Novell Sentinel Log Manager 1.2 Release Notes

February 2011

Novell.

Novell Sentinel Log Manager collects data from a wide variety of devices 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.

- Section 1, “What’s New,” on page 1
- Section 2, “System Requirements,” on page 4
- Section 3, “Installing Novell Sentinel Log Manager,” on page 4
- Section 4, “Defects Fixed and Enhancements,” on page 4
- Section 5, “Known Issues,” on page 7
- Section 6, “Documentation,” on page 8
- Section 7, “Legal Notices,” on page 8

1 What’s New

- Section 1.1, “Enhancements to Licenses,” on page 1
- Section 1.2, “Additional Tags,” on page 2
- Section 1.3, “License Indicators,” on page 2
- Section 1.4, “SLES 11 SP1 Support,” on page 3
- Section 1.5, “Limitations to the Legacy Collector Support,” on page 3
- Section 1.6, “Security Improvements,” on page 3
- Section 1.7, “Plug-Ins Upgrade,” on page 3

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 enterprise features are disabled, and 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 functionalities, 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:

- Section 1.2.1, “OverEPSLimit Tag,” on page 2
- Section 1.2.2, “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 or 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 has been 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, clean installations of Sentinel Log Manager and Collector Manager do not run Legacy Collectors.

NOTE: Legacy Collectors were written using the Legacy Collector Builder application, which is no longer shipped with Sentinel products. Legacy Collectors are replaced by JavaScript Collectors that are written using the Sentinel Plug-In SDK. JavaScript Collectors are available at the Sentinel 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.

1.7 Plug-Ins Upgrade

Sentinel Log Manager 1.2 includes the updated versions of the following plug-ins:

- Syslog Integrator 6.1r4
- Syslog Connector 6r9
- Database Connector 6r8
- Collector based reports

  Password Changes 6.1r3 is a new report, which is a combined and updated version of the `Self Password Changes` and `Password Resets` reports.
- McAfee Network Security Platform Collector 6.1r2

- McAfee policy Orchestrator Collector 6.1r5
- Microsoft Active Directory and Windows 6.1r5 Collector, which is a combined and updated version of the Active Directory 6.1r4 and Windows 6.1r4 Collectors.

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 Defects Fixed and Enhancements

- Section 4.1, "Defects Fixed," on page 4
- Section 4.2, "Enhancements," on page 6

4.1 Defects Fixed

The following table lists the defect numbers and the solutions provided for these defects in Sentinel Log Manager 1.2:

Bug Number	Solution
615111	Using a symbolic link to point to the install directory after it is moved to a different partition now does not result in data management issues.
656093	Security improvements have been made to decrease the vulnerability to session fixation attacks.
652435	Turning on networked storage when there are a number of local closed partitions and decreasing the local storage space now results in moving the partitions to networked storage (with enough space) before the data is deleted from local storage.
652438	When local storage space is running low, the system now attempts to move data to networked storage to free up space before deleting it from local storage.
620681	A sporadic issue in Event Source Management (ESM) where Collector nodes are in the Stop state after a server restart is now fixed. Collector nodes that were in the Running state before the restart now continue to be in the Running state after the restart.

Bug Number	Solution
661335	The `logon.jsp` file now includes the `<body>` tag, which was otherwise missing and caused Access Manager to fail while injecting credentials through the Access Manager Form Fill policy. Novell Access Manager and Single Sign-on products now work seamlessly while interacting with Sentinel Log Manager
624095	Sentinel Log Manager now automatically closes any idle index loggers every time a clean up task is run at the back end, which reduces the number of open files on SLES.
631900	Performance improvements have been made so that running large distributed reports across multiple instances of Sentinel Log Manager now works as expected and does not cause the target server to run out of memory.
626338	The ReportPluginUpload, TruststoreUploadServlet, and LdapCertFileUploadServlet servlets now do not allow unauthorized users to upload files.
652430	Events can now be searched from multiple restored partitions that are prefixed with the same date and/or retention policy.
641361	Events can now be searched from the restored event data that is in the local storage. The event data does not need to be placed in the configured networked storage directory for it to be searchable.
658444	The LEA connector now works as expected with Sentinel Log Manager.
617477	Clicking alt+left on an event field while performing an All Events search now appends a NOT clause to the search query and displays the expected search results.
617663	You can now modify more than one field of an event source at once. After you click *Save* to refresh the page, the new values are reflected in the relevant fields.
619173	The Search Target Name in the Event List report now shows the actual search target name as expected.
628824, 581698	Issue with the `start_tomcat.sh` script not finding the bonded IP address in a NIC bonded setup is now fixed. The `start_tomcat.sh` script now finds the right IP address to be written to the JNLP files on startup and enables ESM to launch successfully.
615088	The EPS limits of Sentinel Log Manager Actions are now documented. For more information, see "Actions EPS Limits" in the *Sentinel Log Manager I.2 Installation Guide*.
608905	The need to restart the services after applying the license key is now not necessary.
618698	Extracting the `installer.tar.gz` file as the `root` user now does not change the ownership or permissions of the files. The ownership and permissions that were set before the extract are preserved.
656600	The issue with connection leaks in the database when the transactions are in an idle state is now fixed.
612557	The `SentinelLogManager` tag now cannot be deleted, which is as expected because it is a system tag and is used to tag the internal events.
618895	While saving a distributed search as a report, the search targets on which the search is performed are now auto-selected by default.
656710	Data transmitted over ActiveMQ is now compressed, which reduces the network bandwidth utilization between a Collector Manager and the server.

Bug Number	Solution
652429	The CustomerVar (cv) fields are now HTML encoded to avoid execution of malicious JavaScripts and prevent any XSS attacks. Therefore, when Novell Audit fields are mapped to custom Sentinel fields, clicking the *details* link in the search results page now works as expected and does not execute any JavaScripts.
619920	The issue with the `dbconfig` command not changing the appuser password is now fixed. Running the `dbconfig` command against the entire `/etc/opt/novell/sentinel_log_mgr/config` directory now changes the appuser password as expected.
615572	While editing the IP address of a search target server, if you change the IP address and click *Save*, the changes are not saved and an appropriate error message is displayed as expected.
616707	In the *Reports* tab, if there are no report definitions, all the report options such as *Delete*, *Export*, and *Tags* are now disabled.
622384	When retention policy names are renamed or when new policies are created, the policy names are now displayed correctly in the local and distributed search results.
616334	In the local and distributed search results, the *get raw data* link now does not appear for users who do not have the View all data permission, which is as expected because these users are restricted from viewing the raw data.
617652	A new command, `ssl_certs`, is now included in the `/opt/novell/sentinel_log_mgr/setup` directory. This command enables you to replace the self-signed SSL certificates with the CA signed certificates. The procedure to replace the default self-signed certificates with CA signed certificates is now documented. For more information, see "Using CA Signed Certificates" in the *Sentinel Log Manager 1.2 Administration Guide*.

4.2 Enhancements

The following table lists the enhancements made in the 1.2 version to improve the usability of Sentinel Log Manager:

Bug Number	Description
538141	You can now select the fields you want to export to the CSV file while you are exporting the search results, rather than manually removing the unwanted fields in the CSV after the export.
654521	While configuring the *Log to Syslog* action, you can now specify the encoding standard that the Syslog Integrator should use.
553141	The Search results page now includes two new links: *Save as Rule* and *Save as Retention Policy*. These links enable you to save the specified search query as a Rule and as a Retention Policy.
619543	You can now create a role with the same name as the name watermarked in the Role Name field.
616069	All the parameters that the installer gets from the unattended install input file are now written into the `install.log` file. This file can be used as a reference for troubleshooting any installation issues.

Bug Number	Description
504049	A *Close* button is now added in the datetime picker dialog boxes, so you can close the datetime picker dialog box after you select the date and time.

5 Known Issues

Bug Number	Description
666893	**Issue:** Sentinel Log Manager 1.2 cannot perform search and run reports on the data that is restored from Sentinel Log Manager 1.1. This is because Sentinel Log Manager 1.1 uses squashfs version 3.4 and Sentinel Log Manager 1.2 uses squashfs version 4.0, which is not backward compatible and cannot open a squashed file system created with previous versions. **Workaround:** None. Contact Novell Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup) for assistance.
673028	**Issue:** On Windows 7 with Firefox as the browser, non-admin users cannot login to the ESM user interface. When you launch ESM, it tries to copy the `ESMWebStart.jnlp` file to the `C:\Program Files (x86)\Mozilla Firefox\` directory. The non-admin users do not have sufficient rights to write to this directory. **Workaround:** Perform either of the following: ◆ Set the %ESEC_DATA_HOME% environment variable to a directory on which the non-admin user has the write permission. ◆ Save the `ESMWebStart.jnlp` file and open the file through Windows Explorer instead of the Firefox browser.
659873	**Issue:** The `Synchronous call Timed out for request` exception is logged in the `tomcat0.0`.log after the installation of Sentinel Log Manager and also each time the services are restarted. **Workaround:** None. Although an exception is logged, the system works as expected.
667611	**Issue:** The *send results to* link in the search results page does not appear for non-admin users. Instead, a *sending* link is displayed, which does not perform any action when it is clicked. **Workaround:** None.
663470	**Issue:** Sentinel Log Manager does not install 64-bit JRE on 64-bit Windows system. **Workaround:** None. This is by design. The Sentinel Log Manager installer only includes 32-bit JRE and does not include 64-bit JRE.
666560	**Issue:** The default SSL certificate has been signed by using a weak hash algorithm (MD5) instead of using the SHA1 algorithm. **Workaround:** You can get the SSL certificate from any trusted CA, which is signed by using the SHA1 algorithm and replace it with the default SSL certificate. For information on replacing the SSL certificate with a CA signed certificate, see "Using CA Signed Certificates" in the *Sentinel Log Manager Administration Guide*.
601697	**Issue:** When Web server (tomcat) dumps memory, the Web server does not restart on its own and becomes inactive. **Workaround:** Restart the Sentinel Log Manager service.

Bug Number	Description
662191	**Issue:** The remote Collector Manager installation does not proceed if the default installation path contains special characters. **Workaround:** Change the default installation path and ensure that the new path you specify does not include special characters.
664393	**Issue:** Sentinel Log Manager does not display the data retention policies if the data is large in the networked storage. The du command runs for a longer time to find the disk usage and a message is displayed in the Web user interface indicating that refreshing retention policies failed. **Workaround:** Increase the timeout period so that Sentinel Log Manager does not timeout before retrieving the disk usage space. 1. Log in to Sentinel Log Manager as novell user. 2. Open the `/etc/opt/novell/sentinel_log_mgr/config/server.xml` file in an editor. 3. Add the taskTimeoutPeriod property in the DiskStatisticsCache component as follows: 4. Modify the *diskStatsCheckInterval* property such that the value is greater than or equal to *taskTimeoutPeriod*. 5. Restart Sentinel Log Manager.

Code for step 3 (bug 664393):

```
<obj-component id="DiskStatisticsCache">
<class>esecurity.ccs.comp.diskstatistics.DiskStatisticsCache
</class>
<property name="emaSmoothingFactor">0.2</property>
<property name="diskStatsCheckInterval">300000</property>
<property name="taskTimeoutPeriod">300000</property>
</obj-component>
```

For the list of known issues in Sentinel Log Manager 1.1 versions, see Novell Sentinel Log Manager 1.1.0.2 Release Notes (http://www.novell.com/documentation/novelllogmanager11/).

6 Documentation

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

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 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.

Copyright © 2011 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.

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.