Novell Sentinel 6.1 Rapid Deployment SP2 Readme

April 2011

Novell.

Sentinel Rapid Deployment is a new packaging option for the Novell market-leading Sentinel Security Information and Event Management solution. Sentinel Rapid Deployment includes the full Sentinel functionality and is ideal for smaller organizations or regional installations.

Sentinel 6.1 Rapid Deployment SP2 is available as a clean installer or an upgrade installer. The upgrade installer applies the latest software fixes and enhancements to an existing installation of Sentinel Rapid Deployment 6.1 SP1.

- Section 1, “What’s New,” on page 1
- Section 2, “System Requirements,” on page 2
- Section 3, “Installing Novell Sentinel Rapid Deployment,” on page 2
- Section 4, “Upgrading to Sentinel Rapid Deployment SP2,” on page 2
- Section 5, “Accessing the Sentinel Rapid Deployment Help Files,” on page 3
- Section 6, “Defects Fixed and Enhancements,” on page 4
- Section 7, “Known Issues,” on page 6
- Section 8, “Documentation,” on page 7
- Section 9, “Legal Notices,” on page 7

1 What’s New

- Section 1.1, “What’s New in Sentinel Rapid Deployment 6.1 SP2,” on page 1
- Section 1.2, “What’s New in Sentinel Rapid Deployment SP1,” on page 2

1.1 What’s New in Sentinel Rapid Deployment 6.1 SP2

- “Support for SLES 11 SP1” on page 1
- “Limitations to Legacy Collector Support” on page 2
- “Security Improvements” on page 2

1.1.1 Support for SLES 11 SP1

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

1.1.2 Limitations to Legacy Collector Support

Novell is in the process of phasing out support for Legacy Collectors in the Sentinel product line. In previous versions of Sentinel Rapid Deployment, the system produces a warning if you import a Legacy Collector. Starting with the SP2 version, clean installations of Sentinel Rapid Deployment and Collector Manager do not run Legacy Collectors. However, upgraded Sentinel Rapid Deployment systems and Collector Managers continue to run Legacy Collectors as before.

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

1.1.3 Security Improvements

Sentinel Rapid Deployment 6.1 SP2 includes multiple updates to improve the security of the product:

- Java Runtime Environment (JRE) has been upgraded to version 1.6.0_24.
- Apache Tomcat has been upgraded to version 6.0.29.
- The PostgreSQL database has been upgraded to version 8.3.12.

1.2 What's New in Sentinel Rapid Deployment SP1

For information on what's new in Sentinel Rapid Deployment 6.1 SP1, see the "Sentinel Rapid Deployment SP1 Readme" (http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85).

2 System Requirements

For detailed information on hardware requirements, supported operating systems, and browsers, see "System Requirements" in the *Sentinel Rapid Deployment Installation Guide*.

3 Installing Novell Sentinel Rapid Deployment

The installation is now simplified and the tar file name is no longer required as input. You can download the installer, extract it to a directory, and then install it as a `root` or non-root user by simply running the script. You can also give command line arguments to create only the user, install the Rapid Deployment server, create service to automatically start Sentinel Rapid Deployment on system startup or install only the Rapid Deployment server without creating the user or service.

To install Novell Sentinel Rapid Deployment 6.1 SP2, see"Installation" in the *Sentinel Rapid Deployment Installation Guide*.

4 Upgrading to Sentinel Rapid Deployment SP2

Before proceeding with the upgrade, ensure that you have installed Sentinel 6.1 Rapid Deployment SP1 on the system where you want to install this service pack:

To upgrade to Sentinel Rapid Deployment 6.1 SP2, see "Upgrading Sentinel Rapid Deployment" in the *Sentinel Rapid Deployment Installation Guide*.

5 Accessing the Sentinel Rapid Deployment Help Files

You can access the online User guide for Sentinel Rapid Deployment by clicking *Help* > *Help* in the Sentinel Control Center. However, if you are working in a secure environment where direct Internet access is denied, you can download and extract the online help file to the Sentinel Rapid Deployment server as a one-time procedure. After the help files are extracted to a specific location, you can access the documentation from either the server or the remote system. You can view the help files through any Web browser.

NOTE: The help files are only in English.

To download the online help:

1. Go to the Sentinel Rapid Deployment documentation site (http://www.novell.com/documentation/sentinel61rd/).
2. Click *zip* in the Downloadable User Guide Help section, then save the `s61rd_user_help.zip` file to your local machine.
3. Use the following commands to copy and extract the downloaded file:

   ```
   cp s61rd_user_help.zip <Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
   ```

   ```
   cd <Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
   ```

   ```
   unzip s61rd_user_help.zip
   ```

   IMPORTANT: You cannot access the help files unless you extract the `s61rd_user_help.zip` file to the specified location.
4. Do either of the following to view the help files:
   - In the Sentinel Control Center, click *Help* > *Help*.
   - Open the `<Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html` file.

   The `Index.html` file lists the topics in the navigation pane. Click the desired topic to open the Help page for that topic.

NOTE: If you download and save the help files to the specified location on the Sentinel Rapid Deployment server, clicking the *Help* menu in the Sentinel Control Center always lists the downloaded help content available on the server.

If you want the *Help* menu to redirect you to the *Sentinel Rapid Deployment User Guide* that is available online, remove the `s61rd_user_help` at `<Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help` folder from the Sentinel Rapid Deployment server.

6 Defects Fixed and Enhancements

- Section 6.1, "Defects Fixed," on page 4
- Section 6.2, "Enhancements," on page 5

6.1 Defects Fixed

The following table lists the defect numbers and the solutions provided for these defects in Sentinel Rapid Deployment 6.1 SP2:

Bug Number	Solution
451892	The Sentinel WebStart application now automatically downloads the required fonts, if necessary.
497131	The latest eDirectory Collector is now able to handle double-byte Japanese characters in the reporting feature.
531114	When any non-report(.zip) files are uploaded by using the Report Web use inteface, the browser now displays an error stating `Error getting a PluginPackage from package.xml`.
556730	The Correlation Engine no longer stores future events that are more than 30 sec into the future, so it does not display an out of memory error.
566973	The Correlation Engine Manager window now displays the list of Correlation Engines even if it is opened in the previously saved Senitnel Control Center session.
569849	Sentinel Rapid Deployment is now bundled with the latest Apache Tomcat version 6.0.29 to fix security vulnerabilities.
573181	For the Sentinel processes, memory is now allocated as percentages. There is also added support for overriding the memory allocations from `memory.conf` file.
600604	Performance improvements have been made such that the system does not run out of memory while running large reports.
607145	Additional audit events are now created to monitor Sentinel administrative activity and configuration changes on data mapping, filters, correlation rules, actions, and Event Source Management (ESM).
621509	The *New Incident* window now displays the events when a user selects the events and creates an incident, and the events are saved as part of the incident.
623834	The `Diskspace usage reached upper threshold` message is displayed only when the usage space reaches the upper threshold value that is calculated based on the actual file system disk space.
625930	The Rule name in the RulePerformanceSummary event no longer appears as null.
626402	Restarting a Connector that has multiple event sources in ESM no longer results in a timeout exception.
629716	The Sentinel Control Center (SCC) instances no longer freeze because of deadlock issues.
641087	Sentinel Rapid Deployment is now bundled with the latest PostgreSQL patch version 8.3.12 to address security vulnerabilities.

Bug Number	Solution
644821	User with a view permission in ESM cannot delete the nodes (Events Sources, Collectors, Collector Manager) by pressing the Delete button on the keyboard.
648554	The Sentinel Data Manager (SDM) configuration file is now created in the user's home directory and not in the location from where the SDM is launched
651181	A Jasper virtualizer is used when running large reports to shorten query time.
651524	The Advisor feed files can now be downloaded by using a proxy server and the proxy password is updated via the download manager.
656595	The connection to the database does not leak any connections, because the locks are released for open transactions that are idle for a long time.
656715	The data transmitted over ActiveMQ is now compressed to improve the network bandwidth.
662213	Sending e-mail to multiple recipient addresses now works in the email event action and the email incident action.
668443	You can now connect to the PostgreSQL database through the command line in addition to connecting through pgadmin.
672058	When you restart an event source that is configured to alert when no data is received for a specified time, the event source no longer generates duplicate events (NoDataAlert) and log messages.
682235	Sentinel Rapid Deployment is now bundled with the latest Java version 1.6.0_24 to fix security vulnerabilities.

6.2 Enhancements

The following table lists the enhancements made in Sentinel Rapid Deployment 6.1 SP2 to improve usability:

Bug Number	Description
547390	You can now configure the offline query limit by setting the max events property in the `das_core.xml` file.
642690	The offline query is enhanced to make subinterval query time configurable in the `das_core.xml` file.
642691	The update status of offline query information is now stored in the `das_core` log file.
648108	The Advisor Status window now shows the information about all of the feed files.
673362	The JasperPrint object file (i.e., the raw result file called results) is not bundled in the report results anymore. This file was not used by Sentinel, and removing it improves report performance and saves disk space.
680054	In a Sentinel Rapid Deployment server, support for bonded IP addresses is added as a failover mechanism.

7 Known Issues

Bug Number	Description
486932	**Issue:** A user can delete an activity associated with an active iTRAC process. **Workaround:** None.
517568	**Issue:** When you try to install Solution Designer separately, it does not install. **Workaround:** Install Solution Designer with either Sentinel Control Center or Sentinel Data Manager.
525334	**Issue:** The Identity Browser displays redundant data for the Active Directory domain. **Workaround:** None.
598473	**Issue:** When the ESM user interface is launched from non-English systems, the 6r9 File Connector does not retrieve the remote files by using the SCP protocol as expected. **Workaround:** None. This will be fixed in File Connector 6r10 version.
674008	**Issue:** Novell icon and copyright information is not visible in the Installshield Wizard on a Linux machine. **Workaround:** None.
674720	**Issue:** Collector Builder information is displayed in license agreement even though support for the Collector Builder option is not included in Sentinel 6.1 Rapid Deployment SP2. **Workaround:** None.

679830	**Issue:** On Windows Collector Manager, the mapping functionality occasionally does not work as expected.
	Workaround: Follow these steps:
	1. Stop the Collector Manager:
	`<install_directory>/bin/sentinel.bat stop`
	2. Open the Collector Manager log `collector_mgr0.0.log` file from the *`<install_directory>`*`/log` directory.
	3. Search for an error similar to the one given below:
	`System temporary directory (java.io.tmpdir property) of C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ appears to be invalid`.
	4. Create a folder named `Temp` in the following location:
	Windows 64-bit systems:
	`C:\Windows\syswow64\config\systemprofile\AppData\Local\`
	Windows 32-bit systems:
	`C:\Windows\system32\config\systemprofile\AppData\Local\`
	5. Restart the Collector Manager:
	`<install_directory>/bin/sentinel.bat start`

Bug Number	Description

680054	**Issue:** The Sentinel Rapid Deployment server fails to automatically determine the IP address.
	Workaround: Follow these steps:
	1. Create a `start_tomcat.properties` file under the <*`install_directory`*>`/sentinel_rd/config` directory.
	Ensure that the user who runs the Sentinel Rapid Deployment server owns this file and has execute permissions.
	2. Specify the IP address in the newly created file by adding the following line:
	`SERVER_IP=<ip_address_value>`
	3. Save the file.
	4. Log in as a user who owns the Sentinel installation files and restart the server by using the following command:
	`sentinel.sh restart`
	5. Check the IP address in the following location to see if the overridden IP address is used:
	`jnlp files under $ESEC_HOME/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads`

680154	**Issue:** The *Tablespace* tab on the Sentinel Data Manager shows incorrect used and free space. The used and free space is calculated based on the sendata1 tablespace instead of the actual disk space. **Workaround:** None.
685187	**Issue:** When you try to install the remote Collector Manager through console mode, the installation fails to import the broker certificate from the server. **Workaround:** You can install the Collector Manager in console mode on a remote system by using `ssh` in graphic mode to connect to the system. For example, `ssh -x` <*`system_IP`*>.

8 Documentation

The updated documentation and release notes are available at the Sentinel Rapid Deployment documentation site (http://www.novell.com/documentation/sentinel61rd/index.html).

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.

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.