Novell.

Product Release Notes

Sentinel™ 5.1.3 with iTRAC™

> **NOTE**: To download Release Note versions in German, French, Italian, Spanish or Brazilian Portuguese, go to http://www.novell.com/documentation/sentinel5.

Description

This is a full Sentinel 5.1.3 release with iTRAC.

This release supports the following types of installations:

- Clean installation of Sentinel 5.1.3 on Windows, Solaris, and Linux (Novell SUSE Linux Enterprise Server 9 and Redhat).
- Data migration upgrade from Sentinel 4.2.x to Sentinel 5.1.3 on Windows and Solaris.
- Installing additional components of Sentinel 5.1.3 into an existing Sentinel 5.1.3 installation on Windows, Solaris, and Linux.

> **NOTE**: If you have an installation of Sentinel 5 previous to version 5.1.3 and would like to patch your installation up to version 5.1.3, you must use a Sentinel 5.1.3 patch installer to do so. The Sentinel 5.1.3 installer that comes with these release notes is not a patch installer. To obtain a Sentinel 5.1.3 patch installer, please contact Technical Support.

Operating Systems and Patches

The supported operating systems and databases for the localized versions of Sentinel 5.1.3 are listed below. Information for the English version is contained in the install guide.

- **Server Operating Systems:**
  o SLES 9 SP3 (German, French, Italian, Spanish, Brazilian Portuguese)
  o Solaris 9 (German, French, Italian, Spanish, Brazilian Portuguese)
  o MS Windows 2003 Server SP1 (German, French, Italian, Spanish, Brazilian Portuguese)
  o MS Windows 2000 Server SP4 (German, French, Italian, Spanish, Brazilian Portuguese)

- **Client Operating Systems:**
  o MS Windows 2000 Professional SP4 (German, French, Italian, Spanish, Brazilian Portuguese)
  o MS Windows XP Professional SP2 (German, French, Italian, Spanish, Brazilian Portuguese)
  o Solaris 9 (German, French, Italian, Spanish, Brazilian Portuguese)

- **Database:**
  o Oracle 9.2.0.7 (English Only)
  o MS SQL 2000 SP3a (English Only)

Installation

Instructions for installing this release are located in the Sentinel Install Guide for Sentinel 5.1.3.

To perform a clean installation of Sentinel, follow the instructions in one of the following chapters as appropriate for the platform you are installing on.

- Chapter 3, Installing Sentinel 5 for Oracle on Solaris
- Chapter 4, Installing Sentinel 5 for Oracle on Linux
- Chapter 5, Installing Sentinel 5 for MS SQL

The following should be done as part of the Oracle Pre-Install on Linux. This change relates to Oracle Doc ID: Note:293988.1.

- On SUSE Linux Enterprise Server 9 SP2, add the following kernel parameter setting to the "/etc/sysctl.conf" file:
  ```
  # Oracle requires MLOCK privilege for hugetlb memory.
  vm.disable_cap_mlock=1
  ```
- Execute the following command to load the modifications to the "/etc/sysctl.conf" file:
  ```
  sysctl -p
  ```

To perform a data migration upgrade from an existing Sentinel 4.2.x installation to Sentinel 5.1.3, follow the instructions in one of the following chapters as appropriate for the platform you are installing on.

- Chapter 6, Data Migration and Patch for Oracle on Solaris
- Chapter 7, Data Migration and Patch for MS SQL

To install additional components of Sentinel 5.1.3 into an existing Sentinel 5.1.3 installation follow the instructions in the following chapter:

- Chapter 14, Adding Components to an Existing Installation

To install additional components of Sentinel 5.1.3 into an existing installation of an earlier version of Sentinel 5 first patch the installation of Sentinel to version 5.1.3 using the appropriate patch installer, then following the instructions in the chapter specified above.

New Features

- This release adds support for several languages including Brazilian Portuguese, French, Italian, German, Spanish and English to the Sentinel Control Console and Sentinel Data Manager.
- The syslog connector has been enhanced to handle NAudit instrumented applications. The enhancement is coupled with an agent that will process NAudit data in general and in particular for the following applications: eDirectory, Netware, Identity Manager, Secure Login and Access Manager. Other enhancements include:
  o Filtering the syslog message body using regular expressions.
  o Collector connector to syslog server auto-reconnection.
  o Flow control for TCP connections – preventing dropped data due to a full message buffer. This is both for syslog TCP and NAudit connections.

Syslog Connector Architecture
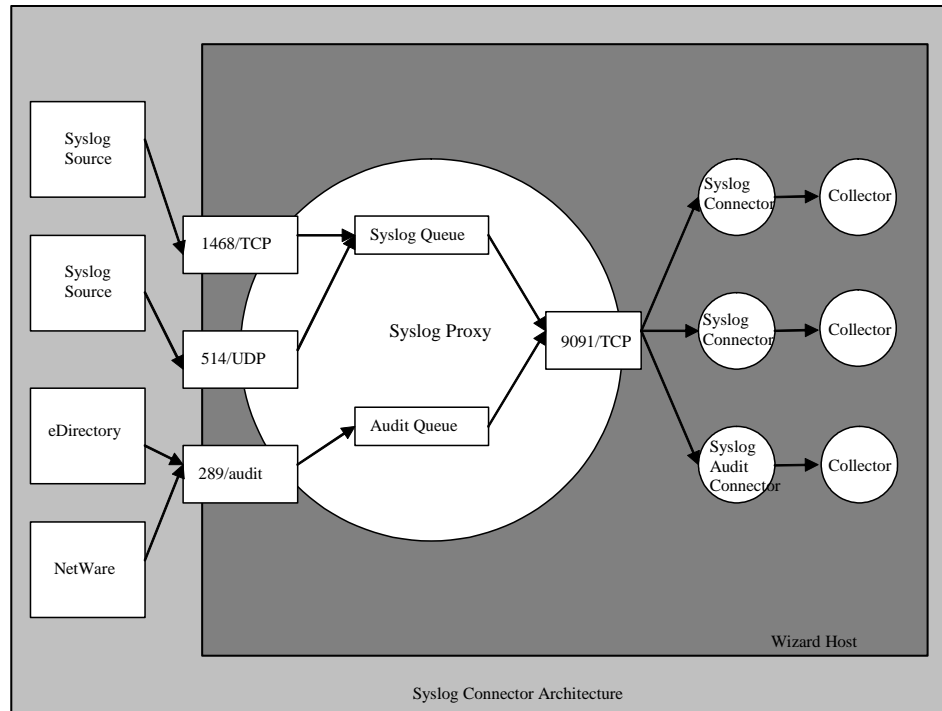
- The syslog connector is now installed with scripts that run on Windows and UNIX as well as improved configuration files. Additionally, the installation of the syslog proxy server as a service has been simplified. To install the syslog proxy server as a service with the default configuration, run the following commands:
  - On Windows:
    1. Log in as an Administrator.
    2. cd /d %ESEC_HOME%\wizard\syslog
    3. .\syslog-server.bat install
  - On UNIX:
    4. Log in as root.
    5. cd $ESEC_HOME/wizard/syslog
    6. ./syslog-server.sh install
- New agent script commands encodemime and decodemime add base 64 encoding and decoding capability.
- CV30-CV34 are expanded from 255 characters to 4000 character limit.
- This release adds support for installing Sentinel Database directly into a MS SQL 2005 database server.
- A new "Server View" screen has been added to the Admin tab of Sentinel Control Center. This screen provides the following functionality:
  - Provides a view of the status of all Sentinel Server processes across the system (requires the "Administration->Server Views->View Servers" privilege). This is similar to the existing Collectors View, but instead displays Sentinel Server processes.
  - It allows you to Start, Stop, or Restart processes (requires viewing as well as "Administration->Server Views->Control Servers" privileges).

	Starts	AutoRestarts	StartTime	State	UpTime	Version
Processes Health						
localhost.localdomain						
Communication Server	1	0	01/20/2006 19:47:09 EST	Running	11:01s	5.1.1.1
Correlation Engine	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
DAS_Binary	2	0	01/20/2006 19:51:59 EST	Running	6:11s	5.1.1.1
DAS_Query	3	1	01/20/2006 19:48:04 EST	Running	10:06s	5.1.1.1
DAS_RT	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
DAS_iTRAC	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
Query Manager	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
RuleLg Checker	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
Sonic Lock Remover	0	0		NOT_INITIALIZED		5.1.1.1

Ready   Refresh   Options   Refreshed At: Fri Jan 20 19:57:26 EST 2006

- The password prompts for the following Wizard process connectors have been enhanced to attempt to mask the password as it is typed in on the command line:
  - dbconnector
  - rdep_client
- The component that generates the Exploit Detection file attackNomarlization.csv file has been modified to use less memory. This will allow better performance on demo hardware.
- Additional configuration options for processes in configuration.xml file:
  - name [default: "Uknown"] – The name of the processes. This is a nice name given to the process that will appear as the process name in log files and in the Sentinel Control Center Server View.
  - auto_restart_threshold [default: "5,10"] – The format of the value is "<#restarts>,<#minutes>". If the process is automatically restarted (e.g. – due to process exiting on its own or being killed via OS command) more then the specified number of restarts in the specified number of minutes, it will no longer be automatically restarted. This is used to prevent a process from being restarted forever when there is probably a configuration error. A "ProcessAutoRestartError" internal event is sent when this occurs.
  - depends [default: <no dependencies>] – The format of the value is a comma separated list of process names, as specified by the new "name" process attribute. The processes specified in the list are the processes that must be running before this process can successfully run.
  - type [default: "normal"] – Valid values are either "normal" or "container". Container specifies that the process is an eSecurity Container process (i.e.- is launched using a container xml file) and can be shut down cleanly by sending a message to the container to shut itself down. Normal specifies all other processes.
- The functionality of the following processes have been rewritten Java in order to provide better functionality or decrease complexity:
  - watchdog
  - data_synchronizer (now part of DAS).
- The Base Sentinel Services feature previously available for separate install has been folded into the DAS install feature. The processes that would previously get activated when Base Sentinel Services was selected for install will now get activated when DAS is selected for install. This was done to decrease the complexity of the installer. Previously allowing this feature to be installed separately provided no known performance benefit.
- Licensing verification has been enhanced to check the user specified license key against all available network interface cards (NICs). If any of the NICs has the correct MAC address, the license verification will succeed.

Bug Fixes

Sentinel

7424

Issue: exploitDetection.csv generation is missing some data.

Fix: Fixed exploit detection generator to add missing data to exploitDetection.csv file.

7460

Issue: On UNIX, if Communication Server was installed by itself, it would never get started automatically. This is because the installer would not install "watchdog", which is responsible for starting the Communication Server on UNIX.

Fix: Moved the Communication Server feature under Sentinel Services in installer, which ensures that "watchdog" gets installed too.

7463

Issue: Exploit Detection Generator will start a 2nd regeneration even if there is one currently processing, causing additional CPU usage on DAS Query.

Fix: Exploit Detection Generator will only process one regeneration at a time.

SEN-2819

Issue: SDM % does not show progress when adding partitions, Stays at 0%.

Fix: Percentage value is continuously increasing according to the completion of SDM activity.

SEN-3684

Issue: Argument type in Incident Command Activity does not work.

Fix: All the parameters (None, Incident Output and Custom) as argument type are now working.

SEN-3713

Issue: Exploit Detection detecting only one attack for each vulnerability

Fix: Exploit Detection will now detect all attacks that are linked to a vulnerability in the Advisor feed as an exploit of that vulnerability if the vulnerability has been reported on the machine being attacked.

SEN-3732

Issue: No longer able to select the "Rejected" state in the Sentinel GUI Incident manager

Fix: The "Rejected" state is added to the Sentinel GUI Incident Manager.

SEN-3760

Issue: Problem passing parameters containing spaces when executing scripts from Right-Click Menu or Correlation Rules.

Fix: Fixed executor of Right-Click Menu and Correlation Rules commands to handle spaces in parameters properly.

SEN-3763

Issue: Exploit Detection does not work sometimes due to multiple Normalized Attack Id's for each Device Attack Name.

Fix: Exploit Detection will now detect all attacks that are linked to a vulnerability in the Advisor feed as an exploit of that vulnerability if the vulnerability has been reported on the machine being attacked.

SEN-3764

Issue: Limit the frequency with which the Exploit Detection Data will be regenerated

Fix: Regeneration is now limited to, by default, once every 30 minutes. This is configurable by editing the das_query.xml file.

SEN-3766

Issue: When the call DAS RT makes to get user preferences fails, it removes all permanent filters

Fix: Error handling is improved to not remove all permanent filters if getting user preferences fails.

SEN-3775 (Enhancement)

Issue: Process event transformations for mapping service that have cyclical dependencies.

Fix: The mapping service will make a best effort to continue to process event transformations even if there is a cyclical dependency. The cyclical dependency must still be fixed by the user, but this enhancement allows the system to work as best as possible even if there is a cyclical dependency problem.

SEN-3779

Issue: The DAS JDBCLoadStrategy is not inserting the events fields RV37, RV38, and RV47-RV48 into the database.

Fix: Fixed JDBCLoadStrategy to insert the missing event fields.

SEN-3781

Issue: Advisor is unable to connect to the server through a proxy.

Fix: Fixed Advisor client so it can now connect to the server through a proxy over https.

SEN-3785

Issue: Seeing a SummaryUpdateFailure event in the SCC

Fix: Fixed error causing this event.

SEN-3788

Issue: Correlation rule "in" and "not in" rule lg is not working well.

Fix: Fixed these aspects of rule lg.

SEN-3792

Issue: When a Correlation Rule triggering results in a command getting executed and the parameter to the command is "%all%", the 26th argument passed to the command is the Event Name set in the Correlation Rule (same as 13th argument) rather than the Event Name from the actual Event that triggered the rule.

Fix: The 13th and 26th arguments are now the Correlation Rule "Event Name" and first Event "Event Name" (that was responsible for triggering the Correlated Event), respectively.

SEN-3793

Issue: No Events are displayed under `Selected Events` section of the Vulnerability Results Window.

Fix: Selected Events are now displayed in Vulnerability Results and Event to Vulnerability Graph.

SEN-3812

Issue: Files does not get deleted from $ESEC_HOME/sentinel/bin/eventfiles/done folder even if they are configured to be deleted after they are processed

Fix: The file will now get deleted after being processed.

SEN-3814(Enhancement)

Issue: Incident Command Activities Text output should return the text as XML

Fix: Added this functionality.

SEN-3835

Issue: If any filter that is saved in a user's preferences is invalid, then all active views with any filter for any user will be treated as a non-permanent active view.

Fix: Error handling is improved to resolve this issue.

SEN-3851

Issue: Quick query does not have options to save data

Fix: Added two buttons on Quick Query panel. One to save it to html file, the other to save it to CSV file.

SEN-3877

Issue: Events are not written to the DB if the transaction log is full.

Fix: Fixed the issue by adding components that will retry to insert events into the DB if there are is a DB error. These components are enabled by default by this installer.

SEN-3880

Issue: Workflow server runs out of connections and hangs after many processes are created via incidents triggered by correlation

Fix: Issue was fixed by ensuring workflow connections are closed after use

SEN-3914

Issue: Event insert retry functionality does not properly handle Correlated Events.

Fix: Fixed event insert functionality to properly handle Correlated Events.

SEN-3916

Issue: Taxonomy is out of date in correlation documentation and correlation rule seed data.

Fix: The correlation rules that are installed as part of the seed data have been updated to make sense with the next taxonomy. Additionally, chapter 7 of the reference guide has been updated to match the new taxonomy and the new correlation rules.

SEN-3800

Issue: A scheduled report will cause problem to the report folder hierarchy displaying in Sentinel.

Fix: GetReports.asp/GetReports.jsp was modified to change the way we retrieve the folder hierarchy from the repository.

SEN-3832

Issue: QuickQuery is not working for the match subnet expressions.

Fix: The query that is issued for the match subnet expression was updated to reflect the change in the databases's storage of IP addresses.

SEN-3924

Issue: Correlation Engine Crashes (Window string operation with !=)

Fix: A segmentation violation was caused when a literal string was compared using the != evaluation in the Window operation. This was fixed. For example window(e.evt!= "bob",10).

SEN-3933

Issue: Piechart not return correct number of events in the quick query upon drill down ,and chunk of piechart does not return anything upon drill down

Fix: The issue that is fixed has to do with an empty label. Since rulelg cannot support an isnull operation, the empty labels are removed from the query. However, this made the indices off, which would make the results incorrect. However, if you only select the empty label and do a drill down, you will get all the events for the time period, not just the events with the empty label. This is due to a limitaiton of rulelg.

SEN-3999 (Enhancement)

Issue: Increase field length for cv30 through cv34 from 255 to 4000

Fix: These fields can hold more string data.

SEN-4056

Issue: Workflow/User permissions problem

Fix: When a user is created with the workflow service unavailable, the user is partially created in one of two databases that hold the user information. This leaves the user is a bad state that is not recoverable from. This problem has been remedied by making user creation more of a transaction.

SEN-4087

Issue: A relevant confirmation message is NOT displayed on clicking on `Remove` button under Advisor tab of an incident

Fix: Confirmation message has been modified to display the proper information while deleting attack in Advisor tab.

SEN-4094

Issue: Menu configurations are not launched in Internal browser when "Use external browser" option is not selected

Fix: Fixed the browser launching.

SEN-4302

Issue: UpgradePortCfgFile files need to be added to FULL installer

Fix: Files added to the installer.

Wizard

7414 (HD 101689)

Issue: Collector Builder crashing at login screen due to poor initialization of variables

Fix: Fixed by initializing variable properly.

WIZ-1649

Issue: Collector Manager truncates SNMP Trap data when a trap value is greater than 57 characters in length. This causes a loss of the entire trap.

Fix: The trap truncation has been fixed to accept large trap values (much larger than 57 characters).

WIZ-1651

Issue: Collector Manager SNMP support only handles "public" community traps.

Fix: Non-public community traps are now also handled by Collector Manager.

WIZ-1656

Issue: Collector Manager handles only SNMP v1 and v3 traps. Specifically, it does not handle SNMP v2 and v2c traps.

Fix: Added support for SNMP v2 and v2c traps in Collector Manager.

WIZ-1661

Issue: Setting the Collector variables s_VULN and s_CRIT while using the EVENT command results in empty Vulnerability and Criticality tag fields.

Fix: These fields are now set properly when using the EVENT command.

WIZ-1664

Issue: If the delimiter is at the beginning of a new block of data read from the source (i.e. -file), that delimiter will be skipped by the Rx state.

Fix: Fixed this error.

WIZ-1665

Issue: If the delimiter size is >1 chars, and the delimiter appears across a block boundary, the Rx state will skip the delimiter.

Fix: Fixed this error.

WIZ-1675

Issue: Sometimes, Collector Manager gets into a state when it is using nearly 100% CPU but is not processing any event, even though Collectorengine are running.

Fix: Fixed error causing this scenario to occur.

WIZ-1676

Issue: Memory leak when using the Alert Command.

Fix: Fixed memory leak.

WIZ-1682

Issue: The database connector runs in an infinite loop when the query contains a table name that doesn't exist in the database.

Fix: Fixed by initializing the result set variable properly

WIZ-1699

Issue: Removing exportvar script command and gui elements for collector builder

Fix: This command has been removed.

WIZ-1713

Issue: The NVP parser doesn't handle 32 bit unsigned into 32 bit signed parsing/stonum doesn't allow more than the maximum signed positive integer to be converted

Fix: These script commands were modified to accept large 32 bit unsigned numbers. All script integers are signed 32 bit values. A large unsigned 32 bit number results in a script variable representing the 32 bit value (with the most significant bit set) as a negative value.

Database

DAT-145

Issue: When dropping partitions, SDM failed to rename index partition P_TEMP to P_MIN

Fix: When dropping partitions, SDM now renames index partition P_TEMP to P_MIN.

DAT-147

Issue: SERVICE_PACK_ID missing from ADV_ATTACK_PLUGIN_RPT_V

Fix: The SERVICE_PACK_ID column is now in the ADV_ATTACK_PLUGIN_RPT_V view.

DAT-151

Issue: Database installer fails if user has TNS_ADMIN set and tnsnames.ora file in a directory other than $ORACLE_HOME/network/admin.

Fix: The database installer has been fixed to handle this situation properly.

DAT-157

Issue: SDM failed to archive EVT_DEST_SMRY_1

Fix: Fixed two cases causing SDM to fail to archive EVT_DEST_SMRY_1. One is a unique constraint caused by the ARCH_SEQ column being too short and the other is on MSSQL logging into SDM using Windows Authentication. This affects all the event and event summary tables.

DAT-161(Enhancement)

Issue: Separate archive and delete partitions of summary table from events tables

Fix: Summary table partitions are now not dropped when dropping event table partitions.

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:
    1. Login to machine running the DAS component as user esecadm.
    2. 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'.
    3. 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.