Novell Sentinel™ 6.1 SP1 Hotfix 1

July 08, 2009

Novell®

This document has the following information about Novell Sentinel™ 6.1 SP1 Hotfix 1:

1 Overview

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

NOTE: Sentinel 6.1 SP1 must already be installed before applying this hotfix.

This hotfix must be installed on all existing Sentinel 6.1 SP1 clients and servers. This includes machines with Sentinel Server, Correlation Engine, Sentinel Database, Collector Manager, Sentinel Control Center, Collector Builder, and Sentinel Data Manager.

2 Prerequisites

- If Sentinel 4.x or 5.x is installed, it must be upgraded to Sentinel 6.1.0.0 using the upgrade installer. Please see the Patch Installation Guide for instructions.
- If Sentinel is not yet installed, install Sentinel using the Sentinel 6.1.0.0 installer. Please see the Sentinel Installation Guide for instructions.
- Ensure that Sentinel 6.1 SP1 is installed.

The complete product documentation and the most recent version of the files are available at the Novell Sentinel 6.1 Documentation Web site (http://www.novell.com/documentation/sentinel61).

3 Installation

1. Login 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_6.1.1.1.zip*> file.

4 Close all Sentinel applications running on this machine, including:
   - Sentinel Control Center (SCC)
   - Sentinel Collector Builder
   - Sentinel Data Manager
   - Solution Designer

5 Stop the Sentinel service running on this 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*.

   6c 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`.

   6d Click *Continue*. If you are logged in as a user without administrative privileges, 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`

8 Press Enter when prompted to start the Hotfix installation procedure.

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

10 Repeat the above steps on every Sentinel server and client machine that has Sentinel software installed.

11 Restart Sentinel services on all machines:
   - On Windows: use *Windows Service Manager* to start the Sentinel services.
   - On UNIX: run `$ESEC_HOME/bin/sentinel.sh start`

NOTE: This Hotfix also contains a mandatory patch for the Sentinel Database.

---

12 Apply the database patch. For information on database patch installation, refer to "Sentinel Database Patch Installation" on page 3

4 Sentinel Database Patch Installation

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

4.1 Sentinel Database Patch Installation on Oracle

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

4.1.1 Prerequisites

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

- User has the Oracle client application sqlplus as the PATH variable.
- User has the environment variable `ORACLE_HOME` set to the directory where the Oracle software is installed.
- User must be a member of the Oracle dba group.
- User has the Java 1.5 executable as the PATH variable.

TIP: The easiest way to apply the patch is to run the PatchDB script directly on the database server machine provided 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 provided 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) 5.0] from the Sun Web site (http://java.sun.com/javase/downloads/index_jdk5.jsp)

4.1.2 Applying the Database Patch

1. Log in to the database server or another machine that has connection to the Sentinel Database.
2. Ensure that your machine meets the Java prerequisites.
3. Extract the <*SENTINEL_6.1.1.1.zip*> file.
4. On the command line, move to the installation directory that was just extracted.
5. Change to the <*install_directory*>/db_patch/bin directory.
6. Enter the `./PatchDb.sh` command to start the installation.
7. 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.

   After you press Enter, the script verifies the specified information and begins the database patch installation.
8. After the script is done with installing the patch, check for any errors. If there are no errors, the Sentinel Database patch installation is complete. Else, resolve the errors by referring to the error log files and re-run the PatchDb utility.
9. Restart the Sentinel services on all machines:
   - On Windows: use *Windows Service Manager* to start the Sentinel services.
   - On UNIX: run `$ESEC_HOME/bin/sentinel.sh start` command.

4.2 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 4
- “Installing Database Patch with Windows Authentication” on page 5
- “Installing Database Patch with SQL Server Authentication” on page 5

4.2.1 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 `esecdba` if you are using SQL Authentication.
- User has Java 1.5 executable as the PATH variable.

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 install Java, download the appropriate Java version [Java Runtime Environment (JRE) 5.0] from the Sun Web site (http://java.sun.com/javase/downloads/index_jdk5.jsp)

4.2.2 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 Server processes that are running.
3. Extract the <*SENTINEL_6.1.1.1.zip*> file.
4. Open the command prompt.
5. Change the directory to the <*install_directory*>\db_patch\bin directory. The <*install_directory*> is the directory where 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.

     After you press Enter, the script verifies the entered information and proceeds if authentication is successful.
8. After the script has done with 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.
9. After the patch runs with no errors, restart the Sentinel services.

4.2.3 Installing 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 Server processes that are running.
3. Extract the <*SENTINEL_6.1.1.1.zip*> file.
4. Open the command prompt.
5. Change the directory to <*install_directory*>\db_patch\bin directory. The <*install_directory*> is the directory where 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.

After you press Enter, the script verifies the entered information and proceeds if authentication is successful.

8 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.

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

5 Post-Installation

The default date and time format in SCC can be overridden. For customizing the date and time format to your local timezone, see the Java Web site (http://java.sun.com/j2se/1.5.0/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 Uncomment the following line and customize the date and time format for SCC event date/time fields.

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

6 Defects Fixed in Sentinel 6.1 SP1 Hotfix 1

This section lists the defects fixed in the Sentinel 6.1 SP1 Hotfix 1.

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

Defect Number	Description
498817	Collector stops working when a Legacy Collector is replaced with a JavaScript Collector.
498827	Connection Mode used by Event Source should default to the default connection mode of the Collector, if the configured connection mode is invalid.
498870	The Start and Stop internal events are not generated when starting or stopping the Javascript Collector.
484423	Collector Manager runs out of memory when a data tap is opened on an active stream for a prolonged time period.
498871	The ESM does not pay attention to the default attribute for Connection Methods.
459625	SDM lets you create impossible configurations with (at least) MS SQL.

Defect Number	Description
491125	The Events View is not updated properly after exceeding 125 partitions (max limit) in MS SQL.
451065	Releasing the Events table partitions does not release the corresponding correlated Events table partitions.
458417	Unable to rename the top node in ESM.
451599	Unable to sort the Correlation rules.
489157	ADV_VULN_SIGNATURES and ADV_ATTACK_SIGNATURES procedures do not contain the RPT_V suffix in Oracle and MS SQL database schema.
452167	The SDM loading is slow.
488526	NullPointerException error in DAS aggregation.
510547	TheSolution Pack framework does not support the Solution Packs that contain unsupported content.
509032	The Help menu displays an incorrect version number of SCC.
500900	Unable to import the Sentinel-core Solution Pack, which has both Crystal and Jasper reports on Sentinel 6.1.
514275	The default route of Global Filter's displays Drop.
486426	McAfee ePO collector fails for a few customers.

7 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

8 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.