually load or unload the eDirectory instrumentation:

- 1** Load `ndscons.exe`.
`ndscons.exe` is usually in the `\novell\nds` directory.
- 2** In the list of installed services, select *Novell 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 Audit Component*.
- 3** Click *Startup*.
- 4** Select the *Automatic* startup type and click *OK*.

On Windows, if you choose to only extend the schema, it automatically exits you from the installer; however, a Novell Audit entry is created in the Add/Remove Programs menu. To install, go to *Add Programs* and click *Modify* to launch the installer.

5.5 Activating Novell Audit

When you install the full version of Novell Audit, the license file is installed with the product and the product is automatically activated; that is, you can configure all the product channels and instrumentations.

If you install the Novell Audit Starter Pack and you want to upgrade to the full version without re-installing the product, you must purchase a product license.

NOTE: The Novell Audit Starter Pack is a scaled down version of Novell Audit. It allows you to configure the File, SMTP and MySQL channels along with the Windows and Log File Parser instrumentations. However, if you want to use any other channel or instrumentation, you must purchase a product license.

If you configure an unlicensed channel or instrumentation without a Novell Audit license, the Secure Logging Server (`lengine`) does not load. You must either remove or disable the channel or instrumentation to allow `lengine` to load.

When you purchase a license for the Novell Audit Starter Pack, you receive a license file with an `.nlf` extension. To activate the full version of Novell Audit, you must copy the license file to the directory that contains the Secure Logging Server program file, `lengine`.

The following table outlines the default `lengine` directory for each platform:

Table 5-1 *Default lengine Directory*

| Platform | Directory |
|----------|--|
| NetWare | <code>sys:\system\naudit.nlf</code> |
| Windows | <code>\program files\novell\nsure audit\audit.nlf</code> |
| Linux | <code>/opt/novell/audit/audit.nlf</code> |
| Solaris | <code>/opt/NOVLnaudit/audit.nlf</code> |

After you copy the license file to the `lengine` directory, you must restart the logging server. For instructions, see “[Secure Logging Server Startup Commands](#)”.

5.6 Activating Novell Audit Report

To activate Novell Audit Report (`lreport`):

- 1 In Novell Audit Report, click *File > Import*, then select *Application Schemata*.
- 2 Specify the IP address of your Novell Audit logging server, then select a language.

After you activate `lreport`, activation messages no longer appear in Novell Audit Report.

Installing the Novell Audit iManager Plug-In

6


The Novell Audit iManager plug-in package file is contained in the `add_ons\iManager_plugins` folder on the Novell Audit 2.0 Installation CD.

On Windows systems, the Novell Audit iManager plug-in package is automatically copied to the current iManager folder. On NetWare, Linux and Solaris systems, the plug-in is copied to the default iManager directory. If you have installed iManager to a different directory, you must copy the Novell Audit iManager plug-in package to the current iManager directory.

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

- [Section 6.1, “Install or Upgrade the iManager Plug-In,” on page 37](#)
- [Section 6.2, “Install or Upgrade the iManager Plug-In in Assigned Mode with Role-Based Services,” on page 38](#)

6.1 Install or Upgrade the iManager Plug-In

- 1 Log in to iManager.
- 2 Click the *Configure* button .
- 3 Under *Module Installation*, click *Available Novell Plug-in Modules*.
- 4 Click *New*, then browse for the `naudit.npm` file.

The `naudit.npm` module package is located in the `add_ons\iManager_plugins` directory on the Novell Audit Installation CD.

- 5 Click *OK*. You are returned to the Available Novell Plug-in Modules page.
- 6 Select the `naudit.npm` file, then click *Install*.

This install takes a few minutes.

- 7 Restart Tomcat.

| Platform | Restart Command |
|-----------------------|--|
| NetWare® 6.5 or later | Enter <code>TC4STOP</code> . Wait at least 1 minute, then enter <code>TOMCAT4</code> to start the service again. |
| Windows | Stop and start the Tomcat service. |
| Solaris | Enter <code>/etc/init.d/imgr stop</code> , then enter <code>/etc/init.d/imgr start</code> . |
| Linux | Enter <code>/etc/init.d/novell-tomcat4 stop</code> , then enter <code>/etc/init.d/novell-tomcat4 start</code> . |

Allow adequate time for Tomcat to fully initialize before attempting to launch iManager.


- 8 Restart Apache.
- 9 Log in to iManager.

- 10 Verify that the Auditing and Logging Role appears in the Roles and Tasks page.

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

IMPORTANT: To reinstall the Novell Audit plug-in (`naudit.npm`), you must first delete the `rbsModule` object for the plug-in from eDirectory™ using the *Module Configuration > Delete RBS Module* task.

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

- 1 Log into iManager as a Collection Owner.
- 2 Click the *Configure* button .
- 3 Click *iManager Configuration > Modules > Install* to install the `naudit.npm` module package.
- 4 Select the `naudit.npm` file to install.


The `naudit.npm` module package is located in the `add_ons\iManager_plugins` directory on the Novell Audit Installation CD.

This install takes a few minutes.

- 5 Restart Tomcat.

| Platform | Restart Command |
|----------------------|--|
| NetWare 6.5 or later | Enter <code>TC4\$STOP</code> . Wait at least 1 minute, then enter <code>TOMCAT4</code> to start the service again. |
| Windows | Stop and start the Tomcat service. |
| Solaris | Enter <code>/etc/init.d/imgr stop</code> , then enter <code>/etc/init.d/imgr start</code> . |
| Linux | Enter <code>/etc/init.d/novell-tomcat4 stop</code> , then enter <code>/etc/init.d/novell-tomcat4 start</code> . |

Allow adequate time for Tomcat to fully initialize before attempting to launch iManager.

- 6 Restart Apache.
- 7 Log in to iManager, then click the *Configure* button .
- 8 Select *Role-Based Services > RBS Configuration*.

The table on the 2.x Collections tabbed page displays any out-of-date modules.

- 9 To update, select the number listed in the Out-of-Date column for the Collection that contains the Novell Audit plug-in (`naudit.npm`).
iManager displays the Collection's list of outdated modules, including `naudit.npm`.
- 10 Select the *Novell Audit* plug-in, then click *Update* at the top of the table.

Configuring the Secure Logging Server

7

The Secure Logging Server manages the flow of information to and from the Novell® auditing system. 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.




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

The following sections review how to configure the Secure Logging Server and how to configure a system with multiple Secure Logging Servers:

- [Section 7.1, “Configuring the Secure Logging Server,” on page 39](#)
- [Section 7.2, “Configuring Multiple Secure Logging Servers,” on page 40](#)
- [Section 7.3, “Configuring a Secure Logging Server with More Than One IP Address,” on page 41](#)

7.1 Configuring the Secure Logging Server

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 *Auditing and Logging Role*, then select *Logging Server Options*.
- 4 Select the Secure Logging Server object, then click *OK*.
 - 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.

Server Configuration: Logging Server

General **Channels** **Notifications** **Log Applications**

Summary | Configuration | Memory | Status

This summary gives you an overview of how your Secure Logging Server is configured. If you wish to configure it you may select Channels, Notifications, Applications above, or you may use the [Secure Logging Server Interactive Configuration Guide](#) to be guided through the configuration process.

For detailed instructions on configuring the Secure logging Server, see “**Configuring the Secure Logging Server**” in the *Novell Audit 2.0 Administration Guide*.

- 6 To minimize server reaction time and ensure high system performance, we recommend that you create a local replica of the Logging Server object and its associated objects on the logging server.
- 7 After you have completed the Secure Logging Server configuration, restart your Secure Logging Server using the following commands:

| Platform | Command |
|----------|---|
| NetWare® | <code>unload lengine</code> <code>load lengine</code> |
| Windows | <ol style="list-style-type: none">1. Click <i>Start > Settings > Control Panel</i>.2. Open the Services window.<ul style="list-style-type: none">• On Windows NT*, select <i>Services</i>.• On Windows 2000 and XP, select <i>Administrative Tools > Services</i>.3. In the list of installed services, right-click <i>Novell Audit Manager</i>, then select <i>Stop</i>.4. Right-click <i>Novell Audit Manager</i>, then select <i>Start</i>. |
| Linux | <code>/etc/init.d/novell-naudit stop</code> <code>/etc/init.d/novell-naudit start</code> |
| Solaris | <code>/etc/init.d/naudit stop</code> <code>/etc/init.d/naudit start</code> |

7.2 Configuring Multiple Secure Logging Servers

By default, the installation program creates the Secure Logging Server in the Logging Services container. The logging server then reads its channel and notification configuration information from

the Channels.Logging Services and Notifications.Logging Services containers and loads the channels and notifications located within these containers.

If you want to provide system redundancy or load balancing in your logging system, you can create multiple Secure Logging Server objects for servers on the same platform in the default Logging Services container. In this way, all the logging servers load the same channels and send data to the same database.

However, if you want to log data to different databases (such as in a WAN environment); load different channels and notifications on each logging server; if you have an extremely large eDirectory™ tree; or if you are running Novell Audit Secure Logging servers on multiple platforms, we recommend that you create separate eDirectory organizational units as containers for each Secure Logging Server's configuration object.

If you want a combination of both configurations—for example, you want to provide system redundancy or load balancing in a WAN environment—you can create multiple eDirectory organizational units with multiple Secure Logging Server objects.

The following sections in the *Novell Audit 2.0 Administration Guide* review how to implement multiple Secure Logging Servers in your logging system based on whether you want to locate the Secure Logging Server objects in the same container, different containers, or a combination of both:

- “Creating Multiple Secure Logging Server Objects in a Single eDirectory Container”
- “Creating Secure Logging Server Objects in Different eDirectory Containers”
- “Creating Multiple Secure Logging Server Objects in Multiple eDirectory Containers”

7.3 Configuring a Secure Logging Server with More Than One IP Address

Secure Logging Servers with more than one IP address have problems running Novell Audit because MDB does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address using an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

Table 7-1 *MDB Configuration File*

| Platform | Directory |
|----------|------------------|
| NetWare | sys:\etc\mdb.cfg |
| Windows | \windows\mdb.cfg |
| Linux | /etc/mdb.conf |
| Solaris | /etc/mdb.conf |

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameter:

```
driver=mbds referral=eDirectory_IP_Address
```

For example,

```
driver=mdbds referral=192.168.123.45.
```

Configuring the Platform Agent and Logging Instrumentations

8

This section contains instructions on installing and configuring the Platform Agent and Instrumentations on servers that will report events to the Secure Logging Server.

- [Section 8.1, “Installing the Logging Components,” on page 43](#)
- [Section 8.2, “Configuring the Platform Agent,” on page 44](#)
- [Section 8.3, “Selecting Logged Events,” on page 45](#)

8.1 Installing the Logging Components

You must install the Platform Agent on every server that you want to report events to the Secure Logging Server. You must also install the Instrumentation associated with every logging application that you want to report events to Novell® Audit.

To install the logging components on servers that will report events to the Secure Logging Server:

- 1 Run the Novell Audit installation.

For specific instructions, see [Chapter 5, “Installing and Activating Novell Audit,” on page 23](#).

- 2 To install only the logging components, select the following install options:

| Platform | Install Option | Description |
|----------|--|--|
| NetWare® | Install Novell Audit Instrumentation Agents | <p>Installs the Platform Agent (<code>logevent.nlm</code>), the NetWare Instrumentation (<code>auditNW.nlm</code>), and the eDirectory Instrumentation (<code>auditDS.nlm</code>).</p> <p>These instrumentations must be installed on any NetWare server that you want to report eDirectory™, file system, or NetWare events.</p> <hr/> <p>IMPORTANT: Before you install the eDirectory instrumentation on NetWare, your server must be updated with the latest version of NCI. See Section 2.2.1, “NCI,” on page 13 for details.</p> |
| Linux | eDirectory Instrumentation Files with Platform Agent | <p>Installs the Platform Agent (<code>liblogevent.so</code>), the eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), and the Log Parser (<code>logparse</code>).</p> <p>The eDirectory instrumentation must be installed on any Linux server that you want to report eDirectory events.</p> |

| Platform | Install Option | Description |
|----------|--|--|
| Solaris | eDirectory Instrumentation Files with Platform Agent | <p>Installs the Platform Agent (<code>liblogevent.so</code>), the eDirectory Instrumentation (<code>libauditDS.so</code>), the Platform Agent (<code>liblogevent.so</code>), and the Log Parser (<code>logparse</code>).</p> <p>The eDirectory instrumentation must be installed on any Solaris server that you want to report eDirectory events.</p> |
| Windows | Instrumentation | <p>Installs the Platform Agent (<code>logevent.dll</code>), the eDirectory instrumentation (<code>auditDS.dlm</code>), the Windows Instrumentation (<code>nauditwin.exe</code>), and the Log Parser (<code>logparse.exe</code>).</p> <p>The eDirectory and Windows instrumentations must be installed on any Windows server that you want to report eDirectory and Windows events.</p> |

- 3** If you are installing the eDirectory Instrumentation on a server that is located in a different tree than your Secure Logging Server, you must also select one of the following install options to add the Novell Audit schema extensions to eDirectory:

| Platform | Install Option |
|-------------------------|-----------------------|
| NetWare | Add Schema Extensions |
| Linux, Solaris, Windows | Extend Schema |

If the eDirectory Instrumentation is located in the same tree as your Secure Logging Server, the schema is extended during the Secure Logging Server installation.

- 4** If you are upgrading from a previous version of Novell Audit and the installation finds an existing Platform Agent configuration file (`logevent.cfg` or `logevent.conf`), the installation asks if you want to overwrite the Platform Agent configuration file. Do not overwrite the existing file unless you want your Platform Agent to revert to the default configuration settings.
- 5** After the installation is complete, configure the Platform Agent on each server as explained in [Section 8.2, “Configuring the Platform Agent,” on page 44](#).

8.2 Configuring the Platform Agent

The Platform Agent, `logevent`, is the client portion of the Novell auditing system. The Platform Agent is required on any server that reports events to Novell Audit. It receives logging information and system requests from authenticated applications and transmits the information to the Secure Logging Server.

The Platform Agent’s configuration settings are stored in a simple, text-based configuration file (`logevent`). The default location of this file is as follows:

Table 8-1 Platform Agent Configuration File

| Operating System | File |
|---|---------------------------------|
| NetWare | /etc/logevent.cfg |
| Linux | /etc/logevent.conf |
| Solaris | /etc/logevent.conf |
| Windows | /windows_directory/logevent.cfg |
| The <i>windows_directory</i> is usually <i>drive:\windows</i> . | |

Storing the Platform Agent’s configuration in a local text file 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 following is a sample `logevent.cfg` file.

```
LogHost=127.0.0.1
LogCacheDir=c:\logcache
LogCachePort=288
LogEnginePort=289
LogCacheUnload=no
LogReconnectInterval=600
LogDebug=never
LogSigned=always
```

For detailed information on `logevent` parameters and the Platform Agent Configuration tool, see “Configuring the Platform Agent” in the *Novell Audit 2.0 Administration Guide*.

8.3 Selecting Logged Events

The Novell Audit logging instrumentations allow you to select which events you want to log to your data store. The following sections review how to configure specific logging Instrumentation’s events:

- [Section 8.3.1, “Configuring eDirectory Events,” on page 45](#)
- [Section 8.3.2, “Configuring NetWare and File System Events,” on page 46](#)
- [Section 8.3.4, “Configuring Windows Events,” on page 47](#)
- [Section 8.3.3, “Configuring Novell Audit Events,” on page 47](#)

8.3.1 Configuring eDirectory Events

The eDirectory Instrumentation for Novell Audit (`auditDS`) allows Novell Audit to log eDirectory events to the Novell Audit database. The eDirectory Instrumentation can log events from the following versions of the directory:

- eDirectory 8.7 (NetWare, Windows, Linux, and Solaris)
- eDirectory 8.8 (NetWare, Windows, Linux, and Solaris)

To log eDirectory events, the eDirectory Instrumentation must be loaded on every server where you want to log eDirectory events. For more information on the eDirectory Instrumentation, see “[eDirectory Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*.

After you have installed the eDirectory Instrumentation, you must determine which eDirectory events you want to log to your data store. For a listing of the eDirectory events that can be logged to Novell Audit, see “[eDirectory Events](#)” in the *Novell Audit 2.0 Administration Guide*.

In previous versions of Nsure™ Audit, the eDirectory events were configured on the NCP Server object. Therefore, administrators were required to configure every NCP Server object where they wanted to log eDirectory events.

Novell Audit 2.0 now allows administrators to create a global filter in the eDirectory Instrumentation object that determines which eDirectory events the Platform Agents send to the Secure Logging Server. However, administrators must still enable the eDirectory events on the NCP Server object.

The following sections review how to configure eDirectory events on both the NCP Server object and the eDirectory Instrumentation:

- “[Configuring eDirectory Events on the NCP Server Object](#)” in the *Novell Audit 2.0 Administration Guide*
- “[Configuring eDirectory Events in the eDirectory Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*

8.3.2 Configuring NetWare and File System Events

The NetWare Instrumentation for Novell Audit (`auditNW`) allows Novell Audit to log NetWare and file system events. The NetWare Instrumentation can log NetWare and file system events from NetWare 6.5.

To log NetWare or file system events, the NetWare Instrumentation must be loaded on every server where you want to log NetWare and file system events. For more information on the NetWare Instrumentation, see “[NetWare and File System Instrumentations](#)” in the *Novell Audit 2.0 Administration Guide*.

After you have installed the NetWare Instrumentation, you must determine which NetWare and file system events you want to log to the data store. For a listing of the NetWare and file system events that can be logged to Novell Audit, see “[NetWare Events](#)” and “[File System Events](#)” in the *Novell Audit 2.0 Administration Guide*.

In previous versions of Nsure Audit, the NetWare and file system events were configured on the NCP Server object. Therefore, administrators were required to configure every NCP Server object where they wanted to log NetWare or file system events.

Novell Audit 2.0 now allows administrators to create a global filter in the NetWare Instrumentation object that determines which NetWare and file system events the Platform Agents send to the Secure Logging Server. However, administrators must still enable the NetWare and file system events on the NCP Server object.

NOTE: If you want to filter events on a volume or directory level, you can create Notification filters that select events based on the volume or directory listed in the Text2 field.

The following sections review how to configure NetWare and file system events on both the NCP Server object and the NetWare Instrumentation:

- “[Configuring NetWare and File System Events on the NCP Server Object](#)” in the *Novell Audit 2.0 Administration Guide*
- “[Configuring NetWare and File System Events in the NetWare Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*

8.3.3 Configuring Novell Audit Events

The Novell Audit Instrumentation (NsureAuditInst) audits Novell Audit events. It is automatically installed with the Secure Logging Server to provide an “audit the auditor” event trail. By reviewing the Novell Audit Instrumentation events, you can determine if your logging server is performing the way you expect. For example, the Novell Audit Instrumentation can log an event every time the Secure Logging Server loads a Channel, Notification, or Application object. It can also log an event each time a Channel driver fails to load or when there is a bad Heartbeat or Notification configuration. For more information on the Novell Audit Instrumentation, see “[Novell Audit Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*.

The Novell Audit Instrumentation object in eDirectory allows you to manage which Novell Audit events are logged. For information on configuring the Novell Audit instrumentation, see “[Configuring Novell Audit Events](#)” in the *Novell Audit 2.0 Administration Guide*.

8.3.4 Configuring Windows Events

To log Windows events, the Windows Instrumentation (nauditwin) must be loaded on every server where you want to log Windows events. The Novell Audit Windows instrumentation runs as a service on Windows 2000, XP, and 2003. It collects events from the Event Viewer and sends them to the Secure Logging Server for processing by Novell Audit. For more information on the Windows Instrumentation, see “[Windows Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*.

The Windows Instrumentation object in eDirectory allows you to manage which Windows events the Platform Agents send to the Secure Logging Server. For information on configuring the Windows Instrumentation, see “[Configuring Windows Events](#)” in the *Novell Audit 2.0 Administration Guide*.

Verifying the Installation

9

After you have completed the instructions in this Installation Guide, you should have the following Novell® Audit components in your environment:

- A Secure Logging Server that is configured to log events to your data store, and send notifications to any additional channels you have configured.
- One or more Platform Agents and the Instrumentations required for the logging applications on each server that logs events to the Secure Logging Server. The Platform Agent on each system should be configured to report events to your Secure Logging Server and each Instrumentation should be configured to report the events you want to monitor.

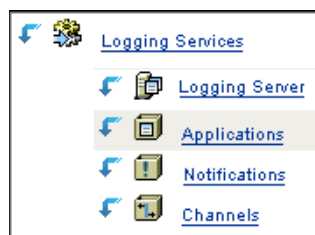
This section contains basic procedures and information to make sure these Novell Audit components are installed and working correctly.

- [Section 9.1, “eDirectory Objects,” on page 49](#)
- [Section 9.2, “Data Store,” on page 50](#)
- [Section 9.3, “Secure Logging Server,” on page 50](#)
- [Section 9.4, “Platform Agent and Logging Instrumentations,” on page 52](#)
- [Section 9.6, “Server and System Statistics,” on page 58](#)

9.1 eDirectory Objects

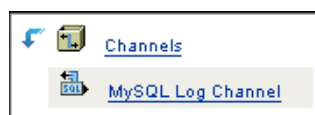
In eDirectory™, verify that you have a Logging Services container at the root of your tree with a Secure Logging Server object. The Logging Services container should also contain an Application, Notification, and Channel container.

Figure 9-1 *Logging Services Container in eDirectory*



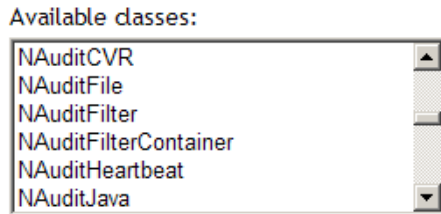
Within the Channel container, you should have a Channel object for your data store.

Figure 9-2 *Channel Container in eDirectory*



If any of these objects are missing, verify that the Novell Audit schema extensions are installed by using the *Schema > Class Information* task. In the class list, verify that the NAudit classes are present:

Figure 9-3 *Novell Audit Schema Class Information*



If these schema extensions are missing, run the AuditExt utility and select the *Add Schema Extensions* option. For a listing of the AuditExt startup commands, see “[AuditExt](#)” in the *Novell Audit 2.0 Administration Guide*.

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.

If you have not done this, follow the instructions in [Chapter 7, “Configuring the Secure Logging Server,”](#) on page 39.

9.2 Data Store

Make sure that your data store is running and is accessible to the Secure Logging Server.

9.3 Secure Logging Server

The Novell Audit Secure Logging Server should be running on your server. The following table outlines the startup commands for each platform:

IMPORTANT: You must individually start or stop each logging server in the tree.

Table 9-1 Secure Logging Server Startup Commands

| Platform | Startup Command |
|----------|--|
| NetWare® | <p><code>Lengine.nlm</code> should be running on the server hosting the Secure Logging Server. This is configured to load automatically at startup during install.</p> <p>To determine if <code>lengine.nlm</code> is loaded, enter <code>m lengine</code> at the NetWare command prompt. If <code>lengine</code> is not loaded, reload it and check the NetWare logger screen for any messages.</p> <p>To manually load the Secure Logging Server on NetWare, enter</p> <pre>load lengine</pre> <p>or</p> <pre>load auditsvr.ncf</pre> <p>If you want to prevent the Secure Logging Server from being unloaded by users with access to the server console, you can append the <code>-n</code> switch to the server startup script. (For example, <code>load lengine -n</code>.)</p> <p>To manually unload the Secure Logging Server on NetWare, enter</p> <pre>unload lengine</pre> <hr/> <p>NOTE: <code>Lengine.nlm</code> and <code>auditsvr.ncf</code> are located in the <code>sys:\system</code> directory.</p> <hr/> |
| Linux | <p>To verify that the Secure Logging Server is running, use the following command:</p> <pre>ps -ef grep lengine</pre> <p>The Linux startup script for the Secure Logging Server is <code>/etc/init.d/novell-naudit</code>. This startup script loads <code>lengine</code> each time the server restarts.</p> <p>To manually start the Secure Logging Server on Linux, enter</p> <pre>/etc/init.d/novell-naudit start</pre> <p>To stop the Secure Logging Server on Linux, enter</p> <pre>/etc/init.d/novell-naudit stop</pre> |
| Solaris | <p>To verify that the Secure Logging Server is running, use the following command:</p> <pre>ps -ef grep lengine</pre> <p>On Solaris, the startup script for the Secure Logging Server is <code>/etc/init.d/naudit</code>. This startup script loads <code>lengine</code> each time the server restarts.</p> <p>To manually start the Secure Logging Server on Solaris, enter</p> <pre>/etc/init.d/naudit start</pre> <p>To stop the Secure Logging Server on Solaris, enter</p> <pre>/etc/init.d/naudit stop</pre> |

| Platform | Startup Command |
|----------|---|
| Windows | <p>To determine if the Novell Audit Manager service is running, open the Services applet from <i>Control Panel > Administrative Tools</i>.</p> <p>On Windows, the startup script for the Secure Logging Server is included in the <code>naudit.exe</code> file. <code>Naudit.exe</code> has an Automatic startup type so <code>lengine.exe</code> loads each time the server restarts.</p> <p>To manually load or unload the Secure Logging Server on Windows, you must start or stop the Novell Audit Manager service:</p> <ol style="list-style-type: none"> 1. Click <i>Start > Settings > Control Panel</i>. 2. Open the Services window. <ul style="list-style-type: none"> • On Window NT, select <i>Services</i>. • On Windows 2000 and XP, select <i>Administrative Tools > Services</i>. 3. In the list of installed services, right-click <i>Novell Audit Manager</i>, then select <i>Start</i> or <i>Stop</i>. |

For more information on the Secure Logging Server, see [Chapter 7, “Configuring the Secure Logging Server,” on page 39](#) and “Configuring the Secure Logging Server” in the *Novell Audit 2.0 Administration Guide*.

9.4 Platform Agent and Logging Instrumentations

You must install the Platform Agent on every server that you want to report events to the Secure Logging Server. You must also install the Instrumentation associated with every logging application that you want to report events to Novell Audit. This section reviews how to verify you are running the Platform Agent and Instrumentations required to log events to the Secure Logging Server:

- [Section 9.4.1, “Platform Agent,” on page 52](#)
- [Section 9.4.2, “NetWare and eDirectory Instrumentations,” on page 53](#)
- [Section 9.4.3, “Windows Instrumentation,” on page 55](#)
- [Section 9.4.4, “Novell Audit Instrumentation,” on page 56](#)
- [Section 9.4.5, “Log Parser Instrumentation,” on page 56](#)

9.4.1 Platform Agent

Each logging application requires a Platform Agent to send events to the Secure Logging Server. Consequently, each logging application’s associated Instrumentation automatically loads the Platform Agent.

The following table outlines commands you can use to verify that the Platform Agent is loaded:

NOTE: In some cases, it might be possible that the Platform Agent is available when `lcache` is not running. The `lcache` process is started by the Platform Agent when an instrumentation attempts to send an event. In the unlikely event that none of the instrumentations are sending events to the Platform Agent, `lcache` will not be running; however, the Platform Agent will still be available.

Table 9-2 *Commands Used to Verify the Platform Agent is Loaded*

| Operating System | Command |
|------------------|---|
| NetWare | To determine if <code>logevent.nlm</code> is loaded on NetWare, enter <code>m logevent</code> at the NetWare command prompt. If <code>logevent.nlm</code> is not loaded, reload it and check the NetWare logger screen for any messages. |
| Linux/Solaris | To verify that the Platform Agent is running on Linux or Solaris, use the following command: <code>ps -ef grep lcache</code> |
| Windows | To determine if the Platform Agent is running on Windows, open <i>Task Manager</i> and verify that <code>lcache.exe</code> is running. |

You can view all Platform Agents connected to the Secure Logging Server in the Secure Logging Server *Monitor* page. For more information, see [Section 9.6, “Server and System Statistics,” on page 58](#).

For more information on the Platform Agent, see “[Configuring the Platform Agent](#)” in the *Novell Audit 2.0 Administration Guide*

9.4.2 NetWare and eDirectory Instrumentations

The NetWare and eDirectory Instrumentations for Novell Audit (`auditNW` and `auditDS`, respectively) allow Novell Audit to log NetWare, eDirectory, and file system events.

To enable NetWare and file system logging, `auditNW` must be loaded on every server where you want to log NetWare and file system events. Additionally, the Platform Agent must be installed on every server where you want to log NetWare, file system, and eDirectory events. `auditNW` and `auditDS` automatically load the Platform Agent (`logevent`) to send events to the Secure Logging Server.

NOTE: Before the Platform Agents are launched, the `LogHost` parameter in the Platform Agent configuration file on each server must be updated with the IP address or DNS name of your Secure Logging Server. For more information, see “[Configuring the Platform Agent](#)” in the *Novell Audit 2.0 Administration Guide*.

Typically, `auditNW` and `auditDS` are automatically loaded each time the server restarts. However, you can also manually load or unload the instrumentation files.

The following table reviews the startup commands for the eDirectory and NetWare Instrumentations.

IMPORTANT: You must individually start or stop the instrumentations on each server in the tree.

Table 9-3 *NetWare and eDirectory Instrumentation Startup Commands*

| Platform | Startup Command |
|----------|--|
| NetWare | <p>On NetWare, the startup scripts for <code>auditNW</code> and <code>auditDS</code> are included in the <code>auditagt.ncf</code> file. <code>Auditagt.ncf</code> is added to the server's <code>autoexec.ncf</code> file during installation. Therefore, the NetWare and eDirectory Instrumentations automatically load each time the server restarts.</p> <p>If you want to prevent <code>auditNW</code> or <code>auditDS</code> from being unloaded by users with access to the server console, you can append the <code>-n</code> switch to the agent startup scripts. (For example, <code>load auditnw -n</code>.)</p> <p>To manually start the NetWare or eDirectory Instrumentation on NetWare, enter</p> <pre>load auditnw</pre> <p>or</p> <pre>load auditDS</pre> <p>To load both the NetWare and eDirectory Instrumentations, enter</p> <pre>load auditagt.ncf</pre> <p>To stop the NetWare and eDirectory Instrumentations on NetWare, enter</p> <pre>unload auditnw</pre> <pre>unload auditDS</pre> <hr/> <p>NOTE: <code>Auditnw.nlm</code>, <code>audit.ds</code>, and <code>auditagt.ncf</code> are located in the <code>sys:\system</code> directory.</p> <hr/> |
| Linux | <p>On Linux systems, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually start the eDirectory Instrumentation on Linux, enter</p> <pre>ndstrace -c "load auditDS"</pre> <p>To manually stop the eDirectory Instrumentation on Linux, enter</p> <pre>ndstrace -c "unload auditDS"</pre> <p>To automatically load the eDirectory Instrumentation each time the server restarts, add the following to the <code>ndsmodules.conf</code> file:</p> <pre>auditDS auto #NSure Audit Platform Agent</pre> <hr/> <p>NOTE: On eDirectory 8.7, the path to the <code>ndsmodules.conf</code> file is <code>/usr/lib/nds-modules/ndsmodules.conf</code>. On eDirectory 8.8, the path is <code>/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf</code>.</p> <hr/> <p>On Linux systems, the startup script is <code>/etc/init.d/novell-naudit</code>.</p> <hr/> |

| Platform | Startup Command |
|----------|---|
| Solaris | <p>On Solaris systems, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually start the eDirectory Instrumentation on Solaris, enter</p> <pre>ndstrace -c "load auditDS"</pre> <p>To manually stop the eDirectory Instrumentation on Solaris, enter</p> <pre>ndstrace -c "unload auditDS"</pre> <p>To automatically load the eDirectory Instrumentation each time the server restarts, add the following to the <code>/usr/lib/nds-modules/ndsmodules.conf</code> file:</p> <pre>auditDS auto #NSure Audit Platform Agent</pre> <hr/> <p>NOTE: On eDirectory 8.7, the path to the <code>ndsmodules.conf</code> file is <code>/usr/lib/nds-modules/ndsmodules.conf</code>. On eDirectory 8.8, the path is <code>/etc/opt/novell/eDirectory/nds-modules/ndsmodules.conf</code>.</p> <hr/> <p>On Solaris systems, the startup script is <code>/etc/init.d/naudit</code>.</p> |
| Windows | <p>On Windows, the eDirectory Instrumentation is managed through the Novell eDirectory Services utility. By default, the eDirectory Instrumentation must be manually loaded on one server per DS Replica.</p> <p>To manually load or unload the eDirectory Instrumentation on Windows:</p> <ol style="list-style-type: none"> 1. Load <code>ndscons.exe</code>. <p><code>Ndscons.exe</code> is usually in the <code>\novell\nds\</code> directory.</p> 2. In the list of installed services, select the <i>Novell Audit Component</i>. 3. Click <i>Start</i> or <i>Stop</i>. <p>To configure <code>auditDS.dlm</code> to load each time the server restarts:</p> <ol style="list-style-type: none"> 1. Load <code>ndscons.exe</code>. <p><code>Ndscons.exe</code> is usually in the <code>\novell\nds\</code> directory.</p> 2. In the list of installed services, select the <i>Novell Audit Component</i>. 3. Click <i>Startup</i>. 4. Select the <i>Automatic</i> startup type, then click <i>OK</i>. |

For more information on the eDirectory and NetWare Instrumentations, see “[eDirectory Instrumentation](#)” and “[NetWare and File System Instrumentations](#)” in the *Novell Audit 2.0 Administration Guide*.

9.4.3 Windows Instrumentation

The Novell Audit Windows instrumentation, `nauditwin.exe`, runs as a service on Windows 2000, XP, and 2003. The Novell Audit Windows instrumentation collects events from the Event Viewer and sends them to the Secure Logging Server for processing by Novell Audit.

To enable logging of Windows events, the Windows Instrumentation must be loaded on every server where you want to log Windows events. Additionally, the Platform Agent (`logevent`) must be

installed on every server where you want to log Windows events. `Nauditwin.exe` automatically loads the Platform Agent to send events to the Secure Logging Server.

NOTE: Before the Platform Agents are launched, the `LogHost` parameter in the Platform Agent configuration file on each server must be updated with the IP address or DNS name of your Secure Logging Server. For more information, see [Section 8.2, “Configuring the Platform Agent,” on page 44](#).

Typically, `nauditwin.exe` is automatically loaded each time the server restarts. However, you can also manually load or unload the instrumentation through Windows Services.

To manually load or unload the Windows Instrumentation, you must start or stop the Novell Audit Windows Instrumentation service:

- 1 Click *Start > Settings > Control Panel*.
- 2 Open the Services window.
 - On Windows NT, select *Services*.
 - On Windows 2000 and XP, select *Administrative Tools > Services*.
- 3 In the list of installed services, right-click *Novell Audit Windows Instrumentation*, then select *Start* or *Stop*.

For more information on the Windows Instrumentation, see “[Windows Instrumentation](#)” in the [Novell Audit 2.0 Administration Guide](#)

9.4.4 Novell Audit Instrumentation

The Novell Audit Instrumentation (`NsureAuditInst`) logs an event every time the Secure Logging Server loads a Channel, Notification, or Application object. It also logs an event each time a Channel driver fails to load or if there is a bad Heartbeat or Notification configuration. Therefore, by reviewing your system’s Audit the Auditor events, you can determine if your logging server is performing the way you expect.

The Novell Audit Instrumentation automatically loads with the Secure Logging Server. We do not recommend that you unload the Novell Audit Instrumentation.

For more information about the Novell Audit instrumentation, see the following sections in the [Novell Audit 2.0 Administration Guide](#):

- “[Novell Audit Instrumentation](#)”
- “[Verifying the Secure Logging Server Configuration](#)”
- “[Novell Audit Events](#)”

9.4.5 Log Parser Instrumentation

The Log Parser Instrumentation, `logparse`, harvests events from Windows text-based log files such as `syslog`, Apache error logs, and Novell Application Launcher™ logs. Events are parsed one line at a time and formatted in the Novell Audit event structure. Parsing text-based log files allows Novell Audit to process and log events from applications that are not currently instrumented for Novell Audit.

The Log Parser Instrumentation must be manually loaded or unloaded. The following table reviews the Log Parser Instrumentation startup commands.

Table 9-4 *Log Parser Instrumentation Startup Commands*

| Platform | Startup Command |
|----------|---|
| NetWare | <p>To manually start the Log Parser Instrumentation on NetWare, enter</p> <pre>load logparse</pre> <p>To stop the Log Parser Instrumentations on NetWare, enter</p> <pre>unload logparse</pre> <p>logparse.nlm is located in the sys:\system directory.</p> <hr/> <p>NOTE: You can add logparse to the auditagt.ncf file to automatically load the Log Parser Instrumentations each time the server restarts.</p> <hr/> |
| Linux | <p>To manually start the Log Parser Instrumentation on Linux, go to the /opt/novell/naudit/ directory and enter</p> <pre>./logparse &</pre> <p>To manually stop the Log Parser Instrumentation on Linux, enter</p> <pre>pkill logparse</pre> |
| Solaris | <p>To manually start the Log Parser Instrumentation on Solaris, go to the opt/NOVLnaudit/ directory and enter</p> <pre>./logparse &</pre> <p>To manually stop the Log Parser Instrumentation on Solaris, enter</p> <pre>pkill logparse</pre> |
| Windows | <p>To manually load or unload the Log Parser Instrumentation on Windows, you must start or stop the Novell Audit Log Parser Instrumentation service:</p> <ol style="list-style-type: none">1. Click <i>Start > Settings > Control Panel</i>.2. Open the Services window.<ul style="list-style-type: none">• On Window NT, select <i>Services</i>.• On Windows 2000 and XP, select <i>Administrative Tools > Services</i>.3. In the list of installed services, right-click <i>Novell Audit Log Parser Instrumentation</i>, then select <i>Start</i> or <i>Stop</i>. |

For more information about the Log Parser Instrumentation and parsing text logs, see “[Log Parser Instrumentation](#)” in the *Novell Audit 2.0 Administration Guide*.

9.5 Verifying Event Logging

The final step in testing is verifying that your data store 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 data store by running queries in

iManager or Novell Audit Report (LReport). For more information, see “[Generating Queries and Reports](#)” in the *Novell Audit 2.0 Administration Guide*.

9.6 Server and System Statistics

The Monitor channel provides logging system statistics in iManager. When the Monitor Channel object is enabled, each Secure Logging Server object includes the Monitor tab as one of its Logging Server Options. For more information, see “[Monitor](#)” in the *Novell Audit 2.0 Administration Guide*.

The Monitor screen provides two statistics pages: *Server* and *System*.

The *Monitor Server* page lists the total number of events logged over the current server uptime and the average number of events logged per second. The number of events logged per second is averaged over a three-second interval.

The *Monitor System* page lists the IP addresses and descriptions of the Platform Agents currently logging events to the current Secure Logging Server, the applications logging events to each agent, and the events logged by each agent. These statistics reflect events logged over the life of the server, not the server uptime.

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.

For detailed information on all the options in the Secure Logging Server Monitor tab, see “[Logging Server Statistics](#)” in the *Novell Audit 2.0 Administration Guide*.