Novell Audit 2.0.2 Readme

August 28, 2008

1 Supported Platforms

The following sections review the supported platforms for the Novell® Audit components.

1.1 Secure Logging Server

- Open Enterprise Server 1.0 SP1 or later (NetWare® and Linux*)
- NetWare 6.5
- Windows* Server* 2003
- Windows Server 2000 SP4 or later
- SUSE® Linux Enterprise Server (SLES) 9 and 10 (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode)
- Red Hat* Linux 3 and 4 AS and ES (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode)
- 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` indicates `Failed SSL Handshake`.

1.2 Platform Agent

- Open Enterprise Server 1.0 SP1 or later (NetWare and Linux)

- NetWare 6.5
- Windows 2000
- Windows Server 2000 SP4 or later
- Windows XP Professional and Home Editions
- Windows Server 2003
- SUSE Linux Enterprise Server 9 and 10 (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode)
- Red Hat* Linux 3 and 4 AS and ES (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode)
- Solaris 8, 9, and 10

1.3 eDirectory Instrumentation

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

1.4 NetWare Instrumentation

- NetWare 6.5
- OES NetWare

1.5 Windows Instrumentation

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

1.6 Log Parser Instrumentation

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

2 Known Limitations

The following issues have been identified for this release of Novell Audit.

2.1 Linux Installation

During installation on some SUSE systems, the installation script quits immediately after extending the schema and configuring the log server. If this occurs, run the `pinstall.lin` script again. When the schema extension tool appears, exit immediately and the rest of the install script will finish.

2.2 Platform Agent Upgrade on Windows

A problem has been found in the Windows *Platform Agent Only* install. It only affects developers installing the agent libraries for development purposes as an upgrade to the 1.0.3 product on Windows platforms. The installation program sees that versions of `lcache.exe` and `logevent.dll` are present and does not handle updating them. To work around this problem, either remove these files from the `\windows\system32` directory or rename them so the new versions of these files are installed.

2.3 jmsSamples.jar File

This product release contains a sample file (`jmsSamples.jar`) that can be used to verify JMS Producer-to-Consumer communications. The Java* classes in this file perform a minimal number of functionality checks. Some users might find that these minimal tests do not sufficiently test their JMS configuration in conjunction with Novell Audit.

An updated `jmsSamples.jar` file will be released with the Novell Audit 2.0 SDK (http://developer.novell.com/wiki/index.php/Category:Novell_Developer_Kit#Download).

JMS testing procedures and a JMS Consumer design framework will also be documented in the SDK.

2.4 JDBC Libraries

Currently, the help system states that Novell Audit automatically installs all required `.jar` files with the iManager plug-in. This is incorrect. Before you create a JDBC Channel object, you must manually copy all required JDBC* libraries (`*.jar`) to the following iManager class paths on your iManager server:

- **NetWare:** `sys:\tomcat\4\common\lib`
- **Linux and Solaris:** `/var/opt/novell/tomcat4/common/lib`
- **Windows:** `c:\program files\novell\tomcat\common\lib`

2.5 JDBC Channel on NetWare

The JDBC channel does not load on NetWare if the MySQL* `.jar` filename is too long.

The error reported to the NetWare logger screen is as follows:

```
LGDJava: [INFO] using classpath
-Djava.class.path=;SYS:/SYSTEM/NAUDIT;SYS:/SYSTEM/NAUDIT.LogEvent.jar;..."
```

Each supported `.jar` file is listed in the error message. If the MySQL `.jar` file is not listed, rename the `.jar` file with a shorter filename and restart `lengine`.

2.6 Unable to Unload lengine

When `lengine` receives events from the logging system's Platform Agents, it sends the events to its log and notification channels. If it is unable to log those events to a given channel (for example, the database is unavailable or SMTP server is down), `lengine` queues the events in system memory until the channel becomes available.

When lengine has queued events, it does not unload from memory until the events are written to the configured channels. If an unavailable channel comes back online, lengine processes its queued events and can be cleanly shut down. If a channel is permanently unavailable, the server continues to function, but the command line is unavailable and it might not be possible to cleanly unload lengine. You might need to power down the server or break into the debugger and exit the OS to unload lengine. If you force the server to unload lengine by using one of these "non-clean" methods, data is lost.

2.7 SecretStore

Novell SecretStore® is integrated with eDirectory 8.8.x and is not a separate product as in previous versions of eDirectory.

SecretStore support is limited to the Windows and NetWare Platform Agents. It is not supported on Linux or UNIX* Platform Agents.

2.8 SLES 10 hosts File

SLES 10 includes two localhost entries in the `/etc/hosts` file: 127.0.0.1 and 127.0.0.2 . To run Novell Audit 2.0 on SLES 10, comment or remove the 127.0.0.2 localhost entry.

2.9 Unloading NDSD on Linux and Solaris

If you unload NDSD and restart it on Linux or Solaris, the Monitor channel might not work properly. If you restart NDSD on several servers simultaneously, lengine might core dump. To avoid potential problems, unload and restart `lengine` anytime you unload NDSD.

2.10 GLIBC Errors Running Logparse on Red Hat Enterprise Server 3

Logparse does not work on Red Hat Enterprise Server 3 because of a GLIBC incompatibility. For more information and possible solutions, see Technical Information Document 3922323 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3922323&sliceId=SAL_Public&dialogID=12954363&stateId=0%200%2012956903).

2.11 Managing the Cache File Size

The maximum cache file size is 2 GB, but you can set a smaller cache file size with the LogMaxCacheSize setting in `logevent.cfg`. By default, when the cache file size reaches 2 GB Novell Audit deletes the current cache file and creates a new one to continue caching.

If desired, you can change this behavior by setting `LogCacheLimitAction=stop logging` in `logevent.cfg`, which stops Novell Audit from logging new events until all old events are uploaded to the SLS.

3 Caveats

The following issues are working as designed. The administrator should be aware of these issues when configuring Novell Audit 2.0.

3.1 Server Won't Load

If you are using an unlicensed server and you have configured any channels other than File, MySQL, or SMTP, the Secure Logging Server automatically unloads and logs an unlicensed warning in `nproduct.log`. If you do not have a licensed server and the Secure Logging Server (`lengine`) does not stay loaded, determine if you have any channels that require a license.

3.2 Notification Channels

Do not attempt to send notifications to the Monitor Channel. There is no way to retrieve specific events from the Monitor; therefore, the notification event cannot be reported.

3.3 Potential Server Abend on NetWare

When hosting the Novell Audit data store on a NetWare server, ensure that you have sufficient disk space on your file server to handle the amount of data that will be committed to your database. If you host the database on a NetWare volume and the volume runs out of disk space, you run the risk of abending your server.

3.4 lengine Fails to Run Properly when Renaming the Current Auditlog File

Do not edit the auditlog file with vi while Novell Audit (lengine) writes to it. Instead, use `tail`, `less`, or `more` to view the contents of `auditlog`. `Auditlog` should be opened only in read-only mode.

3.5 Platform Agent Does Not Connect to LCache

The Platform Agent waits 30 seconds for the LCache process to start. If LCache doesn't start within 30 seconds, the Platform Agent writes the following message to the `nproduct.log` file and stops attempting to connect to LCache.

```
[Novell Audit Platform Agent]: Failed to connect to cache for application
<Application Name>, DISABLING cache mode.
```

If you encounter this problem, you have two options:

- Start the LCache process manually before starting any Instrumentation Applications. You can start LCache manually with the following command:

  ```
  /opt/novell/naudit/lcache &
  ```

- Reduce the cache file size. To do this, reduce the value for the LogMaxCacheSize parameter in the `logevent.conf` file.

4 Support Resources and Updates

- Support (http://www.novell.com/support)
- Documentation (http://www.novell.com/documentation/novellaudit20/index.html)
- Product Information (http://www.novell.com/products/audit)
- Updates (http://support.novell.com/filefinder).

5 Documentation

The following sources provide information about Novell Audit 2.0.2:

- Installation: *Novell Audit Installation Guide* (http://www.novell.com/documentation/novellaudit20/install/data/bktitle.html)
- Online product documentation: *Novell Audit Administration Guide* (http://www.novell.com/documentation/novellaudit20/index.html)

6 Documentation Conventions

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

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

7 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.

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.

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

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