Novell.

Software for the Open Enterprise™

Product Release Notes

Product

Sentinel™ 5.1.3.0 Service Pack 1 (2006-12-08) Release

Contents

Description

This is the Service Pack 1 (2006-12-08) release of Sentinel™ 5.1.3.0 with iTRAC™. It should be installed into an existing Sentinel™ 5.1.3.0 installation. See the Installation instructions for details.

This Service Pack includes support for additional languages, and fixes for Sentinel™ 5.1.3.0 software components.

This Service Pack must be installed on all machines that have Sentinel™ 5.1.3.0 software components installed.

Sentinel™ 5.1.3.0 Service Pack 1 (2006-12-08) is a comprehensive service pack which contains all the hot fixes previously released for Sentinel™ 5.1.3.0.

New Features

- This release adds support to the Sentinel Control Console and Sentinel Data Manager for the languages Simplified Chinese, Traditional Chinese and Japanese.
- In Sentinel Data Manager, the archiving and dropping partition operations for event summary tables and event tables are separated. A new command line switch –tableName is added for SDM command line action archiveData, dropPartitions, deleteData to specify

table names. The manage_data.bat script has been modified to add new steps to archive and drop summary partitions. If you have developed your own script to archive and drop partitions using SDM command line, you should specify –tableName parameter for event tables and add new steps for archiving and dropping summary table partitions.

Installation

NOTE: This Service Pack must be installed on all machines that have Sentinel™ 5.1.3.0 software components installed. This includes both server (e.g. – Sentinel Server, Correlation Engine, Sentinel Database, Agent Manager, etc.) and client (e.g. – Sentinel Control Center, Agent Builder, Sentinel Database Manager, etc.) software.

This is a Service Pack release, which means that this release must only be installed into an existing installation. Installing this Service Pack will apply the latest software fixes to the existing installation.

This service pack is a comprehensive service pack in that it contains all the hot fixes in previously released hot fixes for Sentinel™ 5.1.3.0. Therefore, you do not need to install any previously released hot fixes for Sentinel™ 5.1.3.0 before installing this service pack. Also, this service pack can be installed over any previously released Sentinel™ 5.1.3.0 hot fixes.

The instructions provided in this document are for installing this Service Pack only. If you do not yet have Sentinel™ 5.1.3.0 installed, please see the Sentinel Install Guide for instructions on installing a new instance of or patching to Sentinel™ 5.1.3.0.

This Service Pack must only be run against an existing installation of Sentinel™ 5.1.3.0.

If you do not yet have Sentinel™ 5.1.3.0 installed, please install it using the Sentinel™ 5.1.3.0 installer. Then, run this Service Pack installer to get the latest fixes and enhancements. Please see the Sentinel Install Guide for instructions.

If you have an earlier version of Sentinel™ installed, you must use the Sentinel™ 5.1.3.0 patch installer to patch your installation to Sentinel™ 5.1.3.0. Then, run this Service Pack installer to get the latest fixes and enhancements. Please see the Sentinel Install Guide for instructions.

This Service Pack comes with an automated installer that will backup the existing software components that will be replaced and install the fixes. 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, “SP1_2006-12-20-GMT_bak”.

Installing the Service Pack

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.

Follow these instructions to install the Service Pack fixes for software and database:

1. Login as an Administrator (Windows) or as root (UNIX).
2. Extract the Service Pack ZIP file.
3. Shutdown all Sentinel applications running on this machine, including:
   - Sentinel Control Center
   - Sentinel Collector Builder
   - Sentinel Data Manager

4. Shutdown all Sentinel services running on this machine, including:
   - Sentinel Collector Manager

   On Windows:

   ```
   Use Service Manager to stop the “Sentinel Collector
      Manager” service.
   ```

   On UNIX:

   ```
   Run as the esecadm user:

   $ESEC_HOME/wizard/agent-manager.sh stop
   ```

   - Sentinel Server

   On Windows:

   ```
   Use Service Manager to stop the “Sentinel” and
      “Sentinel Communication” services.
   ```

   On UNIX:

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh stop
   ```

5. On the command line, go into the Service Pack top level directory that was just extracted.
6. 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.

   If you wish to use the Sentinel Control Center or Sentinel Data Manager in a language other than the default language of your operating system, then follow the instructions in the section Setting the Language for Sentinel Control Center and Sentinel Data Manager.
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. For the machine with the Sentinel Database installed, perform the following steps to patch the Sentinel Database:

   For Sentinel Database on Oracle:

   1. Ensure Sentinel Server and Sentinel Database Manager processes are not running.
   2. If you have not already, log into the database machine as the ‘root’ user.
   3. Check your environment variables to ensure that java (version 1.4.2) is in your PATH. You can perform this check by executing the following command on the command line:

      ```
      java -version
      ```

      If the above command does not succeed, then either locate where java is installed on your system or download and install java. Then, update your PATH environment variable to include the java executable. For example, if java is installed in the directory:

```
/opt/Sentinel5.1.3.0/Sun-1.4.2
```

Then add the following to the end of your PATH environment variable:

```
:/opt/Sentinel5.1.3.0/Sun-1.4.2/bin
```

4. If you have not done so already on this machine, extract the Service Pack ZIP file.
5. Change directories to the following directory under the extracted Service Pack directory:

   ```
   db_patch/bin
   ```

6. Enter the command:

   ```
   ./PatchDb.sh
   ```

7. At the prompt, enter the hostname or static IP address of the Oracle Sentinel Database that you want to patch.
8. At the prompt, enter the port number of the Oracle Sentinel Database that you want to patch.
9. At the prompt, enter the Oracle software owner username. For example, 'oracle'.
10. At the prompt, enter the Database Name of the Oracle Sentinel Database that you want to patch.
11. At the prompt, enter the 'esecdba' user password. The script will verify the entered information and begin the database patch.
12. 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.

For Sentinel Database on MSSQL (with 'esecdba' as Windows Authentication Login):

13. Ensure Sentinel Server and Sentinel Database Manager processes are not running.
14. If you have not already, at the database machine, login as the 'esecdba' Windows Domain user.
15. Check your environment variables to ensure that java (version 1.4.2) is in your PATH. You can perform this check by executing the following command on the command line:

    ```
    java -version
    ```

    If the above command does not succeed, then either locate where java is installed on your system or download and install java. Then, update your PATH environment variable to include the java executable. For example, if java is installed in the directory:

    ```
    C:\Program Files\esecurity5.1.3.0\Sun-1.4.2
    ```

    Then add the following to the end of your PATH environment variable:

    ```
    ;C:\Program Files\esecurity5.1.3.0\Sun-1.4.2\bin
    ```

16. If you have not done so already on this machine, extract the Service Pack ZIP file.
17. Open a command prompt.

18. Change directories to the following directory under the extracted Service Pack directory:

    ```
    db_patch\bin
    ```

19. Enter the command:

    ```
    .\PatchDb.bat
    ```

20. At the prompt, enter the hostname or static IP address of the SQL Server of the Sentinel Database that you want to patch.
21. At the prompt, enter the name of the SQL Server Sentinel Database to patch.
22. At the prompt, enter option 1 for Windows Authentication. The script will verify the entered information and begin the database patch.
23. 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.

For Sentinel Database on MSSQL (with ‘esecdba’ as SQL Authentication Login):

24. Ensure Sentinel Server and Sentinel Database Manager processes are not running.
25. If you have not already, log into the database machine.
26. Check your environment variables to ensure that java (version 1.4.2) is in your PATH. You can perform this check by executing the following command on the command line:

    ```
    java -version
    ```

    If the above command does not succeed, then either locate where java is installed on your system or download and install java. Then, update your PATH environment variable to include the java executable. For example, if java is installed in the directory:

    ```
    C:\Program Files\esecurity5.1.3.0\Sun-1.4.2
    ```

    Then add the following to the end of your PATH environment variable:

    ```
    ;C:\Program Files\esecurity5.1.3.0\Sun-1.4.2\bin
    ```

27. If you have not done so already on this machine, extract the Service Pack ZIP file.
28. Open a command prompt.
29. Change directories to the following directory under the extracted Service Pack directory:

    ```
    db_patch\bin
    ```

30. Enter the command:

    ```
    .\PatchDb.bat
    ```

31. At the prompt, enter the hostname or static IP address of the SQL Server of the Sentinel Database that you want to patch.
32. At the prompt, enter the name of the SQL Server Sentinel Database to patch.
33. At the prompt, enter option 2 for SQL Authentication.
34. At the prompt, enter the ‘esecdba’ user password. The script will verify the entered information and begin the database patch.

35. 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.

Setting the Language for Sentinel Control Center and Sentinel Data Manager

1. Make a backup copy of the following files:

   On Windows:

   ```
   %ESEC_HOME%\sentinel\console\run.bat
   %ESEC_HOME%\sdm\sdm.bat
   ```

   On UNIX:

   ```
   $ESEC_HOME/sentinel/console/run.sh
   $ESEC_HOME/sdm/sdm
   ```

2. Using a text editor, open the following file:

   On Windows:

   ```
   %ESEC_HOME%\sentinel\console\run.bat
   ```

   On UNIX:

   ```
   $ESEC_HOME/sentinel/console/run.sh
   ```

3. Edit the user language and user country properties

   On Windows:

   Uncomment the first line listed below by removing “REM”, and replace ##INSTALL.LOCAL## with language code listed in Language and Country Code in lower case. If country code is applicable, uncomment the second line listed below by removing “REM”, replace ##INSTALL.COUNTRY## with the country code listed in Language and Country Code in upper case.

   For example, if the language is Simplified Chinese, the following lines should be changed from

   ```
   REM set SENTINEL_LANG_PROP=-Duser.language=##INSTALL.LOCALE##
   REM set SENTINEL_CTRY_PROP=-Duser.country=##INSTALL.COUNTRY##
   ```

   to

   ```
   set SENTINEL_LANG_PROP=-Duser.language=zh
   set SENTINEL_CTRY_PROP=-Duser.country=CN
   ```

   On UNIX:

   Uncomment the first line listed below by removing “#” at the beginning of the line, and replace ##INSTALL.LOCAL## with language code listed in Language and Country Code in lower case. If country code is applicable, uncomment the second line listed below by removing “#” at the beginning of the line, replace ##INSTALL.COUNTRY## with the country code listed in Language and Country Code in upper case.

   For example, if the language is Simplified Chinese, the following lines should be changed from

   ```
   #SENTINEL_LANG_PROP=-Duser.language=##INSTALL.LOCALE##
   #SENTINEL_CTRY_PROP=-Duser.country=##INSTALL.COUNTRY##
   ```

   to

```
SENTINEL_LANG_PROP=-Duser.language=zh
SENTINEL_CTRY_PROP=-Duser.country=CN
```

4. Save the file in ANSI encoding format.
5. Using a text editor, open the following file:

   On Windows:

   ```
   %ESEC_HOME%\sdm\sdm.bat
   ```

   On UNIX:

   ```
   $ESEC_HOME/sdm/sdm
   ```

6. Edit the user language and user country properties

   On Windows:

   Uncomment the first line listed below by removing “REM”, and replace ##INSTALL.LOCAL## with language code listed in Language and Country Code in lower case. If country code is applicable, uncomment the second line listed below by removing “REM”, replace ##INSTALL.COUNTRY## with the country code listed in Language and Country Code in upper case.

   For example, if the language is Simplified Chinese, the following lines should be changed from

   ```
   REM set SENTINEL_LANG_PROP=-Duser.language=##INSTALL.LOCALE##
   REM set SENTINEL_CTRY_PROP=-Duser.country=##INSTALL.COUNTRY##
   ```

   to

   ```
   set SENTINEL_LANG_PROP=-Duser.language=zh
   set SENTINEL_CTRY_PROP=-Duser.country=CN
   ```

   On UNIX:

   Uncomment the first line listed below by removing “#” at the beginning of the line, and replace ##INSTALL.LOCAL## with language code listed in Language and Country Code in lower case. If country code is applicable, uncomment the second line listed below by removing “#” at the beginning of the line, replace ##INSTALL.COUNTRY## with the country code listed in Language and Country Code in upper case.

   For example, if the language is Simplified Chinese, the following lines should be changed from

   ```
   #SENTINEL_LANG_PROP=-Duser.language=##INSTALL.LOCALE##
   #SENTINEL_CTRY_PROP=-Duser.country=##INSTALL.COUNTRY##
   ```

   to

   ```
   SENTINEL_LANG_PROP=-Duser.language=zh
   SENTINEL_CTRY_PROP=-Duser.country=CN
   ```

7. Save the file in ANSI encoding format.
8. On Windows

   a. Create an empty file in the directory %ESEC_HOME%\sentinel\console naming it console.ja.

   b. Open console.ja file with text editor and add the following line

      -Duser.language=<language_code> -Duser.country=<country_code>

      where language_code and country_code are listed in Language and Country Code

   c. Save the file in ANSI encoding format.

d. Create an empty file in the directory %ESEC_HOME%\sdm naming it sdm_gui.ja.

e. Open sdm_gui.ja file with text editor and add the following line

-Duser.language=<language_code> -Duser.country=<country_code>

where language_code and country_code are mentioned in Language and Country Code

f. Save the file in ANSI encoding format.

Language and Country Code

Language	Language Code	Country Code
English	en	
Spanish	es	
French	fr	
German	de	
Italian	it	
Portuguese	pt	
Simplified Chinese	zh	CN
Traditional Chinese	zh	TW
Japanese	ja	

Bug Fixes

Sentinel

SEN-4262

Issue: Aggregation Service causing "maximum cursor exceed" error on Oracle database.

Fix: Improved exception handling to fix this issue.

SEN-4411

Issue: Aggregation Service stops processing event files.

Fix: Fixed.

SEN-4446

Issue: Unique constraint errors are thrown in DAS Binary when re-inserting events from event file cache.

Fix: Improve error handling in JDBCLoadStrategy to fix this issue.

SEN-4449

Issue: OCI Event Insert Strategy does not properly handle db insert errors, causing event reinsert logic to fail.

Fix: Improved exception handling to fix this issue.

SEN-4451 (Enhancement)

Issue: JDBCLoadStrategy performs poorly because it uses CallableStatement (and stored proc) rather than PreparedStatement (and pure SQL).

Fix: Improved JDBCLoadStrategy performance by using PreparedStatement and directly inserting into the tables.

SEN-4452

Issue: RuleLG error when creating a Filter using EventTime

Fix: Updated data type for ET to fix this issue.

SEN-4460

Issue: Problem creating role names with spaces in iTrac

Fix: Fixed role name validation.

SEN-4465

Issue: When creating a filter that does a comparison on a datetime field (e.g. - CV11), the filter does not compare the time correctly in java processes

Fix: Fixed

SEN-4469

Issue: Unable to run SDM command line in headless environment

Fix: Removed dependency on AWT from SDM command line.

SEN-4627

Issue: Correlation e-mail does not work with %tag% names. It works only with %all%

Fix: Fixed.

SEN-4629

Issue: Found ^M (Ctrl+M) characters in `runalert.sh` and `runattack.sh` files and hence were unable to download the advisor data.

Fix: Fixed.

SEN-4467

Issue: Advisor data update error when using Chinese Traditional Language

Fix: Scripts now ensure default locale is en_US.

Wizard

WIZ-1728

Issue: The syslog server fails to send the events to all the connected clients; it only sends the event to only one of the client.

Fix: The syslog has been updated to send events to all the active clients instead of just one of the active clients.

WIZ-1738

Issue: The syslog server fails to drop the unwanted messages from the queue. Also in case when the rate at which the syslog server receives the message is higher than the eps(events/sec) the syslog client can handle, then the messages are being dropped

Fix: The message unwanted by all the live clients will be discarded, and the syslog server waits until the clients queue has enough space to put the message on the clients queue.

WIZ-1743

Issue: Syslog stops sending events to the buffer for UDP connections

Fix: The processing of UDP data was previously halted when the syslog server buffer was full. The processing wasn't restarted when there's space in the buffer. This has been corrected.

WIZ-1745

Issue: Syslog client does not handle repeated messages correctly

Fix: The parsing is fixed so that the priority, timestamp and ip address are optional and we are expecting only an ip address after the priority or priority followed by timestamp.

Database

DAT-198

Issue: In the OCI Event Strategy, the values of the CV30 thru CV34 tags were truncated to 255 chars in the database when populated with 4000 chars.

Fix: Fixed

DAT-200

Issue: SDM command line tool will not drop old partitions for the SMRY partitions.

Fix: Added **-**tableName switch to SDM command line to specify table names for SDM operation.

NOTE: The manage_data.bat script has been updated to add new steps to archive and drop summary table partitions. If you have developed your own script to archive and drop partitions using SDM command line, you should specify –tableName parameter for event tables and add new steps for archiving and dropping summary table partitions.

DAT-202

Issue: SDM manage_data.bat is not updated for archivePartition and dropPartition.

Fix: Updated manage_data.bat to specify table name for archive and drop partitions.

DAT-204

Issue: The database migration in the 5.1.3 patch breaks the stored procedure for esec_bcpout

Fix: Updated esec_bcpout stored procedure to use the right command line switch for bcp using Windows authentication.

DAT-205

Issue: The manage_data.bat script deletes partitions even if they have not been archived

Fix: Modified SDM to throw exceptions for manage_data.bat script to detect errors.

DAT-209

Issue: The SDM Document and SDM command line help should be updated for deleteData -tablename flag

Fix: Added –tableName flag for deleteData and updated Sentinel documentation.

Documentation

DAT-201

Issue: Documentation is not updated to indicate the addition of –tableName command line switch to Sentinel Data Manager

Fix: Updated Sentinel User’s Guide and Sentinel Installation Guide

SEN-4447

Issue: Unable to change the Event Insertion strategy from JDBC to OCI by the instructions provided in the `513_Sentinel_Install.pdf`

Fix: Improved documentation to make it more clear how to setup OCI Load Strategy, also included more troubleshooting tips.

SEN-4461

Issue: Crystal install guide has wrong information in configuring DEP for windows

Fix: Updated Crystal install guide

SEN-4463

Issue: Need clarification if 64 bit Windows 2003 and MSSQL 2005 is supported

Fix: Documentation updated. If Sentinel Database is the only Sentinel component installed on the database machine, then 64-bit SQL Server is supported. For example, if only Sentinel Database is installed on machine A and the rest of Sentinel is installed on machine B, then machine A can be a 64-bit machine running 64-bit SQL Server.

SEN-4464

Issue: Need to update the usage of dbConfig.bat in User Reference Guide

Fix: Documentation updated.

Known Issues

Installer

- Attempting to take a screenshot of the installer by typing Alt+PrintScreen results in the graphics in the installer being garbled. This is caused by a bug in InstallShield. The workaround is to use only the PrintScreen button.

Sentinel

- WorkFlow will not proceed beyond the Start Eradication Process when attempting to execute arp –a command. Workaround is to:
- Login to machine running the DAS component as user esecadm.
- Open the '.bash_profile' file under esecadm user’s home directory and modify it so that the PATH environment variable includes the directory '/usr/sbin'.
- Modify the template activity to run a different activity.
- When setting a filter in the view options for incidents, Collectors, Collector managers or iTRAC, the attribute fields that hold dates may fail to work properly if included as part of the filter.
- In Sentinel Control Center > Admin Tab, Active User Sessions will temporarily display a session for a user that has logged in to Collector Builder.
- If the Analyst role is empty (on product install it is empty) and an auto response workflow is instantiated, the server assigns _WORKFLOW_SERVER. But when a user is later added to the Analyst role, the assignments are not recalculated and the new user does not get workitems associated with that process. The workarounds follow:

- Before starting any workflow process, make sure that all assigned groups have at least one user. This will prevent the previously described problem.
- If an iTRAC process was instantiated without a assigned group having at least one user, perform the following steps to resolve the issue:
- Add a user to the affected group.
- Edit the corresponding template and save. No change to the template is required for this. You may just double click on the manual activity to popup the customizer dialog, select the same resource again, click OK and save the template.

This should force recalculation of workitem assignments. Users in the analyst group will now see workitems for that activity.

- Cannot edit while creating a user-defined template in the same template customizer after saving. The workaround is after saving the newly created template, to make modifications on the template, close the template window and open again.

Wizard

- When using "Populate Network" capability in Collector Builder, UUIDs are not reset in the copied port configurations. This results in the events from copied port configurations having the same Source Id.
- [WIZ-1684] When debugging a Collector using the Collector Builder, the Collector Builder may exit unexpectedly. This is less likely to happen if the Collector Builder “Execute One Command” and “Resume Command Execution” debugger buttons are clicked slowly (less than once every two seconds).

Novell Technical Support

Website: http://www.novell.com

- Novell Technical Support: http://www.novell.com/support/index.html
- International Novell Technical Support: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- For 24x7 support, 800-858-4000

Disclaimer

The Origin of this information may be internal or external to Novell. Novell makes all reasonable efforts to verify this information. However, the information provided in this document is for your information only. Novell makes no explicit or implied claims to the validity of this information.

Any trademarks referenced in this document are the property of their respective owners. Consult your product manuals for complete trademark information.