Novell Sentinel Log Manager 1.1.0.2 Release Notes

July 28, 2010

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.

You can upgrade Sentinel Log Manager to 1.1.0.2 from the Sentinel Log Manager versions: 1.0.0.4, 1.0.0.5, 1.1.0.0, or 1.1.0.1. The set of new features and fixed defects depend on the version from which you upgrade.

1 What's New

1.1 What's New in Sentinel Log Manager 1.1.0.2

This version includes defect fixes. For more information, see Section 6.1, "Defects Fixed in Sentinel Log Manager 1.1.0.2," on page 6.

1.2 What's New in Sentinel Log Manager 1.1.0.1

This version includes defect fixes. For more information, see Section 6.2, "Defects Fixed in Sentinel Log Manager 1.1.0.1," on page 6.

1.3 What's New in Sentinel Log Manager 1.1

1.3.1 Roles

Administrators can now create roles that can be assigned to any number of users. Each role can be assigned with a different set of permissions, and the users inherit the permissions of the role they belong to.

Sentinel Log Manager includes a few default roles with the required permissions. You can modify the permissions, create more roles, based on your requirements.

For more information on group permissions, see "*Configuring Users and Roles*" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxveru.html) in the *Novell Sentinel Log Manager 1.1 Administration Guide*.

1.3.2 Distributed Search

The Distributed Search feature enables you to search for events not only on your local Sentinel Log Manager server, but also on other Sentinel Log Manager servers distributed across the globe. After you set up the Distributed Search configuration to link multiple servers with the local server (search initiator), you can perform a search on the local server, and optionally instruct the search engine to also perform the search on the linked servers. Corresponding events from all the selected servers are retrieved and displayed in the search results. Each event in the search results displays the server information from which the event is being retrieved.

Exporting search results, sending search results to an action, and retrieving raw data events are enhanced to take advantage of this new feature. The reporting engine is also enhanced to use the same underlying search engine so that reports can include data from multiple Sentinel Log Manager servers.

For more information on Distributed Search, see "Searching and Reporting Events in a Distributed Environment" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bp5lx14.html) in the *Novell Sentinel Log Manager 1.1 Administration Guide*.

1.3.3 Tags

The Tags feature enables you to create and assign one or more searchable tag attributes to Event Source Management (ESM) nodes such as event sources, event source servers, Collector Managers and Collector plug-ins, and also to reports. All the events coming from these ESM nodes are also tagged. By tagging, you can create logical groupings of these ESM nodes, the events themselves, and reports.

Events can be searched based on the tags applied to them, and event sources and reports can be filtered based on the tags they have.

Sentinel Log Manager includes some default tags; however, you can create new tags based on your requirements.

For more information on tags, see "Configuring Tags" (http://www.novell.com/documentation/ novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/ log_manager_admin/data/bp62o80.html) in the *Novell Sentinel Log Manager 1.1 Administration Guide*.

1.3.4 Appliance

The Sentinel Log Manager appliance is a ready-to-run software appliance that combines a Novell SUSE Linux Enterprise Server (SLES) 11 operating system and Novell Sentinel Log Manager software with an update service. This appliance offers an enhanced browser-based user interface that supports collection, storage, reporting, and searching of log data from a wide variety of devices, applications, and protocols.

Sentinel Log Manager 1.1 appliance is available in the following formats:

- A VMware appliance image
- A Xen appliance image
- A hardware appliance Live DVD image that is directly deployable to a hardware server

---

NOTE: Sentinel Log Manager 1.0 users can migrate their installation to a Sentinel Log Manager 1.1 appliance by following the instructions in Section 6.4, "Migrating from 1.0 to 1.1 Appliance" (http:/ /www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/ novelllogmanager11/log_manager_install/data/bq9ckex.html) in the *Novell Sentinel Log Manager 1.1 Installation Guide.*

For more information about Sentinel Log Manager appliance installation, see "Installing the Appliance" in the *Novell Sentinel Log Manager 1.1 Installation Guide* (http://www.novell.com/ documentation/novelllogmanager11/log_manager_install/?page=/documentation/ novelllogmanager11/log_manager_install/data/bookinfo.html).

1.3.5 Enhancements to LDAP Authentication

- A new user interface is provided under the *Users* tab to configure a Sentinel Log Manager server for LDAP authentication.
- LDAP authentication can be performed with or without using anonymous search on the LDAP directory.

For more information on LDAP authentication, see "LDAP Authentication" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bpfef67.html) in the *Novell Sentinel Log Manager 1.1 Administration Guide*.

1.3.6 Enhancements to Reports

Reports are enhanced to enable drill down to the events that make up the report. This drill-down option provides the ability to launch a search with the same query and time frame that was used to generate the report, so users can view details of the events used to generate the report.

Multiple report definitions and report results can be exported at one time and multiple report definitions can be imported at one time either from a report definition export zip file or a Collector Pack file.

For more information on these enhancements, see "Reporting" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxdi87.html) in the *Novell Sentinel Log Manager 1.1 Administration Guide*.

New report templates are added and existing report templates are updated. A few report templates that are not in use are also deleted. For more information on the available report templates, see "Sentinel Log Manager Reports" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bl5jfoz.html) in the *Novell Sentinel Log Manager 1.1 Administration guide*.

1.3.7 Data Restoration

The new data restoration feature can restore the old, lost, or deleted event data. You can also perform a search on the restored event data.

A new *Data Restoration* section has been added in the *storage > Configuration* user interface. You can select specific event partitions to restore event data and configure when the restored event partitions can expire again.

For more information on data restoration, see *Restoring Event Data* in "Configuring Data Storage" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/) in the *Novell Sentinel Log Manager 1.1 Administration guide*.

1.3.8 Upgrading Collectors and Connectors

When you install or upgrade to the Sentinel Log Manager 1.1 version, the Collectors and Connectors are upgraded to the most recent version at the time of that release.

1.4 What's New in Sentinel Log Manager 1.0.0.5

This version includes defect fixes. For more information, see Section 6.4, "Issues Fixed in Sentinel Log Manager 1.0.0.5 Release," on page 7.

2 System Requirements

There are no major changes in the system requirements since the Sentinel Log Manager 1.0 release.

NOTE: Sentinel Log Manager is supported only on the SLES 11 platform. Sentinel Log Manager is not supported on SLES 11 SP1 because of known issues while searching event data in the networked storage. For more information, see 666893 in Section 7, "Known Issues," on page 8.

For a detailed information on hardware requirements and supported operating systems, browsers, and event sources, see the *Novell Sentinel Log Manager 1.1 Installation Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

3 Installing Novell Sentinel Log Manager 1.1

To install Novell Sentinel Log Manager 1.1, see the *Novell Sentinel Log Manager 1.1 Installation Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

4 Upgrading to Novell Sentinel Log Manager 1.1.0.2

To upgrade Novell Sentinel Log Manager to the latest patch, see "Upgrading Sentinel Log Manager" in the Novell Sentinel Log Manager 1.1 Installation Guide (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

5 Verifying Version Numbers After Upgrading

After upgrading the Sentinel Log manager to 1.1.0.2, the components display the following version numbers:

Table 1   *Version Numbers After Upgrading*

Components	Version Numbers
Sentinel Log Manager Server	1.1.0.2_783
Collector Manager	1.1.0.0 (No changes in this patch)

6 Defects Fixed

- Section 6.1, "Defects Fixed in Sentinel Log Manager 1.1.0.2," on page 6
- Section 6.2, "Defects Fixed in Sentinel Log Manager 1.1.0.1," on page 6
- Section 5, "Defects Fixed in Sentinel Log Manager 1.1," on page 5
- Section 6.4, "Issues Fixed in Sentinel Log Manager 1.0.0.5 Release," on page 7

6.1 Defects Fixed in Sentinel Log Manager 1.1.0.2

Bug Number	Description
622002	The search result in Web UI now displays correct number of events in the correct order. Also, expected events are displayed when the search result is exported.
621236	Added additional checks to the code to protect the files owned by user who owns the Sentinel Log Manager install (usually `novell`) from access by unauthenticated users.

6.2 Defects Fixed in Sentinel Log Manager 1.1.0.1

Bug Number	Description
617918	Fixed an issue with the EventRouter that was causing duplicate events to be stored sporadically.

6.3 Defects Fixed in Sentinel Log Manager 1.1

Bug Number	Description
617478	The Top 10 report for Intrusion Detection Systems can now be created as the *DeviceAttackName* field and is now included in the Events fields.
609811	The *TargetUserName* and *InitiatorIP* fields are now populating values as expected when the password for a user is changed.
609814	The *InitiatorIP* field is now populating values as expected when a user logs in to Sentinel Log Manager.
607143	New reports have been created that can be used to perform audits on internal events.
606861	You can now perform a wildcard search on events that contain uppercase characters.
592503	Additional search queries that you add in the *Refine* panel now displays appropriate results.
587831	The *Refine* panel now displays the count of events for the *CustomerVar22* field, when it is added as an extra field to be displayed.
567082	Users with non-standard characters in their passwords can now log in to the Web user interface and ESM interface as expected.
565777	The Trust Management report now includes DEASSOC_TRUST events, which are generated when a user account is removed.
526062	The *Configuration* link in the Web user interface is now replaced with a gear icon, which indicates that the links next to it are configuration links.
524575	All JavaScript pop-up windows such as Search Tips, Run, and Delete now appear as expected on Internet Explorer 8 in French, Spanish, and Italian languages.

Bug Number	Description
503808	ESM now launches as expected the first time Sentinel Log Manager is installed on a server on which it was never installed before.
545436	Internal audit event fields such as initUserName, initIP, and targetUserNamedetails are now populated with appropriate values and are displayed in the search results.

6.4 Issues Fixed in Sentinel Log Manager 1.0.0.5 Release

This section lists the issues fixed in Novell Sentinel Log Manager 1.0.0.5 release.

Table 2   *Issues Fixed in Sentinel Log Manager 1.0.0.5 Release*

Tracking Number	Description
582427	The latest version of agent-manager.jar file is bundled with the hot fix 5 to enable legacy collectors to send event data.
581908	The latest version of `libuuid.jar` file is now bundled with the hot fix 5 build, to enable the collector debugger to function properly.
581912	The installer now checks for the jre64 directory name. Upgrading on a remote 64 bit Linux Collector Manager now works fine.
590171	The *All Vendors All Products Top 10 Report* is now installed when a user upgrades from versions older than Hot Fix 3.
581698	The `start_tomcat.sh` script now attempts to read the user specified SERVER_IP value from the `ipaddress.conf` file. If the `ipaddress.conf` file is not present or if the IP address is not set in the file, then the script determines the IP address automatically. To enable the script to read the SERVER_IP value from the configuration file, create the `ipaddress.conf` file in the `$ESEC_HOME/config` directory and specify the IP address in the following format: `SERVER_IP=<ip address value>` For example, `SERVER_IP=10.0.0.1`
572619	Users can now download raw data files with double byte characters in their names.
583775	Now, when a non-admin user clicks the *Get Raw Data* link, the following error message is displayed in the resulting page: `Must be an Administrator to download Raw Data`
563886	The Collector framework now does not overwrite the event fields other than the rv21-rv25 fields. However, the Sentinel Link collector 6.1r3 still contains a known issue (bug 536119), which causes the Event ID field and the Port fields to be overwritten.
580749	Removed the extra / added to the URL so that if you click the *Help* button from Web UI, the Novell Sentinel Log Manager documentation page opens.

Tracking Number	Description
586957	Clicking *details+* in Web UI now expands even for events with empty rv32 field.
591055, 591059	Issue: Fixed an issue so that after upgrading to Hot fix 4, the data parsed by Collectors is displayed in the generated report.

7 Known Issues

Bug Number	Description
666893	**Issue:** Installing any version of Sentinel Log Manager 1.1 on SLES 11 SP1 causes an incompatibility issue between the mksquashfs tool version 3.4 used by Sentinel Log Manager to archive compressed data and the squashfs kernel module version shipped with SLES 11 SP1 (version 4.0). The squashfs version 4.0 is not backward compatible and cannot open a squashed file system created with previous versions. This incompatibility results in issues while searching and running reports on the event data in the networked storage. **Workaround:** None. If you have already upgraded the system to SLES 11 SP1, contact Novell Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup) for support.
620681	**Issue:** In ESM, the Collector nodes are incorrectly being set to the stopped state during a restart of the server. However, this is a sporadic issue. **Workaround:** After restarting the server, log in to ESM and ensure that Collectors that are supposed to be running are set to the start state.

620100	**Issue:** Legacy Collectors do not work on remote Collector Managers.
	
	Workaround: Modify the `ESEC_HOME/config/collector_mgr.xml` file in the remote Collector Manager machine.
	
	1. Open the `ESEC_HOME/config/collector_mgr.xml` file in any editor.
	2. Change the following lines:
	
	`<property name="workbench.home">..</property>`
	`<property name="properties.file">../config/collector_mgr.properties</property>`
	`<property name="esecurity.home">..</property>`
	
	to
	
	`<property name="workbench.home">${user.dir}/..</property>`
	`<property name="properties.file">../config/collector_mgr.properties</property>`
	`<property name="esecurity.home">${user.dir}/..</property>`
	
	3. Restart the remote Collector Manager services.

Bug Number	Description
617318	**Issue:** After you upgrade an earlier version of Sentinel Log Manager to Sentinel Log Manager 1.1, the *Save as Report* > *Visualization* drop-down list should include only report templates. However, a few Collector-specific reports might still appear in the *Visualization* list because they might not be deleted during the upgrade if they were in use prior to the upgrade. **Workaround:** This happens because the Collector-specific reports that appear in the list were not automatically updated during the upgrade. Download the updated Collector Pack from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/ sentinel61.html) and upload the pack by using the Sentinel Log Manager report upload option.
617663	**Issue:** On the *Collections* > *Event Source Servers* page, when you modify more than one field of an event source and click *Save* to refresh the page, only one field is updated and the other fields show the old values. **Workaround:** Change the values for the fields one at a time. Click *Save* after modifying each field.
617477	**Issue:** Clicking alt+left on an event field in the search results to add a NOT clause to an empty query does not work as expected because purely NOT criteria queries are not allowed. **Workaround:** alt+left clicking works as expected if you begin the search with a sev:[0 TO 5] query instead of an empty query. The events that are retrieved are same for both the queries.
618294	**Issue:** The Event Summary, Top 10 Report, and Top 10 Dashboard base reports display events with -0- value instead of blank values when the Primary field is null. **Workaround:** For the Event Summary and Top 10 reports, do not select the Primary fields that have no data (is null). For the Top 10 Dashboard reports, ignore the graphs of the fields that have -0- as the value in the X axis.
617103	**Issue:** Exceptions are logged in the server_wrapper.log file, when large reports are run with NFS archiving configured. **Workaround:** Run large reports when the EPS is at its lowest (e.g. at night or on weekends). More disks in the local storage RAID array might also help.
614686	**Issue:** Search query times out and exceptions are logged while large reports are run on systems that have about 200 million events. **Workaround:** Avoid running large reports when performing large searches.
613960	**Issue:** The remote Collector Manager Installshield Wizard displays Sentinel 6.1 instead of Sentinel Log Manager. **Workaround:** None. This is a user interface issue.
608905	**Issue:** The Sentinel Log Manager user interface does not prompt to restart Sentinel services after you add a license key and does not perform some operations as expected. **Workaround:** Restart the Sentinel Log Manager server after adding the license key.

Bug Number	Description
606567	**Issue:** On the appliance, the platform version is logged for every two minutes via kernel message to syslog at `/var/log/messages`. **Workaround:** These messages are sent purposely so that the operating system can inform Sentinel Log Manager what version it is. If these messages cause problems for some reason, disable the `wtmpmon` script to prevent them from being generated.
593435	**Issue:** The Sentinel Log Manager server does not function as expected if the Sentinel Log Manager 1.1 installation is relocated to a base directory that has spaces in its path. For example, `/home/user/Sentinel Log Manager`. **Workaround:** Ensure that directory does not include spaces in its path.
560966	**Issue:** While configuring the File Connector, when you click *Browse* to add an event source, the file browser does not appear and exceptions are logged in the control center log file. **Workaround:** Specify or copy/paste the desired file path into the field rather than using the *Browse* button.
577073	With about 3000 event sources, when the raw data partitioning goes from open > log state, the EPS rate goes down to 0. **Workaround:** Install additional instances of Sentinel Log Manager so that the total number of event sources per instance is fewer than the recommended device limits as given in the System Requirements. For more information, see "System Requirements" (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bjx8zq7.html) in the *Novell Sentinel Log Manager 1.1 Installation Guide*.
617350	**Issue:** WebYaST reports a `DBus.Error.LimitsExceeded` error when patch updates are being installed. **Workaround:** Restart the yastws service: `/etc/init.d/yastws restart` Alternatively, click *Reboot* in the Control Panel to restart the machine.
607684	**Issue:** When you boot the machine from an ISO appliance image i.e run the ISO as live CD/DVD, if you run patch updates through WebYast > Updates, the system goes to a non-responsive state. **Workaround:** Install the Live DVD to the hardware and then run the patch updates.
609187	**Issue:** On systems that have more than a million events, after you initiate report generation and click *Cancel* to cancel the report generation, report generation is still in progress and does not cancel. **Workaround:** None.
593788	**Issue:** Sentinel Log Manager takes approximately 5 minutes to log in to the Web User Interface the first time after installation. **Workaround:** None.
510824	**Issue:** After you click the *details++* link for the individual search results, the *all details++* and *all details--* links do not work as intended for the first 25 events. **Workaround:** None.

Bug Number	Description
548515	**Issue:** The sample reports in Sentinel Log Manager show user data such as Full Name, Department, and Workforce ID that are not available in Sentinel Log Manager. **Workaround:** None.
509549	**Issue:** In the Search Results page with more than 75,000 events, when you scroll down to view the events, the scroll bar does not stop at the scrolled point and changes its location frequently. **Workaround:** None.
615572	**Issue:** Sentinel Log Manager allows you to change the IP address of the target server while editing the target server details and does not display any message saying that the specified IP address is different. **Workaround:** None.
545436	**Issue:** When you stop a Collector, the stopcollector internal event is generated twice in the event logs. The second `stopcollector` event that is generated does not show proper values for initUserName, initIP, and targetUserNamedetails event fields. **Workaround:** None.
612557	**Issue:** The `SentinelLogManager` tag, which is a default tag to tag the internal events, can be deleted. However, the internal events are still tagged with the `SentinelLogManager` tag, even after the tag is deleted. **Workaround:** As this is a default tag, do not delete it.
622213	**Issue:** After upgrading Sentinel Log Manager 1.1.0.1, exceptions are logged in the `server0.0.log` file. **Workaround:** You can ignore these exceptions as they do not cause any loss of functionality.
619920	**Issue:** After upgrading, the `dbconfig` command does not modify the `obj-component.ConnectionManager.properties` file. **Workaround:** You must manually modify the `obj-component.ConnectionManager.properties` file.
623885	**Issue:** After upgrading, the syslog event source server configured on the remote Collector Manager appears with a red cross mark. **Workaround:** Restart the remote Collector Manager service.

8 Documentation

The updated documentation and release notes are available at the Sentinel Log Manager documentation site (http://www.novell.com/documentation/novelllogmanager11/).

9 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 © 2010 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.