Sentinel™ 5

Product Release Notes

Product

Sentinel™ 5.1.1 Linux with iTRAC™

Contents

Product Release Notes 1
Product 1
Contents 1
Description 1
Installation 1
New Features 2
Bug Fixes 4
  Sentinel 4
  Wizard 6
  Database 7
Known Issues 8
Product Support 9

Description

This is a full Sentinel™ 5.1.1 Linux release with iTRAC™.

Installation

The Sentinel™ 5.1.1 Linux release with iTRAC™ installer is capable of installing the following components on the following Operating Systems:

- Linux
  - Database
  - Sentinel Services
    - Communication Server
    - Advisor
    - Correlation
    - Data Access Service
  - Agent Service
  - Applications
    - Sentinel Control Center
    - Sentinel Data Manager
  - 3rd-party Integration
    - HP OpenView Service Desk
    - Remedy Integration
- Windows
  - Applications
    - Agent Builder

- Sentinel Control Center

This release contains Sentinel Services and Agent Service (Agent Manager) software for Linux only. Therefore, in order to allow greater flexibility on which operating system platforms the Agent Service can be installed, this release also supports distributed cross-version configurations. Choose the distributed configuration you wish to use from the options below to determine the supported cross-version configuration.

- All Sentinel Services and Agent Services on Linux (basic configuration)
  - Software from Sentinel™ 5.1.1 Linux release running on Linux
    - Sentinel Services
    - Agent Services
  - Software from Sentinel™ 5.1.1 Linux release running on Linux or Windows
    - Sentinel Control Center
  - Software from Sentinel™ 5.1.1 Linux release running on Windows
    - Agent Builder
- Agent Services running on Linux, Windows, or Solaris and Sentinel Services running on Windows or Solaris
  - Software from Sentinel™ 5.1.1.0 release running on Windows or Solaris
    - Sentinel Services
    - Agent Services
    - Sentinel Control Center
  - Software from Sentinel™ 5.1.1.0 release running on Windows
    - Agent Builder
  - Software from Sentinel™ 5.1.1 Linux release running on Linux
    - Agent Services
- Agent Services running on Linux, Windows, or Solaris and Sentinel Services running on Linux
  - Software from Sentinel™ 5.1.1 Linux release running on Linux
    - Sentinel Services
    - Agent Services
  - Software from Sentinel™ 5.1.1 Linux release running on Linux or Windows
    - Sentinel Control Center
  - Software from Sentinel™ 5.1.1 Linux release running on Windows
    - Agent Builder
  - Software from Sentinel™ 5.1.1.0 release running on Windows or Solaris
    - Agent Services

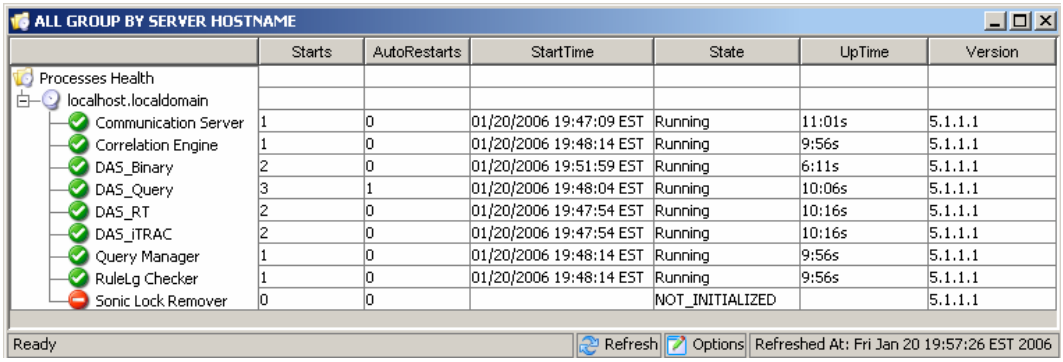
See the following chapter in the Sentinel Install Guide for installing the Sentinel™ 5.1.1 Linux release on Linux or Windows.

- Chapter 4, Installing Sentinel 5 for Oracle on Linux

New Features

- 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 Agents 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).



- 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 syslog connector is now installed with scripts that run on 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 on Unix with the default configuration, run the following commands:
    1. Log in as root.
    2. cd $ESEC_HOME/wizard/syslog
    3. ./syslog-server.sh install
- 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. An “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: Correlation_engine execute command is sending the EventName of the Correlation_event for the real event.

Fix: The 13th and 26th parameter values are now populated with EventName of Correlated Event and the First Event that has triggered the correlation 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.

Wizard

7414 (HD 101689)

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

Fix: Fixed by initializing variable properly.

WIZ-1649

Issue: Agent 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: Agent Manager SNMP support only handles “public” community traps.

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

WIZ-1656

Issue: Agent 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 Agent Manager.

WIZ-1661

Issue: Setting the agent 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, Agent Manager gets into a state when it is using nearly 100% CPU but is not processing any event, even though agentengine are running.

Fix: Fixed error causing this scenario to occur.

WIZ-1676

Issue: Memory leak when using the Alert Command.

Fix: Fixed memory leak.

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.

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, agents, agent 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 Agent 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 Agent Builder, UUIDs are not reset in the copied port configurations. This results in the events from copied port configurations having the same Source Id.

Product Support

- For Technical Support, email at support@esecurity.net
- For information, email at info@esecurity.net
- Website: www.esecurity.net
- For 24x7 support, call technical support directly at 800-474-3131