Novell Sentinel Log Manager 1.2 Release Notes

February 2011

Novell

Novell Sentinel Log Manager collects log data from a wide variety of devyices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources. Novell Sentinel Log Manager provides high event-rate processing, long-term data retention, regional data aggregation, and simple searching and reporting functionality for a broad range of applications and devices.

1 What’s New

1.1 Enhancements to Licenses

The Sentinel Log Manager default license now allows you to use all the features of Sentinel Log Manager, except for the Data Restoration feature, with an unrestricted EPS for up to 60 days. After 60 days the features are disabled, but the system continues to run with the base license key that enables a limited set of features and limited event rate of 25 EPS. The base license key does not expire.

NOTE: All the functionality, including Data Restoration and the ability to view all events, can be restored by upgrading the system to an enterprise license of Sentinel Log Manager.

For more information, see “Managing License Keys” (http://www.novell.com/documentation/novelllogmanager12/log_manager_admin/data/bl5gses.html) in the *Sentinel Log Manager 1.2 Administration Guide*.

1.2 Additional Tags

Sentinel Log Manager now includes the following tags:

- “OverEPSLimit Tag” on page 2
- “CreatedDuringEval Tag” on page 2

1.2.1 OverEPSLimit Tag

On systems that are running with the free license, all events that are received while the system averages more than 25 EPS are tagged with the `OverEPSLimit` tag. The details of these events are not accessible by search nor reports until you upgrade the system to an enterprise event store license.

After you upgrade the system to an enterprise event store license, the full details of all events are available in any new searches performed and any new reports that are generated. You can use the new `OverEPSLimit` tag to specifically search for any such tagged events, by adding `rv145:OverEpsLimit` to your search criteria.

For more information, see “Viewing Search Results” (http://www.novell.com/documentation/novelllogmanager12/log_manager_admin/data/bgt1wlo.html) in the *Sentinel Log Manager 1.2 Administration Guide*.

1.2.2 CreatedDuringEval Tag

On systems that are running with the free license, any report results that are generated do not include the event details of any events that were tagged with the `OverEPSLimit` tag. Sentinel Log Manager tags such report results with the new `CreatedDuringEval` tag.

After you upgrade the system to an enterprise event store license, you can run the tagged reports again to verify if they include any events that were originally tagged as `OverEPSLimit`. To specifically search for the tagged report results, enter `CreatedDuringEval` in the report search criteria.

For more information, see “Viewing the Reports” (http://www.novell.com/documentation/novelllogmanager12/log_manager_admin/data/bhirusz.html#bqetnss) in the *Sentinel Log Manager 1.2 Administration Guide*.

1.3 License Indicators

- “Licensed EPS Indicator” on page 2
- “License Expiry Status Indicators” on page 3

1.3.1 Licensed EPS Indicator

A new Licensed EPS indicator is added to the *Collection* > *Overview* EPS graph, which indicates the licensed EPS rate. The licensed EPS indicator enables you to determine whether the current EPS rate is exceeding the licensed EPS rate or is close to the licensed EPS rate. For more information, see “Viewing Events Per Second Statistics” (http://www.novell.com/documentation/novelllogmanager12/log_manager_admin/data/bles917.html) in the *Sentinel Log Manager 1.2 Administration Guide*.

1.3.2 License Expiry Status Indicators

The Data Restoration feature is not available in the free and trial version of Sentinel Log Manager. Therefore, a message is displayed indicating that you are not licensed to use the feature. In addition to that, after the trial license expires, a message is displayed indicating that the functionality is being limited for the following features:

- Actions
- Rules
- Distributed Search

1.4 SLES 11 SP1 Support

Sentinel Log Manager is now supported on the SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit platform.

1.5 Limitations to the Legacy Collector Support

Novell is in the process of phasing out support for Legacy Collectors in the Sentinel product line. In the previous versions of Sentinel Log Manager, the system displays a warning if you import a Legacy Collector. Starting with version 1.2, Sentinel Log Manager and Collector Manager do not run Legacy Collectors.

NOTE: Legacy Collectors were written by using the Legacy Collector Builder application, which is no longer shipped with Sentinel products. Legacy Collectors are replaced by JavaScript Collectors that are written by using the Sentinel Plug-In SDK. JavaScript Collectors are available at the Sentinel 6.1 Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).

1.6 Security Improvements

Sentinel Log Manager 1.2 includes multiple updates to improve the security of the product:

- Apache Tomcat has been upgraded to version 6.0.29 to fix security vulnerabilities.
- The PostgreSQL database has been upgraded to version 8.3.12 to fix security vulnerabilities.

2 System Requirements

Sentinel Log Manager 1.2 and later require the SLES 11 SP1 platform. Therefore, you must first ensure that the operating system is upgraded to SLES 11 SP1 before you install Sentinel Log Manager 1.2.

For detailed information on hardware requirements and supported operating systems, browsers, and event sources, see "System Requirements" (http://www.novell.com/documentation/novelllogmanager12/log_manager_install/data/bjx8zq7.html) in the *Sentinel Log Manager 1.2 Installation Guide*.

3 Installing Novell Sentinel Log Manager

Sentinel Log Manager 1.2 can only be used for clean installations. To install Novell Sentinel Log Manager 1.2, see the *Sentinel Log Manager 1.2 Installation Guide* (http://www.novell.com/documentation/novelllogmanager12/log_manager_install/data/bookinfo.html).

4 Documentation

The updated documentation and release notes are available at the Sentinel Log Manager documentation site (http://www.novell.com/documentation/novelllogmanager12/).

5 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 deliverable. 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 the Novell International Trade Services Web page (http://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.

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.