Novell Sentinel™ 6.0 SP2

Released January 10, 2008

The information in this ReadMe file pertains to Novell Sentinel™ 6.0 SP2, which 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.

This Service Pack will apply the latest software fixes and enhancements to an existing installation of Sentinel 6.0 or Sentinel 6.0 SP1. Sentinel 6.0.0.0 must already be installed before applying this Service Pack, but SP1 is not necessary; SP2 is inclusive of all fixes and feature that are in SP1.

The Service Pack must be installed on all machines, client and server, with an existing Sentinel 6.0 or Sentinel 6.0 SP1 installation. This includes machines with Sentinel Server, the Correlation Engine, Sentinel Database, Collector Manager, Sentinel Control Center, Collector Builder, and Sentinel Data Manager.

- If Sentinel is not installed yet, it must be installed using the Sentinel 6.0.0.0 installer. Please see the Sentinel Installation Guide for instructions
- If Sentinel 5.x is installed, it must be upgraded to Sentinel 6.0.0.0 using the upgrade installer. Please see the Patch Installation Guide for instructions.
- If Sentinel 4.x is installed, Sentinel 6.0.0.0 must be installed using the Sentinel 6.0.0.0 installer. Some data can be migrated to the Sentinel 6.0.0.0 installation. Please see the Patch Installation Guide for instructions.

The full product documentation and the most recent version of this file are available at the following URL: http://www.novell.com/documentation/sentinel6.

What's New in Sentinel 6.0 SP2

Sentinel 6 SP2 is a maintenance release for Sentinel that is inclusive of SP1. In addition to bug fixes, it contains a limited number of new and enhanced features.

Solution Designer (added in SP2)

Sentinel 6 SP2 introduces the Sentinel Solution Designer, a new application that is used to package a set of Sentinel content, organized into controls that address common regulatory concerns. The Solution Designer packages Sentinel correlation rules, dynamic lists, maps, reports, and iTRAC workflows along with a description of the requirement the control was designed to fulfill, implementation instructions, and testing steps to ensure that the control is working as expected. The Solution Designer packages all of this information into a single, easily-installed Solution Pack, creating an integrated solution to solve a specific business problem.

Solution Designer functionality is described in detail in the “Solution Packs” chapter of the Sentinel Installation Guide.

Solution Manager (added in SP2)

The Sentinel Solution Manager is a new interface in the Sentinel Control Center, designed to install and manage Solution Packs created using Solution Designer. Solution Packs may be custom or provided by Novell. Combinations of Sentinel content are managed as integrated controls, simplifying the process of installing, implementing, and testing the Sentinel system.

Solution Manager functionality is described in detail in the “Solution Packs” chapter of the Sentinel Installation Guide.

JavaScript-based Correlation Actions (added in SP2)

Sentinel 6 SP2 includes the ability to create powerful and flexible correlation actions using JavaScript. These scripts can make calls to the Sentinel correlation API and can be debugged in the Sentinel Control Center.

JavaScript Correlation Action functionality is described in detail in the "Execute Script" section of the *"Correlation"* chapter of the *Sentinel User Guide*. Documentation on the correlation API can be found under Sentinel JavaScript Correlation Action API on the Novell documentation site:

http://www.novell.com/documentation/sentinel6

Advisor Updates

Sentinel 6 SP2 includes a new release of the Advisor vulnerability and exploit data feed. This new release expands the devices and signatures that are supported. Current Advisor users will need to be aware of several issues as they move to the new Service Pack:

- **Integration with Novell Login**: The new Advisor system uses a Novell eLogin account associated with the customer's purchase information to connect to the Advisor server, the same account used to log into the Novell Customer Care portal. The previous credentials supplied with the Advisor license are not valid after the SP2 patch is applied. Contact Novell Technical Support for any questions about creating a Novell eLogin account with the appropriate entitlements to Sentinel.
- **Increased data storage requirements:** Because the Advisor feed now supports a much larger set of devices and signatures the data storage requirements have increased. Novell recommends approximately 50 gigabytes dedicated to store Sentinel Advisor data.
- **Sentinel 6 Advisor Core Data DVD:** The Sentinel 6 Exploit Detection and Advisor Core Data disk, which contains a snapshot of the Advisor data, significantly decreases the amount of time and network bandwidth required to perform the initial data load. This package is available as a download or a media kit through the Novell Customer Care Portal. Novell highly recommends that Advisor users obtain this DVD prior to applying Service Pack 2.

IMPORTANT;

With Service Pack 2, previously downloaded Advisor tables are no longer used and are dropped during service pack installation. If Advisor is installed with the Direct Internet Download option, the system will start downloading the new data on the previously scheduled basis. However, due to the increased quantity of data, direct internet download of the entire database is not recommended.

To minimize bandwidth usage, Novell recommends either immediately installing the data snapshot using the Sentinel 6 Exploit Detection and Advisor Core Data disk or temporarily disabling the scheduled downloads using crontab or the Windows Scheduler until the data snapshot can be loaded.

Advisor functionality and how to use the Advisor Core Data DVD is described in detail in the *"Advisor"* chapter of the *Sentinel Installation Guide.*

Red Hat Enterprise Linux 4 Support (added in SP1)

Sentinel 6 supports Red Hat Enterprise Linux 4 on x86_64 hardware.

Enhancements to the ESM Framework (added in SP1)

The new Event Source Management framework in Sentinel 6 has been enhanced to improve performance and usability. The Graphical view now automatically contracts child nodes into the parent if more than 20 children are present, and adds a dedicated frame to manage child nodes. This prevents performance degradation and display clutter that can occur with large numbers of nodes. A new "Magnifying Glass" option is also included that enlarges a portion of the screen without changing the overall view.

Export Raw Events to a File (added in SP1)

A new configuration option on all Connector nodes allows the raw data from that connector to be saved to a text file. This can be used to store the raw data in unaltered form. This also is useful for debugging and testing Sentinel data collection.

New JavaScript Based Collector Engine (added in SP1)

Sentinel 6 includes a new technology that allows collector development using JavaScript based event collectors in addition to the existing proprietary Sentinel collectors. This provides a platform for Novell's customers and partners to build high quality, feature-rich collectors using an industry standard programming language. Sample collectors written in JavaScript are available on request from Novell Technical Support.

Installation

The instructions provided in this document are for installing this Service Pack only. This Service Pack can be run against an existing installation of Sentinel™ 6.0 or Sentinel™ 6.0 SP1.

Service Pack Installation

This Service Pack comes with an automated installer that will backup the existing software components that will be replaced. The backup files are placed in a directory named "SP<id>_<date>_bak" under the ESEC_HOME directory, where <id> is the numeric identifier of the service pack and <date> is the date of the Service Pack (for example, "SP2_2008-01-03-GMT_bak").

NOTE: It is highly recommended that a complete backup be made of the machine on which you are installing the service pack. If this is not possible, then at a minimum a backup of the contents of the ESEC_HOME directory should be made. This will help protect your system against unexpected installation errors.

To install the Service Pack:

1. Login as an Administrator (Windows) or as root (UNIX).
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 Service Pack zip file.
4. Close all Sentinel applications running on this machine, including:
   - Sentinel Control Center
   - Sentinel Collector Builder
   - Sentinel Data Manager

5. Shut down Sentinel service running on this machine:

   On Windows, use Windows Service Manager to stop the “Sentinel” services.

   On UNIX, run $ESEC_HOME/bin/sentinel.sh stop
6. On the command line, return to the extracted Service Pack top level directory and run the service_pack script to start the Service Pack installer:

   On Windows:

   ```
   .\service_pack.bat
   ```

   On Unix:

   ```
   ./service_pack.sh
   ```
7. When prompted, press the <ENTER> key to start the Service Pack installation procedure.
8. Repeat the steps above on every machine with Sentinel software installed. This is required for all machines with any Sentinel software, including Sentinel server and client software.
9. This Service Pack also contains a mandatory patch to the Sentinel Database. Apply the database patch by performing the appropriate steps below for the database platform you are using.

Database Patch Installation on Oracle

The following steps must be performed on the machine with an Oracle Sentinel Database installed to prepare the database for SP2. The Sentinel Database patches for Oracle include two scripts:

- The first part is a “pre-patch” script (PrePatchDb_60.sh) that must be run directly on the database server machine.
- The second part is the main patch script (PatchDb.sh). Although it is easiest to run both scripts directly on the database server machine, local policies may prohibit this (for example, if you cannot install Java on the database server). Therefore, this script can be run remotely from any machine that has Java version 1.5 and the Oracle client tools installed.

Pre-Patch Script for Oracle

There are several prerequisites to running the pre-patch script for Oracle:

- The patch must be copied to a machine that is running the Oracle Sentinel Database and a UNIX operating system supported for Sentinel
- Administrator must be able to log in as a user with Oracle DBA operating system group permissions

How to run the pre-patch script for the Oracle database:

1. Shut down the Sentinel Server processes (if they are running).
2. Log into the machine as a user that meets the installation prerequisites for this script.

   NOTE: The *root* user typically does not have these permissions. In a default install, the *oracle* user has the necessary permissions.
3. Go to the following directory under the extracted Service Pack directory:

   ```
   ./db_patch/bin
   ```

4. Execute the following command to initiate the “pre-patch” install step.

   ```
   ./PrePatchDb_60sp1.sh <database_name>
   ```

   For Example:

   ```
   ./PrePatchDb_60sp1.sh ESEC
   ```

Main Patch Scripts for Oracle

There are several prerequisites to running the pre-patch script for Oracle:

- The patch must be copied to a machine that is running a UNIX operating system supported for Sentinel
- User has the Oracle client application *sqlplus* in its *PATH*
- User has the environment variable *ORACLE_HOME* set to the directory where the Oracle software is installed.
- User has the Java 1.5 executable *java* in its *PATH*

TIP: If you cannot run the main patch script directly on the database server, any other machine with Sentinel 6.0 or above already has the necessary version of Java installed and might be an easy location to initiate the main patch installation.

However, the $ESEC_HOME/jre directory does not allow the oracle user access by default. Therefore, you can add the oracle user 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 using a non-Sentinel machine, the Java version and PATH variable settings can be verified by running the following command from a command line:

```
java -version
```

If necessary, the PATH environment variable can be updated to include the java installation directory, for example:

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

If Java is not installed on the non-Sentinel machine, the correct Java version [Java Runtime Environment (JRE) 5.0] can be downloaded from the following URL:

http://java.sun.com/javase/downloads/index_jdk5.jsp

To run the main patch script for Oracle:

1. Log in to the database server or another machine as a user that meets the installation prerequisites for this script.
2. Verify that your machine meets the Java prerequisites for running this script.
3. Extract the Service Pack zip file.
4. On the command line, go into the Service Pack top level directory that was just extracted.
5. Change directories to the following directory under extracted Service Pack top level directory.

   ```
   db_patch/bin
   ```

6. Enter the following command.

   ```
   ./PatchDb.sh
   ```

7. Follow the prompts and enter the following information:

- Hostname or static 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 final time, the script will verify the entered information and begin the database patch.

8. After the script is done applying the patch, check for any errors. If there are no errors, you are done with the Sentinel Database patch. If there are errors, resolve the errors and re-run the PatchDb utility.

Database Patch Installation on SQL Server

The following steps must be performed on the machine with a Microsoft SQL Server database to prepare the database for SP2. There is one main patch script for SQL Server (PatchDb.bat).

Main Patch Scripts for SQL Server

There are several prerequisites to running the pre-patch script for SQL Server:

- The patch must be copied to the machine that is running the Sentinel database.
- The patch must be run using the Sentinel Database User credentials, *esecdba* if using SQL Authentication

To run the database patch script for database on MSSQL with Windows Authentication:

1. Log into the database machine as the Windows Domain user that is the Sentinel Database User.
2. Shut down the Sentinel Server processes (if this has not already been done).
3. Extract the Service Pack ZIP file (if this has not already been done).
4. Open a command prompt.
5. Change directories to the following directory under the extracted Service Pack directory:

   ```
   db_patch\bin
   ```

6. Enter the command:

   ```
   .\PatchDb.bat
   ```

7. Follow the prompts and enter the following information:
   - Hostname or static 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 final time, the script will verify the entered information and proceed if authentication is successful.

8. Enter the language character set support option (1 for Unicode Database or 2 for ASCII Database).

NOTE: For the character set support prompt, select the same option you selected when you initially installed the Sentinel 6.0 Database. If your database was initially installed using Sentinel 5.x, it was installed as an ASCII database.

After you press *Enter*, the script will begin applying the database patch.

9. After the script is done applying the patch, check for any errors. If there are errors, resolve the errors and re-run the PatchDb utility.
10. After the patch runs with no errors, Sentinel services can be restarted.

To run the database patch script for database on MSSQL with SQL Authentication:

1. Log into the database machine as the Windows Domain user that is the Sentinel Database User.
2. Shut down the Sentinel Server processes (if this has not already been done).
3. Extract the Service Pack ZIP file (if this has not already been done).
4. Open a command prompt.
5. Change directories to the following directory under the extracted Service Pack directory:

   ```
   db_patch\bin
   ```

6. Enter the command:

   ```
   .\PatchDb.bat
   ```

7. Follow the prompts and enter the following information:
   - Hostname or static 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's password

   After you press *Enter* the final time, the script will verify the entered information and proceed if authentication is successful.
8. Enter the language character set support option (1 for Unicode Database or 2 for ASCII Database).

NOTE: For the character set support prompt, select the same option you selected when you initially installed the Sentinel 6.0 Database. If your database was initially installed using Sentinel 5.x, it was installed as an ASCII database.

After you press *Enter*, the script will begin applying the database patch.

9. After the script is done applying the patch, check for any errors. If there are errors, resolve the errors and re-run the PatchDb utility.
10. After the patch runs with no errors, Sentinel services can be restarted.

Updating Permissions for Solution Designer and Manager

After installing the service pack, you must update the permissions for any users who will use Solution Designer or Manager.

To grant permissions for the Solution Pack:

1. Log into the Sentinel Control Center as a user with permissions to use the User Manager.
2. Go to the *Admin* tab.
3. Open the User Configuration folder.
4. Open the *User Manager* window.
5. Click the *Permissions* tab.
6. Select Solution Designer, Solution Manager, or Solution Pack (which will automatically select both child permissions). The new permissions will be applied the next time the user logs in.

Installing Advisor Data Snapshot

Although the initial Advisor data load can be performed using the scheduled service (Direct Internet Download) or even manually, with the additional signatures added to the data feed starting in Sentinel 6.0 SP2, this approach is no longer recommended.

The Sentinel 6 Exploit Detection and Advisor Core Data significantly decreases the amount of time and network bandwidth required to perform the initial data load. This snapshot of the Advisor data is available as a download or a media kit from the Novell Customer Care Portal.

The initial data load may take as long as 24 hours, depending on the machine specifications and other loads on the database server.

After the initial data load, incremental updates can be loaded manually or using the Direct Internet Download feature.

IMPORTANT:

The data installer for Advisor works only with Sentinel 6.0 SP2 and above after the appropriate database patches have been applied as part of the patch installation process. The upgrade process and data installer drop and replace all Advisor data that was downloaded prior to Sentinel 6.0 SP2.

To download data snapshot of Advisor:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel 6 Advisor Core Data installation disk.
3. Start the installation program by going to the install directory on the CD-ROM and
   - On Solaris/Linux, run advisor_bcp_in.sh
   - On Windows, run advisor_bcp_in.bat
4. In the console, provide the appropriate DB credentials:
   - On Linux, enter the database user name (esecdba by default), password, and Oracle SID (instance name).
   - On Windows, enter the database host name, database name (ESEC by default), and authentication mode for the database. If using SQL Authentication, you must also enter the database user name (esecdba by default) and password.
5. Enter the time to pause in seconds between processing each file. The default is 0 seconds, but this can be paused if database load is high to introduce a pause between processing data files.
6. To increase the efficiency of the data loading process, the system disables indexes and constraints on the Advisor tables and truncates the Advisor tables. The following message is displayed:

```
Disabling indexes on the Advisor tables…

Successfully disabled indexes on the Advisor tables

Disabling constraints on the Advisor tables...

Successfully disabled constraints on the Advisor
   tables

Truncating Advisor tables...

Successfully truncated Advisor tables
```

7. The Advisor script starts and the bulk data is fed into the appropriate table. The snapshot of the data is stored in the database.
8. After all files in the snapshot have been loaded, it enables constraints, rebuilds indexes, and displays the following messages:

   ```
   Successfully enabled constraints on the Advisor tables

   Successfully rebuilt indexes on the Advisor tables
   ```

9. On completion of bulk feed, the system displays successful completion message.

Regular incremental Advisor data updates should be planned (either scheduled using Direct Internet Download or manually) to bring and keep the Advisor database up to date.

Resetting Advisor Authentication (Direct Download Only)

If you were running Advisor in Direct Download mode in Sentinel 6.0 SP1 or before, the credentials used for Advisor authentication must be updated after applying the SP2 service pack.

There is no need to update the password if you are running Advisor in a Standalone configuration. In this mode, the password is entered manually and not stored in a file.

To reset the password for automatic Advisor downloads:

1. For UNIX, log into the machine where Advisor is installed as the Sentinel Administrator User (esecadm by default). For Windows, login as a user with administrative rights.
2. Go to the following location:

   For UNIX:

   ```
   $ESEC_HOME/bin
   ```

   For Windows:

   ```
   %ESEC_HOME%\bin
   ```

3. Execute the following command:

   For UNIX:

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   For Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

   where <newpassword> is the updated Advisor password.

To reset the username for automatic Advisor downloads:

1. For UNIX, log into the machine where Advisor is installed as the Sentinel Administrator User (esecadm by default). For Windows, login as a user with administrative rights.
2. Edit the advisor_client.xml file.
3. Change the username value to the Novell eLogin username. For example:

   <property name="username">BobJones</property>

4. Save the file.

Updating the Web Server for Direct Report Publication

Publishing (or deleting) reports directly from the Solution Manager to (or from) the Crystal Report Server is possible if the web server is configured properly.

The following procedure assumes that the Crystal Server has already been configured to run Sentinel reports. If the Crystal Server has not been configured yet, see Crystal Reports for Linux or Crystal Reports for Windows in *Sentinel Installation Guide* and follow all of the instructions there.

To configure direct report publishing for Apache Tomcat:

1. Perform all other web configuration steps for Sentinel. For more information, see the "Patching Crystal Reports for Use with Sentinel" section of the Crystal Reports for Linux chapter in the *Sentinel Installation Guide*.
2. Verify that the following directory has been created:

   ```
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/
   ```

3. Go to reports_patch/Tomcat in the service pack top-level directory and copy the files publish_report.jsp and delete_report.jsp to the esec-script directory.
4. Set the permissions and ownership for these two files to the following values:

   ```
   -rwxr-xr-x 1 crystal bobje
   ```

5. If Crystal was installed in a non-default location or was installed as a system install, modify the String BOBJHome setting in publish_report.jsp and delete_report.jsp files to the Crystal Reports installation path. For example:

   ```
   String BOBJHome =
      ”/opt/crystal_xi/bobje/enterprise115"
   ```

   If Crystal was installed as the designated Crystal user into the default location, no changes should be necessary to this parameter.
6. After modifying the .jsp files, you must restart the Tomcat web server so the changes take effect.

To configure direct report publishing for Microsoft IIS:

1. Perform all other web configuration steps for Sentinel. For more information, see the "Patching Crystal Reports for Use with Sentinel" section of the Crystal Reports for Windows chapter in *Sentinel*

Installation Guide. The steps in this section also incorporate the steps below.

2. Create a Sentinel subdirectory in the Crystal installation directory, which is the following subdirectory of Business Objects by default:

   ```
   \BusinessObjects Enterprise 11.5\Web
      Content\Enterprise115\WebTools\
   ```

3. Go to reports_patch\IIS in the service pack top-level directory and copy the files publish_report.aspx and delete_report.aspx to the Sentinel subdirectory in the Crystal installation directory.
4. Open the web.config file in the Crystal install directory for editing.
5. Add two new entries to the `<assemblies>` section of the web.config file for Enterprise.PluginManager and Enterprise.Desktop.Report. The following example shows a sample `<assemblies>` section:

   ```
   <assemblies>

   <add assembly="CrystalDecisions.CrystalReports.Engine,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234" />

   <add assembly="CrystalDecisions.ReportSource,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Shared,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Web,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Enterprise,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Enterprise.Framework,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Enterprise.InfoStore,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add assembly="CrystalDecisions.Enterprise.Shared,
      Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add
      assembly="CrystalDecisions.Enterprise.PluginManager
      , Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   <add
      assembly="CrystalDecisions.Enterprise.Desktop.Repor
      t, Version=11.5.3300.0, Culture=neutral,
      PublicKeyToken=123abcd1234a1234” />

   </assemblies>
   ```

IMPORTANT: The new entries should use the same Version, Culture, and PublicKeyToken values as the other entries in your file.

Defects Resolved in this Release

Resolved in SP2

DAT-325 – On Oracle only, when the time of scheduled partition jobs is changed, the job will run at the scheduled time once and then revert to the time specified during installation. FIXED. The job runs consistently at the newly scheduled time.

SEN-3515 – If the parent permission Process Management is granted but the child permission Control Processes is not granted, users are still able to terminate iTRAC processes. FIXED. Users must have the Control Processes permission in order to terminate an iTRAC process.

SEN-6572, SEN-6891 – Correlation Rule deployments with more than one configured Create Correlated Event action generate a unique constraint violation in the DAS Binary log file:

```
ORA-00001: unique constraint (ESECDBA.CORRELATED_EVENTS_ABC)
```

Also, triggered events cannot be viewed. FIXED. Only the first Create Correlated Event action configured is executed by the correlation engine. This situation can be avoided by associating only one Create Correlated Event action with a Correlation Rule.

SEN-6732 – The Sentinel Control Center viewer configuration for attachments is stored by user in the database, but attachment associations and viewer information for attachments may vary for a user between one machine and another. FIXED. The viewer information for attachments is now stored locally.

SEN-6932 – The embedded browser in the Sentinel Control Center does not format reports properly. The workaround is to configure the Sentinel Control Center to use an external browser. FIXED. The embedded browser is removed and all reports are run through an external browser.

SEN-7246 – Running a right-click command from an event table (such as in the Active View or Historical Event Query) that opens in a browser generates a run-time exception. FIXED. The embedded browser is removed and all reports run in an external browser.

SEN-7190 – Imported correlation rules that contain new line characters cannot be deployed or read by the correlation engine manager. FIXED. The correlation rule import process strips extraneous new line characters.

SEN-7413 – When debugging a JavaScript Collector with the FILE Connector, the debugger throws a “RuntimeException - Sentinel-EOF” when the end of the input file is reached. FIXED. When the end of the input file is reached, a notification appears.

Resolved in SP1

DAT-160 – Import summary table partitions function has been fixed for SQL Server 2005.

DAT-216 – Summary table insertions are now successful even if SQL Server 2005 is writing to P_MAX.

DAT-284 – Multiple Sentinel Data Manager jobs may now run simultaneously with no conflict.

DAT-294 – Attempting to “archive and drop” partitions that are already archived on SQL Server 2005 will now archive the selected unarchived partitions and then drop all selected partitions.

DAT-305 – On SQL Server 2005, aggregation functions properly at high event rates.

DAT-306 – On SQL Server 2005, attempting to archive and drop partitions when the archive destination is invalid will now result in an error. The partitions will not be dropped without being archived in this situation.

SEN-4066 – Users with only View Status permissions for Event Source Management are now unable to start and stop nodes, even if multiple nodes are selected simultaneously.

SEN-5284 – Starting a child node in Event Source Management will now start its parent node(s) also. Stopping a parent node in Event Source Management will not stop its child node(s).

SEN-5843 - When installing the Collector Manager with it set connect to Sentinel Server via the proxy, it is no longer necessary to restart DAS.

SEN-6198 – With Collectors that do not have an Event Source (e.g., ODBC collectors), "Trust Event Source Time" cannot be set in the Event Source Management GUI. Now "Trust Event Source Time" may be set at the Collector level and will apply to all child nodes.

SEN-6532 – Users can no longer import scripts into the Plug-in Repository with only "View Scratch Pad" permissions.

SEN-6591 – When modifications or deletions are performed on a subrule during the creation of a composite rule and the Cancel button is clicked, the modifications or deletions are now rolled back.

SEN-6629 – When the parameters of a Collector Script plug-in are changed and the changes are imported into Sentinel, the parameters for any deployed Collectors using that plug-in are now immediately updated.

SEN-6703 – Event Sources used to show connections to both the Event Source Server and the Connector. For clarity when there are a large number of Event Sources, connections are now shown between Event Sources and their Connector and between the Event Source Server and its Connector. Event Source Servers are no longer connected to Event Source nodes in the interface.

SEN-6747 – Collector imports from 511_SP2_06_GA now work properly.

SEN-6779 – Users are now prevented from creating a sequence rule without subrules.

SEN-6783 – Windows Authentication users may now be created in Sentinel Control Center even if the user is already in the SQL Server 2005 list of user logins.

SEN-6784 – Deployed correlation rules can now be selected or copied. By design, deployed correlation rules still may not be edited.

SEN-6800 – Users are now warned if they attempt to import a correlation rule that refers to a dynamic list that doesn't exist in the target system.

SEN-6818 – The "Error" checkbox in the "Attribute Filter" in Event Source Management now displays filtered nodes properly.

SEN-6821 – The updateMapData command in the Sentinel Data Manager command line interface has been removed. Maps may be updated using the Sentinel Control Center->Admin->Mapping Configuration GUI or using either %ESEC_HOME%\MapUpdateUtility.bat or $ESEC_HOME/MapUpdateUtility.sh.

SEN-7239 – *Switch View* in the Servers View now works as expected.

Known Issues and Limitations in this Release

For known issues with Sentinel 6.0 installation, see the release notes for Sentinel 6.0.

DAT-213 – In SQL Server 2005 only, partitions cannot be added to the database when the current online partition is P_MAX.

DAT-280 – If the Sentinel Data Manager application is left open for an extended period of time, an error occurs: "ORA-01000: maximum open cursors exceeded." To avoid this situation, close SDM when it is not in use.

SEN-3897 – The Server View Manager will display processes that are not installed a particular machine with a state of NOT_INITIALIZED. For example, Sentinel on Windows will show the "UNIX Communication Server" process as NOT_INITIALIZED and Sentinel on UNIX will show the "Windows Communication Server" process as NOT_INITIALIZED. The processes that are displayed with a state of NOT_INITIALIZED should be ignored.

SEN-4617 – On UNIX only, only the Sentinel Administrative User (esecadm) is able to run the Sentinel Control Center. To enable other users to run the Sentinel Control Center, please see the Technical Information Document (TID) titled "On UNIX only, only the Sentinel Administrative User (esecadm) is able to run the Sentinel Control Center" (TID #3515705) on the Novell Technical Services web site.

SEN-4634, SEN-4726 –Float variable assignments and comparisons are not handled properly in iTRAC workflows. The workaround is to use integer, Boolean, or string variables within workflows.

SEN-5906 – If an iTRAC activity associated with an iTRAC template is deleted, iTRAC processes attempting to use that activity will fail. The workaround is to verify that an activity is not being used before deleting it.

SEN-5931 – If a Collector reaches a Stop state in the debugger mode, the Step Into, Pause, and Stop buttons are still enabled but will not have any effect. The workaround is to close the debugger and reopen it.

SEN-6182 – If a running Collector Script reaches a Stop state, the child nodes of the Collector will not stop. Therefore, the Collector may be stopped, but its Connectors and Event Sources will still appear to be running in the Live View for Event Source Management. No events will be processed. The workaround is to right click on the Collector and stop it manually.

SEN-6265 – Stopping a Collector does not always stop its child Connector and Event Source.

SEN-6397 - When setting Formatter Name to “xml” in a Send Email action in the Correlation Action Manager, the body of the email is sent in name value pair format.

SEN-6398 - When the Send Email action is triggered for a correlation rule, the email attachment appears blank because it is in XML format. The workaround is to open the file in an application that displays XML.

SEN-6429 - If you create two role names in the Role Manager on the Admin tab that differ only in case (e.g., Admin and admin), user additions and deletions to one role will also impact the other role. The workaround is to ensure that all role names differ by more than just case.

SEN-6473 – In the Event Source Management Live View, when a filter condition is added to a node from a raw data tap and then the OK button is selected to save the new filter condition, the state of the node will be set back to what it was before the raw data tap was opened.

SEN-6573 – If all attributes are selected in the Attribute List as “group by” fields in a composite, aggregate, or sequence rule, an “invalid RuleLg” message is displayed.

SEN-6698 – The correlation rule language does not support the e.all operator. Rules imported from previous versions of Sentinel that use e.all will not work.

SEN-6701 – Moving or cloning a node that is related to an Event Source Server, either directly or through a parent or child, fails. The workaround is to export the node and then import it.

SEN-6895 – On Windows only, if a non-Unicode database is selected at install time, there is no enforcement of Latin characters in the GUI.

SEN-7257 – Some Collectors that were deployed in a Sentinel 5.1.3 system must be redeployed manually and may require some modifications. The *Sentinel User’s Guide* and the documents under the *Migrating to Sentinel 6* section of the Sentinel documentation page provide helpful information. These documents may be found at http://www.novell.com/documentation/sentinel6.

SEN-7519 – If the Navigator or Worklist dockable frames in the Sentinel Control Center are closed and the preferences are saved when closing, the Navigator and Worklist can only be

restored by forcing the Sentinel Control Center executable to ignore saved preferences. To do this, append "-nopref" (without quotes) to the console.jar entry in the control_center.sh or control_center.bat file ("console.jar -nopref"). The frames are restored when you run control_center.sh or control_center.bat from the command line. Other preferences, such as saved views, must be recreated and saved. To re-enable the use of saved preferences, remove the "-nopref" argument from the control_center file.

SEN-7522 – Changing a Collector's status in Event Source Management while the collector debugger is running disables the debugger

SEN-7539 – The "None" option does not work when choosing the start or end date for an offline query. The workaround is to select a specific date.

SEN-7646– If the JavaScript correlation action debugger is run and closed abruptly (without first stopping the debugger) multiple times, the debugger may display a blank screen instead of the JavaScript code. This situation can be prevented or resolved by clicking the Stop button before attempting to rerun the script in the debugger.

SEN-7666 – In the Solution Designer running using Cygwin X Server, content cannot be added to the Solution Pack using drag and drop. The workaround is to use the *Add Selected Content* button.

SEN-7668 – In the Solution Manager and Designer running on UNIX, attachments cannot be viewed directly. Also, the Solution Pack documentation preview (using the Create PDF button Solution Manager) cannot open a PDF reader. The workaround is to save the file to the local machine and open it from there.

SEN-7670 – In the Content Palette of the Solution Designer running on Solaris, the drop-down to select report folders does not work. The workaround is to select the *Show contents of subfolders* option.

WIZ-1839 – The ALERT command in the collector scripting language does not automatically send the ConnectorID (RV23), EventSourceID (RV24), and TrustDeviceTime fields. The workaround is to append these fields to the alert message in any Collectors that use the ALERT command or to update Collectors to use the EVENT command. For code samples, see the Sentinel Reference Guide.

Changes in the Sentinel Control Center may not display or refresh immediately. This has been observed in the following areas:

- SEN-4689, SEN-5698 – When a timeout or alert transition takes place in an iTRAC workflow, the work item GUI is not refreshed even though the work item progresses successfully to the next step specified by the transition in the iTRAC template. The workaround is for the user to restart the Sentinel Control Center.
- SEN-6285 – If a filter is added to the current view in the Process View Manager for iTRAC, the view is not updated immediately. The workaround is to click Refresh.
- SEN-6608 – Maps added to the top level "Maps" folder in the Mapping Service GUI are not visible until a refresh occurs. The workaround is to create new maps in a subfolder.
- SEN-7238 – If a user adds multiple Global Filters or Color Filters, clicks the X button, and selects "No" in the Save Changes dialog, the filters still display when the Global Filters or Color Filters is reopened. The workaround is to restart the Sentinel Control Center.

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 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 at 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.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Third Party Legal Notices

This product may include the following open source programs that are available under the LGPL license. The text for this license can be found in the Licenses directory.

- edtFTPj-1.2.3 is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html
- Esper. Copyright © 2005-2006, Codehaus.
- FESI is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions, see http://www.lugrin.ch/fesi/index.html.
- jTDS-1.2.2.jar is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- Tagish Java Authentication and Authorization Service Modules, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp

This product may include software developed by The Apache Software Foundation (http://www.apache.org/) and licensed under the Apache License, Version 2.0 (the "License"); the text for this license can be found in the Licenses directory or at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The applicable open source programs are listed below.

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/
- Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache Lucene, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Bean Scripting Framework (BSF), licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.

- Xalan and Xerces, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.

This product may include the following open source programs that are available under the Java license.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html
- JavaMail. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html and click download > license.

This product may also include the following open source programs.

- ANTLR. For more information, disclaimers and restrictions, see http://www.antlr.org
- Boost. Copyright © 1999, Boost.org.
- Concurrent, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes
- Java Ace, by Douglas C. Schmidt and his research group at Washington University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Service Wrapper. Portions copyrighted as follows: Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. For more information, disclaimers and restrictions, see http://wrapper.tanukisoftware.org/doc/english/license.html.
- JLDAP. Copyright 1998-2005 The OpenLDAP Foundation. All rights reserved. Portions Copyright © 1999 - 2003 Novell, Inc. All Rights Reserved.
- OpenSSL, by the OpenSSL Project. Copyright © 1998-2004. For more information, disclaimers and restrictions, see http://www.openssl.org.
- Rhino. Usage is subject to Mozilla Public License 1.1. For more information, see http://www.mozilla.org/rhino/.
- Tao (with ACE wrappers) by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Tinyxml. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html.
- yWorks. Copyright © 2003 to 2006, yWorks.

NOTE: As of the publication of this documentation, the above links were active. In the event you find that any of the above links are broken or the linked web pages are inactive, please contact Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.