Novell Sentinel 6.1 SP2

April 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 monitor, report, and respond automatically to network events across the enterprise.

1 Overview

This service pack applies the latest software fixes and enhancements to an existing installation of Sentinel 6.1 SP1, Sentinel 6.1 SP1 Hotfix 1, and Sentinel 6.1 SP1 Hotfix 2.

The service pack must be installed on all existing Sentinel 6.1 SP1 client and server machines. This includes machines with the Sentinel server, Correlation Engine, Sentinel Database, Collector Manager, Sentinel Control Center (SCC), Collector Builder, and Sentinel Data Manager (SDM).

This service pack is mandatory for all users who subscribe to the Advisor data service.

2 What’s New in Sentinel 6.1 SP2

2.1 Supported Platforms

Sentinel 6.1 SP2 now supports the following platforms and databases:

- SUSE® Linux Enterprise Server (SLES) 11 64-bit
- Oracle* database 11g Release 2
- Oracle 10g with the latest patch 10.2.0.4

For more information, see System Requirements (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgmq7g2.html) in the *Sentinel 6.1 SP2 Installation Guide*.

2.2 New Features

Download Manager is a new feature that helps you to automatically update the Advisor data feed on your Sentinel 6.1 server. The Download Manager also enables you to configure automated downloads at specific intervals and notifies the Advisor process to process the downloaded feed on the Sentinel 6.1 server after the Advisor feed is downloaded.

For more information on Download Manager, see Download Manager (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bmfw15j.html) in the *Sentinel 6.1 SP2 User Guide*.

2.3 Enhancements

- "Advisor" on page 2
- "LDAP Authentication" on page 2
- "Database Cleanup Utility" on page 3

2.3.1 Advisor

This version of Sentinel includes a complimentary sample of the Advisor subscription data, which enables exploit detection.

A new user interface has been added to the SCC that enables you to:

- Download the Advisor data feed.
- Process the downloaded data feed either automatically or manually.
- Configure the Advisor products that need to be included for exploit detection.
- View the status of the processed feed.

For more information on Advisor, see Advisor (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bhj32op.html) in the *Sentinel 6.1 SP2 User Guide*.

2.3.2 LDAP Authentication

- LDAP authentication is now supported on Windows* and Solaris* platforms in addition to Linux* platform.

- A new option named *LDAP* is added in the *Admin* > *User Configuration* > *Add User* window of the SCC, which enables you to create user accounts using LDAP authentication.
- LDAP authentication can be performed with or without Anonymous searches on the LDAP directory.
- You can configure one or more LDAP servers as failover servers for LDAP authentication.

For more information on configuring a Sentinel server for LDAP authentication, see LDAP Authentication (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bmubfr0.html) in the *Sentinel 6.1 SP2 Installation Guide*.

2.3.3 Database Cleanup Utility

In addition to the option of cleaning the Incidents and Identities data from the Sentinel database, the database cleanup utility now enables you to clean the Advisor, Asset, and Vulnerability data from the Sentinel database.

For more information on the Database Cleanup utility, see Database Cleanup (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bhjo270.html) in the *Sentinel 6.1 SP2 User Guide*.

3 What's New 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.

- Section 3.1, "Global Filters," on page 3
- Section 3.2, "JRE Upgrade," on page 3
- Section 3.3, "LDAP Authentication," on page 3
- Section 3.4, "Collector Manager," on page 4

3.1 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).

3.2 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.

3.3 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).

3.4 Collector Manager

The EventRouter component of the Collector Manager handles internal functions such as processing maps and applying global filters on the events parsed by the Collector Manager. These processes can cause high CPU and RAM usage on a remote system.

With Sentinel 6.1 SP1 Hotfix 2 and later, you can configure a lightweight version of the Collector Manager on remote systems that have limited CPU and RAM. The internal functions of a Lightweight Collector Manager (LWCM) are handled by the Sentinel server (or whichever system is running DAS), so they consume less CPU and RAM on the remote system.

The EventRouter must be configured to operate in server and client modes on the DAS system and Collector Manager system. The Collector Manager system on which the EventRouter is configured to run in the client mode is referred to as the LWCM.

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).

4 What’s New in Sentinel 6.1 SP1 Hotfix 1

The Sentinel 6.1 SP1 Hotfix 1 applies the latest software fixes and enhancements to an existing installation of Sentinel 6.1 SP1. This patch does not include any new features.

5 Sentinel 6.1 SP2 Installation

- Section 5.1, “Prerequisites,” on page 4
- Section 5.2, “Installing Sentinel 6.1 SP2,” on page 6

5.1 Prerequisites

The prerequisites depend on the Sentinel system version and platform. Sentinel 6.1 SP2 must be installed on machines that have Sentinel 6.1 SP1 or later. Carefully read each section below to determine the steps that apply to your environment.

- If Sentinel 4.x or 5.x is installed, it must be upgraded to Sentinel 6.1.0.0 by using the upgrade installer. See the *Patch Installation Guide* for instructions.
- If Sentinel is not yet installed, install it by using the Sentinel 6.1 SP2 full installer. See the *Installation Guide* for instructions.
- If Sentinel 6.1 is installed, ensure that you have upgraded it to Sentinel 6.1 SP1.

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

- “Back Up the Sentinel System” on page 5
- “Back Up the AUDIT_RECORD Table” on page 5
- “Back Up the CONFIGS and USERS Tables” on page 5
- “Add Partitions in the AUDIT_RECORD TABLE” on page 6

5.1.1 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.

5.1.2 Back Up the AUDIT_RECORD Table

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

Starting with Sentinel 6.1 SP1 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 was not partitioned or archived prior to Sentinel 6.1 SP1 Hotfix 1, 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, use the following SQL command to truncate the `AUDIT_RECORD` table:

  ```
  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 depends on your environment; consult your Database Administrator (DBA) for adequate settings.

5.1.3 Back Up the CONFIGS and USERS Tables

The `CONFIGS` and `USERS` tables are modified when you install Sentinel 6.1 SP2. Therefore, you should back up these tables before installing this service pack.

There are several methods to back up the database tables. 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 `CONFIGS` and `USERS` tables:

   ```
   exp esecdba/<esecdba_password> tables=users,configs
   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:

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

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

5.1.4 Add Partitions in the AUDIT_RECORD TABLE

If the Online Current partition is at P_MAX level in the AUDIT_RECORD table, you should add partitions in the AUDIT_RECORD table by using SDM.

5.2 Installing Sentinel 6.1 SP2

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

- **Linux/Solaris:** Log in as `root`.
- **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 one of the following commands:

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

3 Extract the *`<SENTINEL_6.1.2.zip>`* file.

4 Close all 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 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, you are prompted to authenticate as an administrative user.

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

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

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

8 Depending on whether Sentinel 6.1 SP1 is installed, decide whether to continue with the installation of the service pack:

- **Linux/Solaris:** If Sentinel 6.1 SP1 is already installed, press y and continue with the installation. If Sentinel 6.1 SP1 is not installed, press n to terminate the installation and install Sentinel 6.1 SP1.
- **Windows:** If Sentinel 6.1 SP1 is already installed, press Enter and continue with the installation. If Sentinel 6.1 SP1 is not installed, press Ctrl+C to terminate the installation and install Sentinel 6.1 SP1.

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

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

11 Repeat Step 1 through Step 2 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.

6 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 6.1, “Sentinel Database Patch Installation on Oracle,” on page 7
- Section 6.2, “Upgrading the Database from Oracle 10g to Oracle 11g,” on page 9
- Section 6.3, “Sentinel Database Patch Installation on SQL Server,” on page 10

6.1 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 8
- “Applying the Database Patch” on page 8

6.1.1 Prerequisites

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

- The user has the PATH variable set to $ORACLE_HOME/bin.
- The user has the ORACLE_HOME environment variable set to the directory where the Oracle software is installed.
- The user must be a member of the Oracle OS user group.
- The user has the Java* 1.6 executable included in 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, 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).

6.1.2 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.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 rerunning 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.

6.2 Upgrading the Database from Oracle 10g to Oracle 11g

NOTE: There are several methods to upgrade the database from Oracle 10g to Oracle 11g. This section provides instructions on upgrading the database manually.

1 Shut down all the Sentinel applications.

2 Install the Oracle 11g software on a new `ORACLE_HOME` and `ORACLE_BASE` directory. For more information, refer to the Oracle Documentation Web site (http://www.oracle.com/technology/documentation/database.html).

3 Verify the database for upgrading to Oracle 11g by using the pre-upgrade information tool (`utlu111i.sql`).

The SQL script is available at the Oracle 11g location, `oracle_home/rdbms/admin/utlu111i.sql.` Run the script from the source database (Oracle 10g).

4 Connect to the database `sysdba` and run the following script:

```
SQL>spool upgrade_info.log
SQL>@/11g_oracle_home/rdbms/admin/utlu111i.sql
```

5 Open the `upgrade.info` log file and check for any errors. If there are any errors, download and install the required patch files from the Oracle Web site (https://support.oracle.com/).

6 Specify the following parameters in the initialization parameter file:

```
diagnostic_dest= $ORACLE_BASE/diag
memory_max_target=1GB
memory_target= 800m
compatible= 11.1.0
```

7 Shut down the Oracle 10g database:

```
SQL>shutdown immediate
```

8 Set the `ORACLE_HOME` and `ORACLE_BASE` environment variables to the Oracle 11g software.

9 Use the new parameter values to Connect to Oracle 11g.

10 Start the database in the upgrade mode:

```
SQL> startup upgrade
```

11 Use the `catupgrd.sql` script to upgrade the database:

```
SQL> spool upgrade.log
SQL> @/rdbms/admin/catupgrd.sql
```

12 Open the `upgrade.log` file and check for errors. If there are any errors, download and install the required patch files from the Oracle Web site (https://support.oracle.com/).

13 Run the utlu111s.sql post upgrade script:

```
SQL>startup
SQL>@/rdbms/admin/utlrp.sql
```

14 Check the status of database components and ensure that all components are using the Oracle 11g version.

```
SQL>select comp_name,version,status from dba_registry
```

15 Copy the tnsnames.ora, listener.ora, sqlnet.ora files from the Oracle 10g source ORACLE_HOME to the Oracle 11g ORACLE_HOME.

16 Shut down the database and start the database, database listener, Sentinel, and all other services.

6.3 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 10
- "Applying the Database Patch" on page 10

6.3.1 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 must have the Java 1.6 executable included in 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 runtime environment (JRE) 6.0 from the Sun Web site (http://java.sun.com/javase/downloads/index.jsp).

6.3.2 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.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 service pack 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).
- 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 and rerunning the PatchDb utility

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

7 Post-Installation

- Section 7.1, "Changing the Date and Time Settings," on page 11
- Section 7.2, "Changing the SCC and SSD Shortcut Icon Properties," on page 11

7.1 Changing the Date and Time Settings

The default date and time format in SCC 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.

- **Linux/Solaris:**

  `$ESEC_HOME/config/SentinelPreferences.properties`

- **Windows:**

  `%ESEC_HOME%\config\SentinelPreferences.properties`

2 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
```

7.2 Changing the SCC and SSD Shortcut Icon Properties

The following procedure is applicable only if you have upgraded Sentinel 6.1 from 6.1 SP1 Hotfix 2 to Sentinel 6.1 SP2 and if you had modified the SCC and SSD shortcut icon properties after applying 6.1 SP1 Hotfix 2.

1 Right-click the SCC or SSD shortcut icon.

2 Select *Properties* > *Shortcut*.

3 Change the filename in the *Target* field.

SCC: Replace the `%ESEC_HOME%\bin\control_center.bat` file extension with `%ESEC_HOME%\bin\control_center.exe`.

SSD: Replace the `%ESEC_HOME%\bin\solution_designer.bat` file extension with `%ESEC_HOME%\bin\solution_designer.exe`.

8 Defects Fixed in Sentinel 6.1 SP2

The following table lists the defects fixed in Sentinel 6.1 SP2.

Table 1 *Defects Fixed in Sentinel 6.1 SP2*

Defect Number	Resolution
557842	JavaScript* Actions or framework works without any memory leakage.
548450	The Sonic Management Console works with JRE version 1.6.
559451	Sentinel 6.0 SDM archives can be successfully imported to Sentinel 6.1.
556521	Variables can be added or edited in the iTRAC^{TM} process.
546679	The Sentinel Control Center can be launched when connected through VPN.
544821	Duplicate events in the `das_binary.xml` file allow data insertion to complete in MS SQL.
542156	All the events generated in a remote Collector Manager machine are successfully transferred to the Sentinel server.
451593	Attachments with short filenames (fewer than 3 characters) can be viewed in the Solution Manager.
451099	Importing of a database partition works as expected when the archive contains the EventInsertionFailed-*-Failed internal event.
521698	Advisor processes all the downloaded feed files as expected and resumes processing the feed files if it was stopped abruptly.
477615	The Event Configuration window in the Sentinel Control Center > *Admin* tab can be opened.
556249	The raw data that is written to the files by the Connectors in ESM is in JSON* format.
542772	Internal DbSpaceLow events are generated as expected in MS SQL 2008.
570411	The *Tablespace* tab in SDM displays as expected even when the database size exceeds terabytes.

9 Known Issues in Sentinel 6.1 SP2

The following table lists the known defects in Sentinel 6.1 SP2.

Table 2 Known Issues in Sentinel 6.1.2

Defect Number	Description
596621	The `esec_insert_AUDIT_RECORD_P_MAX` and `esec_insert_AUDIT_RECORD_P_MIN` procedures of the AUDIT_RECORD table are missing in the MS SQL database schema. **Issue:** When the Online Current partition is at P_MAX level in the AUDIT_RECORD table and you install Sentinel 6.1 SP2, Sentinel does not initialize as expected. **Workaround:** Before installing Sentinel 6.1 SP2, add partitions to the AUDIT_RECORD table by using SDM.
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).
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.
577377	On the Windows platform, the `clean_database.bat` script does not work if you select the `All` option. **Issue:** While executing the `clean_database.bat` script, if you select the `All` option, the script deletes only the Incidents and Identities data, and exits the screen. The script does not delete the Assets, Advisor, and Vulnerabilities data. **Workaround:** Use the specific options for deleting the individual data.
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.

Defect Number	Description
577345	The clean_database script goes into an infinite loop if invalid information is specified while executing the script. **Issue:** While executing the clean_database script, if you specify an invalid option other than the options displayed, the script goes into an infinite loop. **Workaround:** Cancel the script, then rerun the script and provide valid information.
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.
576974	An invalid message is displayed in Download Manager while you add or edit a download configuration. **Issue:** If you add or edit a download configuration, then click the *Validate* button to validate the URL and login credentials, the `Url and Credentials are invalid` message is displayed even if the specified URL and login credentials are valid. **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.

539514	A blank dialog box is displayed when you testing 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.

Defect Number	Description
561825	Environment variables are not deleted when you uninstall Sentinel 6.1 SP2. **Issue:** Environment variables such as `ESEC_HOME`, `ESEC_JAVA_HOME`, `ESEC_VERSION`, `ESEC_CONF_FILE`, `WORKBENCH_HOME`, and entries in the `PATH` variable are not deleted when you uninstall Sentinel 6.1 SP2, and they block the Sentinel installation unless they are deleted. **Workaround:** Delete all the ESEC environment variables manually. ◆ Linux: 1. Open the `/etc/profile.d/sentinel_env.sh` and `/etc/profile.d/sentinel_env.csh` files in a text editor. 2. Delete the installshield variable section and reboot the machine. ◆ Windows: 1. Right-click *My Computer* > *Properties* > *Advanced* > *Environment Variables*. 2. Select `ESEC_VERSION` and click *Delete*. 3. Click *OK* and restart the machine.
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).

10 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 3** Defects Fixed in Sentinel 6.1 SP1 Hotfix 2*

Defect Number	Resolution
486590	Event Source Management (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.
520100	The active user session no longer displays the IP address in hexadecimal format for client sessions.

Defect Number	Resolution
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.

11 Defects Fixed in Sentinel 6.1 SP1 Hotfix 1

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

Table 4 *Defects Fixed in Sentinel 6.1 SP1 Hotfix 1*

Defect Number	Resolution
498817	Collectors work as expected when a Legacy Collector is replaced with a JavaScript Collector.
498827	Connection Mode used by Event Source selects 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 you start or stop the JavaScript Collector.
484423	Collector Manager works as expected when a data tap is opened on an active stream for a prolonged time period.
498871	Connectors set with the `default` attribute for Connection methods are now displayed as the default connectors in Event Source Management.
491125	The Events View is now updated properly after exceeding 125 partitions (max limit) in MS SQL.
451065	Releasing the Events table partitions now releases the corresponding correlated Events table partitions.
458417	You can now rename the top node in ESM.
451599	Correlation rules can now be sorted.
489157	ADV_VULN_SIGNATURES and ADV_ATTACK_SIGNATURES procedures now include RPT_V as suffix in Oracle and MS SQL database schema.
452167	The SDM loading is now much faster.
488526	Oracle does not throw a NullPointerException error in DAS aggregation.

Defect Number	Resolution
510547	The Solution Pack framework now supports Solution Packs that contain unsupported content.
509032	The Help menu in SCC displays the correct version number of SCC.
500900	You can now import Sentinel-core Solution Pack that has both Crystal and Jasper reports on Sentinel 6.1.
514275	The default route of Global Filter now displays Database and GUI.
486426	The McAfee* ePO collector works as expected.

12 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 (® , ™, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark

13 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.

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.