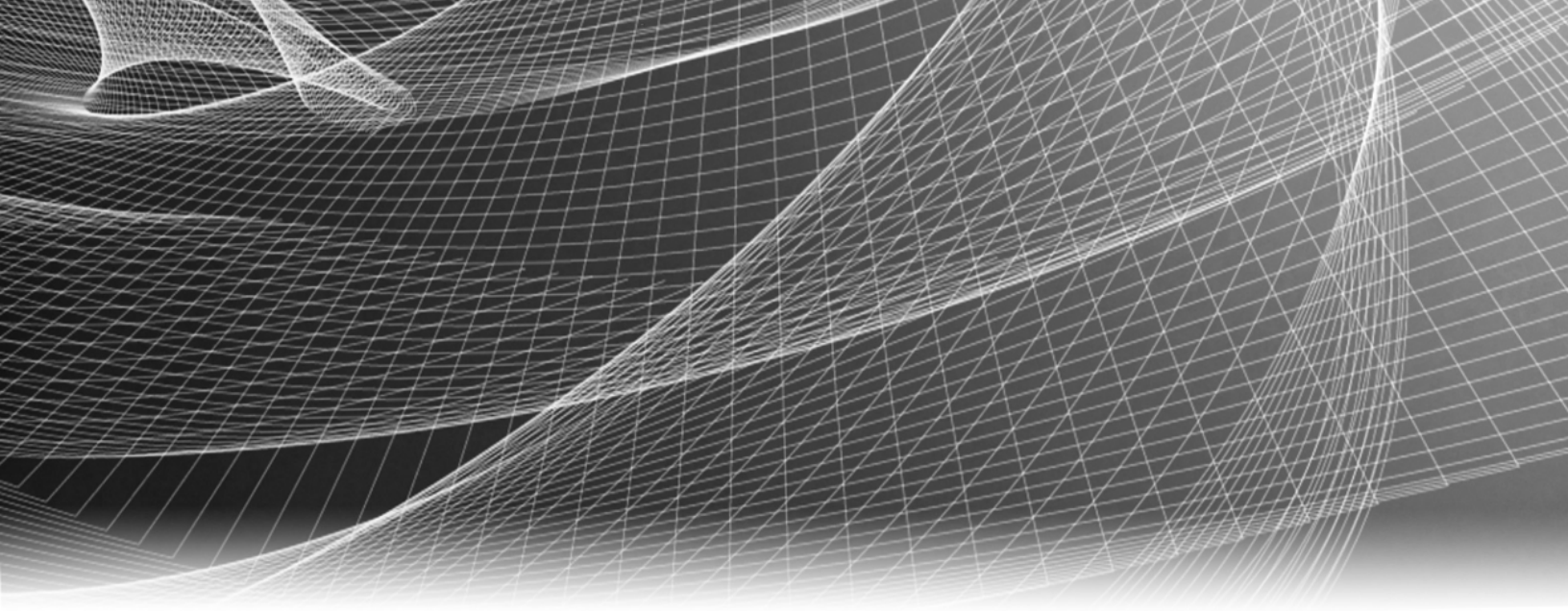


RSA Security Analytics

User Documentation

RSA

EMC²

Trademarks

License Agreement

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 in the thirdpartylicenses.pdf file.

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.

Security Analytics 10.5 Upgrade Instructions

Security Analytics 10.5 Upgrade Instructions

This document contains instructions for upgrading to Security Analytics v10.5.

Context

Security Analytics 10.5 provides new features, enhancements, and fixes for all products in the Security Analytics suite. These include: Security Analytics Server, Broker, Concentrator, Log Decoder and Decoder, Hybrid, All-in-One, Malware Analysis, Archiver, Event Stream Analysis, Log Collector, Security Analytics Warehouse, Workbench, Reporting Engine, and IPDB Extractor.

Introduction

This topic describes the upgrade paths to Security Analytics 10.5 and the major changes in the release.

Upgrade Paths

The following upgrades paths are supported for Security Analytics 10.5.

- v10.4.0.2 to v10.5
- v10.4.1 to v10.5
- v10.4.1.1 to v10.5

Caution: 1.) If you are running version 9.8, please contact Customer Support for upgrade instructions.

2.) If you are running Security Analytics version 10.3.x, you must upgrade to 10.4.1 before upgrading to 10.5. See the ***RSA Security Analytics 10.4.1 Upgrade Guide*** on SCOL (https://knowledge.rsasecurity.com/scolcms/set.aspx?id=10745) for detailed instructions on upgrading from 10.3.x to 10.4.1. **You cannot access the 10.4.1 upgrade RPMs from the SA Server Repository (using SMC Update). This means that you must download the 10.4.1 upgrade RPMs from SCOL.**

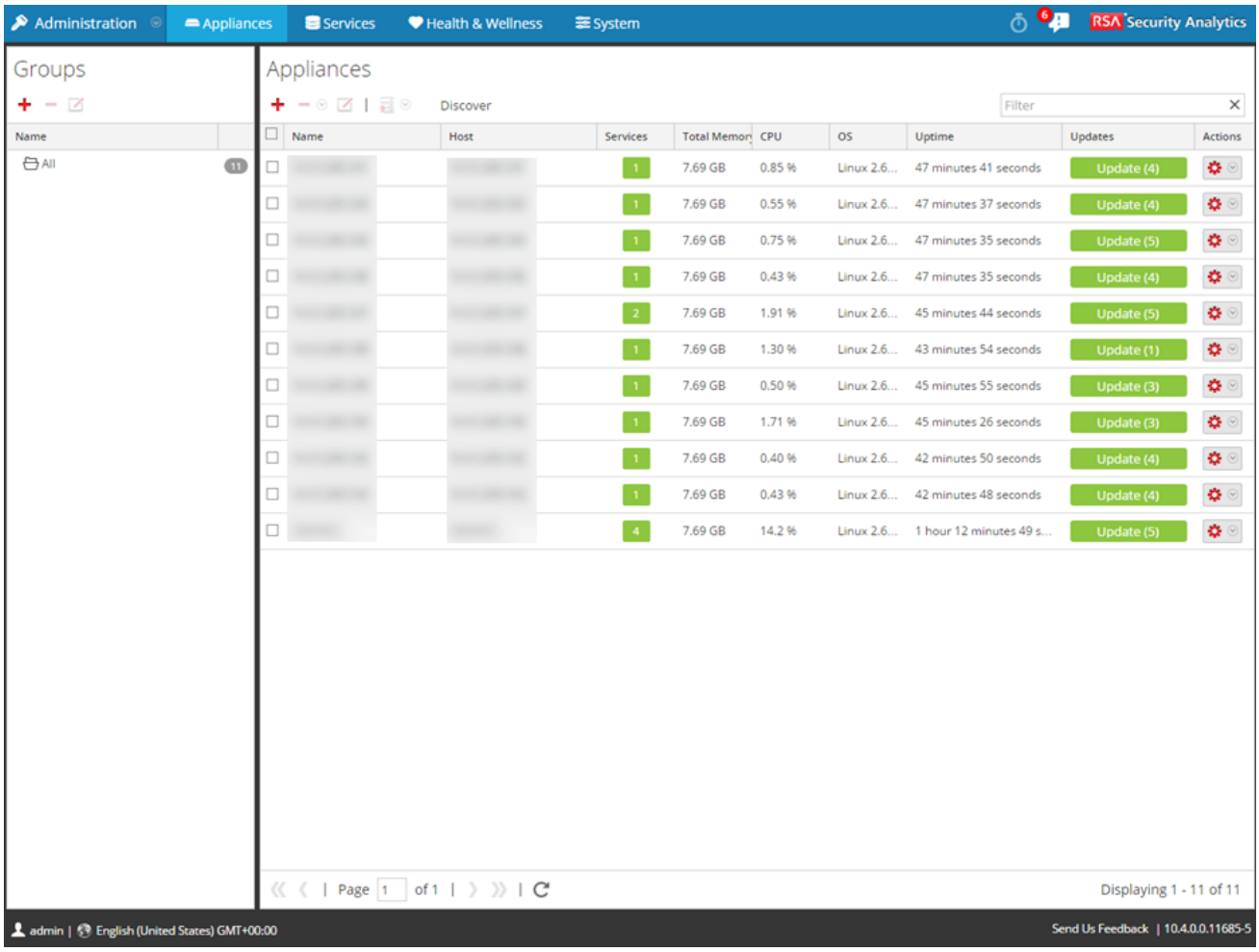
Note:

1.) Do not upgrade to Security Analytics v10.5 if you use Federal Information Processing Standards (FIPS). Security Analytics v10.5 does not support FIPS.

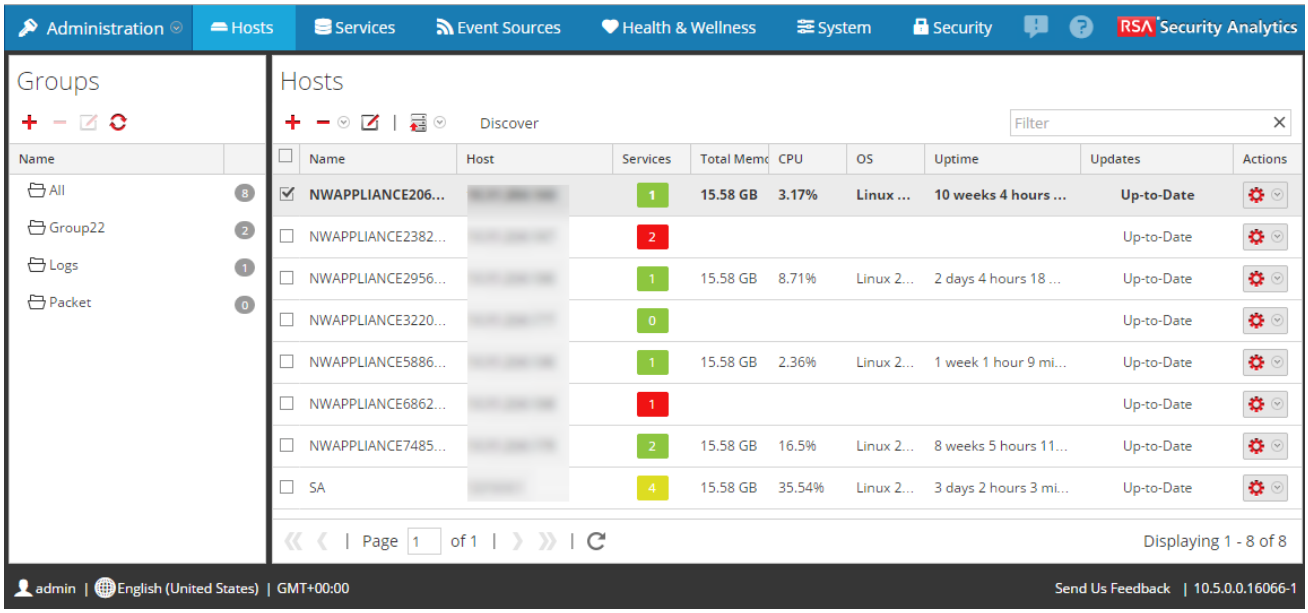
2) Security Analytics v10.5 only supports Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening if you applied DISA STIG prior to 10.5. In addition, Security Analytics Warehouse (SAW) MapR is not supported in 10.5 for DISA STIG.

Changed "Appliance" to "Host"

In 10.4.x Security Analytics Interface, an appliance represented the physical or virtual machine on which Security Analytics services ran.



In 10.5, RSA replaced the Administration > Appliances view with the Administration > Hosts view. This means all instances of the term "appliance" is now "host" in the 10.5 Security Analytics Interface and documentation. As a result, in 10.5, the term host represents the physical or virtual machine on which Security Analytics services run.



Required Upgrade Configuration Validation Scripts

RSA supplies a series of scripts that validate your configuration before, during, and after you upgrade to 10.5. You must run these scripts. Please refer to https://rsaportal.force.com/customer/articles/How_To/Pre-Upgrade-Script-Information for information on how to download and run these scripts.

The `preupgrade.py` script:

- Validates:
  - Bootloader config, kernels, grub.conf and files required to configure the bootloader including the symlinks files.
  - Connectivity and local configuration of the Security Analytics / RSA yum repository.
  - NTP synchronization and verbosely explain findings.
- Generates warnings if there are:
  - Unwanted repositories enabled (mostly the CentOS repos).
  - Highly-used file systems.

The `preRebootCheck.py` script validates that the grub.conf configuration file exists and generates the `preReboot.log` file.

The `postUpgradeCheck.py` script validates that Puppet is configured correctly and generates the `postUpgrade.log` file.

Upgrade Preparation Tasks

Complete the following procedures to prepare to upgrade to Security Analytics v10.5

Task 1 - Review Core Ports in 10.5 and Open Firewall Ports

Review the changes to Core ports in the **Network Architecture and Ports** (https://sadocs.emc.com/0_en-us/089_105InfCtr/100_Dep/10_NetPrt) topic in the Security Analytics10.5 Help (https://sadocs.emc.com/) so that you can reconfigure Security Analytics services and your firewall.

Note: Port 50514 is required for Audit logging.

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

Task 2 - Verify That All Services Running on Same SA Host Used Same Host/IP Address

Make sure that you used the same hostname/IP address to add all the services running on the same SA host. Please refer to **Change the Name and Hostname of a Host** (https://sadocs.emc.com/0_en-us/089_105InfCtr/120_AppSerCon/00_ApSvGtSt/20_AddlApplPr/aaChgNmeHst) and **Edit or Delete a Service** (https://sadocs.emc.com/0_en-us/089_105InfCtr/120_AppSerCon/00_ApSvGtSt/30_AddlServProc/EditDelServ) topics in the Security Analytics Help (https://sadocs.emc.com) for instructions on how to edit a hostname and IP address for hosts and services.

Example

If the SA host has a hostname/IP address of 1.1.1.1 and the Reporting Engine and Broker services are running on this SA host, make sure you used the 1.1.1.1 or 127.0.0.1 address for both the Reporting Engine and Broker when you added them to the SA host in the **Administration** > **Services** view.

Task 3 - Populate SA Server Update Repository

The following topic points you to the the instructions for the two options from which you can choose to populate the update repository.

Option 1 - Security Analytics Connected to Internet (SA LIVE Account)

To populate the SA Server Update Repository with the 10.5 upgrade packages using the SA Server Live account:

1. Make sure that you have configured SMCUPDATE.
   Please refer to the **Configure SMCUPDATE (**https://sadocs.emc.com/0_en-us/089_105InfCtr/215_SysAdm/ManageUpd/10_PopUpdsRepo/00_Opt1fromLive/00_ConfigSMCUPDATE) topic in the Security Analytics10.5 Help (https://sadocs.emc.com/) for instructions.
2. In Security Analytics menu, select **Administration** > **System**
   The **Info** view is displayed.
3. In the left panel, select **Updates**.
4. In the Updates Repository tab, click **Sychronize Now**.
   The Updates Repository tab is displayed with the updates you retrieved by synchronizing.

Option 2 - Security Analytics Not Connected to Internet (Download from SCOL)

To populate the SA Server Update Repository with the 10.5 upgrade packages from Download Central:

1. Download the SA-v10.5-UpgradePack.zip, which contains all the Security Analytics v10.5 Upgrade files, from Download Central (https://download.rsasecurity.com/) to a local directory.
2. In Security Analytics menu, select **Administration** > **System**.
3. In the left panel, select **Updates**.
4. In the **Manual Updates** tab, click **Upload Files**.
   The Upload File dialog is displayed.
5. Click + and browse to the local directory where you put the Service Pack 10.5 upgrade zip file and select the file.
6. Click **Upload**.

   Note: The zip file is very large so you may have problems uploading it into Security Analytics. If this occurs, please unzip the file and upload the files in smaller groups.

   The 10.5 Upgrade rpms display in the **Manual Updates** tab.
   The upload status is displayed in the lower left corner. When the upload is complete, SA server unzips all the rpm packages and displays them in the **Manual Updates** tab.
8. Select all files in the Manual Updates list and click **Apply**.
   This moves the rpm files into the SA Server Updates Repository and makes them available to hosts.

Task 4 - For Multiple SA Server Deployments Only - Designate Primary and Secondary SA Servers

Overview

If you have a Multiple SA Server deployment, you must designate a primary SA and secondary SA servers and check the `rsa.repo`.

Procedure

If you deploy multiple SA servers:

1. Before you upgrade the SA server host to 10.5, designate a primary SA server and secondary SA servers. Please refer to the **Host Upgrade Sequence** (https://sadocs.emc.com/0_en-us/089_105InfCtr/100_Dep/Host_Upgrade_Sequence) topic in the Security Analytics10.5 Help (https://sadocs.emc.com/) for a description of this deployment.
2. Before you upgrade the rest of the hosts to 10.5, check the `rsa.repo` file and make sure the baseurl is pointing to the primary SA server with the following command string.
   ```
   # cat /etc/yum.repos.d/rsa.repo
   ```
   The following output is displayed.
   ```
   baseurl=http://Primary-SA-IP-Address/rsa/updates
   ```

Caution: A secondary SA has the following limitations:

- The Updates column on the Appliances view is valid for the primary SA exclusively. It reflects the wrong status a secondary SA so you must not click it.
- You cannot use the Health & Wellness views.
- You cannot use the trusted connections feature.

Task 5 - Back Up Reporting Engine Database and Make Sure There Is Sufficient Space for 10.5 Database

Overview

Reporting Engine data is migrated to new databases as part of this upgrade. Before the upgrade, make sure that there is sufficient disk space available for the migration. RSA also recommends that you backup the Reporting Engine database so that you can revert back to it if you face an unusual problem like those described in **Monitor Migration of the Reporting Engine**.

1. Back up the `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db` file so you can revert to this file if you encounter migration issues.
   a. SSH to the Reporting Engine host.
   b. Stop the Reporting Engine service using the following command string.
   `stop rsasoc_re`
   c. Create a `tar.gz` of the `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db` file using the following command string.
   `tar cvfj statusdb.tar.gz  /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
   d. Move the backup file to another storage location.
   e. Retain the backup file until the migration of `statusmanager.h2.db` has completed successfully.
2. Make sure that you have minimum free disk space of 1.2 times the size of `statusmanager.h2.db` in the volume where the file exists.
   For example, if the `statusmanager.h2.db` is of size 1 Gigabyte, at least 1.2 Gigabytes of free disk space must be available to migrate the database.

   Note: Security Analytics allocates 200 Gigabytes of space for the Reporting Engine which is used both by the Reporting Engine service and its database.

   - Use the following command to determine the amount of disk space available in the volume where `statusmanager.h2.db` file exists.
     `df -h`

     The example shows 198 Gigabytes of free disk space.

     ```
     Filesystem            Size  Used Avail Use% Mounted on
     /dev/mapper/VolGroup02-rsasoc
                           200G  2.3G  198G   2% /home/rsasoc
     ```

   - Use the following command to determine the size of the `statusmanager.h2.db`.
     `du -h /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`

     If `statusmanager.h2.db` file size is 1 Gigabyte, but available free space is only 1 Gigabyte, free up at least 0.2 Gigabytes of disk space as explained in the next step.

   - If you do not have enough disk space, the following tasks may help you free up disk space.

- Move archived files from /`home/rsasoc/rsa/soc/reporting-engine/archives/` to an other volume. The following command is an example of how to move archived files:
  `mv /home/rsasoc/rsa/soc/reporting-engine/archives/contentstore.20150302170101.tgz target-directory`
- Remove unwanted files in the volume in which `statusmanagerdb` exists.

Task 6 - Make Sure That /var/netwitness Directory Has Enough Space to Upgrade

Make sure that the usage of the `/var/netwitness` directory on the SA host is 80 percent or less before you upgrade. If directory usage is greater than 80 percent, after the upgrade, the SA server host will not be running and the logs will indicate that the migration failed.

Task 7 - Back Up Your Configuration

RSA recommends that you take a backup of your configuration before you perform the upgrade.

Please refer to **Back Up and Restore Data for Hosts and Services** (https://sadocs.emc.com/0_en-us/089_105InfCtr/215_SysAdm/BackupRest) topic in the Security Analytics10.5 Help (https://sadocs.emc.com/) for guidelines on how to back up your configuration.

Task 8 - (Conditional - For Customers Using DISA STIG in 10.4.x Only) Prepare STIG for Upgrade.

If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening rpm in Security Analytics v10.4.x, you must perform the following task to migrate it to 10.5.

For all hosts with STIG applied:

1. SSH to the host.
2. `yum update glibc`
3. `reboot`

At this point, you can proceed to the Upgrade Tasks.

Upgrade Tasks

Complete the following procedures to upgrade to SA v10.5.

Task 1 - Upgrade the SA Server Host

You must use the yum command to upgrade the SA Host to SA v10.5.

Note: For All in One (AIO) host,

- Submit the following commands to upgrade all services:

```
yum install rsa-sa-gpg-pubkeys
yum install rsa-puppet-scripts
yum update -y
reboot
```

To update the SA host to Security Analytics v10.5:

1. SSH into the SA host.
2. Refresh the yum repository.
   ```
   [root@sasrv yum.repos.d]# yum clean all
   yum check-update
   ```
   A list of all the updates available in v10.5 are displayed.
3. Update public keys.
   ```
   yum install rsa-sa-gpg-pubkeys
   ```
4. Update puppet.
   ```
   yum install rsa-puppet-scripts
   ```
5. Apply updates on SA.
   - If the Broker service is on the SA host:
     ```
     [root@sasrv yum.repos.d]# yum update --exclude=nwbroker -y
     ```
   - If the Broker is not on the SA Host:
     ```
     [root@sasrv yum.repos.d]# yum update -y
     ```
6. Reboot the SA host.
   ```
   [root@sasrv yum.repos.d]# reboot
   ```

7. Perform checks to verify that SA is up and running properly.

> **Note:** The following services will be added to hosts in the **Administration** > **Services** view in the SA User Interface automatically after the upgrade.
>
> 127.0.0.1 – Incident Management
> 127.0.0.1 – IPDB Extractor
> 127.0.0.1 – Malware Analysis
>
> The `rabbitmq`, `mcollective`, `rsa-sms` services will take approximately 10 to 15 minutes to start running after reboot. The Incident Management service will take approximately five minutes to start running after reboot.

a. Connect to Security Analytics through your browser and make sure that the correct version number is displayed.
If you cannot connect to the browser after 20 minutes, reboot the SA server again.

b. SSH to the SA host.

c. Verify that the RabbitMQ service is running.
```
service rabbitmq-server status
```

d. Verify that the mcollective service is running
```
service mcollective status
```

e. Verify that the MongoDB service is running.
```
service tokumx status
```

f. Verify that the Puppet service is running.
```
service puppetmaster status
```

g. Ping the mcollective once to verify that it is working properly.
```
mco ping
```

h. Verify that the SMS service is running.
```
service rsa-sms status
```

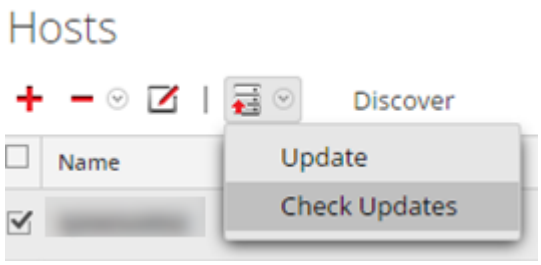
> **Note:** If you encounter a host or service migration failure, please refer to **Troubleshooting Health & Wellness** (https://sadocs.emc.com/0_en-us/089_105InfCtr/215_SysAdm/MonitorHlth/80Troubleshoot) in the Security Analytics10.5 Help (https://sadocs.emc.com/).

Task 2 - Upgrade All Other Hosts

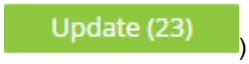
To upgrade each non-SA host to Security Analytics v10.5:

Note: You do not need to complete this task for an All in One (AIO) Hosts because you updated all the services in Task 1 - Upgrade the SA Server Hosts.

1. SSH to each host and update public keys then update puppet.
   a. Update public keys.
      ```
      yum install rsa-sa-gpg-pubkeys
      ```
   b. Update puppet.
      ```
      yum install rsa-puppet-scripts
      service mcollective restart
      ```
2. Log into Security Analytics.
3. In the Security Analytics menu, select **Administration** > **Hosts**.
4. Update hosts in the sequence recommended in the **Host Upgrade Sequence** (https://sadocs.emc.com/0_en-us/089_105InfCtr/100_Dep/Host_Upgrade_Sequence) topic in the Security Analytics10.5 Help (https://sadocs.emc.com/).
5. For each host:
   a. Select the host and click **Update** > **Check Updates**.



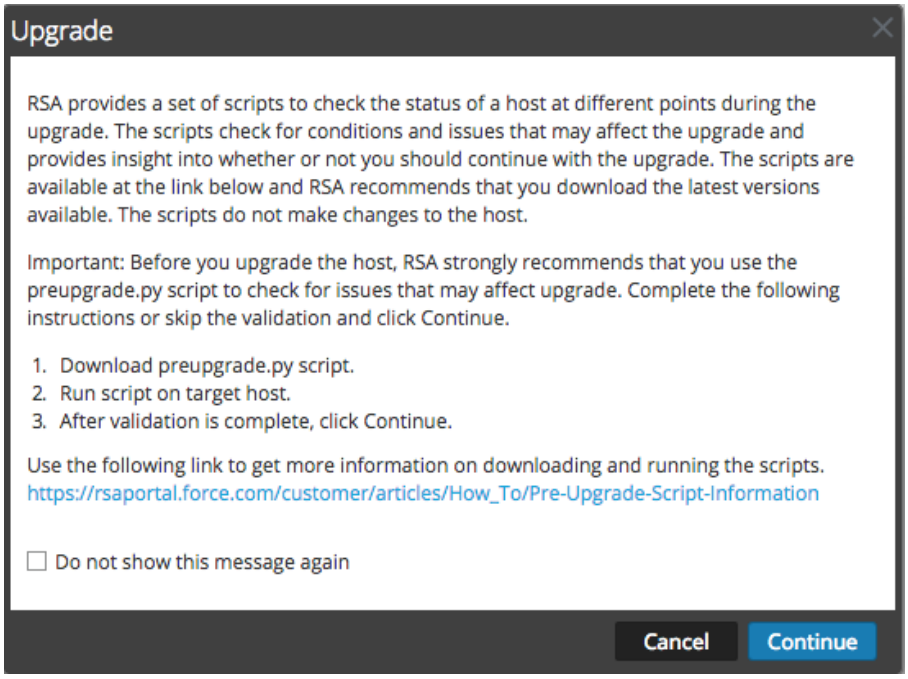
Checking... is displayed in the Updates column as Security Analytics retrieves the latest updates for 10.5. After it finishes retrieving all the 10.5 updates, it displays **Update (*number-of-update-files*)** in the **Updates** column (for example,



) .

   b. Click **Update (*number-of-update-files*)**.

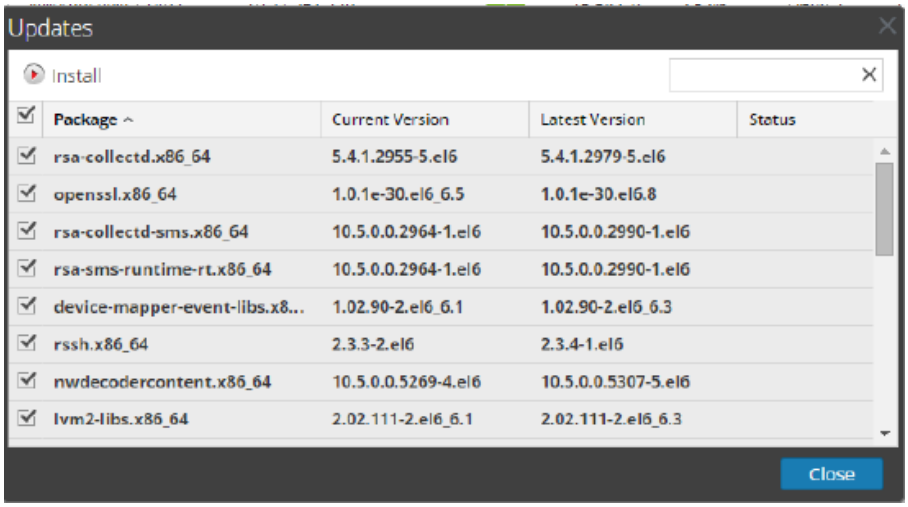
The following dialog is displayed.



The https://rsaportal.force.com/customer/articles/How_To/Pre-Upgrade-Script-Information links takes you to Knowledgebase Article (number 000029911) that tells you where to download the `preupgrade.py`, `preRebootCheck.py`, and `postUpgradeCheck.py` scripts and instructions on how to run the scripts on the target host.

After you click **Continue**, the **Updates** dialog is displayed.

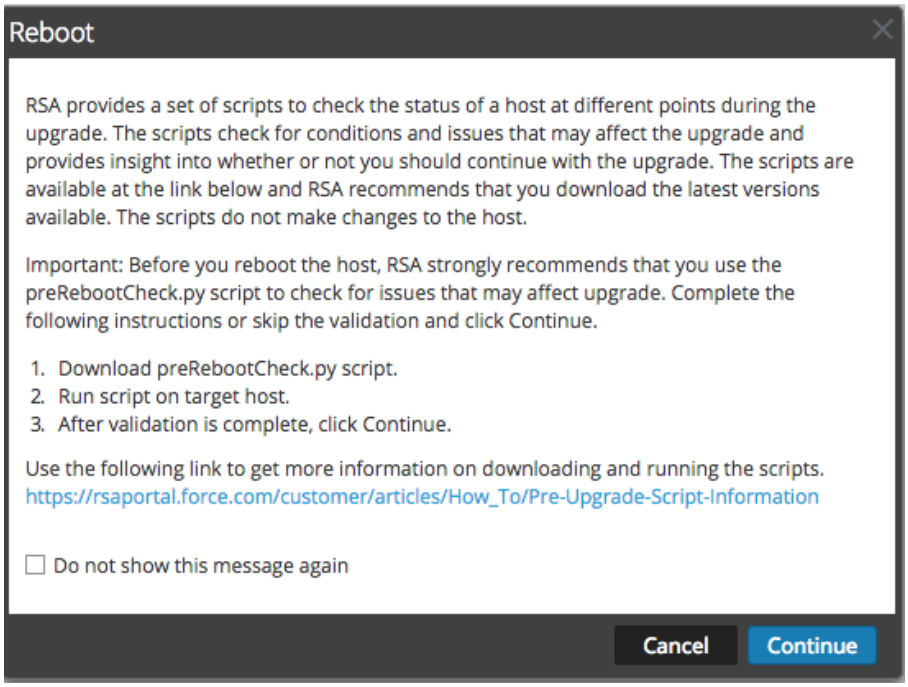
c. Select all the packages and click Install.



After all the 10.5 packages are installed, **Reboot Required** is displayed in the **Updates** column.

d. Click **Close** to close the **Updates** dialog and click **Reboot Required**.

> **Note:** When you reboot the host running the SA service, this starts data migration for:
>
> **Health & Wellness (H&W) statistics**. You must wait for the migration to complete before you can see local statistics in Stats Browser, Monitoring, and Policies views. For example, if you try to create a policy and add rules with statistical parameters to this policy, you may not be able to see the statistical parameters until the migration completes. You can see statistics from other hosts in the H&W views while the migration is in progress.
>
> **Reporting Engine**. Before you enable the host running the SA service and Reporting Engine, please refer to the Monitor Migration of Reporting Engine for instructions.



6. SSH to each host and update `rsa-sa-tools`.
   ```
   yum install rsa-sa-tools
   ```

Task 3 - (Optional) Upgrade or Install Legacy Windows Log Collection

Please refer to the **RSA {{SA}} v10.5 Legacy Windows Collection Upgrade & Installation Instructions** on SCOL (https://knowledge.rsasecurity.com) for the details on how to install or upgrade Legacy Windows collection.

Post-Upgrade Tasks

Complete the following procedures after you upgrade to 10.5.

Task 1 - Monitor Migration of Reporting Engine Data

This topic tells you how to monitor migration of the Security Analytics Reporting Engine data to 10.5. It also tells you how to troubleshoot failures if you encounter any.

Note: Security Analytics upgrade to 10.5 automatically triggers migration of Reporting Engine data. This topic tells you how to monitor the migration. Normally, you will not encounter the problems listed in this topic. The information provided in this topic gives you troubleshooting tips in case you face a problem. Please contact Customer Care if you have difficulty resolving these problems.

Internally, the Reporting Engine data migration process has two stages:

- Stage 1 - Copy Statistics and Latest Historical Execution Data
- Stage 2 - Copying Remaining Data and Cleanup

For informational purposes only, During the migration process, Security Analytics copies content:

- From: `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
- To: `home/rsasoc/rsa/soc/reporting-engine/statusdb/alertstatusmanager.h2.db` and `/home/rsasoc/rsa/soc/reportingengine/statusdb/reportstatusmanager.h2.db`

Context

This topic covers the following subjects.

- Approximate time estimates of the migration.
- Reporting Engine Migration Process.
- Location of the migration log file and how to interpret it.
- Troubleshooting.

Estimating Migration Duration

The estimates in the following table are based on the time it took for the migration to complete in the RSA test environment. Stage 1 completes before the Reporting Engine starts up so you can use the stage 1 information in the table to roughly estimate how long the start-up might take. Stage 2 starts in the background after the start-up so you can use the stage 2 information in the table to roughly estimate how long you may have to monitor migration logs for any potential errors.

Caution: The metrics in the following table were derived in a lab environment so they are only estimates for planning purposes.

Security Analytics allocates 200 Gigabytes of space for the Reporting Engine which includes the complete Reporting Engine service and the database.

Typical Data volume of status db in RE (Giga bytes)	Number of Alerts	Number of Reports	Stage 1 Time taken (seconds)	Stage 2 Time taken (minutes)
3.5	2139046	15169	10	17
10	2139046	205171	16	23
40	2139046	1395171	20	70

Reporting Engine Migration Process

The following procedure explains what happens internally during Security Analytics Reporting Engine data migration process.

Note: You can continue to create, schedule, and execute reports, alerts, and charts even though the migration is in progress. However, all of the historical execution data will not be available until the migration completes successfully.

After you complete the upgrade of the SA Host by rebooting the host, the Reporting Engine migration process automatically starts. The migration has two stages:

Stage 1 - Copy Statistics and Latest Historical Execution Data: Reporting Engine copies the statistics and latest alert and report execution records upon startup.

If stage 1 tasks are successful, the latest twenty thousand reports and alerts execution records are successfully copied to the new database. You can now view the statistics and latest execution data in the Security Analytics Interface.

Stage 2 - Copying Remaining Data and Cleanup: After the Reporting Engine is up and running, stage 2 starts in the background. During this stage, the rest of the execution records get copied over in batches, making those records available to users in User Interface. After all of the records are successfully copied, the old data is deleted.

Locate and Interpret Migration Log File

The migration logs are stored in `/home/rsasoc/rsa/soc/reporting-engine/logs/migration.log`. Please look for `begin`, `end`, `progress`, and error messages during migration.

- After the data migration starts, the following message is displayed.

  ```
  **************Database migration Started **************
  ```

- If you do not have enough free disk space for the migration (that is, disk space equivalent to at least 1.2 times the size of `statusmanager.h2.db` file) the Reporting Engine service fails to start and a message similar to the following error message is displayed.
  ```
  Available Disk Space : 8,112 MB . Required disk space 10,048 MB.
  CRITICAL : Available Disk Space is not sufficient to proceed with migration. Shutting down reporting engine. Please cleanup data and start reporting engine
  ```
  Please refer to **Problem 1: Reporting Engine will not start**, **Possible Cause 2** in the **Troubleshooting** section of this task.

- During migration, Security Analytics writes log messages indicating the number of records copied to the destination database. For example:
  ```
  '20,000' out of 29,812 Records are inserted into 'AlertStatus' table
  ```

- After the migration is complete, the following message is displayed.
  ```
  **************Database migration Completed **************
  ```

- If the copying of an alert or report statistics fails, Security Analytics logs the following message.
  ```
  Migration of Report/Alert Statistics failed. Interpreted property re.proceed_if_stats_init_fails as: false. Shutting down reporting engine
  ```
  Please refer to **Problem 1: Reporting Engine will not start.** in the **Troubleshooting** section of this task.

- If the migration does not complete because it failed to copy any of the records, the legacy `statusmanager.h2.db` is not cleaned up and Security Analytics logs the following message.
  ```
  Additional rows are available for migration. Cannot clean up DB objects just now
  ```
  Please refer to the following messages in the **Troubleshooting** section of this task.

  - **Problem 2: Need to restart migration from the beginning**

- **Problem 3: Migration successfully migrates all records, but the `statusmanager.h2.db` still exists.**

- If all the records migrate successfully, but the cleanup of the legacy `statusmanager.h2.db` file fails, Security Analytics logs the following message.
  ```
  Failed to cleanup legacy status manager database
  ```
  Please refer to **Problem 3: Migration successfully migrates all records, but the statusmanager.h2.db still exists**. in the **Troubleshooting** section of this task.

Troubleshooting

Note: If you cannot resolve any migration issue using the following troubleshooting solutions, please contact Customer Care.

Problem 1	**Reporting Engine will not start.**
Possible Cause 1	Failed to migrate the correct historical report and alert execution statistics records.
Solution 1	Review the log messages and fix the issue that caused the failure. If you cannot fix an issue encountered while the statistics are being copied, ignore the failure and proceed with migration. Set the JVM system property to `true`: in `/home/rsasoc/rsa/soc/reporting-engine/conf/server.conf: re.proceed_if_stats_init_fails=true` to ignore the failure in stats migration and start Reporting Engine service. If you choose to ignore the failure of statistics migration and the migration proceeds, the new statistics available in Reporting Engine override the old statistics.
Possible Cause 2	You do not have enough disk space.
Solution 2	You need a minimum of 1.2 times the size of `statusmanager.h2.db` file of free disk in the volume in which `statusmanager.h2.db` exists to migrate. If you do not have enough disk space, the following methods may help you free up disk space. • Free up some space by moving archived files from /`home/rsasoc/rsa/soc/reporting-engine/archives/` to any other volume that has free space. The following command is an example of how to move archived files: `mv /home/rsasoc/rsa/soc/reporting-engine/archives/contentstore.20150302170101.tgz` *`target-directory`* • Remove unwanted files in the volume in which `statusmanager.h2.db` exists.

Problem 2	**Need to restart migration from the beginning (Stage 1).**
Possible Cause	Found failures while monitoring migration (for example, `statusmanager.h2.db` was corrupted during migration).

Solution	1. Retrieve the backup you made of the `statusmanager.h2.db`.
	2. SSH to the host that runs the Reporting Engine.
	3. Stop the Reporting Engine using the following command string.
	`stop rsasoc_re`
	4. Delete the corrupted `db` file using the following command string:
	`rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
	5. Delete the new `db` files that were created during migration using the following command strings.
	`rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/alertstatusmanager.h2.db`
	`rm /home/rsasoc/rsa/soc/reportingengine/statusdb/reportstatusmanager.h2.db`
	6. Remove the bookmarks folder that tracks the current migration status using the following command string.
	`rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/bookmarks`
	7. Restore the backed up `statusmanager.h2.db` file to `/home/rsasoc/rsa/soc/reporting-engine/statusdb/` directory using the following command string.
	`tar –xvf statusdb.tar.gz`
	8. Make sure that the restored `statusmanager.h2.db` has permission for `rsasoc` user. If not, use the following command string to reinstate the user privilege.
	`chown –R rsasoc:rsasoc /home/`

	`rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
	9. Start the Reporting Engine using the following command string.
	`start rsasoc_re`

Problem 3	**Migration successfully migrates all records, but the `statusmanager.h2.db` still exists.**
Possible Cause	Migration failed to remove the `statusmanager.h2.db` file.

Solution 1	Archive the legacy `statusmanager.h2.db` file.
	1. Stop Reporting Engine using the following command string.
	`stop rsasoc_re`
	2. Create a `tar.gz` of the `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db` using following command string.
	`tar cvfj statusdb.tar.gz /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
	3. Move the file to another storage location.

Solution 2	Delete the `statusmanager.h2.db` file with the following command string. `rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`

(Conditional) Task 2 - Restore Incident Management Customizations

Before executing the 10.5 upgrade, Security Analytics backs up v10.4.x Incident Management mail templates, scripts, and fields directories and created a zip file that includes these directories. If you customized Incident Management mail templates, scripts, and fields in v10.4.x, you restore this information from the contents of the backup zip file.

Note: If you did not customize mail templates, scripts, or fields in v10.4.x, you do not need to perform the following procedure.

To restore the customized Incident Management information:

1. Unzip the `/opt/rsa/im/backup/timestamp.zip`.
   The zip file contains the following directories:
   ```
   mailtemplates
   scripts
   fields
   ```
2. To restore your customized Incident Management data from the contents of `/opt/rsa/im/backup/timestamp.zip`:
   - **Mail templates**, overwrite the 10.5 `/opt/rsa/im/mailtemplates` directory with the `mailtemplates` directory from the zip file.
   - **Scripts**, merge your 10.4.x scripts in the `scripts` from the zip file with the contents of the 10.5 `/opt/rsa/im/scripts` directory.
   - **Fields**, merge your 10.4.x fields in the `fields` from the zip file with the contents of the 10.5 `/opt/rsa/im/fields` directory.

Task 3. (Conditional - For Customers Using DISA STIG in 10.4.x Only) Migrate DISA STIG to 10.5.

If you applied the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) hardening rpm in Security Analytics v10.4.x, you must perform the following task to migrate it to 10.5.

For all hosts with STIG applied:

1. SSH to the host.
2. `cd /opt/rsa/AqueductSTIG/`
3. `./GEN000400.sh`
4. `./GEN001120.sh`
5. `reboot`

Task 4. Reboot SA Host and Malware Analysis Hosts If Error Occurs

Look for multiple error messages similar to the following message on the host running Malware Analysis in the `/var/lib/netwitness/rsamalware/spectrum/logs/spectrum.log` file after you upgrade 10.5.

```
2015-05-12 12:53:32,818 [ActiveMQ BrokerService[2437abe8-51ed-46ec-
bcf7-b76e533eea83] Task-2] ERROR org.apache.activemq.broker.TransportConnector - Could
not accept connection from tcp://10.31.204.101:45728:
javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
```

If you see this type of error, you must:

1. SSH to SA host.
2. `reboot`
3. SSH to the host running Malware Analysis.
4. `reboot`

Task 5. (Conditional) Make Sure Reporting Engine Service Is Started with Java v1.8

After you upgrade to 10.5, some of the reporting features such as rule execution or import may not work. This occurs if the Reporting Engine is started with Java 1.7 instead of Java 1.8 on upgrade.

Perform the following steps make sure that the java version is updated to 1.8 and restart the Reporting Engine service.

1. Open the latest reporting-engine.sh* file from the `/home/rsasoc/rsa/soc/reporting-engine/logs/` folder.
   If the Reporting Engine is using java version 1.7, **Current java version is java version "1.7.0_75"** is displayed. If this message is displayed, please go to step 2. If the Reporting Engine is already using Java 1.8, then **Current Java version** (without any version number) message will be displayed, in that case you do not need to complete step 2.
2. Make sure the the java version for the Reporting Engine is updated from v1.7 to v1.8.
   a. Submit the following command string to find out if execution of the puppet agent responsible for updating the java alternatives is completed.
      `ps -ef | grep -i puppet`

      If the puppet agent for updating the java alternatives is in-progress the **puppet agent: applying configuration** process is displayed. After the java version is updated to1.8, **puppet agent: applying configuration** is no longer displayed.

   b. After the Puppet agent completes the configuration process, submit the following command string to determine if java alternatives are updated to 1.8.
      `ls -l /etc/alternatives/java`
   c. After the java version is updated to 1.8, restart the Reporting Engine service.

Task 6. (Conditional) - Restore Overwritten CA-Certificates

If you have a CA-signed certificate configured in Security Analytics before the upgrade, Security Analytics replaces it with a Puppet self-signed certificate during the upgrade to 10.5. Please reconfigure to bind the CA-signed certificates according to the instructions in the ***Installing a Public CA Certificate on RSA Security Analytics 10.4.0.2*** on RSA SecurCare Online (https://knowledge.rsasecurity.com).

Contacting Customer Care

RSA SecurCare:	https://knowledge.rsasecurity.com
Phone:	1-800-995-5095, option 3
International Contacts:	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email:	nwsupport@rsa.com
Community:	http://www.emc.com/security/security-analytics/security-analytics.htm
Basic Support:	Technical Support for your technical issues is available during 8am to 5pm your local time, Monday through Friday.
Enhanced Support:	Technical Support is available by phone 24 x 7 x 365 days of the year 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:

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

Revision History

Revision	Date	Description	Author
1.0	08-Jun-2015	Initial Release	Info Design & Devel (dfo)