

An abstract graphic at the top of the page consisting of a white wireframe grid that curves and flows across a dark background, creating a sense of depth and movement.

RSA | Security Analytics

Release Notes
for Version 10.6.6.1

Copyright © 1994–2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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 EMC, 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 EMC.

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

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

Contents

Introduction	5
Fixed Issues	5
Security Fixes	5
Log Collector Fixes	5
Investigation Fixes	5
Event Stream Analysis Fixes	5
Core Fixes	5
Build Numbers	6
Update Instructions	7
Update Preparation Tasks	7
Task 1. Review Core Ports and Open Firewall Ports	7
Task 2. Make Sure IPDB Mount Points Are Accessible	7
Task 3. Fix Your Rules	7
Task 4. Designate Primary and Secondary Security Analytics Servers	8
Task 5. Back Up Your Configuration	8
Task 6 – Stop Data Capture and Aggregation	9
Task 7. Prepare Event Stream Analysis, Malware Analysis, and Security Analytics Host	11
Task 8. Configure Reporting Engine for Out-of-the-Box Charts	11
Update Tasks	11
Task 1. Populate Local Update Repository	11
Task 2. Update Security Analytics Hosts to 10.6.6.1	12
Task 3: Update the Security Analytics Service Hosts to 10.6.6.1	13
Update or Install Legacy Windows Collection	14
Post Update Tasks	14
Task 1 – Start Data Capture and Aggregation	14
Task 2 – Set Permissions for Context Hub Service	15
Task 3. Restore Malware Analysis Custom Parameters Values to Newly Created Configuration File	17
Task 4 – Restore /etc/init.d/pf_ring and /etc/pf_ring/mtu.conf files	17
Task 5 – Migrate DISA STIG to 10.6.6.1	17
Task 6 – Reset Stable System Value of Log Collector Lockbox	17
Task 7 – Check Health and Wellness Policies for Changes from Update	18
Task 8 – (Optional) Security Update for MapR 3.1 or MapR 4.1	18
Troubleshooting	18

Product Documentation	18
Feedback on Product Documentation	19
Contacting Customer Care	19
Preparing to Contact Customer Care	19
Revision History	20

Introduction

RSA Security Analytics 10.6.6.1 release addresses bug fixes and security fixes. Read this document before deploying or updating this patch.

RSA Security Analytics 10.6.6.1 is a patch for Security Analytics 10.6.6.0.

Fixed Issues

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

Security Fixes

Tracking Number	Description
ASOC-72911	CVE-2019-3725, Command Injection Vulnerability. https://nvd.nist.gov/vuln/detail/CVE-2019-3725?cpeVersion=2.2

Log Collector Fixes

Tracking Number	Description
SACE-11001/ SACE-9479	Segmentation error occurs during the checkpoint process, as a result of the change in the checkpoint library.

Investigation Fixes

Tracking Number	Description
SACE-10876	Investigation > Events view displays incorrect event time.

Event Stream Analysis Fixes

Tracking Number	Description
SACE-10340	When you edit and save the Ignore case? parameter, the change is not reflected on the Security Analytics UI.

Core Fixes

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

Tracking Number	Description
SACE-10380	Concentrator crashes when you perform certain queries in Investigation view.
SACE-10224	CEF parser is not able to parse logs if the username contains backslash (\).
SACE-9798	When you transfer a file using the SMB protocol, an incorrect file is extracted on the Investigation view.

Build Numbers

The following table lists the build numbers for various components of RSA Security Analytics version 10.6.6.1.

Component	Version Number
Security Analytics Web Server	10.6.6.1-190424063615.5
Security Analytics Decoder	10.6.6.1-7235.5
Security Analytics Concentrator	10.6.6.1-7235.5
Security Analytics Broker	10.6.6.1-7235.5
Security Analytics Log Decoder	10.6.6.1-7235.5
Security Analytics Log Collector	10.6.6.1-14198.5
Security Analytics IPDB Extractor	10.6.6.1-17287.5
Security Analytics Incident Management	10.6.6.1-1066.5
Security Analytics Reporting Engine	10.6.6.1-5644.5
Security Analytics Warehouse Connector	10.6.6.1-1957.5
Security Analytics Archiver (Workbench)	10.6.6.1-7235.5
Security Analytics Event Stream Analysis	10.6.6.1-337.g92d5746.5
Security Analytics Malware Analysis	10.6.6.1-8310.5
Security Analytics Context Hub	10.6.6.1-612.5

Update Instructions

This section provides procedures for updating Security Analytics from version 10.6.6.0 to version 10.6.6.1.

Complete the following tasks to prepare for the update to Security Analytics 10.6.6.1.

The following update path is supported for Security Analytics 10.6.6.1:

- Security Analytics 10.6.6.0 to 10.6.6.1

Update Preparation Tasks

Task 1. Review Core Ports and Open Firewall Ports

Review the changes to the Core ports. See *Network Architecture and Ports* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83308>) so that you can reconfigure Security Analytics services and your firewall. The following port must be available for 10.6.6.1: Event Stream Analysis (ESA) Context Hub Service Port.

Make sure that the ESA host running the Context Hub service can access port 50022.

Caution: Do not proceed with the update until the ports on your firewall are configured.

Task 2. Make Sure IPDB Mount Points Are Accessible

Make sure that all the IPDB Extractor mount points are accessible. For more information on how to configure IPDB mount points, see **Step 1. Mount the IPDB** topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83168>).

Task 3. Fix Your Rules

All queries and rule conditions in Security Analytics Core services must follow these guidelines:

All string literals and time stamps must be quoted. Do not quote number values and IP addresses.

For example:

- `extension = 'torrent'`
- `time='2018-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Note: The space on the right and the left of an operator is optional. For example, you can use `service=80` or `service = 80`.

For information about how to find rules that need to be updated to conform to these guidelines, see *Rule and Query Guidelines* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83104>).

Task 4. Designate Primary and Secondary Security Analytics Servers

If you have a multiple Security Analytics server deployment, you must designate a Primary Server and Secondary Servers and check the **RSASoftware.repo** file. For more information on the type of deployment, see *Multiple Security Analytics Server Deployment* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83307>).

If you deploy multiple Security Analytics Servers:

1. Before you update the Security Analytics Server Host to 10.6.6.1, designate a Primary Server and Secondary Servers. For more information on the deployment, see *Update Hosts in Correct Sequence* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83515>).
2. Before you update the rest of the hosts to 10.6.6.1, check the **RSASoftware.repo** file and make sure the `baseurl` is pointing to the Primary Server Host with the following command string.

```
# cat /etc/yum.repos.d/RSASoftware.repo
```

The following output is displayed.

```
baseurl=http://Primary-SA-IP-Address/rsa/updates
```

Caution: A Secondary RSA SA Server has the following limitations: The version update functionality on the Hosts view is valid for the Primary RSA SA Server exclusively. It reflects the wrong status for Secondary RSA SA Servers so you must not update to new RSA SA versions from the Hosts view of a Secondary RSA Server.

- You cannot use the Health and Wellness views.
- You cannot use the trusted connections feature.

Task 5. Back Up Your Configuration

RSA recommends that you take a backup copy of your configuration before you perform the update. For more information on how to back up your configuration, see *Back Up and Restore Data for Hosts and Services* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-84594>).

Note: If you customized the `/etc/init.d/pf_ring` script to use MTU from the `/etc/pf_ring/mtu.conf` file, back up the following files:

```
/etc/init.d/pf_ring  
/etc/pf_ring/mtu.conf
```

Back Up Malware Analysis Configuration File to Another Directory:

1. Back up `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` to another, safe directory. You need to retrieve your custom parameter values from this backup after you update the Malware Analysis host to 10.6.6.1. The update creates a new configuration file with all the

parameters set to the default values.

2. Delete `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml`.

Task 6 – Stop Data Capture and Aggregation



RSA recommends that you stop packet and log capture and aggregation before updating to 10.6.6.1.

Stop Packet Capture

To stop packet capture:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.
2. Select each **Decoder** service.

The screenshot displays the RSA Security Analytics interface. The top navigation bar includes 'Administration', 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', 'Security', and 'RSA Security Analytics'. Below the navigation bar, there is a toolbar with buttons for 'Change Service', 'Decoder', 'System', 'Upload Packet Capture File', 'Stop Capture', 'Host Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content area is divided into two columns: 'Decoder Service Information' and 'Appliance Service Information'. The 'Decoder Service Information' section shows details for 'Decoder-0 (Decoder)', including its version, memory usage (2209 MB), CPU usage (2%), running since time (2016-May-13 14:16:50), uptime (5 days 3 hours 11 minutes 40 seconds), and current time (2016-May-18 17:28:30). The 'Appliance Service Information' section shows details for 'Decoder-0 (Host)', including its version, memory usage (20224 KB), CPU usage (3%), running since time (2016-May-12 18:44:59), uptime (5 days 22 hours 43 minutes 32 seconds), and current time (2016-May-18 17:28:31). Below these sections are 'Decoder User Information' and 'Host User Information'. The bottom status bar shows the user 'admin', language 'English (United States)', and time zone 'GMT+00:00', along with a 'Send Us Feedback' link.

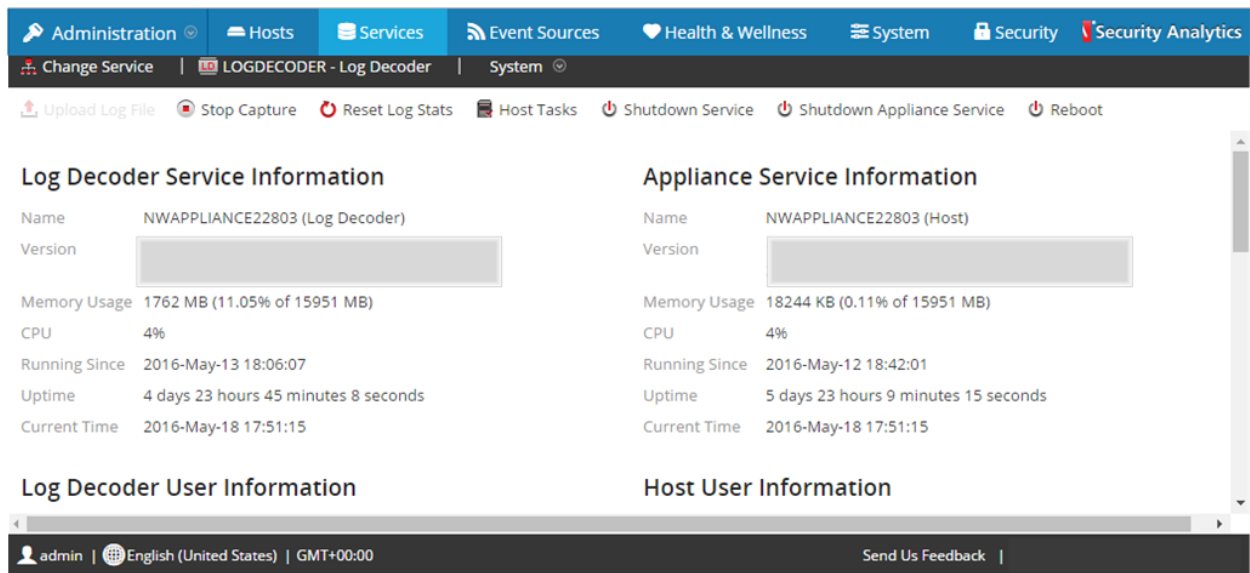
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Stop Capture**.

Stop Log Capture

To stop log capture:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.

2. Select each **Log Decoder** service.



3. Under  (actions), select **View > System**.

4. In the toolbar, click  **Stop Capture**.

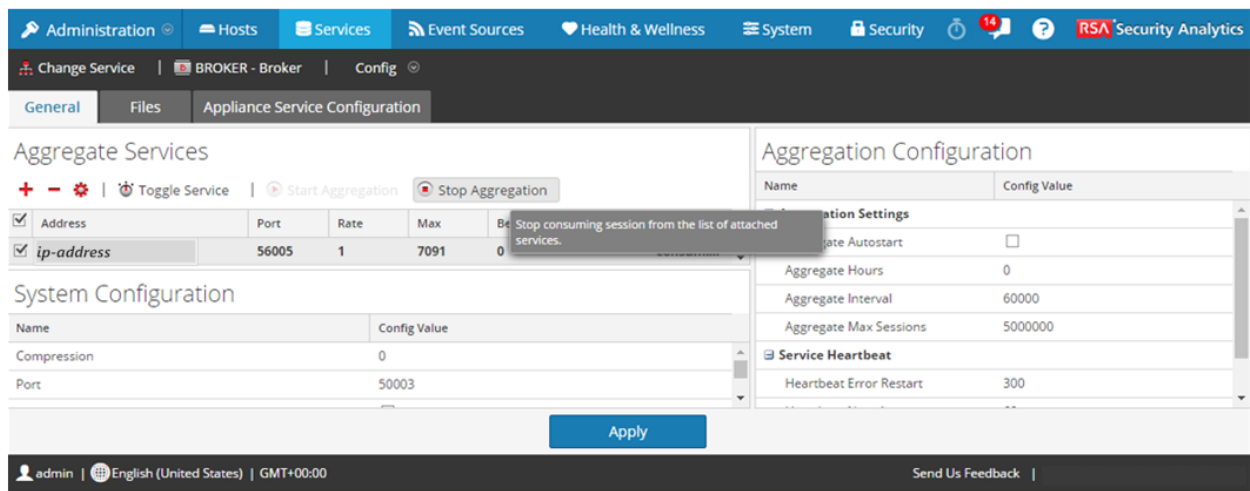
Stop Aggregation

1. In the **Security Analytics** menu, select **Administration > Services**.

2. Select the **Broker** service.

3. Under  (actions), select **View > Config**.

4. The **General** tab is displayed.



5. Under **Aggregated Services** click .

Task 7. Prepare Event Stream Analysis, Malware Analysis, and Security Analytics

Host

Run the following command on Event Stream Analysis (ESA), Malware Analysis (MA), and RSA SA (SA) appliances to ensure that authentication works properly during investigations:

```
chattr -i /var/lib/puppet/lib/puppet/provider/java_ks/keytool.rb
```

Task 8. Configure Reporting Engine for Out-of-the-Box Charts

For Out-of-the-Box charts to run after the update, you must configure the default data source on the Reporting Engine Configuration page before you perform the update. If you do not perform this task, you must manually set up the data source after the update. For more information on the Reporting Engine data sources, see *Reporting Engine Configuration Guide* in the Security Analytics help (<https://community.rsa.com/docs/DOC-83726>).

Update Tasks

This topic contains the tasks you must complete for the following update path:

Note: If you are upgrading an All-in-One Logs appliance, before you begin the update process described in this section, SSH to Security Analytics and run `puppet agent -t`.

Task 1. Populate Local Update Repository

Download version updates from RSA Link under Downloads (<https://community.rsa.com/>)

To populate your Local Update Repository from RSA Link:

1. Download the files below, which contain all the Security Analytics 10.6.6.1 update files, from RSA Link (<https://community.rsa.com/>) to a local directory:
 - sa-10.6.6.1-upgradepack-1-of-5-el6.zip
 - sa-10.6.6.1-upgradepack-2-of-5-el6.zip
 - sa-10.6.6.1-upgradepack-3-of-5-el6.zip
 - sa-10.6.6.1-upgradepack-4-of-5-el6.zip
 - sa-10.6.6.1-upgradepack-5-of-5-el6.zip
2. In the Security Analytics menu, select **Administration > System**.
3. In the left panel, select **Updates**.
4. In the **Settings** tab, make sure the **Connect to Live Update Repository** checkbox is not selected.
5. In the **Manual Updates** tab, click **Upload Files**.
The Upload File dialog is displayed.

6. Click **+** and browse to the local directory where you put the following files, select all the files, and click **Upload**.

sa-10.6.6.1-upgradepack-1-of-5-el6.zip

sa-10.6.6.1-upgradepack-2-of-5-el6.zip

sa-10.6.6.1-upgradepack-3-of-5-el6.zip

sa-10.6.6.1-upgradepack-4-of-5-el6.zip

sa-10.6.6.1-upgradepack-5-of-5-el6.zip

The upload status is displayed in the progress bar. When the upload is complete, the zip files are displayed in the Manual Updates tab.

7. Select all the files in the Manual Updates list and click **Move to Repo**.

This moves the RPM files into the Local Update Repository on the Security Analytics Server and makes them available to hosts.

Task 2. Update Security Analytics Hosts to 10.6.6.1

Note: When you update the Security Analytics (SA) Server Host, Security Analytics backs up the System Management Service (SMS) configuration files (excluding the `wrapper.conf` file) from the `/opt/rsa/sms/conf` directory to the `/opt/rsa/sms/conf_%timestamp%` directory. This is a precautionary measure for the rare occasion when you may need to restore the SMS configuration from backup. To do this, replace the files in the `/opt/rsa/sms/conf` directory with the files backed up to the `/opt/rsa/sms/conf_%timestamp%` directory after the update.

1. **(Conditional) For Multiple Security Analytics Server deployments only**, SSH to each Secondary SA Server Host and make sure the puppetmaster is enabled using the following commands:

```
service puppetmaster start
```

```
service puppet start
```

2. Log in to Security Analytics.
3. In the Security Analytics menu, select **Administration > Hosts**.
4. Select the Security Analytics Server Host, and then select 10.6.6.1 as the version to update to in the **Update Version** column.
5. From the toolbar, click **Update**. The Updates Available dialog is displayed with a summary of the changes available.
6. Click **Begin Update**.

The following message is displayed:

```
Running pre-update checks on host.
```

The **Status** column describes what is happening in each of the following stages of the update:

- Downloading update packages
 - Checking your current version configuration to ensure that it has no conflicts. Displays:
 - **Update warning.** [View details](#) if there is a kernel update.
 - **Update conflict.** [View details](#) if there is a potential conflict.For more information on how to address these configuration warnings and conflicts, see *Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83519>).
 - Initiating the update if there are no conflicts.
 - Installing update packages.

Displays **Error in Update.** [View details](#) if there is an error applying a package that blocks the update. For more information on how to resolve these errors, see *Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors* in the Security Analytics help (<https://community.rsa.com/docs/DOC-83519>).

After the host is updated, Security Analytics prompts you to **Reboot Host**.
7. Wait until Security Analytics refreshes, and then from the toolbar, click **Reboot Host**. Security Analytics shows the status as **Rebooting** until the host comes back online. After the host comes back online, the **Status** shows **Up-to-Date**. [Contact Customer Care](#) if the host does not come back online.

Task 3: Update the Security Analytics Service Hosts to 10.6.6.1

1. Log in to Security Analytics.
2. In the Security Analytics menu, select **Administration > Hosts**.

Note: If you have a non-Security Analytics Server host running a version that is earlier than the supported 10.6.6.1 update path (that is, earlier than 10.6.6) and you updated your Security Analytics Server Host to 10.6.6.1, the non-Security Analytics Server host will display “**Update Path Not Supported**” in the **Status** column of the Hosts view and you cannot update it from this view. [Contact Customer Care](#) to update the non-Security Analytics Server host on the unsupported path.

3. Update hosts in the sequence recommended in the *Update Hosts in Correct Sequence* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-83515>). Select the device you want to update, and in the **Update Version** column, select **10.6.6.1**.
4. Click **Update** from the toolbar. The **Status** column tells you what is happening in each of the following stages of the update:

- Downloading update packages.
- Checking your current version configuration to ensure that it has no conflicts. Displays:
 - **Update warning.** [View details](#) if there is a kernel update.
 - **Update conflict.** [View details](#) if there is a potential conflict.
For more information on how to address the configuration warnings and conflicts, see *Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors* in the Security Analytics help (<https://community.rsa.com/docs/DOC-83519>).
- Initiating the update if there are no conflicts.
- Installing update packages.
Displays **Error in Update.** [View details](#) if there is an error applying a package that blocks the update. For more information on how to resolve the errors, see *Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors* in the Security Analytics help (<https://community.rsa.com/docs/DOC-83519>).
After the host is updated, Security Analytics prompts you to **Reboot Host**.

5. From the toolbar, click **Reboot Host**.

Security Analytics shows the status as **Rebooting** until the host comes back online. After the host comes back online, the status shows **Up-to-Date**. [Contact Customer Care](#) if the host does not come back online.

Note: If you have DISA STIG enabled, opening core services can take an additional 5 to 10 minutes. This delay is caused by the generation of new certificates.

Update or Install Legacy Windows Collection

For information on how to install or update Legacy Windows collection, see the *Legacy Windows Collection Update & Installation Instructions* in the Security Analytics help (<https://community.rsa.com/docs/DOC-41196>).

Note: After you update or install Legacy Windows Collection, reboot the system to ensure that Log Collection functions correctly.

Post Update Tasks

This topic contains the tasks you must complete after you update to 10.6.6.1.

Task 1 – Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 10.6.6.1.

To start packet capture:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.

2. Select each **Decoder** service.

3. Under  (actions), select **View > System**.

4. In the toolbar, click .

To start log capture:

1. In the **Security Analytics** menu, select **Administration > Services**.
The Services view is displayed.

2. Select each **Log Decoder** service.

3. Under  (actions), select **View > System**.

4. In the toolbar, click .


To start aggregation:

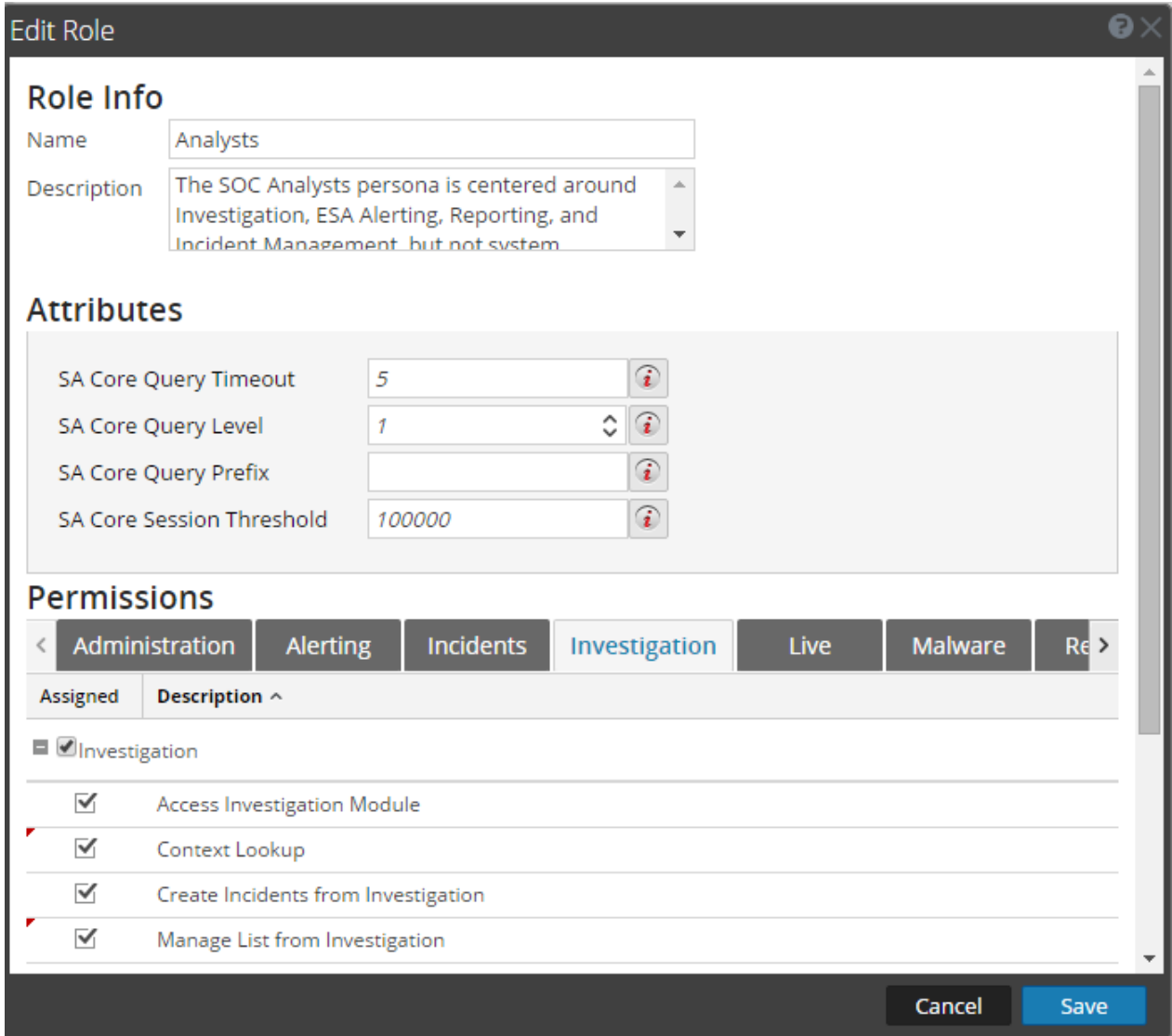
During the update to 10.6.6.1, the Broker Service is restarted and this automatically starts aggregation.

Task 2 – Set Permissions for Context Hub Service

You must set the **Investigation-Context Lookup** and **Investigation-Manage List from Investigation** permissions for the appropriate roles after you update to 10.6.6.1.

To set the **Context Lookup** and **Manage List from Investigation** permissions:

1. Log in to Security Analytics.
2. Go to the **Administration > Security > Roles** tab.
3. Select the role for which you want to set the permission and click .
4. Click **Investigation** under **Permissions** and select the **Context Lookup** and **Manage List from Investigation**.



Edit Role

Role Info

Name: Analysts

Description: The SOC Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Incident Management, but not system

Attributes

SA Core Query Timeout: 5

SA Core Query Level: 1

SA Core Query Prefix:

SA Core Session Threshold: 100000

Permissions

Administration | Alerting | Incidents | **Investigation** | Live | Malware | Re >

Assigned | Description ^

Investigation

- Access Investigation Module
- Context Lookup
- Create Incidents from Investigation
- Manage List from Investigation

Cancel Save

5. Click **Save**.

Task 3. Restore Malware Analysis Custom Parameters Values to Newly Created Configuration File

Replace defaults in the newly created

`/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` configuration file with custom parameter values from the `malwareCEFDictionaryConfiguration.xml` backed up before updating to 10.6.6.1.

1. Compare `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` and the backed up `malwareCEFDictionaryConfiguration.xml` file.
2. Replace the defaults in the updated version of the product in `thenew/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` file with the custom values from the back up to retain defaults for new parameters added in 10.6.6.1.

Task 4 – Restore `/etc/init.d/pf_ring` and `/etc/pf_ring/mtu.conf` files

If you customized the `/etc/init.d/pf_ring` script to use MTU from the `/etc/pf_ring/mtu.conf` file, restore the following files that you backed up during the pre-update tasks:

```
/etc/init.d/pf_ring
/etc/pf_ring/mtu.conf
```

Note: Restore `/etc/init.d/pf_ring` and `/etc/pf_ring/mtu.conf` files.

Task 5 – Migrate DISA STIG to 10.6.6.1

If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening RPM in Security Analytics, you must perform the following task to migrate it to 10.6.6.1.

For all hosts with STIG applied:

1. SSH to the host.
2. Switch to `root` and enter the following command strings.

```
cd /opt/rsa/AqueductSTIG/
./GEN000400.sh
reboot
```

Task 6 – Reset Stable System Value of Log Collector Lockbox

You must reset the **Stable System Value** of the Log Collector Lockbox because of kernel updates. If you do not reset the **Stable System Value**, the **Lockbox Access Failure** rule will trigger a critical alarm in the **Administration > Health & Wellness > Alarms** view for the Log Collector.

Task 7 – Check Health and Wellness Policies for Changes from Update

Check your Health and Wellness policies for any changes that the upgrade may have made. For more information on how to check your Health and Wellness policies, see *Monitor Health and Wellness of Security Analytics* topic in the Security Analytics help (<https://community.rsa.com/docs/DOC-84587>). You can also refer to the *System Maintenance Checklist* in the Security Analytics help (<https://community.rsa.com/docs/DOC-84580>).

Task 8 – (Optional) Security Update for MapR 3.1 or MapR 4.1

Update security fixes on MapR 3.1 or 4.1. For more information on how to update security fixes on MapR 3.1 or 4.1, see *RSA Security Analytics MapR 3.1 or 4.1 Security Updates* guide in Security Analytics help (<https://community.rsa.com/docs/DOC-63202>).

Troubleshooting

Note: If you cannot resolve any update issue using the following troubleshooting solutions, contact [Customer Care](#).

Problem	Description
Problem 1	Pre-update server configuration issues
Possible Cause	RSA SA displays conflicts, If the pre-update server configuration has any configuration issues that would prevent a successful update to 10.6.6.1,
Solution	For instructions on how to resolve pre-update errors, see <i>Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors</i> in the Security Analytics help (https://community.rsa.com/docs/DOC-83519)
Problem 2	Errors during update process
Possible Cause	If Security Analytics encounters an error during the update process, it displays Update Error in the Updates column of the Hosts view.
Solution	For more information on how to resolve update errors, see <i>Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors</i> in the Security Analytics help (https://community.rsa.com/docs/DOC-83519).

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/1066>

Feedback on Product Documentation

You can send an email to sahelpfeedback@emc.com to provide feedback on RSA NetWitness Platform documentation.

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	30 April, 2018	Final Draft