Novell Sentinel 6.1 SP1 Hotfix 2

September, 2009

Novell®

This document has the following information about Novell® Sentinel™ 6.1 SP1 Hotfix 2:

1 Overview

This hotfix applies the latest software fixes and enhancements to an existing installation of Sentinel 6.1 SP1 and 6.1 SP1 Hotfix 1.

This hotfix must be installed on all existing Sentinel 6.1 SP1 clients and servers. This includes machines with the Sentinel server, correlation engine, Sentinel database, Collector Manager, Sentinel Control Center, Collector Builder, and Sentinel Data Manager.

2 New Features in Sentinel 6.1 SP1 Hotfix 2

Sentinel 6.1 SP1 Hotfix 2 is a maintenance release for Sentinel 6.1 SP1 and Sentinel 6.1 SP1 Hotfix 1. In addition to bug fixes, enhancements are made to the following features.

2.1 Global Filters

- JavaScript* actions have now been associated with global filters
- An *Action Manager* button has been added in the Global Filter Configuration window, which enables you to add, modify, and delete actions.

For more information on global filters, see Global Filters (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bhjlkyb.html#bhjlkye).

2.2 JRE Upgrade

The Java* Runtime Environment* (JRE*) has been upgraded from 1.5 to 1.6 as Java 2 Platform, Standard Edition (J2SE)* 5.0 will be unsupported by Sun* as of October 30, 2009.

2.3 LDAP Authentication

A Sentinel 6.1 server can now be configured for LDAP authentication to enable users to login to Sentinel using a Novell eDirectory™ or Microsoft* Active Directory* username and password.

NOTE: LDAP authentication is currently supported only on Linux* servers.

For more information on configuring a Sentinel server for LDAP authentication, see Configuring Sentinel 6.1 Server for LDAP Authentication (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/blutcr3.html).

2.4 Collector Manager

By default, the EventRouter, which is one of the components of the Collector Manager, runs in the standalone mode. In this mode, the EventRouter handles internal functions such as maps and applying global filters on events parsed by the Collector Manager.

Sentinel 6.1 SP1 Hotfix 2 enables the EventRouter to operate in server and client modes on both DAS machines and Collector Manager machines. The Collector Manager installation on which the EventRouter is configured to run in client mode is referred to as Light Weight Collector Manager.

NOTE: You should configure a Light Weight Collector Manager on machines that have limited CPU and RAM for the Collector Manager process.

For more information on configuring a Light Weight Collector Manager, see Configuring the Light Weight Collector Manager (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgms016.html#bl53pzx).

3 Prerequisites

The prerequisites for the hotfix depend on the Sentinel version and platform. Read each section carefully to determine whether the steps apply to your environment.

- If Sentinel 4.x or 5.x is installed, it must be upgraded to Sentinel 6.1 by using the upgrade installer. See the *Patch Installation Guide* for instructions.
- If Sentinel is not yet installed, install Sentinel by using the Sentinel 6.1 installer. See the *Sentinel Installation Guide* for instructions.
- If Sentinel 6.1 is installed, ensure that you have upgraded to Sentinel 6.1 SP1.

The complete product documentation is available at the Novell Sentinel 6.1 Documentation Web site (http://www.novell.com/documentation/sentinel61).

NOTE: If your system is running an older version of Sentinel, then it is mandatory to upgrade it to Sentinel 6.1 SP1 before applying this hotfix.

3.1 Back Up Sentinel

This prerequisite applies to all Sentinel systems, regardless of the version or platform.

You should have a complete backup of the machines on which you are installing the patch, including the Sentinel database. If you cannot back up all the files, then at a minimum you need a backup of the contents of the `ESEC_HOME` directory. This protects your system against unexpected installation errors.

3.2 Back Up the AUDIT_RECORD Table

This prerequisite is not necessary if you have already applied Sentinel 6.1 Hotfix 1, Sentinel 6.1 SP1, or Sentinel 6.1 SP1 Hotfix 1. It is necessary only if Sentinel 6.1 Hotfix 1 or Sentinel 6.1 SP1 has not been applied yet.

Starting with Sentinel 6.1 Hotfix 1, the AUDIT_RECORD table, which contains internal audit events for the Sentinel system, is configured for partitioning and archiving for better table management. Because the existing table is not partitioned or archived, the PatchDb script might fail if the AUDIT_RECORD table is too large relative to the amount of temporary tablespace available.

There are two approaches to ensure that the PatchDb script runs successfully, depending on whether it is critical to your organization to preserve the data in the AUDIT_RECORD table:

- If the AUDIT_RECORD data is not important, truncate the AUDIT_RECORD table by using the following SQL command:

  ```
  TRUNCATE TABLE AUDIT_RECORD
  ```

- If the AUDIT_RECORD data is important and needs to be preserved, add more space to the temporary tablespace. The amount of space to be added depends on your environment; consult your Database Administrator (DBA) for adequate settings.

4 Installation

1. Log in to every machine that has Sentinel installed.
   - On Linux*/Solaris*, log in as `root`.
   - On Windows* Vista*, log in as any user if User Access Control is enabled. If User Access Control is disabled, you must log in as an `Administrator`.
   - On other (non-Vista) Windows systems, log in as an `Administrator`.
2. Verify that the environment variables for Sentinel are set by running one of the following commands:
   - On Linux/Solaris: `echo $ESEC_HOME`
   - On Windows: `echo %ESEC_HOME%`
3. Extract the `SENTINEL_6.1.1.2.zip` file.
4. Close all Sentinel applications running on the machine, including:
   - Sentinel Control Center (SCC)

- Sentinel Collector Builder
- Sentinel Data Manager
- Solution Designer

5 Stop the Sentinel service running on the machine:

- On Windows: use Windows Service Manager to stop the Sentinel service.
- On Linux/Solaris: run the `$ESEC_HOME/bin/sentinel.sh stop` command.

6 Open the command prompt.

For most Windows systems and Linux/Solaris, you can log in as any user to open the prompt. For Windows Vista, you must open the command prompt as an Administrator, using the following instructions.

6a Go to *Start* > *All Programs* > *Accessories*.

6b Right-click *Command Prompt* and select *Run as administrator*.

If User Access Control is enabled and you are logged in as a user with administrator privileges, a User Access Control window appears to notify that Windows needs your permission to continue.

6c Click *Continue*.

If you are logged in as a user without administrative privileges, then you are prompted to authenticate as an administrative user.

7 On the command line, return to the extracted hotfix top-level directory and run the script to start the hotfix installer:

- On Windows: `service_pack.bat`
- On Unix*: `./service_pack.sh`

After you run the script, the `Sentinel 6.1 SP1 is the prerequisite for this hotfix installation` message appears.

8 Perform the following:

- On Windows: Press Enter if Sentinel 6.1 SP1 is already installed and continue with the installation or Ctrl+C to terminate the installation and install Sentinel 6.1 SP1.
- On Unix: Press y if Sentinel 6.1 SP1 is already installed and continue with the installation or n to terminate the installation and install Sentinel 6.1 SP1.

9 Press Enter when prompted to start the hotfix installation procedure.

10 After the installation completes, log out and log in to apply the environmental variable changes.

11 Repeat Step 1 through Step 10 on every Sentinel server and client machine that has Sentinel software installed.

12 Restart Sentinel services on all machines:

- On Windows: use the Windows Service Manager to start the Sentinel services.
- On Unix: run `$ESEC_HOME/bin/sentinel.sh start`

5 Sentinel Database Patch Installation

This hotfix also contains a mandatory patch for the Sentinel database. In addition to applying patches to the Sentinel components, you must run a script to apply the patch to the Sentinel database. The installation instructions differ depending on the database you have.

- Section 5.1, "Sentinel Database Patch Installation on Oracle," on page 5
- Section 5.2, "Sentinel Database Patch Installation on SQL Server," on page 6

5.1 Sentinel Database Patch Installation on Oracle

The following sections describe the prerequisites and the procedure to install the database patch on Oracle*:

- "Prerequisites" on page 5
- "Applying the Database Patch" on page 6

5.1.1 Prerequisites

The machine and account from which the database patch is run must meet the following requirements:

- The user has Oracle client application sqlplus as the PATH variable.
- The user has the environment variable ORACLE_HOME set to the directory where the Oracle software is installed.
- The user must be a member of the Oracle dba group.
- The user has the Java 1.6 executable as the PATH variable.

TIP: You can run the PatchDb script directly on the database server machine if the prerequisites are met. However, in some environments, local policies prohibit this type of installation (for example, you cannot install Java on the database server). In this situation, the script can be run from any other machine if the prerequisites are met.

By default, all Sentinel 6.1 machines have the required version of Java, but the default Java installation done by Sentinel does not allow Oracle users to access the `$ESEC_HOME/jre` directory. You can add Oracle users to the esec group (for example, `groupmod -A oracle esec`), temporarily modify the permissions on the directory (for example, `chown -R oracle $ESEC_HOME/jre`), or install a second instance of Java.

If you are using a machine that does not have Sentinel installed on it, run the following commands:

- To verify the Java version and PATH variable settings:

  ```
  java -version
  ```

- To update the PATH environment variable to include the Java installation directory:

  ```
  export PATH=/opt/novell/sentinel6/jre/bin:$PATH
  ```

To install Java, download the appropriate Java version, Java Runtime Environment (JRE) 6.0, from the Sun* Web site (http://java.sun.com/javase/downloads/index.jsp).

5.1.2 Applying the Database Patch

1. Log in to the database server or another machine that has a connection to the Sentinel database.
2. Ensure that your machine meets the Java prerequisites.
3. Stop the Sentinel services.
4. Extract the `SENTINEL_6.1.1.2.zip` file.
5. On the command line, move to the installation directory that was just extracted.
6. Change to the `<install_directory>/db_patch/bin` directory.
7. Enter the `./PatchDb.sh` command to start the installation.
8. Follow the prompts and specify the following information:
   - Hostname or IP address of the Oracle Sentinel database that you want to patch.
   - Port number of the Oracle Sentinel database that you want to patch.
   - Database net service name.
   - Database service name of the Oracle Sentinel database that you want to patch.
   - esecdba user password.
9. Press Enter.

   The script verifies the specified information and begins the database patch installation.
10. After the installation is complete, check for any errors.

    If there are no errors, the Sentinel database patch installation is complete. If there are errors, resolve the errors by referring to the error log files and re-run the PatchDb utility.
11. Restart the Sentinel services on all machines:
    - On Windows: use Windows Service Manager to start the Sentinel services.
    - On Unix: run the `$ESEC_HOME/bin/sentinel.sh start` command.

5.2 Sentinel Database Patch Installation on SQL Server

This section describes the prerequisites and the procedure to install the database patch on SQL Server*.

The main patch script for SQL Server is `PatchDb.bat`.

- "Prerequisites" on page 6
- "Installing Database Patch with Windows Authentication" on page 7
- "Installing the Database Patch with SQL Server Authentication" on page 7

5.2.1 Prerequisites

The following are the prerequisites for applying the SQL Server patch:

- The patch must be copied to the machine that is running the Sentinel database.
- The patch must be run by using the Sentinel Database User credentials or by `esecdba` if you are using SQL Authentication.
- The user has the Java 1.6 executable as the PATH variable.

If you are using a machine that does not have Sentinel installed on it, run the following command to verify the Java version and PATH variable settings:

```
java -version
```

To install Java, download the appropriate Java version, Java Runtime Environment (JRE) 6.0, from the Sun Web site (http://java.sun.com/javase/downloads/index.jsp).

5.2.2 Installing Database Patch with Windows Authentication

To install the database patch with Windows authentication, you need the credentials for the Sentinel database user.

1. Log into the database machine as the Windows Domain user (Sentinel database user).
2. Stop the Sentinel services.
3. Extract the `SENTINEL_6.1.1.2.zip` file.
4. Open the command prompt.
5. Change to the `install_directory\db_patch\bin` directory.

   The install_directory is the directory where the Sentinel hotfix is installed.
6. Enter the `PatchDb.bat` command.
7. Follow the prompts and enter the following information:
   - Hostname or IP address of the SQL Server Sentinel database machine.
   - SQL Server database instance name, if any.
   - Port number of the SQL Server database.
   - Name of the SQL Server database to patch (ESEC by default).
   - 1 for the Windows Authentication option.
8. Press Enter.

   The script verifies the entered information and proceeds if the authentication is successful.
9. After the installation is complete, check for any errors.

   If there are no errors, the Sentinel Database patch installation is complete. If there are errors, resolve the errors by referring to the error log files and re-run the PatchDb utility
10. After the patch runs with no errors, restart the Sentinel services.

5.2.3 Installing the Database Patch with SQL Server Authentication

To install the database patch with SQL Server authentication, you need the credentials for the Sentinel database user.

1. Log into the database machine as the Windows Domain user (Sentinel database user).
2. Stop the Sentinel services.
3. Extract the `SENTINEL_6.1.1.2.zip` file.
4. Open the command prompt.
5. Change to the `install_directory\db_patch\bin` directory.

   The install_directory is the directory where the Sentinel hotfix is installed.
6. Enter the `PatchDb.bat` command.

7 Follow the prompts and specify the following information:

- Hostname or IP address of the SQL Server Sentinel database machine.
- SQL Server database instance name, if any.
- Port number of the SQL Server database.
- Name of the SQL Server database to patch (ESEC by default).
- 2 for the SQL Authentication option.
- esecdba user password.

8 Press Enter.

The script verifies the entered information and proceeds if authentication is successful.

9 After applying the patch, check for any errors. If there are no errors, the Sentinel Database patch installation is complete. If there are errors, resolve the errors by referring to the error log files and re-run the PatchDb utility.

10 After the patch runs with no errors, restart the Sentinel services.

6 Post-Installation

The default date and time format in Sentinel Control Center can be overridden. For customizing the date and time format to your local time zone, see the Java Web site (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1 Edit the `SentinelPreferences.properties` file.

On Windows:

```
%ESEC_HOME%\config\SentinelPreferences.properties
```

On UNIX:

```
$ESEC_HOME/config/SentinelPreferences.properties
```

2 Remove the comment from the following line and customize the date and time format for Sentinel Control Center event date/time fields.

```
com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

For more information on post-installation setup, see Section 8, “Known Issues in Sentinel 6.1 SP1 Hotfix 2,” on page 9.

7 Defects Fixed in Sentinel 6.1 SP1 Hotfix 2

The following table lists the defects fixed in the Sentinel 6.1 SP1 Hotfix 2.

Table 1 *Defects Fixed in Sentinel 6.1 SP1 Hotfix 2*

Defect Number	Description
486590	Event Source Managemet (ESM) shuts down the collector as expected when a JavaScript collector is imported on top of a Legacy collector.
452100	SDM features that were present in Sentinel 6.0 SP2 HF5 are now included in Sentinel 6.1.
520098	SDM usage help is now complete.

Defect Number	Description
520100	The active user session no longer displays the IP address in hexadecimal format for client sessions.
529027	The JavaScript runtime error that appears while executing JavaScript actions on Sentinel 6.x platforms is now fixed.
532534	The exception error that appears when uninstalling a control whose namespace is deleted manually is now fixed.
532536	The Vulnerability tag does not get deleted from the *Event Configuration* window when uninstalling the solution pack that contains the Vulnerability tag.
534257	Custom indexing can now be used for the FIRST_ROWS in Oracle.
529072	Advisor reports now work.
451588	The IsNull operator works as expected on Filters.
534842	Active Views are now getting refreshed as expected when a filter is edited.

8 Known Issues in Sentinel 6.1 SP1 Hotfix 2

The following table lists the known defects in Sentinel 6.1 SP1 Hotfix 2.

Table 2 *Known Issues in Sentinel 6.1 SP1 Hotfix 2*

Defect Number	Description
530554	Sentinel Control Center (SCC) and Sentinel Solution Designers (SSD) launchers (shortcuts) do not launch the respective Sentinel applications on WIndows. Workaround: For SCC, right-click the shortcut icon > select *Properties* > *Shortcut* > replace the ...\control_center.exe file extension with ...\control_center.bat in the *Target* field. For SSD, right-click the shortcut icon > select *Properties* > *Shortcut* > replace the ...\solution_designer.exe file extension with ...\solution_designer.bat in the *Target* field.
532860	Database authentication fails if an invalid LDAP server hostname or IP address is entered while configuring Sentinel 6.1 for LDAP authentication. Solution: Ensure that a valid LDAP server hostname or IP address is entered.
534395	Exceptions are getting logged to the das_query_0.0.log file when the DAS query is started.
534306	Uninstallation of Sentinel fails as the Installshield still looks for JRE 1.5. Workaround: Uninstall Sentinel manually. For more information on uninstalling Sentinel, see Sentinel Settings (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4lc.html#bgpq4ld).

Defect Number	Description
537309	An exception error, `Invalid column index` appears when you try to import an Online Archived partition through the SDM GUI. Solution: Import operation is allowed only on the partitions that are in the Offline state. Delete the Online Archived partition from the SDM and then import.

9 Defects Fixed in Sentinel 6.1 SP1 Hotfix 1

The following table lists the defects fixed in Sentinel 6.1 SP1 Hotfix 1.

Table 3 *Defects Fixed in Sentinel 6.1 SP1 Hotfix 1*

Defect Number	Description
498817	A Collector no longer stops working when a legacy Collector is replaced with a JavaScript Collector.
498827	The connection mode used by Event Source now defaults to the default connection mode of the Collector, if the configured connection mode is invalid.
498870	The Start and Stop internal events are generated as expected when starting or stopping the JavaScript Collector.
484423	Collector Manager no longer runs out of memory when a data tap is opened on an active stream for a prolonged time period.
498871	ESM pays attention to the default attribute for Connection methods.
459625	SDM no longer lets you create impossible configurations with (at least) MS SQL.
491125	The Events View now gets updated properly after exceeding 125 partitions (max limit) in MS SQL.
451065	Releasing the Events table partitions releases the corresponding correlated Events table partitions.
458417	You can now rename the top node in ESM.
451599	You can now sort the Correlation rules.
489157	ADV_VULN_SIGNATURES and ADV_ATTACK_SIGNATURES procedures now contain the RPT_V suffix in the Oracle and the MS SQL database schema.
452167	SDM loading is now faster.
488526	There is no longer a NullPointerException error in DAS aggregation.
510547	The Solution Pack framework supports the Solution Packs that contain unsupported content.
509032	The SCC Help menu no longer displays an incorrect version number for SCC.
500900	You can now import the Sentinel-core Solution Pack, which has both Crystal* and Jasper* reports on Sentinel 6.1.
514275	The default route in the Global Filter configuration window no longer displays Drop.
486426	The McAfee* ePO collector now works as expected.

10 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

11 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 deliverables. 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.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web Page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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.