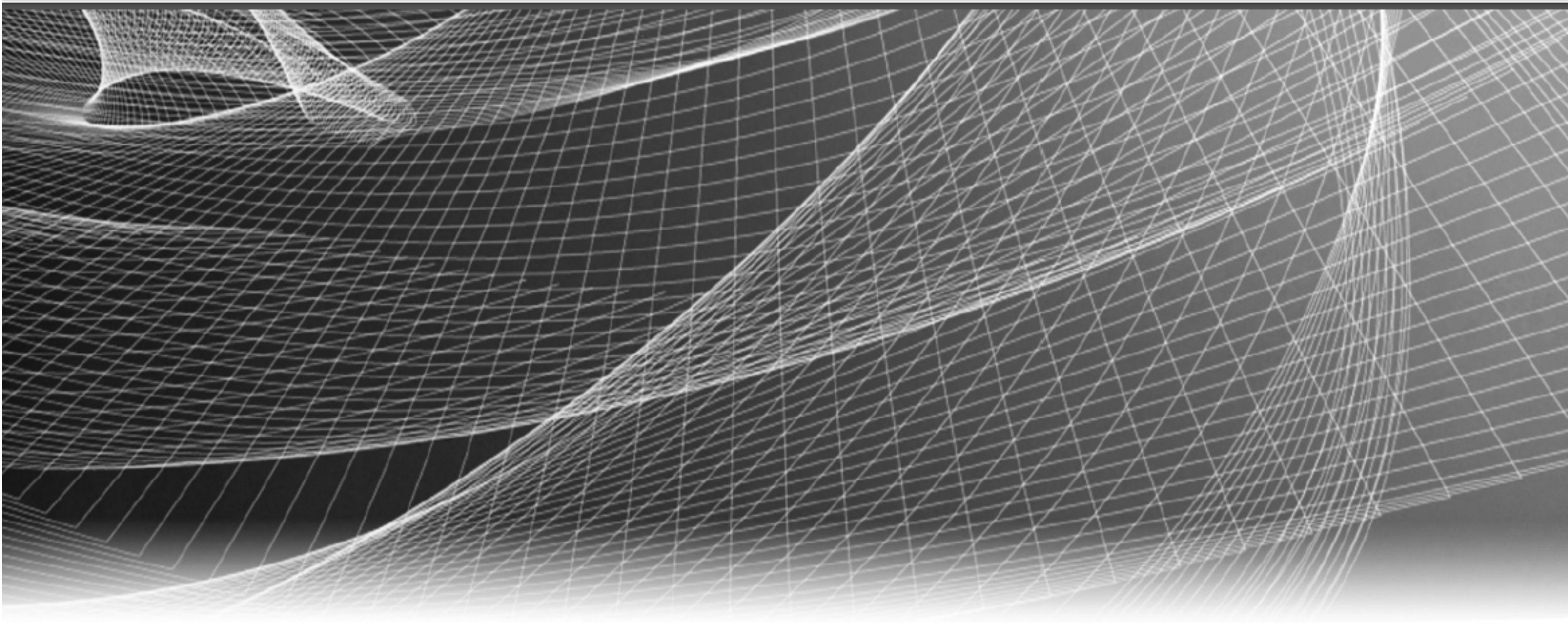


RSA Security Analytics

10.6.6.0 Update Instructions

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

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.

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

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Security Analytics 10.6.6.0 Update Introduction

Security Analytics 10.6.6.0 provides fixes for all products in the Security Analytics suite. The components of the suite are the Security Analytics Server, Broker, Concentrator, Log Decoder and Decoder, Hybrid, All-in-One, Malware Analysis, Archiver, Event Stream Analysis, Context Hub, Log Collector, Warehouse Connector, Workbench, Reporting Engine, and IPDB Extractor. The instructions in this guide apply to both physical and virtual hosts unless stated to the contrary.

Note: Refer to the *RSA Security Analytics Virtual Host Setup Guide* (https://community.rsa.com/) for information on installation and configuration of Security Analytics hosts running in a virtual environment.

Update Path

The following update paths are supported for Security Analytics 10.6.6.0.

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

- 10.6.5.1 to 10.6.6.0
- 10.6.5.2 to 10.6.6.0

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

Terminology Changes in 10.6.0.0

The following table lists the changes in Security Analytics terminology introduced in 10.6.0.0. It lists each new term, the term it replaced from prior versions, and a description of each term.

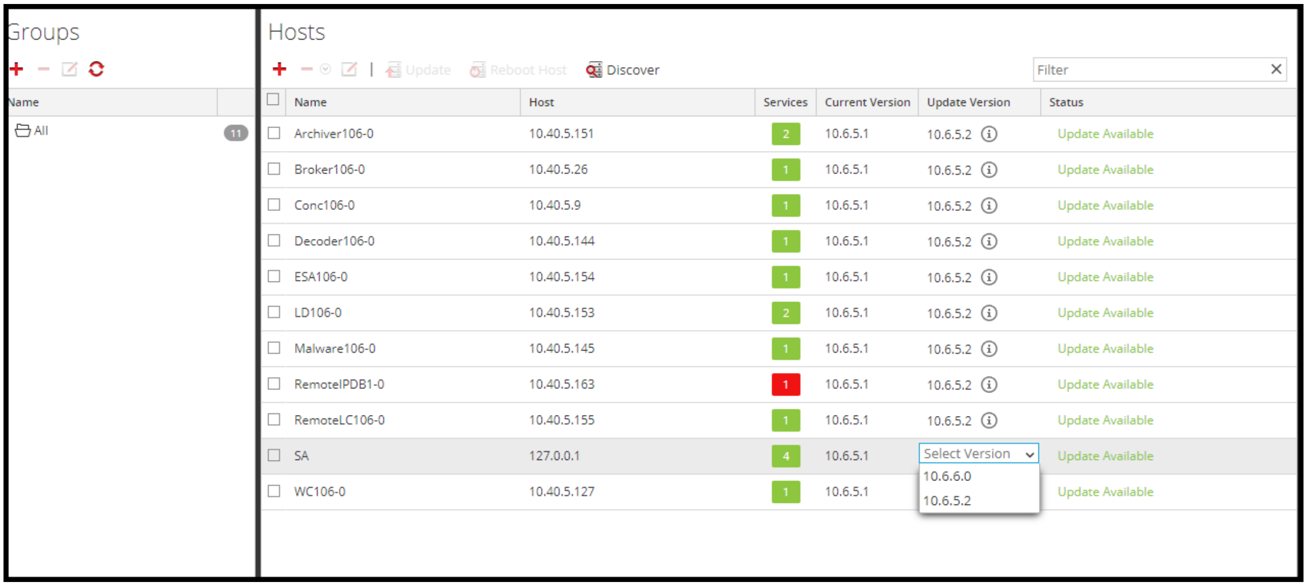
10.6.0.0	Prior to 10.6.0.0	Description
Live Update Repository	yum repository, yum repo, SMCUPDATE	Live repository to which RSA posts Security Analytics software version updates on a regular basis.
Local Update Repository	SA server repo, SA yum repo	Local repository in your Security Analytics deployment from which you apply software version updates to a host. You have two options to populate the Local Update Repository in your Security Analytics deployment: • Option 1 - Connect to the Live Update Repository. • Option 2 - Download version updates from RSA Link and upload them to your Local Update Repository.

Enhancements to the Host Update Process

Changes to the Hosts View

You use the Hosts view to update a host to a new version. In 10.6.0.0, this view has had several changes. When there are version updates available for a host, Update Available is displayed in the **Status** column and you choose the available update version you want from the **Select Version** column. The **Status** column tells you the current status of update process as it progresses and prompts you for actions if required. See ***Updating a Host Version*** under ***The Basics*** in the ***Hosts and Services Getting Started Guide*** in the Security Analytics help (https://community.rsa.com/) for more information on the Host view and the enhanced update process.

> **Note:** The **Total Memory**, **CPU**, **OS**, and **Uptime** statistics are no longer displayed in the Hosts view. You can monitor this information in **Administration** > **Health & Wellness** > **Monitoring**.

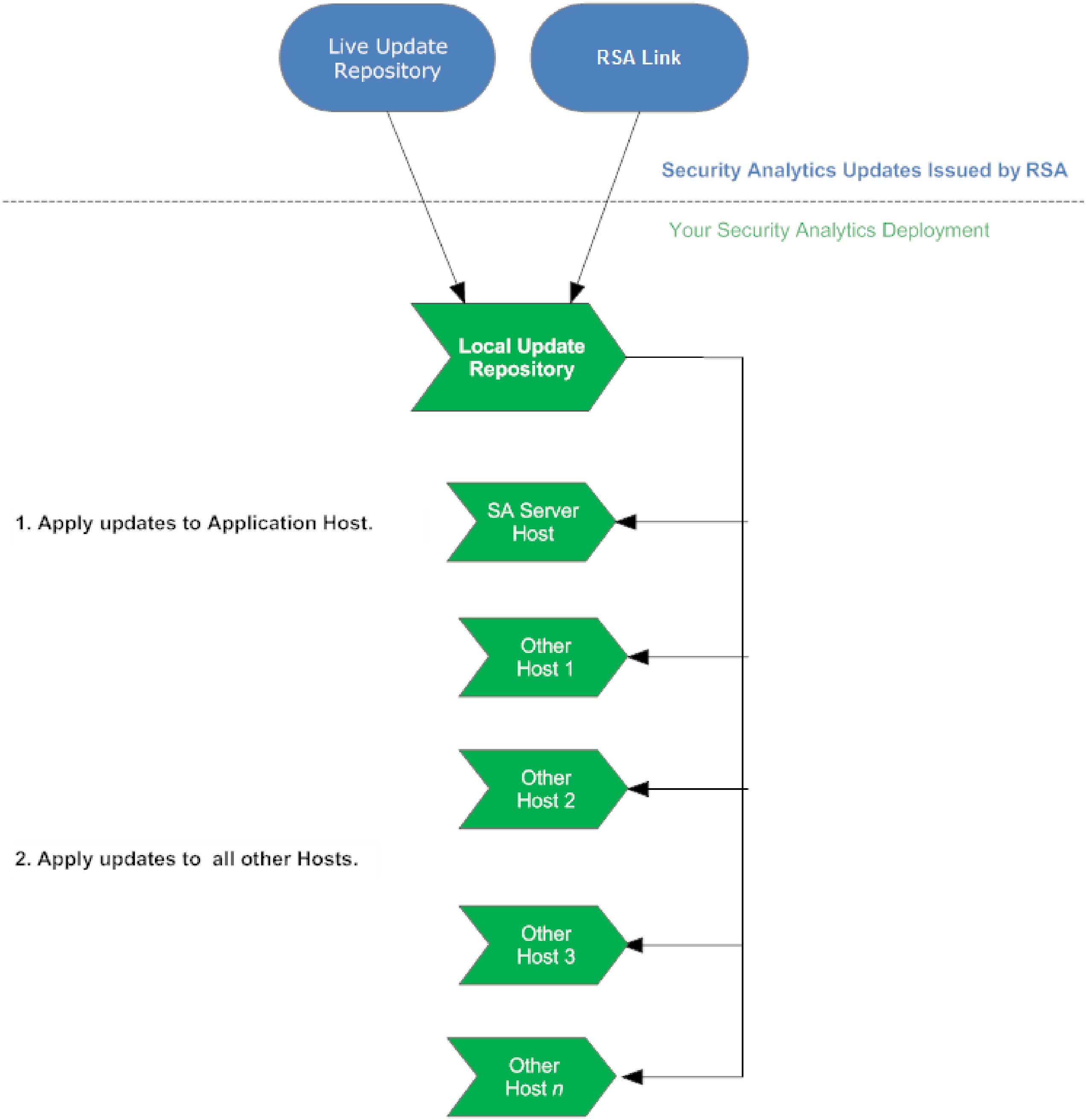


□	Name	Host	Services	Current Version	Update Version	Status
□	Archiver106-0	10.40.5.151	2	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	Broker106-0	10.40.5.26	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	Conc106-0	10.40.5.9	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	Decoder106-0	10.40.5.144	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	ESA106-0	10.40.5.154	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	LD106-0	10.40.5.153	2	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	Malware106-0	10.40.5.145	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	RemoteIPDB1-0	10.40.5.163	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	RemoteLC106-0	10.40.5.155	1	10.6.5.1	10.6.5.2 ⓘ	Update Available
□	SA	127.0.0.1	4	10.6.5.1	Select Version 10.6.6.0 10.6.5.2	Update Available
□	WC106-0	10.40.5.127	1	10.6.5.1		Update Available

Security Analytics Update Process

The following figure illustrates how you populate the Local Update Repository with the latest Security Analytics version updates and apply these updates to hosts.

Security Analytics Software Update Process


Live Update Repository
RSA Link
Security Analytics Updates Issued by RSA
Your Security Analytics Deployment
Local Update Repository
1. Apply updates to Application Host.
SA Server Host
Other Host 1
Other Host 2
2. Apply updates to all other Hosts.
Other Host 3
Other Host *n*

Note: There are no separate quarterly security patch releases. The quarterly security fixes are now part of the Security Analytics releases.

Update Preparation Tasks

Complete the following tasks to prepare for the update to Security Analytics 10.6.6.0.

Task 1. Review Core Ports and Open Firewall Ports

Review the changes to Core ports in the 'Network Architecture and Ports' topic in the *Deployment Guide* in the Security Analytics help (https://community.rsa.com/) so that you can reconfigure Security Analytics services and your firewall. The Event Stream Analysis (ESA) Context Hub Service Port must be available for 10.6.6.0. 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. Refer to 'Mount the IPDB' in the *IPDB Extractor Service Configuration Guide* in the Security Analytics help (https://community.rsa.com/) for detailed instructions on how to configure IPDB mount points.

Task 3. Fix Your Rules

All queries and rule conditions such as those used in Application and Correlation Rules on Decoders and Reporting Engine rules applied against 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=‘2015-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 the topic 'Rule and Query Guidelines' in the *Decoder and Log Decoder Configuration Guide* on RSA Link in the Security Analytics help (https://community.rsa.com/).

Task 4. Designate Primary and Secondary Security Analytics Servers

If you have a Multiple Security Analytics server deployment, you must designate a Primary Security Analytics Server and Secondary Security Analytics Servers and check the **RSASoftware.repo** file. Refer to 'Multiple Security Analytics Server Deployment' in the *Security Analytics Deployment Guide* in the help (https://community.rsa.com/) for more information on this type of deployment.

If you deploy multiple Security Analytics Servers:

1. Before you update the Security Analytics Server Host to 10.6.6.0, designate a primary Security Analytics Server and Secondary Security Analytics Servers. Refer to the 'Update Hosts in Correct Sequence' topic in the *Hosts and Services Getting Started Guide* in the Security Analytics help (https://community.rsa.com/) for a description of this deployment.

2. Before you update the rest of the hosts to 10.6.6.0, check the **RSASoftware.repo** file and make sure **baseurl** is pointing to the Primary Security Analytics Server Host with the following command string.

   ```
   #grep baseurl /etc/yum.repos.d/RSASoftware.repo
   ```

   The following output is displayed.

   ```
   baseurl=http://<puppetmaster.local|IP_Primary_SA_Server>/rsa/updates
   ```

Caution: A Secondary Security Analytics Server has the following limitations: The version update functionality on the Hosts view is valid for the Primary Security Analytics Server exclusively. It reflects the wrong status for Secondary Security Analytics Servers so you must not update to new Security Analytics versions from the Hosts view of a SecondarySecurity Analytics Server.
You cannot use the Health and Wellness views.
You cannot use the trusted connections feature.

Task 5. Backup Your Configuration

RSA recommends that you make a backup copy of your configuration before you perform the update.

Refer to the 'Back Up and Restore Data for Hosts and Services' topic in the *System Maintenance Guide* in the Security Analytics help (https://community.rsa.com/) for guidelines on how to back up your configuration.

Note: If you use the 10G Decoder hardware driver and you customized the `/etc/init.d/pf_ring` script to use MTU from the `/etc/pf_ring/mtu.conf` file, the files `/etc/init.d/pf_ring` and `/etc/pf_ring/mtu.conf` are automatically backed up during the update process. However, you must manually restore them after the update. The backed-up files will be located in the `../etc/init/pfring_bkup` directory.

Backup Malware Analysis Configuration File to Another Directory

1. Make a backup of the following file:
   `/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 10.6.6.0. The update creates a new configuration file with all the parameters set to the default values.

2. Delete the following file:
   `/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 just prior to updating Security Analytics service hosts to 10.6.6.0.

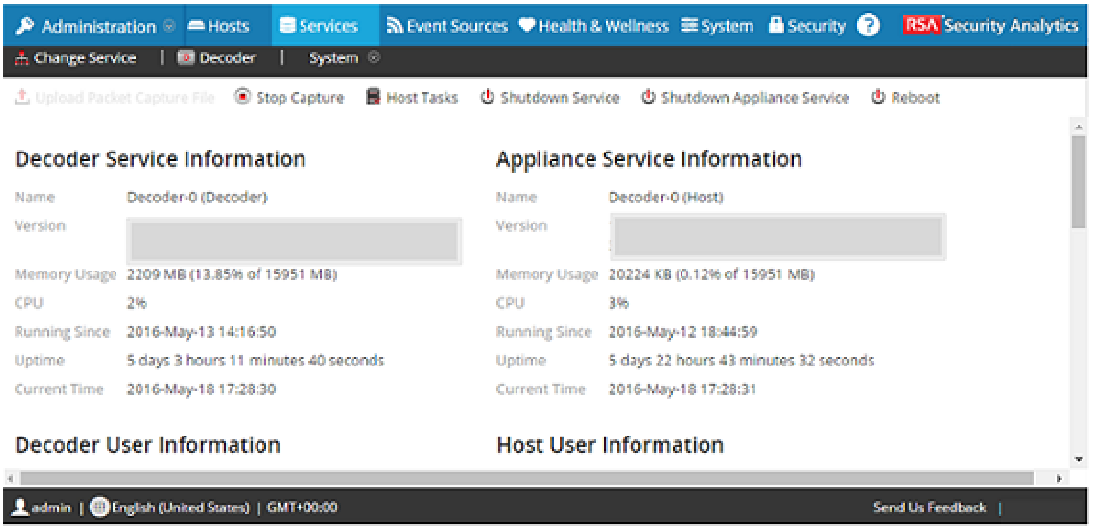
Packet Decoders - Stop Packet Capture

To stop packet capture:

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

2. Select each **Decoder** service.

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



Decoder Service Information

Name	Decoder-0 (Decoder)
Version	[redacted]
Memory Usage	2209 MB (13.85% of 15951 MB)
CPU	2%
Running Since	2016-May-13 14:16:50
Uptime	5 days 3 hours 11 minutes 40 seconds
Current Time	2016-May-18 17:28:30

Appliance Service Information

Name	Decoder-0 (Host)
Version	[redacted]
Memory Usage	20224 KB (0.12% of 15951 MB)
CPU	3%
Running Since	2016-May-12 18:44:59
Uptime	5 days 22 hours 43 minutes 32 seconds
Current Time	2016-May-18 17:28:31

Decoder User Information

Host User Information

4. In the toolbar, click ● Stop Capture .

Log Decoders - Stop Log Capture

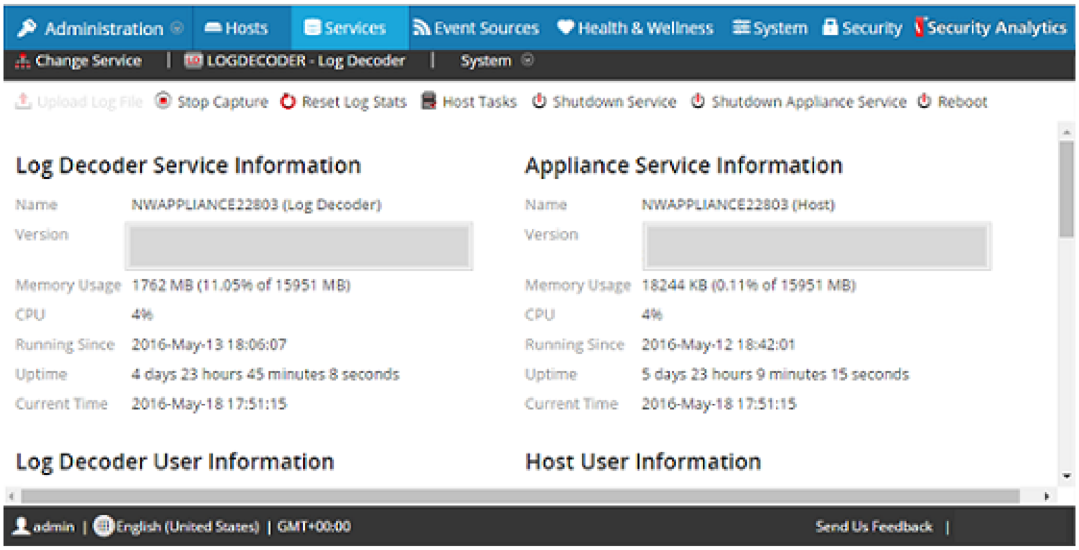
To stop log capture:

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**.



Log Decoder Service Information

Name	NWAPPLIANCE22803 (Log Decoder)
Version	
Memory Usage	1762 MB (11.05% of 15951 MB)
CPU	4%
Running Since	2016-May-13 18:06:07
Uptime	4 days 23 hours 45 minutes 8 seconds
Current Time	2016-May-18 17:51:15

Appliance Service Information

Name	NWAPPLIANCE22803 (Host)
Version	
Memory Usage	18244 KB (0.11% of 15951 MB)
CPU	4%
Running Since	2016-May-12 18:42:01
Uptime	5 days 23 hours 9 minutes 15 seconds
Current Time	2016-May-18 17:51:15

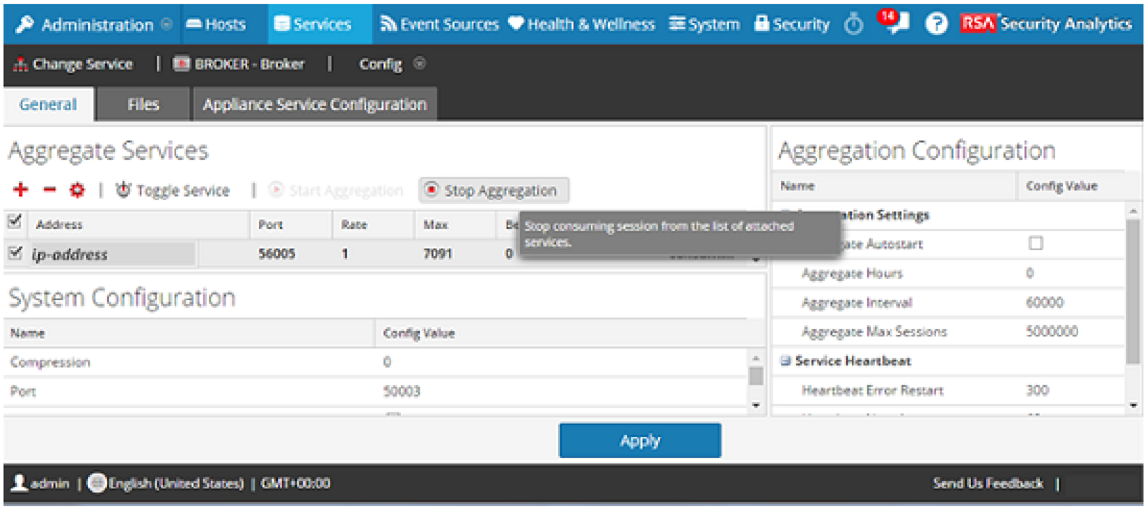
Log Decoder User Information

Host User Information

4. In the toolbar, click Stop Capture.

Archivers, Concentrators and Brokers - Stop Aggregation

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select an **Archiver**, **Broker** or a **Concentrator** service.
3. Under ⚙ (actions), select **View** > **Config**.
4. The **General** tab is displayed.



Aggregate Services

Stop consuming session from the list of attached services.

☑	Address	Port	Rate	Max	Be
☑	ip-address	56005	1	7091	0

System Configuration

Name	Config Value
Compression	0
Port	50003

Aggregation Configuration

Name	Config Value
ation Settings	
ate Autostart	□
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	5000000
⊟ Service Heartbeat	
Heartbeat Error Restart	300

5. Under **Aggregated Services** click Stop Aggregation.

Task 7. Prepare ESA, MA, and SA Appliances

Run the following command on Event Stream Analysis (ESA), Malware Analysis (MA), and Security Analytics (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 Reporting Engine data sources, see the *Reporting Engine Configuration Guide* (https://community.rsa.com/).

At this point, you can proceed to the update instructions.

Update Tasks for 10.5.5.0 to 10.6.6.0

You must perform the following tasks to update from 10.5.5.0 to 10.6.6.0.

- Task 1. Populate Local Update Repository
- Task 2. Update Security Analytics Servers from 10.5.5.0 to 10.6.6.0

Task 1. Populate Local Update Repository

You have two options to populate the Local Update Repository:

- Option 1 - Connect to the Live Update Repository.
  This connects your Security Analytics Local Update Repository to the RSA Live Update Repository through the Internet using your LIVE account.
- Option 2 - Download version updates from RSA Link (https://community.rsa.com/).
  If you do not allow your Security Analytics deployment to connect to the Internet, you must download the update packages from RSA Link to a local directory and then upload them to your Security Analytics Local Update Repository.

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`.

Option 1 - Connect to Live Update Repository

Access to the Live Update Repository requires and uses the Live Account credentials configured under **Administration** > **System** > **Live**.

Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 6 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your Security Analytics Server's Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository.

To connect to the Live Update Repository:

> **Note:** If you need to use a proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. Refer to 'Configure Proxy for Security Analytics' in the *Security Analytics System Configuration Guide* in the help on RSA Link (https://community.rsa.com/).

1. Navigate to the **Administration** > **System** view, select **Live Services** in the options panel and ensure that credentials are configured. If they are not configured, do so now, click **Test Connection**, and click **Apply**.
   Make sure that Test Connection is successful because this account is used to access the Live Update Repository.

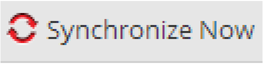
2. Select the **Updates** > **Settings** tab.

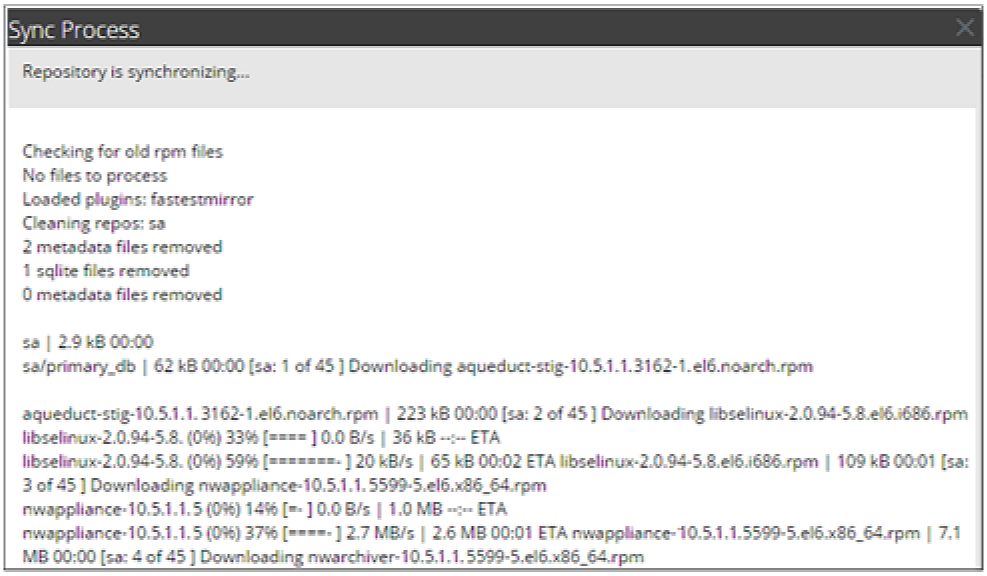
3. Select the **Enable** check box and click **Apply**.

4. Use the **Test Connection** button to check for connectivity. Make sure that this is successful.
   An **RSASoftware.repo** file is automatically created in the Security Analytics Server Host **/etc/yum.repos.d/** directory, which is used by your Local Update Repository to communicate with the Live Update Repository.
   After it is enabled, the Local Update Repository will synchronize and download all available packages from the Live Update Repository on the next scheduled event. You can also force a synchronize job from the **Updates Repository** tab using the **Synchronize Now** option.
   After you update both of the Update Repositories (Live and Local), you can see all downloaded RPM packages in the **Updates Repository** tab of the **Administration** > **Updates** panel.

5. In the Security Analytics menu, select **Administration** > **System**.
   The Info view is displayed.

6. In the left panel, select **Updates**.

7. In the **Updates Repository** tab, click . A message similar to the following is displayed.



Repository is synchronizing...

```
Checking for old rpm files
No files to process
Loaded plugins: fastestmirror
Cleaning repos: sa
2 metadata files removed
1 sqlite files removed
0 metadata files removed

sa | 2.9 kB 00:00
sa/primary_db | 62 kB 00:00 [sa: 1 of 45 ] Downloading aqueduct-stig-10.5.1.1.3162-1.el6.noarch.rpm

aqueduct-stig-10.5.1.1. 3162-1.el6.noarch.rpm | 223 kB 00:00 [sa: 2 of 45 ] Downloading libselinux-2.0.94-5.8.el6.i686.rpm
libselinux-2.0.94-5.8. (0%) 33% [==== ] 0.0 B/s | 36 kB --:-- ETA
libselinux-2.0.94-5.8. (0%) 59% [=======- ] 20 kB/s | 65 kB 00:02 ETA libselinux-2.0.94-5.8.el6.i686.rpm | 109 kB 00:01 [sa:
3 of 45 ] Downloading nwappliance-10.5.1.1.5599-5.el6.x86_64.rpm
nwappliance-10.5.1.1.5 (0%) 14% [=- ] 0.0 B/s | 1.0 MB --:-- ETA
nwappliance-10.5.1.1.5 (0%) 37% [====- ] 2.7 MB/s | 2.6 MB 00:01 ETA nwappliance-10.5.1.1.5599-5.el6.x86_64.rpm | 7.1
MB 00:00 [sa: 4 of 45 ] Downloading nwarchiver-10.5.1.1.5599-5.el6.x86_64.rpm
```

The **Updates Repository** tab is displayed with the updates you retrieved by synchronizing.

Option 2 - Download Version Updates from RSA Link

You would need to populate Security Analytics update repository from RSA Link (https://community.rsa.com/) for the following reasons:

- If the version updates that you want are not in your Local Update Repository (that is, they are not listed in the **Updates Available** list for a host in the **Updates** column in the Hosts view).
- If your Security Analytics deployment does not have Internet access.

Warning: After you update a host to 10.6.6.0 from the Local Update Repository, you may not be able to access earlier versions to update other hosts. This is determined by the amount of available space in your Local Update Repository and the size of the update packages. For example, if you updated the Security Analytics Server Host to 10.5.5.0 and then to 10.6.6.0, 10.5.5.0 may have been removed and will not be available to update other hosts. If you needed to update another system to 10.5.5.0 (before updating to 10.6.6.0), you would need to download 10.5.5.0 or later from RSA Link and manually update the Local Update Repository again.

To populate your Local Update Repository from RSA Link:

1. Download the files below, which contain all the Security Analytics 10.6.6.0 Update files, from RSA Link (https://community.rsa.com/) to a local directory:

   sa-10.6.6.0-upgradepack-1-of-8-el6.zip

   sa-10.6.6.0-upgradepack-2-of-8-el6.zip

   sa-10.6.6.0-upgradepack-3-of-8-el6.zip

   sa-10.6.6.0-upgradepack-4-of-8-el6.zip

   sa-10.6.6.0-upgradepack-5-of-8-el6.zip

   sa-10.6.6.0-upgradepack-6-of-8-el6.zip

sa-10.6.6.0-upgradepack-7-of-8-el6.zip
sa-10.6.6.0-upgradepack-8-of-8-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 **Enable** 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-10.6.6.0-upgradepack-1-of-8-el6.zip
   sa-10.6.6.0-upgradepack-2-of-8-el6.zip
   sa-10.6.6.0-upgradepack-3-of-8-el6.zip
   sa-10.6.6.0-upgradepack-4-of-8-el6.zip
   sa-10.6.6.0-upgradepack-5-of-8-el6.zip
   sa-10.6.6.0-upgradepack-6-of-8-el6.zip
   sa-10.6.6.0-upgradepack-7-of-8-el6.zip
   sa-10.6.6.0-upgradepack-8-of-8-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 files in the Manual Updates list and click **Apply**.
   This moves the RPM files into the Local Update Repository on the Security Analytics Server and makes them available to hosts.

8. If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening RPM in Security Analytics, you must perform the following tasks on all components, including the Security Analytics server, to migrate it to 10.6.6.0.

   Note: These steps apply only to STIG. Do not perform these steps for any non-STIG system, including FIPS.

   a. `SSH` to the host.

   b. `yum update glibc`

   c. `reboot`

Task 2. Update Security Analytics Servers from 10.5.5.0 to 10.6.6.0

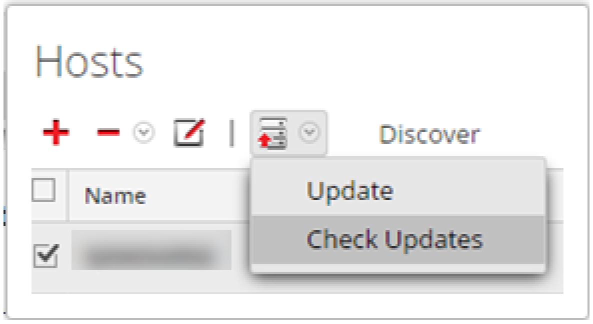
For more information about this task, see the topic 'Apply Software Version Updates from Hosts View' in the *Security Analytics System Maintenance Guide* in the help (https://community.rsa.com/)

> **Note:** When you update the Security Analytics 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 `/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 Host Deployments only)**, **SSH** to each Secondary Security Analytics Server Host and make sure that Puppet Master is enabled using the following commands:

   ```
   service puppetmaster start
   service puppet start
   ```

2. Log into Security Analytics.
3. In the Security Analytics menu, select **Administration** > **Hosts**.
4. Select the Security Analytics Server Host and click **Update** > **Check Updates**.

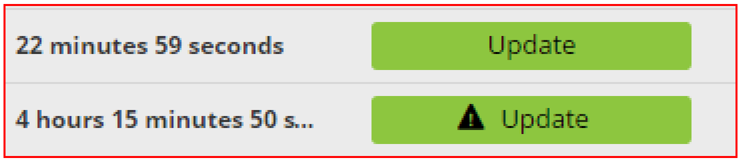
   Checking is displayed in the **Updates** column as Security Analytics retrieves the latest updates for 10.6.6.0.

   After it finishes retrieving all the 10.6.6.0 updates, it displays Update in the Updates column.

   Update displays in two ways:

   Without a caution triangle - indicates that the update includes package updates exclusively.

With a caution triangle - indicates that the update includes package updates plus additional updates such as a kernel. For example:



22 minutes 59 seconds

4 hours 15 minutes 50 s...

Note: If the pre-update host configuration has any configuration issues that would prevent a successful update to 10.6.6.0, Security Analytics displays ⚠ Conflicts (2). See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for instructions on how to resolve pre-update errors.

5. Click **Update**.

   The **Updates** dialog is displayed.

   You can click on a hostname to display the 10.6.6.0 packages to be applied to that host.

   Note: If you receive the following message in the Update dialog after you click **Update**, the kernel on the host is older than the kernel supported by 10.6.6.0. This is not a blocking error. You can continue with the update if you want to update the kernel on the host with the version supported by 10.6.6.0.

   ```
   Kernel version on the host is older than the version n.n.nn-
   nnn.nn.n supported by Security Analytics. If you click Begin
   Update, the kernel version n.n.nn-nnn.nn.n will be installed on
   the host.
   ```

6. Click ⊙ Begin Update.

   Initiating is displayed in the **Updates** column as Security Analytics starts to apply the latest updates for 10.6.6.0.

   After all the 10.6.6.0 packages are installed for the Security Analytics Server Host, ↻ Reboot Required is displayed in the **Updates** column.

7. Click ↻ Reboot Required.

   Note: Ensure that the Security Analytics UI is up to date. Also ensure that there are no RPMs left for the upgrade in the back end by running `yum update`.

   After the reboot, the Security Analytics Server Host is updated to 10.6.6.0 so the 10.5.5.0 Host view is no longer available and the message

   ```
   This webpage is not available
   ```

   is displayed.

> **Note:** If you have DISA STIG enabled, opening Core Services can take up to an additional 15 minutes. This delay is caused by the generation of new certificates.

Task 3: Update the Security Analytics Service Hosts to 10.6.6.0

1. Log in to Security Analytics.
2. In the Security Analytics menu, select **Administration** > **Hosts**.
3. Update hosts in the sequence recommended in the 'Update Hosts in Correct Sequence' topic in the *Hosts and Services Getting Started Guide* in the Security Analytics help (https://community.rsa.com/). Select **10.6.6.0** as the version you want to apply from the **Update Version** column. If you want to update more than one host to that version, select the checkbox to the left of the hosts.
   Update Available is displayed in the Status column if you have a version update in your Local Update Repository for the selected hosts.
   If you:
   - Cannot find the version you want, see Task 1. Populate Local Update Repository.
   - Do not have enough disk space in your Local Update Repository to download a version update, the Repository Space Management dialog is displayed with the contents and disk space status of the repository. You can delete versions that you do not need to free enough disk space to download the version you want. See the topic 'Free Local Update Repository Disk Space' in the *Host and Services Getting Started Guide* in the help (https://community.rsa.com/) for instructions.
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 conflict.
       See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to address these configuration warnings and conflicts.
   - Initiating the update if there are no conflicts.

- Updating update packages.

  Displays Error in Update. View details if there is an error applying a package that blocks the update. See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to resolve these errors.

  After the host is updated, Security Analytics prompts you to **Reboot Host**.

5. Click **Reboot Host** from the toolbar.

   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**. If the host does not come back online, contact Customer Support (go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

Note: If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generation of new certificates.

Update Tasks for 10.6.x.x to 10.6.6.0

This topic contains the tasks you must complete for updating from 10.6.x.x to 10.6.6.0.

> **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

You have two options to populate the Local Update Repository:

- Option 1 - Connect to the Live Update Repository.
  This connects your Security Analytics Local Update Repository to the RSA Live Update Repository through the Internet using your LIVE account.
- Option 2 - Download version updates from RSA Link (https://community.rsa.com/).
  If you do not allow your Security Analytics deployment to connect to the Internet, you must download the update packages from RSA Link to a local directory and then upload them to your Security Analytics Local Update Repository.

Option 1 - Connect to Live Update Repository

Access to the Live Update Repository requires and uses the Live Account credentials configured under **Administration** > **System** > **Live Services**.

> **Note:** If this is the first time that you using the Live Update Repository to upgrade Security Analytics systems, you must run the following command on the Security Analytics server to create a **.pem** file:
>
> ```
> # touch /etc/pki/CA/certs/RSACorpCAv2.pem
> ```
>
> You do not need to run this command if you have previously used Live Update to upgrade the system to 10.6.x.x, or if you are using Option 2 - Download Version Updates from RSA Link.

> **Note:** When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 6 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your Security Analytics Server's Internet connection and the traffic of the RSA Repository. It is NOT mandatory to use the Live Update Repository.

To connect to the Live Update Repository:

> **Note:** If you need to use a proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. Refer to 'Configure Proxy for Security Analytics' in the *Security Analytics System Configuration Guide* in the help on RSA Link (https://community.rsa.com/).

1. Navigate to the **Administration** > **System** view, select **Live Services** in the options panel and ensure that credentials are configured. If they are not configured, do so now, click **Test Connection**, and click **Apply**.
   Make sure that Test Connection is successful because this account is used to access the Live Update Repository.
2. Select the **Updates** > **Settings** tab.
3. Select the **Connect to Live Update Repository** check box and click **Apply**.
4. In the Security Analytics menu, select **Administration** > **System**.
5. In the left panel, click **Updates** and select the **Settings** tab.
6. Click **Check Updates**. The following message is displayed:
   ```
   New updates found that may apply to hosts. Navigate to host page to apply.
   ```
   In **Administration** > **Hosts**, the update versions are available in the **Update Version** column.

Option 2 - Download Version Updates from RSA Link

You would need to populate Security Analytics update repository from RSA Link (https://community.rsa.com/) for the following reasons:

- If the version updates that you want are not in your Local Update Repository (that is, they are not listed in the **Updates Available** list for a host in the **Updates** column in the Hosts view).
- If your Security Analytics deployment does not have Internet access.

To populate your Local Update Repository from RSA Link:

1. Download the files below, which contain all the Security Analytics 10.6.6.0 update files, from RSA Link (https://community.rsa.com/) to a local directory:
   sa-10.6.6.0-upgradepack-1-of-8-el6.zip
   sa-10.6.6.0-upgradepack-2-of-8-el6.zip
   sa-10.6.6.0-upgradepack-3-of-8-el6.zip
   sa-10.6.6.0-upgradepack-4-of-8-el6.zip
   sa-10.6.6.0-upgradepack-5-of-8-el6.zip

sa-10.6.6.0-upgradepack-6-of-8-el6.zip
sa-10.6.6.0-upgradepack-7-of-8-el6.zip
sa-10.6.6.0-upgradepack-8-of-8-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. Also make sure that the Live service is not configured in **Administration** > **System** > **Live Services** prior to the update, as it deletes the repository when the Security Analytics server is rebooted.
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-10.6.6.0-upgradepack-1-of-8-el6.zip
   sa-10.6.6.0-upgradepack-2-of-8-el6.zip
   sa-10.6.6.0-upgradepack-3-of-8-el6.zip
   sa-10.6.6.0-upgradepack-4-of-8-el6.zip
   sa-10.6.6.0-upgradepack-5-of-8-el6.zip
   sa-10.6.6.0-upgradepack-6-of-8-el6.zip
   sa-10.6.6.0-upgradepack-7-of-8-el6.zip
   sa-10.6.6.0-upgradepack-8-of-8-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.
8. If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (**STIG**) hardening RPM in Security Analytics, you must perform the following tasks on all components, including the Security Analytics Server, to migrate it to 10.6.6.0.

   > **Note:** These steps apply only to **STIG**. Do not perform these steps for any non-STIG system, including FIPS.

a. `SSH` to the host.

b. Edit the **/etc/yum.repos.d/RSASoftware.repo** file to version:

```
FROM: baseurl=http://puppetmaster.local/rsa/updates/$sarelease/
```

to

```
TO: baseurl=http://puppetmaster.local/rsa/updates/10.6.6/
```

c. `yum update glibc`

d. `reboot`

Task 2. Update Security Analytics Servers to 10.6.6.0

Note: When you update the SA (Security Analytics) 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 Security Analytics Server Host and make sure Puppet Master 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 10.6.6.0 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. The following message is displayed:

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

6. Click **Begin Update**. 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.
    See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to address these configuration warnings and conflicts.
- 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. See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to resolve these errors.
  After the host is updated, Security Analytics prompts you to **Reboot Host**.

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

Task 3: Update the Security Analytics Service Hosts to 10.6.6.0

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 10.6.6.0 update path (that is, earlier than 10.5.5.0) and you updated your Security Analytics Server Host to 10.6.6.0, 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. To update the non-Security Analytics Server host on the unsupported path, contact Customer Support (go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

3. Update hosts in the sequence recommended in the 'Update Hosts in Correct Sequence' topic in the *Hosts and Services Getting Started Guide* in the Security Analytics help (https://community.rsa.com/). Select the device you want to update, and in the **Update Version** column, select **10.6.6.0**.
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.
    See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to address these configuration warnings and conflicts.
- 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. See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to resolve these errors.
  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**. If the host does not come back online, contact Customer Support (go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

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

Refer to the ***RSA Security Analytics Legacy Windows Collection Update & Installation Instructions*** on RSA Link (https://community.rsa.com/) for details about how to install or update Legacy Windows collection.

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

Post Update Tasks

This topic contains the tasks you must complete after you update to 10.6.6.0.

Task 1 - Update ssl.cipher.list Configurations and Restart Services

This step applies a fix that disables support for DES and 3DES ciphers, which resolves SWEET32 vulnerability. Update the **ssl.cipher.list** configuration setting in Explore mode of service in **sys** > **config** for each of thefollowing services and their respective ports:

Host Type	Ports
Decoder	56004 56006 50104
Log Decoder	56002 56006 50102
Concentrator	56005 56006 50105
Log Collector / Remote Log Collector	56001 56006 21
Broker	56003 56006 50103
Archiver	56008 56006 50108
Workbench	56007 50107
Warehouse Connector	56020 56006

Host Type	Ports
IPDB	56025 56006

To update the **ssl.cipher.list** file:

1. Log into the Security Analytics user interface.
2. Go to **Administration** > **Services** and select a service.
3. Click ⚙ and go to **View** > **Explore**.
4. In the left pane, expand the list for the service and go to **sys** > **config**.
   The configuration file is displayed in the right pane.
5. Go to **ssl.cipher.list** and append the following value:
   `:!DES:!3DES`
   For example, `-ALL:!aNULL:HIGH:`**`!DES:!3DES`**
6. In left pane, expand the list for **deviceappliance** and go to **sys** > **config**
7. Go to **ssl.cipher.list** and append the following value:
   `:!DES:!3DES`
   For example, `-ALL:!aNULL:HIGH:`**`!DES:!3DES`**
8. Save the configuration.
9. Stop capture or aggregation and restart the service running on the corresponding ports (see the table above) . For example, you would need to restart the **nwappliance** service for port 56006, and to restart the **nwdecoder** service for port 56004.
   a. Log into the SSH console of the appliance.
   b. Restart the service.
      For example,
      run `restart nwappliance`
      run `restart nwdecoder`

To disable static ciphers for port 21:

1. Run the following command `vi/etc/vsftpd/vsftpd.conf` on SSH.
2. Find **ssl_ciphers** and replace with **ssl_ciphers=HIGH:-3DES:-aNULL:-kRSA**

Note: The above steps are not mandatory to be executed as this may break comunication with external devices.

Task 2 – Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 10.6.6.0.

Packet Decoders - Start Packet Capture

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 ● Start Capture.

Log Decoders - Start Log Capture

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 ● Start Capture.

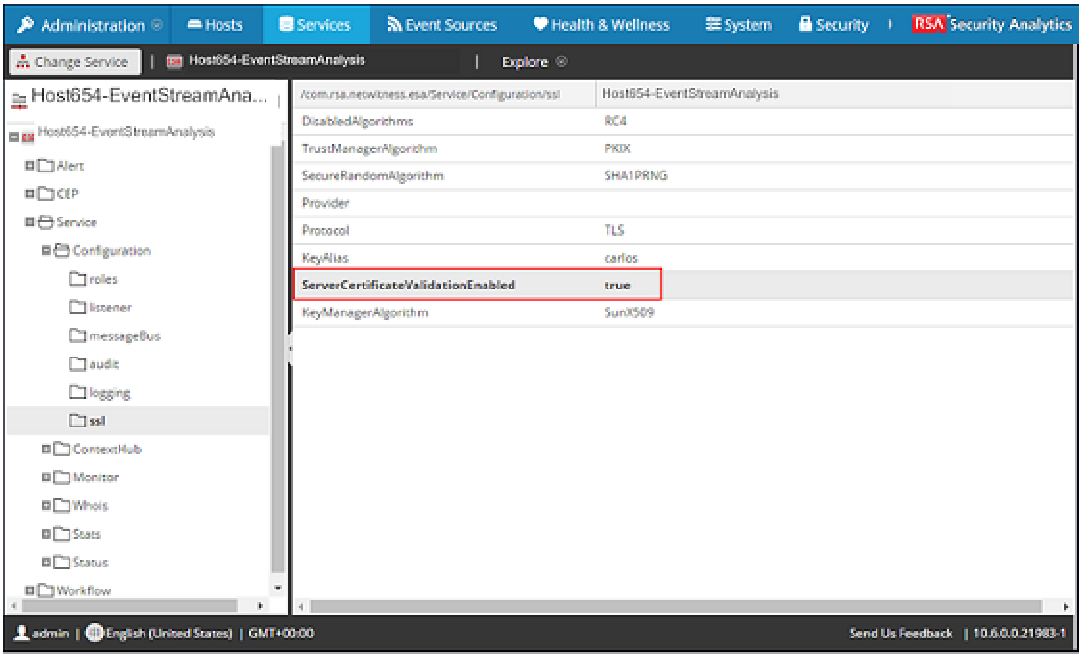
Archivers, Concentrators and Brokers - Start Aggregation

During the update to 10.6.6.0, if services are configured to automatically restart, the services are restarted and this automatically starts aggregation. However, if services are not configured to start automatically, they must be restarted manually (select a service, go to **View** > **Config**, on the General tab, click **Start Aggregation**).

For Updating from 10.5.5.0 only: Task 3: Ensure Truststore has Certificates for TCP Mode Syslog Notification

If you set TCP mode for Syslog notification and the `ServerCertificateValidateEnable` parameter was set to `false` prior to updating to 10.6.6.0:

1. Set the Event Stream Analysis `ServerCertificateValidateEnable` parameter to `true`.



/com.rsa.netwitness.esa/Service/Configuration/ssl	Host654-EventStreamAnalysis
DisabledAlgorithms	RC4
TrustManagerAlgorithm	PKIX
SecureRandomAlgorithm	SHA1PRNG
Provider	
Protocol	TLS
KeyAlias	carlos
ServerCertificateValidationEnabled	**true**
KeyManagerAlgorithm	SunX509

2. Add the Syslog Client certificates to the Event Stream Analysis Java keystore.

For Updating from 10.5.5.0 only: Task 4. Enable Context Hub Service

When you updated the Event Stream Analysis (ESA) host to 10.6.6.0, the Context Hub was installed on the ESA host, but it was disabled by default. Context Hub is an optional service, so only enable it if you want to use this service. See 'Context Hub Service Overview' in the *Security Analytics Hosts and Services Configuration Guide* in the help (https://community.rsa.com/) for more information about this service.

> **Note:** You can only have one Context Hub service instance in your Security Analytics deployment.

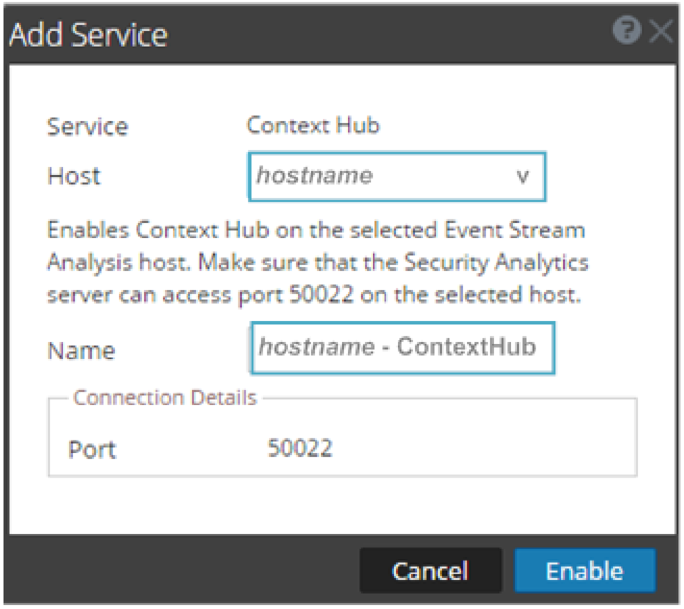
To enable the Context Hub service:

1. Log into Security Analytics.
2. Click **Administration** > **Services**.
3. Click + and select **Context Hub**.

   The Add Service dialog is displayed.
4. Select the ESA host for the **Host** and click **Enable**.

   Security Analytics fills the service **Name** with the ESA ***hostname*** **- Context Hub** by default.

You can change the service name if you want.



Add Service

Service Context Hub

Host *hostname*

Enables Context Hub on the selected Event Stream Analysis host. Make sure that the Security Analytics server can access port 50022 on the selected host.

Name *hostname* - ContextHub

Connection Details

Port 50022

Note: Ensure that the ESA host running the Context Hub service can access port 50022.

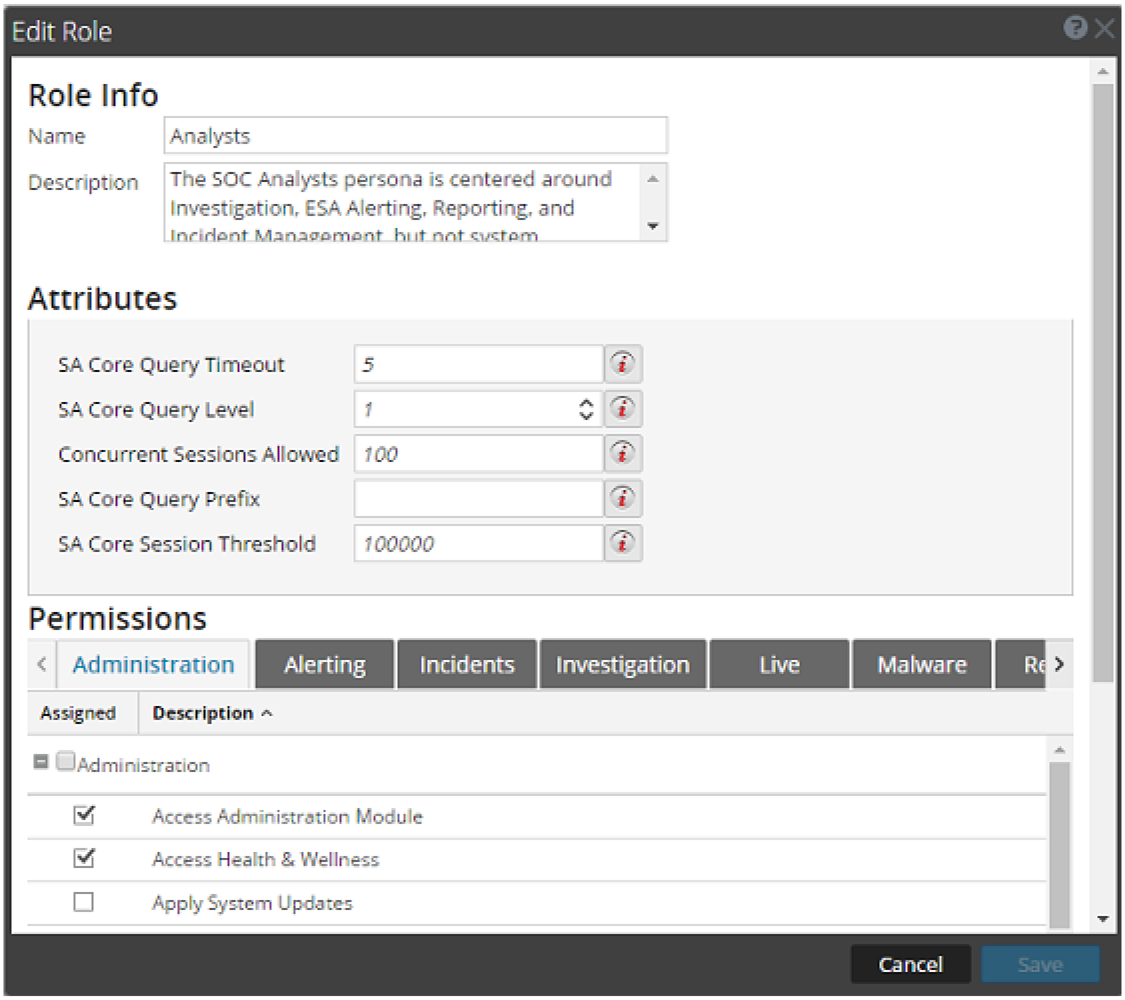
Task 5. Set Permissions for Context Hub Service

You must set the **Investigation-Context Lookup** and **Investigation-Manage List from Investigation** permissions for the appropriate roles after you update to 10.6.6.0.

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

1. Log into 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**.



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
Concurrent Sessions Allowed	100
SA Core Query Prefix	
SA Core Session Threshold	100000

Permissions

Assigned	Description ^
⊟ □	Administration
☑	Access Administration Module
☑	Access Health & Wellness
□	Apply System Updates

5. Click **Save**.

Task 6. Restore Malware Analysis Custom Parameters Values to Newly Created Configuration File

Replace the defaults in the new `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` configuration file with custom parameter values from the `malwareCEFDictionaryConfiguration.xml` that was backed up before updating to 10.6.6.0.

1. Do a diff between `/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 the `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` file with the custom values from the backup to retain defaults for new parameters added in 10.6.6.0.

(Optional) Task 7. Restore /etc/init.d/pf_ring and /etc/pf_ring/mtu.conf files

If you use the 10G Decoder hardware driver and 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
```

The files are located in the `../etc/init/pfring_bkup` directory.

Task 8. Migrate DISA STIG to 10.6.6.0

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 10.6.6.0.

> **Note:** These steps apply only to **STIG**. Do not perform these steps for any non-STIG system, including FIPS.

For all hosts with **STIG** applied:

1. `SSH` to the host.
2. Enter the following command strings.

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

Task 9. Reset Stable System Value of Warehouse Connector Lockbox

You must reset the **Stable System Value** of the Warehouse Connector Lockbox because of kernel updates.

Task 10. 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 11. Check Health and Wellness Policies for Changes from Update

If you have previously created a custom Health and Wellness policy by copying a default monitoring policy or have previously disabled the default monitoring policy, check your Health and Wellness policies for any changes that the upgrade may have made. For information about how to check your Health and Wellness policies, see the topic 'Monitor Health and Wellness of Security Analytics' in the *Security Analytics System Maintenance Guide* on RSA Link (https://community.rsa.com/). You can also refer to the 'System Maintenance Checklist' also located in the *Security Analytics System Maintenance Guide* on RSA Link (https://community.rsa.com/).

Task 12. (Optional) Security Update for MapR3.1 or MapR4.1

To update security fixes on MapR 3.1 or 4.1, refer to the article that describes this procedure in RSA Link at https://community.rsa.com/docs/DOC-63202.

Task 13. Ensure that ODBC Driver Names are Correct

In Security Analytics 10.6.2 and later, the Open Database Connectivity (ODBC) driver has been updated to end with **27.so**. Get the latest ODBC driver from Live. Then check the driver names in your Data Source Names (DSNs), and if the driver filenames still end with **26.so**, update them to **27.so** in `/etc/netwitness/ng/odbc.ini`. For example, in the default template MSSQL_Server_Windows_Template, you would update `/opt/netwitness/odbc/lib/R3sqls`**`26.so`** to `/opt/netwitness/odbc/lib/R3sqls`**`27.so`**.

Task 14. (Optional) Update Thai Fonts in Reporting Engine PDF Reports

To update Thai fonts in Reporting Engine PDF reports, you must install the following RPMs:

> **Note:** You must download the latest version of these RPMs from the CentOS repository.

- thai-scalable-fonts-common
- thai-scalable-waree-fonts

Task 15. Enable TCP Destnation Ports for IPDB.

On IPDB standalone device

1. Stop the iptables using `service iptables stop`
2. Navigate to `/etc/sysconfig/`
3. Run `vi iptables`
4. Add or modify the below 2 rules:
   - A INPUT -p tcp -m multiport --dports 50125 -m comment --comment "6 IPDB REST Port" -j ACCEPT
   - A INPUT -p tcp -m multiport --dports 56025 -m comment --comment "5 IPDB Service SSL Port" -j ACCEPT
5. Save the file
6. Save the iptables rules Run `service iptables save`
7. Start the iptables Run `service iptables start`

Task 16. Disable Firewall Rules.

> **Note:** Aafter upgrade if the duplicate firewall rules are seen you need to follow the below step to disable or remove the duplicate rules.

After the upgrade, on Log Collector or Log Decoder device, if you find duplicate firewall rule entries in the file `/etc/sysconfig/iptables` follow the below steps to disable the Rules:

1. Login as root user
2. Run the following command to flush all chains `iptables-f`

3. Run the following command for puppet agent `puppet agent-t`

Troubleshooting

Note: If you cannot resolve any update issue using the following troubleshooting solutions, contact Customer Support (go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

Problem 1	**Unable to access earlier versions to update hosts**
Possible Cause	After you update a host to a version from the local update repository, you may not be able to access earlier versions to update other hosts. This is determined by the amount of available space in your Local Update Repository and the size of the update packages. For example, if you updated the Security Analytics Server host to 10.5.5.0 and then to 10.6.6.0, 10.5.5.0 will not be available to update other hosts. If you needed to update another system to 10.5.5.0 (before updating to 10.6.6.0), you would need to download 10.5.5.0 from RSA Link and manually update the Local Update Repository again.
Solution	Download 10.5.5.0 from RSA Link and manually update the local update repository again.
Problem 2	**Pre-update server configuration issues**
Possible Cause	If the pre-update server configuration has any configuration issues that would prevent a successful update to 10.6.6.0, Security Analytics displays conflicts.
Solution	See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for instructions on how to resolve pre-update errors.
Problem 3	**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	See 'Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors' in the *Security Analytics Getting Started Guide* in the help (https://community.rsa.com/) for more information on how to resolve update errors.
Problem 4	**When you update Security Analytics to 10.6.2.0 or later, the add-on fiber card is missing from the `ifconfig` command output.**

Solution

You must boot the new kernel. Perform the following steps:

1. Check latest installed kernel using the following command:
   `rpm -qa | grep kernel | sort`
2. Ensure an entry exists for the latest kernel in the following location:
   `/boot/grub/grub.conf`
3. Reboot the operating system and select the corresponding entry for the new kernel.
   This boots the kernel and loads the pfring drivers.
4. To verify if p2p1 and p2p2 exist, run `ifconfig`.
5. If p2p1 and p2p2 exist, edit the `/boot/grub/grub.conf` file to change the default from `1` to `0`(with the assumption that the latest kernel version is listed first in `grub.conf`).
   The system will use the new kernel as the default kernel on next operating system reboot.