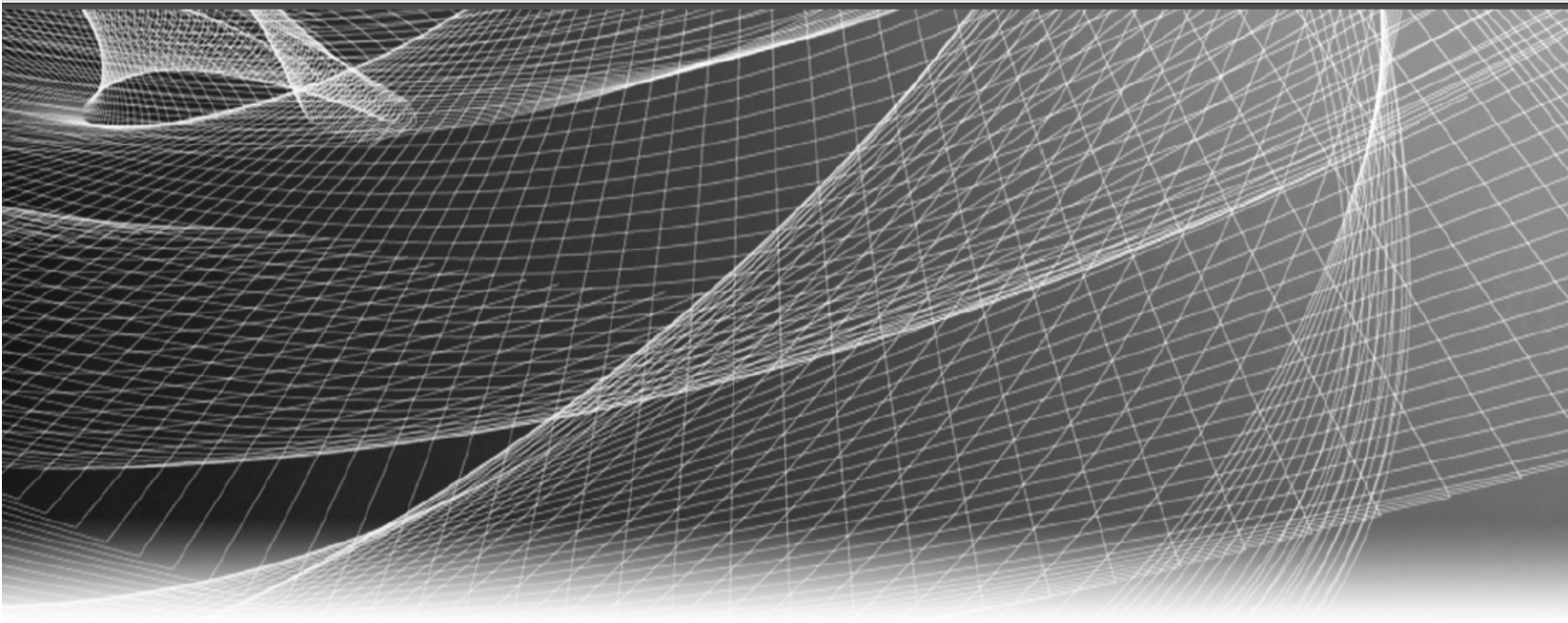

RSA Security Analytics

Release Notes

for Version 10.6.6

RSA

EMC²

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

Introduction

This document lists what's new and changed in RSA® Security Analytics, as well as workarounds for known issues. Read this document before deploying or updating RSA Security Analytics.

RSA Security Analytics 10.6.6.0 is a service pack for Security Analytics 10.6.x.x.

Build Numbers

The following table lists the build numbers for various components of RSA Security Analytics version 10.6.6.0.

Component	Version Number
Security Analytics Web Server	10.6.6.0-180725110545.5
Security Analytics Decoder	10.6.6.0-7228.5
Security Analytics Concentrator	10.6.6.0-7228.5
Security Analytics Broker	10.6.6.0-7228.5
Security Analytics Log Decoder	10.6.6.0-7228.5
Security Analytics Log Collector	10.6.6.0-14190.5
Security Analytics IPDB Extractor	10.6.6.0-17284.5
Security Analytics Incident Management	10.6.6.0-1061.5
Security Analytics Reporting Engine	10.6.6.0-5639.5

Security Analytics Warehouse Connector	10.6.6.0-1952.5
Security Analytics Archiver (Workbench)	10.6.6.0-7228.5
Security Analytics Event Stream Analysis	10.6.6.0-321.g8da04fc.5
Security Analytics Malware Analysis	10.6.6.0-8306.5
Security Analytics Context Hub	10.6.6.0-608.5

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA Security Analytics 10.6.6.0 Online Help	https://community.rsa.com/community/products/netwitness/1065 **Note:** Refer to 10.6.5 documentation for 10.6.6.x release.
RSA Security Analytics 10.6.6.0 Update Instructions	https://community.rsa.com/community/products/netwitness/1066
RSA Security Analytics 10.6.6.0 Update Checklist	https://community.rsa.com/community/products/netwitness/1066

What's New

RSA Security Analytics 10.6.6.0 is a service pack for Security Analytics 10.6.x.x. This release includes the following new enhancements.

Administration

Automatic Scheduler: Automatic scheduler is introduced to remove older jobs (such as exported PCAP, Logs and Packets) from the UI.

Reporting Engine

DB Intensive Operations: You can increase the DB size on Reporting Engine to 6500 values per hour.

Log Collector

Access Key Characters: Log collection custom configuration parameters are now increased to allow up to 4096 characters for standard values and 8192 characters for encrypted values.

Improved "Pass-Through-Logic" for non-conformant Syslog: The RLC now accepts all non-conformant syslog messages except for those with an empty message header/body. Unwanted messages should be filtered out at the syslog collection using event filters. See the "Configure Event Filters" for a Collector section in the *Log Collection Guide*. Refer to syslog RFC3164 and RFC5424 for details about syslog format.

Update Notes

The following update paths are supported for Security Analytics 10.6.6.0:

- Security Analytics 10.5.5.0 to 10.6.6.0
- Security Analytics 10.6.0.0 to 10.6.6.0
- Security Analytics 10.6.0.1 to 10.6.6.0
- Security Analytics 10.6.0.2 to 10.6.6.0
- Security Analytics 10.6.1.0 to 10.6.6.0
- Security Analytics 10.6.1.1 to 10.6.6.0
- Security Analytics 10.6.2.0 to 10.6.6.0
- Security Analytics 10.6.2.1 to 10.6.6.0
- Security Analytics 10.6.2.2 to 10.6.6.0
- Security Analytics 10.6.3.0 to 10.6.6.0
- Security Analytics 10.6.3.1 to 10.6.6.0
- Security Analytics 10.6.3.2 to 10.6.6.0
- Security Analytics 10.6.4.0 to 10.6.6.0
- Security Analytics 10.6.4.1 to 10.6.6.0
- Security Analytics 10.6.4.2 to 10.6.6.0
- Security Analytics 10.6.5.0 to 10.6.6.0
- Security Analytics 10.6.5.1 to 10.6.6.0
- Security Analytics 10.6.5.2 to 10.6.6.0

Note: The update paths supported are for 10.5.5.0 and 10.6.x.x patches released on or before the 10.6.6.0 release.

For more information on updating to 10.6.6.0, see the Update Instructions in the Product Documentation section.

Fixed Issues

This section lists issues fixed since the last Security Analytics release.

Security Fixes

Tracking Number	Description
SACE-8926	The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.
SACE-8392	The IPTables may allow connection attempts from non random port ranges.
ASOC-55341	kernel Security Update: https://access.redhat.com/errata/RHSA-2018:1319
ASOC-54882	openjdk Security Update: https://access.redhat.com/errata/RHSA-2018:1188
ASOC-54869	patch Security Update: https://access.redhat.com/errata/RHSA-2018:1199
ASOC-54868	openjdk Security Update: https://access.redhat.com/errata/RHSA-2018:1270
ASOC-55802	dhcp Security Update: https://access.redhat.com/errata/RHSA-2018:1454
ASOC-54444	libvorbis Security Update: https://access.redhat.com/errata/RHSA-2018:0649

Server Fixes

Tracking Number	Description
SACE-8839	Unable to share the dashboard when you log in as an analyst (Active Directory user).
SACE-8589	The Security Analytics UI becomes unresponsive due to increase in size of h2db.

SACE-8192	While configuring a global notification syslog server using TCP port, you can see the "length 0" response packet sent from syslog server.
SACE-7348	On the Decoder configuration Feeds and Parsers tabs, if you sort by ascending or descending order, the list is not sorted.
SACE-9121	RabbitMQ stops responding due to the large number of messages in a queue.
SACE-9136	Event Source Monitoring displays incorrect "Elapsed Time" when the alarm time is not cleared.
SACE-8827	On the Charts, the overlapping text is displayed because of the tooltip.
SACE-8619	Syslog Default Template on Event Source Management is linking all the "src" values to a single meta value.
SACE-8090	Automatic scheduler to remove older jobs (such as export PCAP, Logs and Packets) from the Security Analytics UI is not available.
SACE-9127/SACE-9124	Feed wizard does not display the editing page due to the session timeout.
SACE-8177	Log Decoder App Rules error is displayed due to which alert is not explicitly specified.
SACE-9190	Incorrect notification is displayed when a new App Rule is created in the Decoder.
SACE-9174	Security Analytics stops responding due to high logstash messages.
SACE-9070	Unable to edit Feeds after an update to 10.6.5.1.
SACE-8966	Out of memory error occurs when you export logs.

Health&Wellness Fixes

Tracking Number	Description
SACE-9267	Custom Event Source Monitoring does not clear the alarms automatically.
SACE-9099	Due to high Log Decoder events queue, an error occurs in the Health and Wellness statistics.

Investigation Fixes

Tracking Number	Description
SACE-8967/SACE-8791/SACE-9043/SACE-9025	Exact visualization timeline charts are not displayed on the Investigation view.
SACE-8969	Meta values are not loaded when idle time is set to 4 minutes.
SACE-9552	Investigation query breaks if the IP address is in single quotes.

Reporting Fixes

Tracking Number	Description
SACE-8875	Reports are not generated due to bad IM rules.
SACE-8514	On the Charts view, high chart reports overlap each other due to usehtml attribute.
SACE-8957	Reporting Engine deletes information on h2db.
SACE-8949	Deadlock errors on Reporting Engine due to incomplete reporting tasks.
SACE-8800	The PDF file does not display table columns when you generate reports from Reporting Engine.
SACE-8222	The sessionID results are not handled correctly by Broker due to which the test reports are not clear.

Log Collector Fixes

Tracking Number	Description
SACE-8350	Secure copy (SCP) fails on Virtual Log Collector (VLC) due to missing shared libraries.
SACE-9225	HPNonStop event source logs are missing syslog messages due to incorrect header format.

SACE-9171	File collection stops when you upgrade to 10.6.5.x or later due to lack of permissions for the executables.
SACE-8592	Incorrect warning message is displayed for the syslog collection.
SACE-9428	Issue in configuring Identity Feed.
SACE-9281	Azure plugin collection does not work due to incorrect permissions given to /etc/netwitness/ng and the sub folders.
SACE-9200	Log Collector service is restarted automatically when the plug-in event source is stopped.

Event Stream Analysis Fixes

Tracking Number	Description
SACE-8321	When you execute a script, the fields containing < and > are not displayed correctly in the Alert Summary.
SACE-8876	Whenever a recurring in-memory table is updated from SA, the recurring in-memory table on the ESA becomes empty.

Core Fixes

Security Analytics Core Services include Broker, Concentrator, Decoder, and Log Decoder.

Tracking Number	Description
SACE-9072/SACE-9028	Bad cast errors in the logs when any new native parser is trying to parse unknown logs.
SACE-8996	Reconstruction of an email fails due to bad character set conversion.
SACE-9401	Issue in Log Decoder service while upgrading to latest version.
SACE-8816	Security Analytics Console crashes due to _sharedConfig file.
SACE-8136	An error occurs in Investigation reconstruction view while parsing Unicode characters.

Warehouse Connector Fixes

Tracking Number	Description
SACE-8590	Temporary Warehouse Connector service is unavailable due to channel breakage.
SACE-8508	When you change Log Decoder or Packet Decoder, the lockbox for Warehouse Connector Service requries a change in the password.

Warehouse Fixes

Tracking Number	Description
SACE-9045/SACE-8851	When you run a test rule on Reporting Engine, the results are not loaded continuously.

Malware Fixes

Tracking Number	Description
SACE-8960	Malware fails to process doc files due to an internal error with apache-commons-compress.
SACE-9161	Malware is unable to get data from Broker due to a timeout on sdk-query.
SACE-8809	Unable to deploy Malware PE Artifacts rule.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

IPDB Extractor

Unable to execute IPDB Reports during SSL handshake due to failure in certificate validation.

Tracking Number: ASOC-57214

Problem: When you try to generate data from the IPDB to Reporting Engine using a query, the data is not downloaded.

Workaround: If IPDBExtractor setup is configured with SSL mode, you need to set the SSL mode to false (non-SSL) to generate data from the Reporting Engine. Follow the steps below to disable the SSL mode.

1. Log in to the REST API of IPDBEXRACTOR config. For example, http://<IPDBEXTRACTOR IP>:50125/ipdbextractor/config.
2. Set the parameter `SSL (transport.ssl)` to false.
3. Restart `nwipdbextractor` service.
4. Log in to Security Analytics and navigate to **Reporting Engine** >  > **View** > **Config** > **Sources** tab.
5. Delete the existing IPDB data source and then add IPDB data source.
6. Add the IPDB rule and run the reports.

Malware Analysis

Issue in SSL handshake when the files are uploaded for manual Malware scan.

Tracking Number: ASOC-57052

Problem: The certificate in the Malware appliance do not match the Malware "cloud.netwitness.com" as new certificates are updated in the cloud.

Workaround: You must install the latest available "ca-certificates" package on the Malware appliance OR manually add the certificate provided by "cloud.netwitness.com" using the below steps.

1. Back up the existing cacerts from `/etc/pki/java/cacerts`
2. Obtain the certificate of cloud.netwitness.com:
   ```
   openssl s_client -connect cloud.netwitness.com:443 -tls1_2
   ```
3. Copy the certificates to the file `mycert.crt`

4. Using the key tool import the certificate into cacerts.
   ```
   keytool -import -trustcacerts -keystore /etc/pki/java/cacerts -
   storepass changeit -noprompt -alias mycert -file mycert.crt
   ```
5. Restart the Malware appliance.

Investigation

Unable to export logs from Events View for Log Decoder.

Tracking Number: ASOC-59144

Problem: After you update the Admin Server to 10.6.6, and you export the logs for the Log Decoder, the exported file is empty even though the logs are available in the Log Decoder.

Note: The below mentioned workaround is not required if you do not have a specific reason to export logs from Log Decoder. You can continue to investigate and export logs from Log Decoder through Concentrator by applying the filters did=<decode_id>.

Workaround: You must index the medium meta if you want to export logs for the Log Decoder. The following steps indexes the new events and you can export these events.

1. Update the custom index config file index-logdecoder-custom.xml
   <key description="Medium" level="IndexValues" name="medium" format="UInt8" valueMax="100" defaultAction="Hidden">
   <aliases>
   <alias format="$alias" value="1">Ethernet</alias>
   <alias format="$alias" value="2">Tokenring</alias>
   <alias format="$alias" value="3">FDDI</alias>
   <alias format="$alias" value="4">HDLC</alias>
   <alias format="$alias" value="5">NetWitness</alias>
   <alias format="$alias" value="6">802.11</alias>
   <alias format="$alias" value="7">802.11 Radio</alias>
   <alias format="$alias" value="8">802.11 AVS</alias>
   <alias format="$alias" value="9">802.11 PPI</alias>
   <alias format="$alias" value="10">802.11 PRISM</alias>
   <alias format="$alias" value="11">802.11 Management</alias>
   <alias format="$alias" value="12">802.11 Control</alias>
   <alias format="$alias" value="13">DLT Raw</alias>
   <alias format="$alias" value="32">Logs</alias>
   <alias format="$alias" value="33">Correlation</alias>
   <alias format="$alias" value="34">Relationship</alias>
   </aliases>

</key>

2. Restart the Log Decoder.
   If the Log Decoder is not restarted, you need to wait until the next index-save.

Reporting Engine

The Reporting Engine Sources tab does not load when you add or remove a data source.

Tracking Number: ASOC-59524

Problem: After you add or delete a data source in the Sources tab, the tab does not display the changes due to the ConcurrentModificationException error.

Workaround: You must refresh Security Analytics UI to view the changes.

Deadlock errors on Reporting Engine due to incomplete reporting tasks.

Tracking Number: ASOC-55445

Problem: When the load limit exceeds 6500 values per hour on Reporting Engine, Deadlock errors are displayed in the Reporting Engine logs.

Workaround: None

Contacting Customer Care

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com/
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/rsa-customer-support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA Security Analytics product or application you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
1.0		RTO