Novell Sentinel 6.1 SP2 Hotfix 1

June 7, 2010

Novell.

Novell Sentinel is a security information and event management solution that provides a real-time, holistic view of security and compliance activities, while helping customers automatically monitor, report, and respond to network events across the enterprise.

- Section 1, “Overview,” on page 1
- Section 2, “Sentinel 6.1 SP2 Hotfix 1 Installation,” on page 1
- Section 3, “Sentinel Database Patch Installation,” on page 4
- Section 4, “Changing the Sentinel Control Center Date and Time Settings,” on page 6
- Section 5, “Renaming the Novell Built-In Collectors in the Database,” on page 7
- Section 6, “Defects Fixed in Sentinel 6.1 SP2 Hotfix 1,” on page 8
- Section 7, “Known Issues in Sentinel 6.1 SP2 Hotfix 1,” on page 9
- Section 8, “Documentation,” on page 11
- Section 9, “Legal Notices,” on page 11

1 Overview

This hotfix applies the latest software fixes and enhancements to an existing installation of Sentinel 6.1 SP2.

The hotfix must be installed on all existing Sentinel 6.1 SP2 client and server machines. This includes machines with the Sentinel server, Correlation Engine, Sentinel Database, Collector Manager, Sentinel Control Center (SCC), and Sentinel Data Manager (SDM).

For more information on the list of bugs fixed for this release, see Section 6, “Defects Fixed in Sentinel 6.1 SP2 Hotfix 1,” on page 8.

2 Sentinel 6.1 SP2 Hotfix 1 Installation

- Section 2.1, “Prerequisites,” on page 1
- Section 2.2, “Installing Sentinel 6.1 SP2 Hotfix 1,” on page 2

2.1 Prerequisites

The prerequisites depend on the Sentinel system version and platform. Carefully read each section below to determine the steps that apply to your environment.

- “Ensure That You Have the Correct Version of Sentinel Installed” on page 2
- “Back Up the Sentinel System” on page 2
- “Back Up the EVT_AGENT Table” on page 2
- “Add Partitions in all the Tables” on page 2

2.1.1 Ensure That You Have the Correct Version of Sentinel Installed

- If Sentinel is not yet installed, install it by using the Sentinel 6.1 SP2 full installer. See the *Sentinel 6.1 SP2 Installation Guide* for instructions.
- If Sentinel 6.1 is installed, ensure that you have upgraded it to Sentinel 6.1 SP2.

2.1.2 Back Up the Sentinel System

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

You should have a complete backup of the files on all the machines on which you are installing the patch, including the Sentinel database. At a minimum, you need a backup of the contents of the *ESEC_HOME* directory. This protects your system against unexpected installation errors.

2.1.3 Back Up the EVT_AGENT Table

The EVT_AGENT table is modified when you install Sentinel 6.1 SP2 Hotfix 1. Therefore, you should back up this table before installing the hotfix.

There are several methods to back up the database tables. Consult your DBA about the best method for your environment.The following examples use the Export utility of Oracle and BCP utility of MS SQL to back up the database tables:

Oracle

1 Log in to the Sentinel database server as the `oracle` user.

2 Execute the following command to export the `EVT_AGENT` table:

```
exp esecdba/<esecdba_password> tables=evt_agent
file=sentinel_sp2_tables.exp log=sentinel_sp2_tables.log
```

MS SQL

1 Log in to the Sentinel database server as the `administrator` user.

2 Execute the following command in the command prompt:

```
bcp <DB_NAME>.dbo.evt_agent out <BACKUP_DIR>\evt_agent.bcp -T -t "~" -n -U
<esecdba_username> -P <esecdba_password> -S <DB_HOST_NAME> -e
<BACKUP_DIR>\evt_agent.err
```

2.1.4 Add Partitions in all the Tables

If the Online Current partition is at P_MAX level, you should manually add partitions in all the tables by using SDM. Enable the SDM jobs by using the SDM partition configuration so that the Online Current partition does not reach the P_MAX level in future.

2.2 Installing Sentinel 6.1 SP2 Hotfix 1

1 Log in to the machine that has the Sentinel installation you want to update.

- **Linux/Solaris:** Log in as the `root` user.
- **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.
- **Other Windows Systems:** Log in as an Administrator.

2 Verify that the environment variables for Sentinel are set by running the following command:

- **Linux/Solaris:** `echo $ESEC_HOME`
- **Windows:** `echo %ESEC_HOME%`

3 Extract the *`<SENTINEL_6.1.2.1.zip>`* file.

4 Close all the Sentinel applications running on the machine, including:

- Sentinel Control Center
- Sentinel Collector Builder
- Sentinel Data Manager
- Sentinel Solution Designer (SSD)

5 Stop the Sentinel services running on the machine:

- **Linux/Solaris:** Run the `$ESEC_HOME/bin/sentinel.sh stop` command.
- **Windows:** Use Windows Service Manager to stop the Sentinel service.

6 Open the command prompt.

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

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 administrative 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, 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 installation

- **Linux/Solaris:** `./service_pack.sh`
- **Windows:** `service_pack.bat`

After you run the script, the `Sentinel 6.1 SP2 is the prerequisite for this patch installation` message appears.

8 Depending on whether Sentinel 6.1 SP2 is installed, decide whether to continue with the installation of the hotfix:

- **Linux/Solaris:** If Sentinel 6.1 SP2 is already installed, press y and continue with the installation. If Sentinel 6.1 SP2 is not installed, press n to terminate the installation, then install Sentinel 6.1 SP2.
- **Windows:** If Sentinel 6.1 SP2 is already installed, press Enter and continue with the installation. If Sentinel 6.1 SP2 is not installed, press Ctrl+C to terminate the installation, then install Sentinel 6.1 SP2.

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

10 After the installation is complete, log out and log in again to apply the environmental variable changes.

11. Repeat Step 1through Step 10 on every Sentinel server and client machine that has the Sentinel software installed.
12. Restart Sentinel services on all machines:
    - **Linux/Solaris:** Run `$ESEC_HOME/bin/sentinel.sh start`.
    - **Windows:** Use the Windows Service Manager to start the Sentinel services.

3 Sentinel Database Patch Installation

In addition to patching the Sentinel components, you must run a script to patch the database. The instructions are different depending on which database you have.

- Section 3.1, "Sentinel Database Patch Installation on Oracle," on page 4
- Section 3.2, "Sentinel Database Patch Installation on SQL Server," on page 5

3.1 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 4
- "Applying the Database Patch" on page 5

3.1.1 Prerequisites

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

- The `PATH` variable is set to `$ORACLE_HOME/bin`.
- The `ORACLE_HOME` environment variable is set to the directory where the Oracle software is installed.
- The user must be a member of the Oracle OS user group.
- The `PATH` environment variable is set to the Java 1.6 installation directory.

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, you can run the script 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`) and revert the permissions after executing the PatchDb script, 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 runtime environment (JRE) 6.0 from the Sun Web site (http://java.sun.com/javase/downloads/index.jsp).

3.1.2 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_6.1.2.1.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, then rerun the PatchDb utility.
11. Restart the Sentinel services on all machines:
    - **Linux/Solaris:** Run the `$ESEC_HOME/bin/sentinel.sh start` command.
    - **Windows:** Use Windows Service Manager to start the Sentinel services.

3.2 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 5
- "Applying the Database Patch" on page 6

3.2.1 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 `PATH` environment variable is set to the Java 1.6 installation directory.

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 runtime environment (JRE) 6.0 from the Sun Web site (http://java.sun.com/javase/downloads/index.jsp).

3.2.2 Applying the Database Patch

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

1. Log in to the database machine as the Windows Domain user (Sentinel database user).
2. Stop the Sentinel services.
3. Extract the *<SENTINEL_6.1.2.1.zip>* file.
4. Open the command prompt.
5. Change to the `<`*`installation_directory`*`>\db_patch\bin` directory.

   The install_directory is the directory where the Sentinel 6.1 SP2 Hotfix was just extracted.
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).
   - 1 for the Windows Authentication option or 2 for the SQL 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, then rerun the PatchDb utility.
10. After the patch runs with no errors, restart the Sentinel services.

4 Changing the Sentinel Control Center Date and Time Settings

The default date and time format in Sentinel Control Center is in the yyyy-mm-dd and HH:mm:ss.SSSZ format. You can customize the date and time format to your local time zone.

1. Log in to the Sentinel 6.1 server as the `administrator` user (Windows) or the `esecadm` user (Linux).

2 Edit the `SentinelPreferences.properties` file.

- **Linux/Solaris:**

  `$ESEC_HOME/config/SentinelPreferences.properties`

- **Windows:**

  `%ESEC_HOME%\config\SentinelPreferences.properties`

3 Remove the comment from 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
```

For more information, see the Java Web site (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

5 Renaming the Novell Built-In Collectors in the Database

This section is applicable if you have installed Sentinel 6.1 SP2 by using the full installer. The steps in this section are not applicable if you upgraded your machines to 6.1 SP2 from a previous version.

The Sentinel 6.1 SP2 full installer affects the reports for many of the Collectors that are built into the system as well as the reports for any Collectors that were run on Sentinel 6.1 SP2 before applying Sentinel 6.1 SP2 Hotfix 1 (this release). Collector specific reports do not return any data because the Collector name on which the reports filter does not match the Collector name in the Sentinel database.

The reason for this is that there are two representations of the Collector name, the internal name and the display name. The display name is used for report filtering (in the WHERE clause for the reports) and should be stored in the database in the AGENT field of the EVT_AGENT table when you run the Collector. Instead, the Sentinel 6.1 SP2 full installer stores the internal name.

Sentinel 6.1 SP2 Hotfix 1 fixes the issue by storing the Collector display name in the AGENT field of the EVT_AGENT table in the database, but you need to run a script that corrects the names that have already been stored in the database.

The script replaces the underscores (_) and hyphens (-) in the Collector name with a space in the Sentinel database, which makes the AGENT column equivalent to the Collector display name.

5.1 Fixing Built-In and Novell Written Collectors

1 Log in to the machine where you downloaded the Sentinel 6.1 SP2 Hotfix 1.

2 Change to the `Migration` directory.

   Oracle: `<`*`installation directory`*`>/db_patch/ddl/oracle/Migration`

   MS SQL: `<`*`installation directory`*`>\db_patch\ddl\mssql\Migration`

3 Run the script:

   Oracle: Run the following command as the `oracle` user at the SQL prompt:

```
sqlplus esecdba/(password)@(Oracle SID) < (installation directory)/
db_patch/ddl/oracle/Migration/update_collector_name.sql
```

   MS SQL: Double-click the `updated_collector_name.sql` file, connect to the Sentinel database as the `esecdba` user, then click *Execute*.

A message is displayed indicating that the Collector name is changed. For example, Microsoft_Active-Directory_6.1r3 is changed to Microsoft Active Directory 6.1r3.

NOTE: If the Collector name is not changed due to a name collision, you get a message indicating that the Collector name is not changed. You must modify the report such that it refers to the Collector by using both its internal name and display name. If you get any errors related to duplicate key rows, ignore the errors.

If a custom Collector name is changed as a result of executing the script, you must manually change the Collector name to its original name in the database.

5.2 Fixing SDK-Written Custom Collectors

Collectors that are written by using the Sentinel SDK follow the same naming conventions for display and internal names as Collectors written by Novell. To fix these custom Collectors, follow the instructions in Section 5.1, "Fixing Built-In and Novell Written Collectors," on page 7.

5.3 Fixing non-SDK-Written Custom Collectors

Custom Collectors that were not created by using the Sentinel SDK might not use the same naming conventions as Novell Collectors. Therefore, the script included with this hotfix will not fix the reporting issue.

For any custom reports that filter on a Collector name, the developer must be sure that the name in the report's WHERE clause matches the name in the AGENT field of the EVT_AGENT column for the Sentinel database. The developer can update the AGENT field or the report filter to address the issue.

6 Defects Fixed in Sentinel 6.1 SP2 Hotfix 1

Defect Number	Resolution
610613	The default Advisor feed is now getting processed as expected.
577377	Selecting the ALL option while running the `clean_database.bat` script now deletes all data that includes Incidents, Identities, Assets, Advisor, and Vulnerabilities.
596621	Sentinel initializes as expected when you install Sentinel 6.1 SP2 even while the Online Current partition is at P_MAX level in the AUDIT_RECORD table.
588031	Searching the database using DAS_Query is now much faster.
600039	A remote machine with only the Correlation Engine now routes events as expected without any errors.
592008	Events in the *Incidents* view now populate as expected even upon querying large datasets.
600038	The Collector Manager on the DAS server now routes events as expected.
578642	SDM partitions can now be imported without any errors, and the status changes from `Offline Archived` to `Online Archived Imported` as expected.

Defect Number	Resolution
593464	DAS_BINARY retrieves database statistics successfully even when the database size is over 6 TB.
543065	Collectors function as expected in the debug mode and identify the right directory in which the Collector plug-in is deployed.
604113	The Import Configuration icon now successfully imports an exported configuration to Event Source Management.

7 Known Issues in Sentinel 6.1 SP2 Hotfix 1

Defect Number	Description
605574	Unable to create PDF in Sentinel core solution pack.
582698	Sentinel 6.0 archive files can not be imported to the Sentinel 6.1 database.
610261	After you import the Asset backup data, the Asset data is not populated in the Asset report when you right-click an event or multiple events and click *Analyze* > Asset data. **Issue:** When you import the Asset backup data, the Asset data is imported to the Sentinel database, but the Asset data does not populate in the Asset report. **Workaround:** Clean up the Asset data, then run the generic Asset data Collector to get the new Asset data. The Asset report now populates the Asset data for the selected events. However, you can not view the Asset report for the Asset backup data. For information on cleaning up the Asset data, refer to the Database Backup and Cleanup section (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bhjo270.html).
605921	On a Windows Server 2003 platform with an MS SQL Server 2005 database (Windows Authentication), exceptions are logged while deleting a Domain user account. **Issue:** In Sentinel Control Center > *Admin* > *User Configuration* > *User Manager*, when you delete a domain user, the user account is deleted, but an error message is displayed indicating that `Error deleting user` and also exceptions are logged in the `das_query.log` file. **Workaround:** None. This is a user interface issue.
583540	An error is displayed indicating that JRE 1.6 is required when you upgrade the Sentinel database component machine from Sentinel 6.1 SP1 or Sentinel 6.1 SP1 Hotfix 1 to Sentinel 6.1 SP2. **Issue:** When you run the Patch_Db script to upgrade the Sentinel database component machine, an error is displayed indicating that the JRE 1.6 is required and it does not upgrade the Sentinel database. **Workaround:** Download and install Java SE Runtime Environment 6u12 from the Java Web site (http://java.sun.com/products/archive).

Defect Number	Description
552992	On a Windows Server 2008 platform with an MS SQL Server 2008 database, the Sentinel installation fails when you enter a weak password. **Issue:** The Sentinel installation fails if you specify a weak password while creating users such as esecadm, esecdba, esecapp, and esecrpt. An error is logged in the installation log files indicating that the password does not meet Windows policy requirements. **Workaround:** Specify a complex and strong password that meets the Windows policy requirements.
576963	On the Solaris platform, configuring multiple LDAP servers for failover does not work as expected. **Issue:** The Sentinel Server times out when logging into SCC/SSD as an LDAP user, if multiple LDAP servers are configured for failover and the primary LDAP server is powered off. **Workaround:** None. **NOTE:** Configuring multiple LDAP servers for failover works as expected only if the directory service is stopped in the primary LDAP server instead of shutting down the primary LDAP server machine.
577343	In Windows, the `Transaction Failed` message is logged in the incident cleanup log files after the Incidents are deleted. **Issue:** When you execute the `clean_database.bat` script to delete Incidents data, the data is deleted. However, the `Transaction Failed` message is included in the Incident clean up log files. **Workaround:** None. This is a user interface issue.

559096	SDM jobs do not trigger on the SLES 11 platform.
	Issue: SDM jobs are not triggering because the Oracle CJQ processes that run the scheduled jobs hang without generating any trace files.
	Workaround:
	1. Log in as the `oracle` user.
	2. Run the command to find the process ID:
	`ps -ef | grep cjq0`
	The process ID is in the following format:
	`ora_cjq0_<SENTINEL_DB_NAME>`
	3. Run the kill -9 command.
	`kill -9 <cjq processid>`
	4. Restart the Sentinel database.
	These steps should be performed only once after installing Sentinel 6.1 SP2.

Defect Number	Description
539514	A blank dialog box is displayed when you test the Sentinel Link Integrator configuration. **Issue:** Import a Sentinel Link Integrator. When you attempt to configure the Sentinel Link Integrator, if you click *Test Configuration* button in the Integrator Configuration Summary page, a blank dialog box is displayed. **Workaround:** In the Integrator Manager window, click *Save* to save the configuration, select the Integrator that you have configured, and test the configuration by using the *Test* button.
452116	The das_binary restarts automatically and creates memory dumps at `$ESEC_HOME/log` when the events are generated at a higher level. **Issue:** The das_binary restarts automatically and creates memory dumps while the system is under a load for database insertions and also when the DAS services are installed on a system with low amounts of RAM (2 GB), which does not meet Sentinel requirements. **Workaround:** Increase the `Xmx` parameter in the `$ESEC_HOME/config/configuration.xml` file to give additional memory to the das_binary for its large buffers. For more information, refer to the Novell support site (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005202&sliceId=2&docTypeID=DT_TID_1_1&dialogID=117088193&stateId=0%200%20117086548).

8 Documentation

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

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 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.