Novell Identity Audit

These are the release notes for Identity Audit 1.0.

1.0 Documentation

The following sources on the Novell documentation web site provide information about Novell® Identity Audit 1.0:

- Identity Audit 1.0 Guide: Installation, Usage, and Maintenance:
- Product guides for supported Novell identity and security applications

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

3.0 Product Overview

Novell Identity Audit 1.0 is an easy to use, lightweight tool for collecting, aggregating and storing events from Novell Identity Manager, Novell Access Manager, Novell eDirectory, and other Novell identity and security products and technologies. Key features include:

- Web-based administration and reporting interfaces
- Full-event search tool allows searches across multiple event fields
- Selected event output to several channels
- Embedded Jasper Reports engine to allow the use of open source tools for customizing included reports or creating new reports
- Built-in database to eliminate the need for external database licenses or administration
- Simple, intuitive data management tools

3.1 Comparison to Novell Audit 2.0.2

Novell Identity Audit 1.0 is designed as a replacement product for the Novell Audit product line, which leaves general support in February 2009. Identity Audit is comparable in functionality, but with major improvements in architecture, reporting, and data management. Novell Identity Audit 1.0 is a drop-in replacement for the Novell Audit 2.0.2 Secure Logging Server for products in the Novell Identity and Security product line. Because Novell Identity Audit uses a new embedded database, customers should keep existing Novell Audit events in the archived Novell Audit database rather than attempting to migrate legacy data.

The Novell Audit client component, also known as the Platform Agent, is still used as the data transport mechanism for Novell Identity Audit. This will continue to be supported according to the lifecycles of Novell Identity and Access Management products that still use the Platform Agent.

3.2 Comparison to Novell Sentinel

Novell Identity Audit is built on a robust technological foundation, as much of the underlying code is shared with Novell Sentinel. However, Sentinel collects data from a broader range of devices, supports a higher event rate, and provides more tools than Novell Identity Audit. Sentinel provides additional Security Information and Event Management (SIEM) features, such as real-time dashboards, multi-event correlation, incident tracking and automated remediation, and data collection from non-Novell products. Identity Audit is designed to integrate into a future Sentinel deployment.

Novell Identity Audit 1.0 is not part of the Novell Compliance Management Platform (CMP), and does not include the advanced identity and security integration features delivered in that platform. Sentinel 6.1 is presently the identity audit and monitoring component of the CMP.

4.0 Supported Platforms

Identity Audit 1.0 is certified to run on 64-bit SuSE Linux Enterprise Server 10 SP1 and SP2. It collects data from the following applications:

- Novell Access Manager
- Novell eDirectory
- Novell Identity Manager
- Novell NMAS
- Novell SecretStore
- Novell SecureLogin

For version information about supported event sources, Audit Platform Agent, and browsers, see the Identity Audit product documentation at the Novell documentation Web site

5.0 Installing Novell Identity Audit

The Identity Audit installation package installs everything you need to run Identity Audit: the Identity Audit application and message bus, the database to store events and configuration information, the web-based user interface, and the reporting server. A simple installation as root is described here. There is also a multi-step installation procedure that uses root as little as possible, which is described in the main product documentation.

5.1 Quick Installation (as root)

This simple installation must be run as root.

1. Log in as root to the server where you want to install Identity Audit.
2. Download or copy `identity_audit_1.0_x86-64.tar.gz` to a temporary directory.
3. Change to the temporary directory (if necessary).
4. Extract the install script from the file using the following command:

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup
   ```

5. Run the `root_install_all.sh` script with root privileges.

   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```

NOTE: You can log in as root and run the command above or use the `sudo` command to run the command.

6. Choose a language by entering a number.

   The end user license agreement displays in the selected language.

7. Read the end user license and enter `1` or `y` if you agree to the terms and want to continue installation.

   The installation begins. If the previously selected language is not available for the installer (for example, Polish), the installer will continue in English.

8. The novell user and novell group are created, if they do not already exist.

9. Enter the password for database administrator (dbauser).

10. Confirm the password for database administrator (dbauser).

11. Enter the password for the admin user.

12. Confirm the password for the admin user.

13. The dbauser credentials are used to create tables and partitions in the PostgreSQL dat abase.

14. Identity Audit is configured to start up with runtime levels 3 and 5 (Multi-User Mode with boot-up in console or X-Windows mode).

After the Identity Audit service starts, you can log in to the URL specified in the in stallation outputhttps://hostIP:8443/novellidentityaudit.The system will start processing internal audit events immediately, and it will be fu lly functional after you configure event sources to send data to Identity Audit.

5.2 Configuring Event Sources

Refer to the individual event source documentation for information about how to config ure auditing levels for each Novell application on the available platforms.

5.3 Logging into Identity Audit

The administrative user created during the install can log into the Identity Audit app lication and create more users, run preloaded reports, upload new reports, perform event searches, and more. Even before the event s ources are configured, it is possible to log in and view system events from Identity Audit.

To log into Identity Audit:

1. Open a supported Web browser.

2. Go to the Identity Audit login page.

3. If this is the first time you have logged into Identity Audit, you will be presented with a certificate. You must accept it to proceed.

4. Enter `admin`.

5. Enter the admin password you configured during installation.

6. Select the language for the Identity Audit interface.

7. Click *Login*.

6.0 Known Issues

The known issues for Identity Audit are in the Release Notes posted at the Novell documentation Web site.

6.1 General Issues

These issues are known issues that are not assigned a bug number.

- When the PostgreSQL connection is configured to use SSL, the JBDC connection experienc es fatal errors and communication with the database hangs. Therefore, SSL is disabled by default.

- The Daily, Weekly, Monthly, and Prior Day reports are based on the local time of the Identity Audit server. The reports that use Custom Date Range and the user explicitly selects a start time and end time use the lo cal browser time.

- There is a 1K size limit on events sent to syslog (including the message header). Long er messages will be truncated.
- If more than one Tomcat server is installed on the Identity Audit server, they must be configured to use different ports. The default ports are 8080, 8443, and 8005.

6.2 Installation Issues

This issue relates to installation.

- The localized documentation includes the following command in the Quick Installation (as root) procedure:

```
tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
```

This command only provides access to English installer. To run the installer in other languages, run the following command instead:

```
tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup
```

6.3 Audit Connection Issues

These issues are related to the connection made between Identity Audit and the event s ources and the Collection part of the Identity Audit interface.

CON-285:
When the Audit Platform agent loses connection to the Sentinel box, the event source s hows as disconnected. However, when it reconnects, the event source status may not change back to healthy. You can verify tha t events are coming into the system by viewing the event rate (eps) on the Collection Health page.

SCT-200:
When the Audit Server is turned off, all events stop coming into the Identity Audit sy stem. However, the individual event source states do not change status and therefore may be “green” even though no data is being receive d. The Audit Server must be on in order to receive data.

CON-309: Turning the Audit Server off on the *Collection* page may generate a SocketException error in the log files even though the server is working properly.

CON-312:
When more than one Novell identity or security application is installed on a machine a nd one or more applications loses connection to Identity Audit, the health status for all applications may not be reported correctly. The `netstat` command may be used to verify connection status, and the event rate (eps) on the Collection Health page shows whethe r data is being received by Identity Audit.

SCT-187: Identity Audit does not collect or process log event that uses double-byte characters .

6.4 Reporting Issues

These issues relate to running and displaying reports.

SCT-184:
Identity Audit may experience out of memory errors (java.lang.OutOfMemoryError: PermGe n space) when many reports are run at once. The workaround is to schedule commonly requested reports to be run during hours when a ctivity is low.

SCT-195:
Identity Audit does not validate the Date Range for a report and require that a user s et the beginning time for a report before the end time for the report.

SCT-220:
Using the File > Save As to save a report PDF does not work as expected in some browse rs. The workaround in Firefox 2 is to choose File > Save As and then enter a filename including a .pdf extension. The workaround in Firefox 3 instead of using File > Save As is to use the Save Copy button, which is part of the Adobe Acrobat embedded controls.

SCT-250:
When a report result set is extremely large, the time required to generate the results PDF may exceed the web server time-out and the browser shows a 500 error. The workaround is to extend the sync time-out used by the T omcat server by editing the `bin/setenv.sh` script by adding the following line at end of the file to increase the time-out to 180 seconds (or more). Restart the Identity Audit server when you are done.

```
export CATALINA_OPTS=-Desecurity.remote.timeout=180
```

7.0 Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or us e of this documentation, and specifically disclaims