RSA NETWITNESS® PLATFORM

SA and RE Consolidation Tool Guide

Contact Information

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

Trademarks

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

License Agreement

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

March 2019

Contents

Overview of Consolidation Tool

This tool is for customers who have Security Analytics 10.6.6 with multiple SA and RE instances. Since multiple instances of SA and RE are not supported in 11.3, you must consolidate the configurations and data before you upgrade to 11.3. To overcome this issue, the consolidation tool has been implemented. This consolidation tool, will enable the 10.6.6 users having multiple SA and RE instances to collate the data on one target instance of 10.6.6, which then can be upgraded to 11.3 successfully or seamlessly using the usual upgrade procedures.

Note: For customers with STIG enabled deployments, this consolidation tool will not work as the root access is disabled in such deployments.

Prerequisites

Before you begin the consolidation process for Security Analytics Server and Reporting Engine instances. You must back up your configurations and data using the nw-backup script on every SA node that needs to be consolidated.

Back Up Commands

Run the following commands to backup your configurations:

a. `get-all-systems.sh <IP-address>` . For example: `./get-all-systems.sh 10.1.1.1`

b. `ssh-propogate.sh <location-of-all-systems-file>` . For example: `./ssh-propagate.sh /var/netwitness/database/nw-backup/all-systems`

c. `nw-backup` with local backup option. For example: `./nw-backup -l`

For more information, see the Physical Host Upgrade Guide.

SSH Propagate Commands

Run the following commands on the target SA node:

a. `get-all-systems.sh <IP-address-Source-Node>`. For example: `./get-all-systems.sh 10.1.1.1`

b. `ssh-propogate.sh <location-of-all-systems-file>` . For example: `./ssh-propagate.sh /var/netwitness/database/nw-backup/all-systems`

c. `get-all-systems.sh <IP-address-Target-Node>` . For example: `./get-all-systems.sh 20.2.2.2`

d. `ssh-propogate.sh <location-of-all-systems-file>` . For example: `./ssh-propagate.sh /var/netwitness/database/nw-backup/all-systems`

Note: Make sure you delete the manually added hosts and services from the target node because they might be already provisioned in one of the source nodes. If not, it may cause the consolidation to fail due to the name conflict.

Tool Location

You can download the **rsa-nw-consolidator-bundle.tar.zip** from RSA link:

https://community.rsa.com/community/products/netwitness/113/downloads

Tool Contents

You must unzip the **rsa-nw-consolidator-bundle.tar.zip** file using the below command:

1. `unzip rsa-nw-consolidator-bundle.tar.zip`
2. `mkdir rsa-nw-consolidator`
3. `tar -xvzf rsa-nw-consolidator-bundle.tar.gz --directory rsa-nw-consolidator`
4. `cd rsa-nw-consolidator`

```
[root@NWAPPLIANCE10909 rsa-nw-consolidator]# ll
total 24
drwxr-xr-x. 2 root root  4096 Mar 22 11:18 bin
drwxr-xr-x. 2 root root  4096 Mar 14 09:19 log
-rwx------. 1 root root 11111 Mar 13 06:41 rsa-nw-consolidator.sh
drwxr-xr-x. 2 root root  4096 Mar 22 11:18 scripts
[root@NWAPPLIANCE10909 rsa-nw-consolidator]#
```

After you unzip and access the folder, you will see the following:

- bin – contains the jar files required for SA and RE consolidation
- log – contains the logs of the executions
- script – contains the script files required for SA and RE consolidation
- rsa-nw-consolidator.sh – contains the consolidation tool launch script.

Note: If you copy paste the commands from PDF to Linux SSH terminal, the characters do not work. It is recommended to type the commands.

SA Server Consolidation

SA Server consolidation is a tool used to consolidate Hosts, Services, Users, Roles and Custom feeds with multiple deployments. You can consolidate from a single SA source instance to a single SA destination instance at a time. After the consolidation process is complete, all the services, hosts, configurations and other relevant data will be displayed in the target node.

In case of name conflicts, Hosts and Services there will not be any change, for User and Roles the target node takes precedence and for Custom Feeds, they are automatically renamed during the consolidation process.

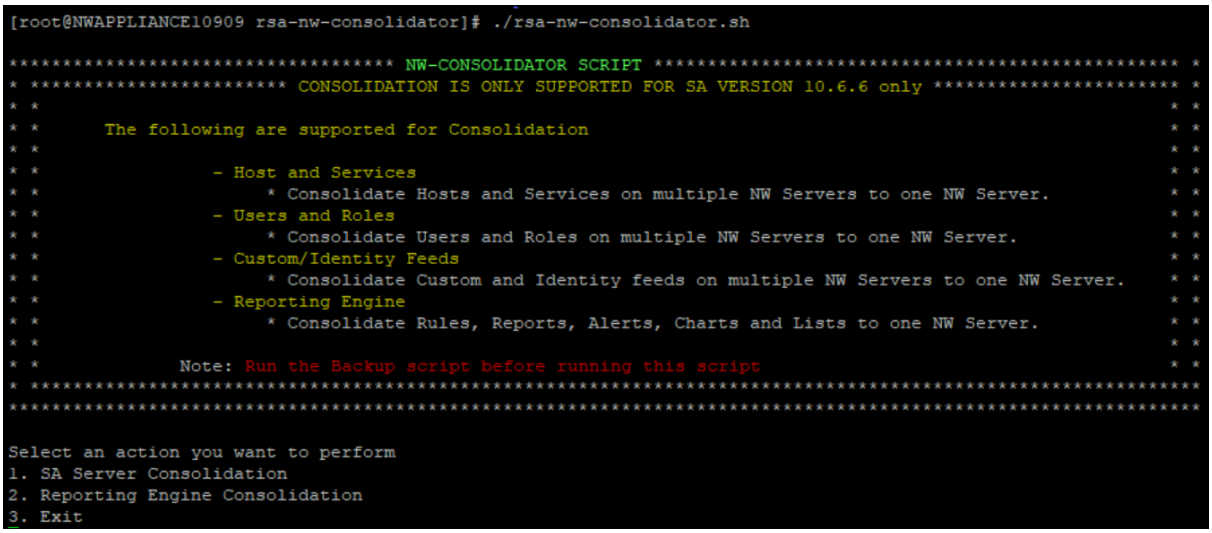
The following table describes the entities that will be consolidated as part of the SA consolidation process, if they exist in the SA environment.

Entities	Configurations	Comments
Users	Yes	External users are not consolidated.
Roles	Yes	
Hosts	Yes	Groups are not consolidated.
Services	Yes	Groups are not consolidated.
Custom/Identity Feeds	Yes	As hosts and services **groups** are not consolidated, feeds on these groups will not be consolidated. Hence the recurring feeds on groups must be manually redeployed.

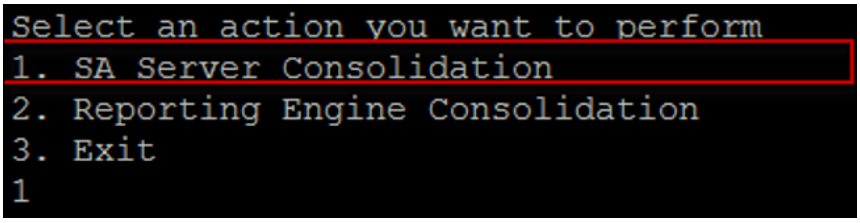
Using the Tool

After you have completed the prerequisites, perform the following steps:

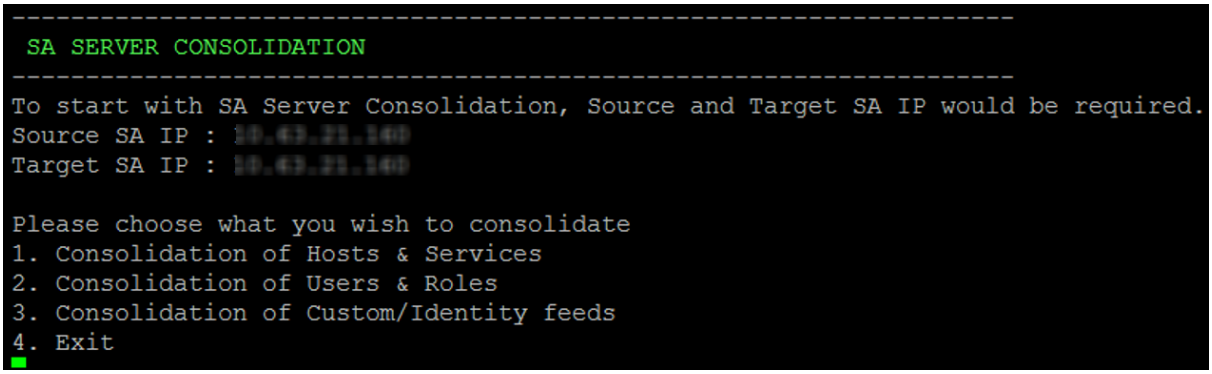
1. SSH to the target node and run the `rsa-nw-consolidator.sh` script .
   The log in command window is displayed.



2. Select **Option 1** to begin the SA Server consolidation process.

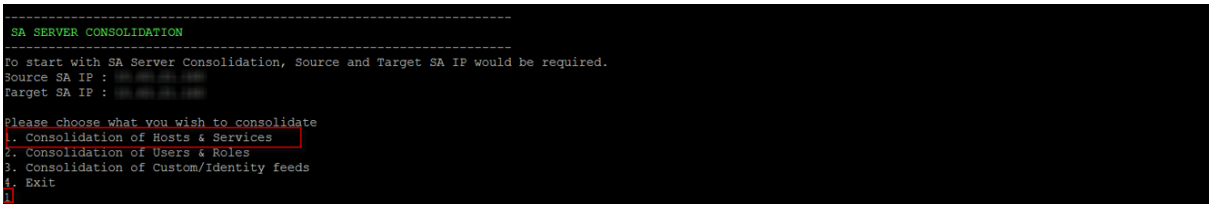


3. Enter the IP address of the target and source nodes.
   The consolidation options are displayed.

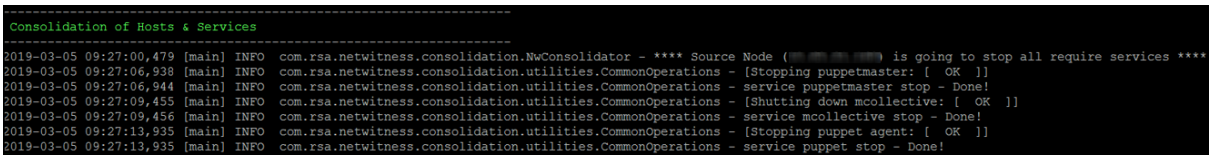


Option 1 – Consolidation of Hosts and Services

1. Under the SA Server Consolidation option, select **Option 1** to begin the consolidation of Hosts and Services.

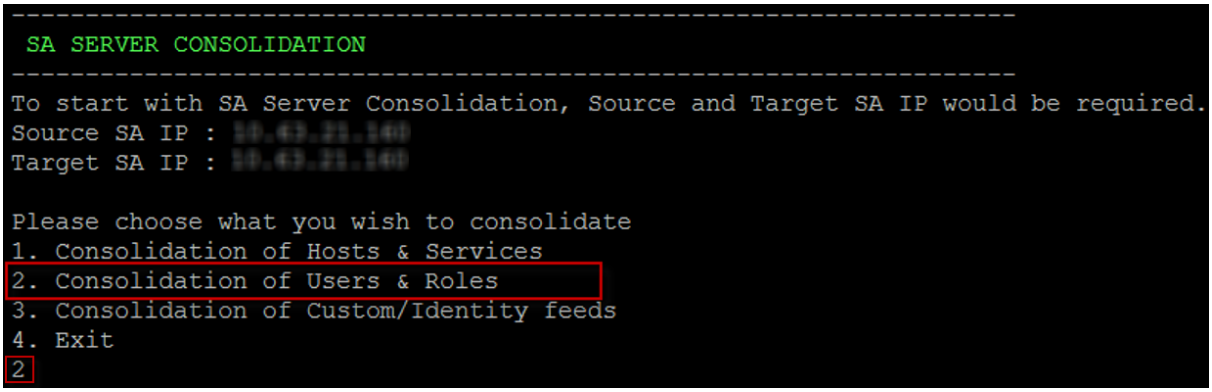


2. All the Hosts and Services data is consolidated.
   After the consolidation of Hosts and Services, you must manually enable the consolidated Hosts. For more information see, Security Analytics User Interface View Post Consolidation

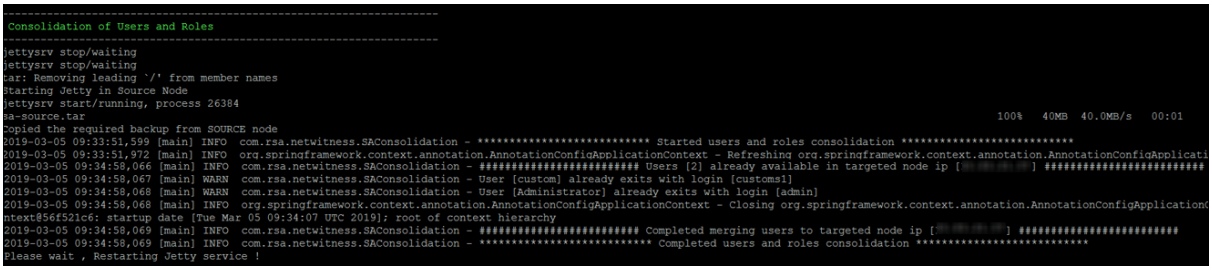


Option 2 – Consolidation of Users and Roles

1. Under the SA Server Consolidation option, select **Option 2** to begin the consolidation of Users and Roles.



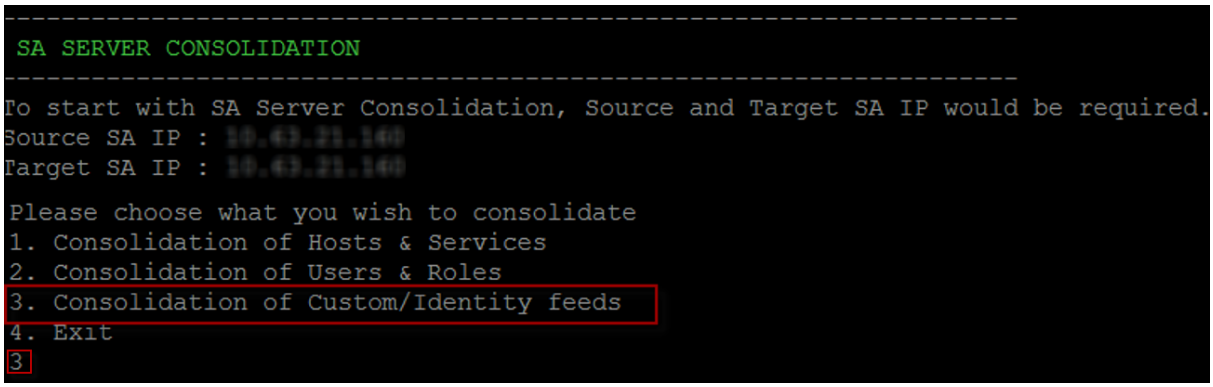
2. All the Users and Roles data is consolidated.



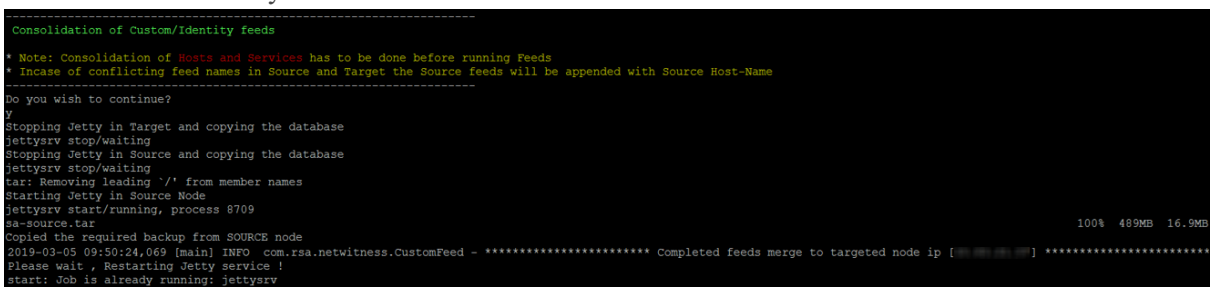
Option 3 – Consolidation of Custom/Identity feeds

Make sure you enable the Hosts after consolidation, before you begin to consolidate Custom/Identity feeds. For more information see, Security Analytics User Interface View Post Consolidation .

1. Under the SA Server Consolidation option, select **Option 3** to begin the consolidation of Custom/Identity Feeds.

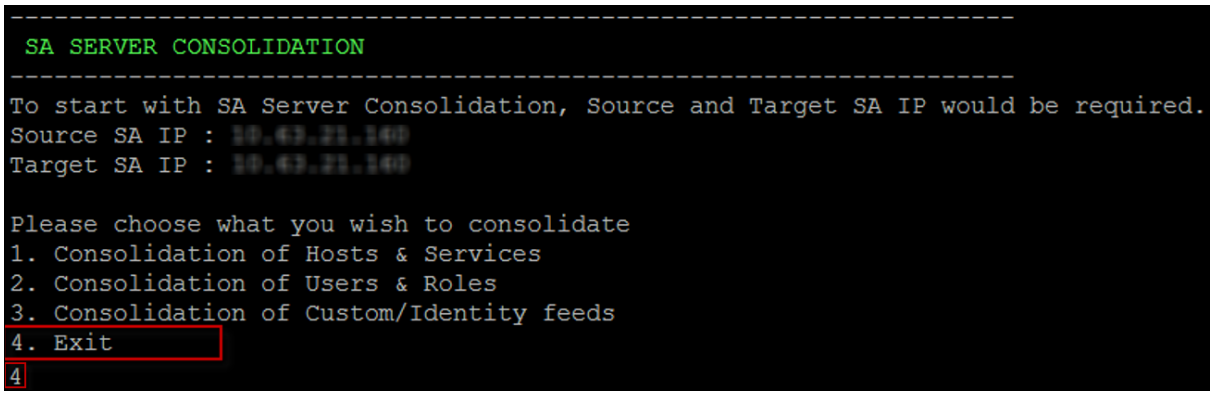


2. All the Custom/Identity Feeds data is consolidated.



Option 4 – Exit

1. Under the SA Server Consolidation option, select **Option 4** to exit the consolidation process. It exits from the command console.



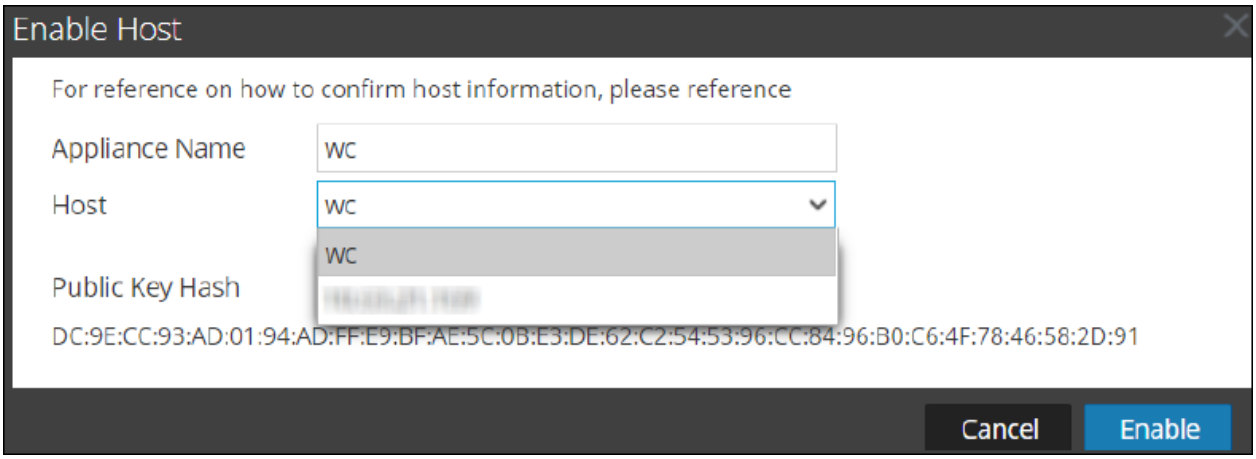
Note: If you exit the process after completing **Option 1**, you must re-run the script and initiate **Option 2** consolidation process.

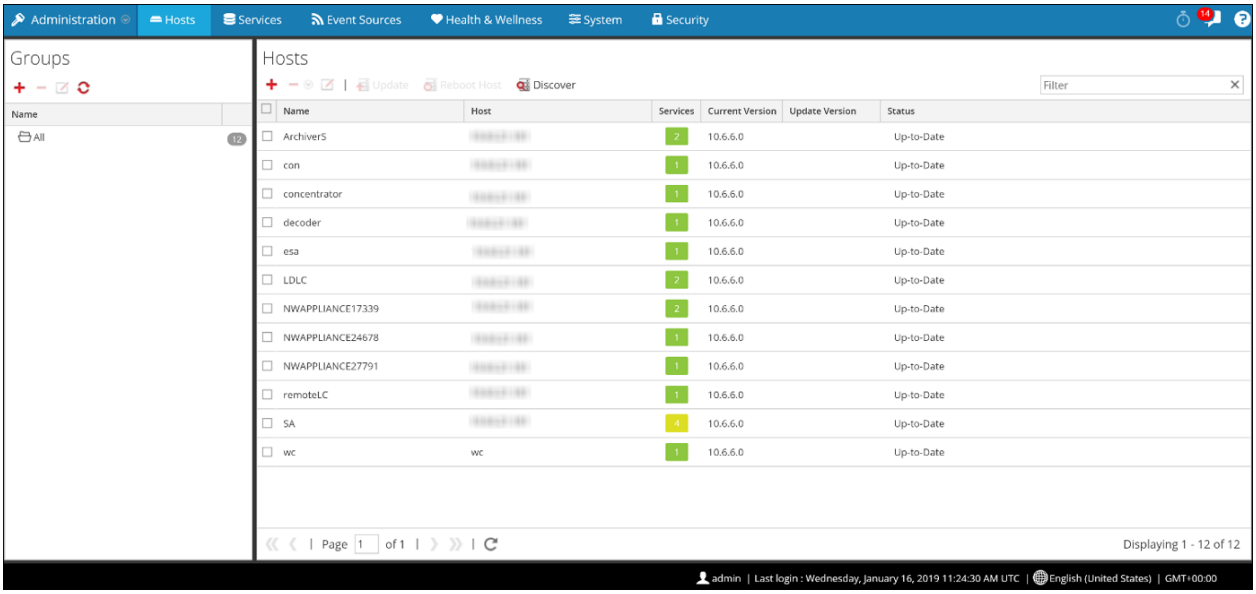
Security Analytics User Interface View Post Consolidation

After you complete SA consolidation process, the target node user interface will be displayed as follows:

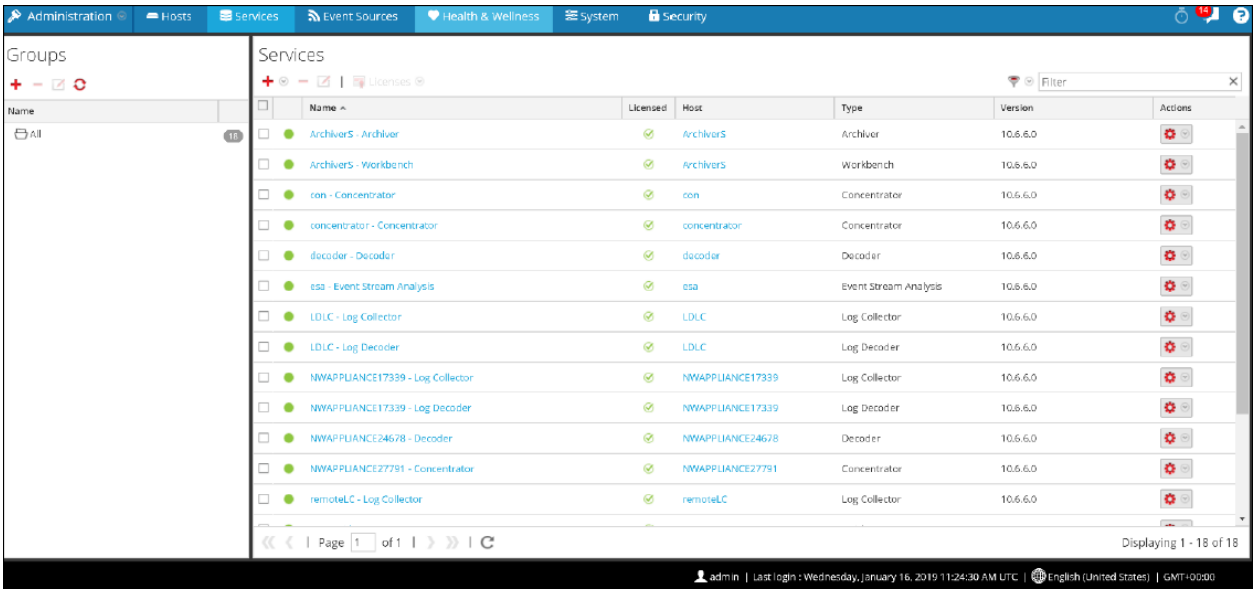
Hosts View

Note: Make sure you click **Enable** on the Hosts page and that the host name in the target node is same as in the source node.

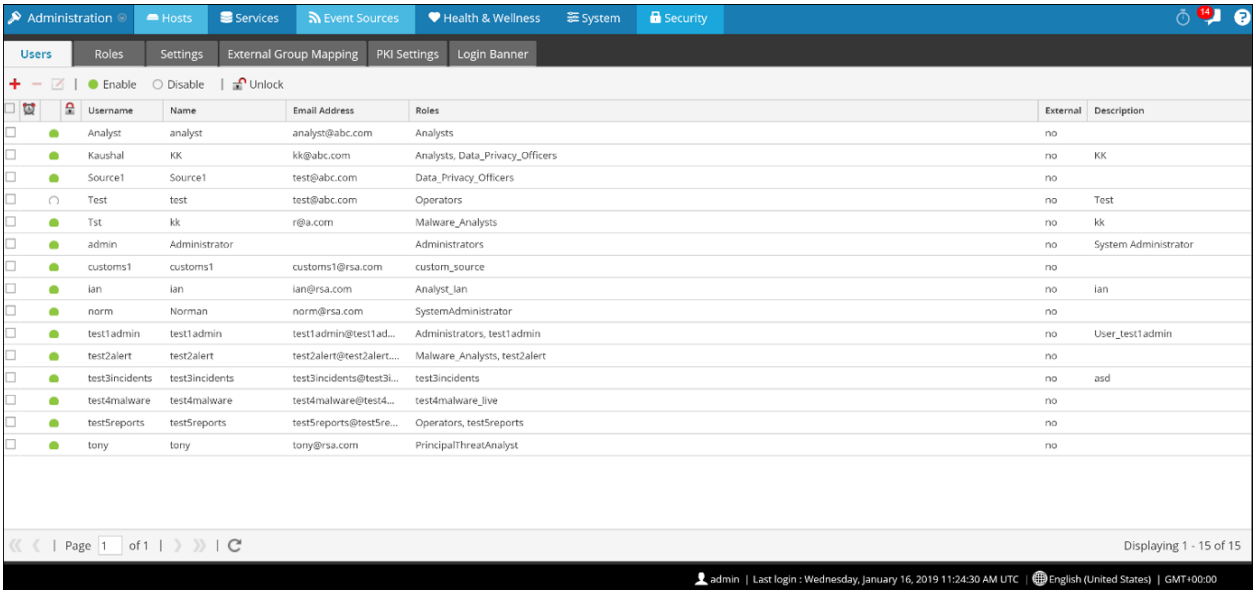




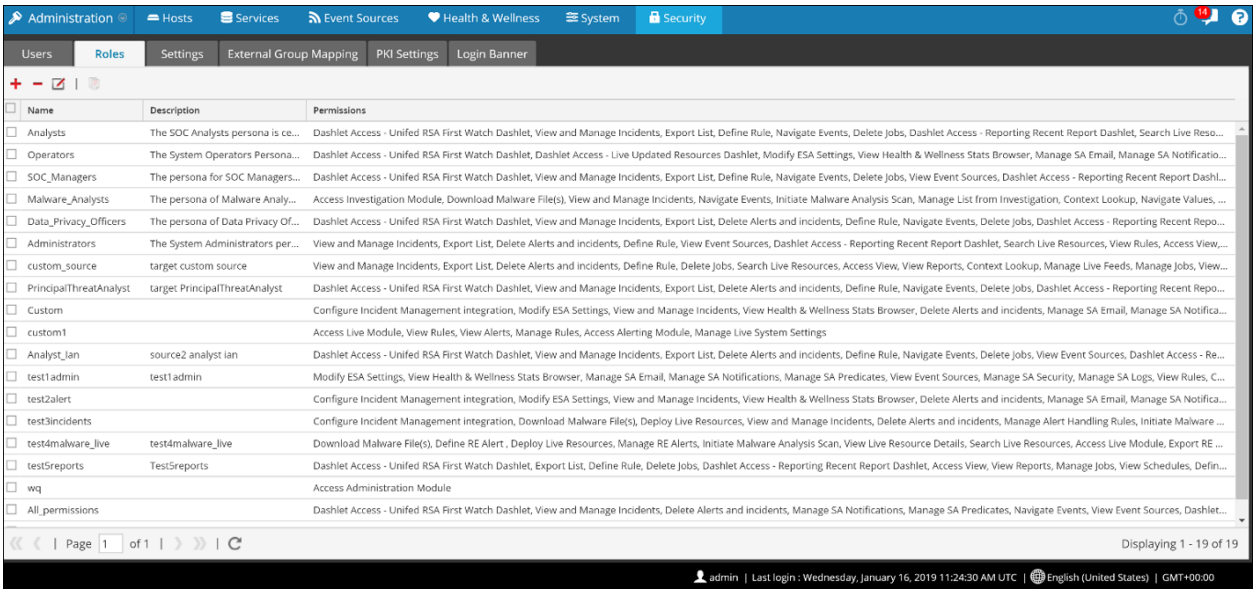
Services View



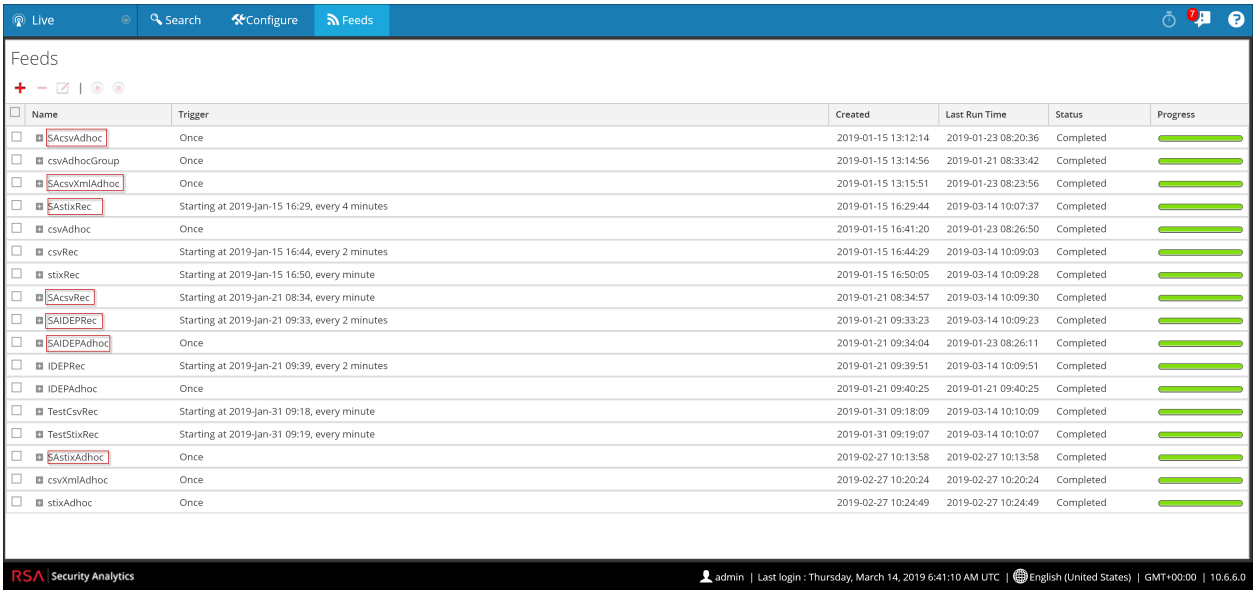
Users View



Roles View



Custom Feeds View



Note: The entries highlighted in red are the Custom Feeds that are consolidated.

Post Consolidation Task for Security Analytics

If you need consolidation of any other data and configurations, you can use the import and export feature available in Security Analytics or perform the configuration manually.

Troubleshooting Scenarios for SA Server Consolidation

Problem	Solution
When running hosts and services consolidation, execution log has “Connection failed to <appliance ip>”	Run `ssh-propagate` for the corresponding SA host on target SA again.
"Device <number> unavailable” or “Group <number> unavailable” for consolidated feeds in UI	Edit and Redeploy the feed manually.
When running Users and Roles consolidation, execution log has “ssh: connect to host <sa-ip> port 22: Connection refused”	Re-run ssh-propagate for the corresponding SA host on the target SA node.

Reporting Engine Consolidation

Before you begin the Reporting Engine consolidation process, you need to make sure that all the prerequisites are performed. RE consolidation is a tool used to consolidate configurations and data of multiple reporting-engine deployments. Make sure to have the required space on the target node for RE data consolidation.

The consolidation of Reporting Engine is a two-step process, after which the post-consolidation process begins:

1. **(Mandatory) Configuration Consolidation**: In this step all the RE configuration is consolidated all at once and a reporting-engine directory is created that contains all the consolidated configurations. It consolidated definitions of Rule/Report/Alert/Chart/List/Scheduler/alert_templates. You cannot consolidate data, until the configuration consolidation process is complete.
2. **(Optional) Data Consolidation**: In this step all the accumulated previous RE data is consolidated, one instance or multiple instance at a time depending upon the available space on the machine you choose for consolidation. In case you consolidate the data one instance at a time, then you can delete the data of the previously consolidated instance to optimize space. If you do not consolidate the data consolidation and if the data is available in the Core devices, you can regenerate the data later.

The following table describes the entities that will be consolidated as part of the RE consolidation process, if they exist in the RE instances:

Entities	Configurations	Data	Comments
Rule	Yes	NA*	
Report	Yes	Yes	
Report Group	Yes	NA*	Report Group structure is moved under group named with corresponding RE-instance-IP.
Rule Group	Yes	NA*	Rule Group structure is moved under group named with corresponding RE-instance-IP.
Alert	Yes	No**	
Chart	Yes	No**	

Entities	Configurations	Data	Comments
Chart Group	Yes	NA*	Chart Group structure is moved under group named with corresponding RE-instance-IP.
List	Yes	Yes	
List Group	Yes	NA*	List Group structure is moved under group named with corresponding RE-instance-IP.
Sub Reports / Iterative Reports	Yes	Yes	
Schedules	Yes	Yes	
Images / Logos	No**	Yes	Refer to the post consolidation tasks.
Warehouse Analytics	No**	No**	
Alert Templates	Yes	NA*	
Permissions	Yes	Yes	The Administrator must provide the required permissions for the new RE-instance-IP groups from the SA UI.

NA* - Not Applicable, No** - Applicable but tool does not perform the task.

Prerequisites for Reporting Engine Data Consolidation:

Make sure to check the following:

You have enough space for backup on the target node.

Run the following commands on source nodes and manually add the total disk usage size of individual source to get the disk space required in the target node.

a. Check the space for configuration using the command:
```
du -cbh /home/rsasoc/rsa/soc/reporting-engine/statusdb | grep total
```

b. Check the space for data using the command:
```
du -cbh /home/rsasoc/rsa/soc/reporting-engine/resultstore | grep total
```

To determine space available for the partition, run the following commands on the target node:

a. `df -kh /var/netwitness/database`

b. `df -kh /home/rsasoc/`

Space available in the combined partition of **/home/rsasoc and /var/netwitness/database** for target instance 10.1.1.3 should be more than

2 X (Space used by **/home/rsasoc/rsa/soc/reporting-engine/statusdb** and **/home/rsasoc/rsa/soc/reporting-engine/resultstore** for 10.1.1.1 and 10.1.1.2 instances)

Let's consider the following space assumptions of the instances.

10.1.1.1 : space used by **/home/rsasoc/rsa/soc/reporting-engine/statusdb** = 2GB

10.1.1.1 : space used by **/home/rsasoc/rsa/soc/reporting-engine/resultstore** = 100GB

10.1.1.2 : space used by **/home/rsasoc/rsa/soc/reporting-engine/statusdb** = 1GB

10.1.1.2: space used by **/home/rsasoc/rsa/soc/reporting-engine/resultstore** = 200GB

Total space in source nodes 10.1.1.1 and 10.1.1.2 = 2GB + 100GB + 1GB + 200GB = 303GB

Total minimum space required in partition **/home/rsasoc/** on target machine 10.1.1.3 = 303GB

Total space required in partition **/var/netwitness/database** on target machine 10.1.1.3= 303 GB

Total space required in target 10.1.1.3 = 606GB

Note: To determine this space use the command `df -kh`. It is recommended to have 303 GB available space in the target node of **/var/netwitness/database** partition for data consolidation of all instances at once. In case space is not available, you can perform the data consolidation of an instance one-by-one and hence approximately a minimum of 200 GB (space of 10.1.1.2) will be required as per the above example.

Using the Tool

Run the consolidation tool and select the relevant option based on your requirements.

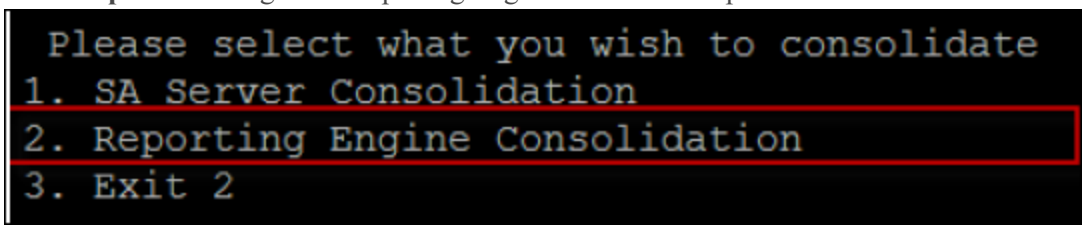
1. SSH to the target node and run the script `rsa-nw-consolidator.sh`
   The log in command window is displayed.

```
[root@NWAPPLIANCE10909 rsa-nw-consolidator]# ./rsa-nw-consolidator.sh

************************************ NW-CONSOLIDATOR SCRIPT ************************************************ *
* ************************ CONSOLIDATION IS ONLY SUPPORTED FOR SA VERSION 10.6.6 only ********************** *
* *                                                                                                          * *
* *      The following are supported for Consolidation                                                       * *
* *                                                                                                          * *
* *               - Host and Services                                                                        * *
* *                    * Consolidate Hosts and Services on multiple NW Servers to one NW Server.             * *
* *               - Users and Roles                                                                          * *
* *                    * Consolidate Users and Roles on multiple NW Servers to one NW Server.               * *
* *               - Custom/Identity Feeds                                                                    * *
* *                    * Consolidate Custom and Identity feeds on multiple NW Servers to one NW Server.     * *
* *               - Reporting Engine                                                                         * *
* *                    * Consolidate Rules, Reports, Alerts, Charts and Lists to one NW Server.             * *
* *                                                                                                          * *
* *            Note: Run the Backup script before running this script                                        * *
* ************************************************************************************************************
************************************************************************************************************

Select an action you want to perform
1. SA Server Consolidation
2. Reporting Engine Consolidation
3. Exit
```

2. Select **Option 2** to begin the Reporting Engine consolidation process.

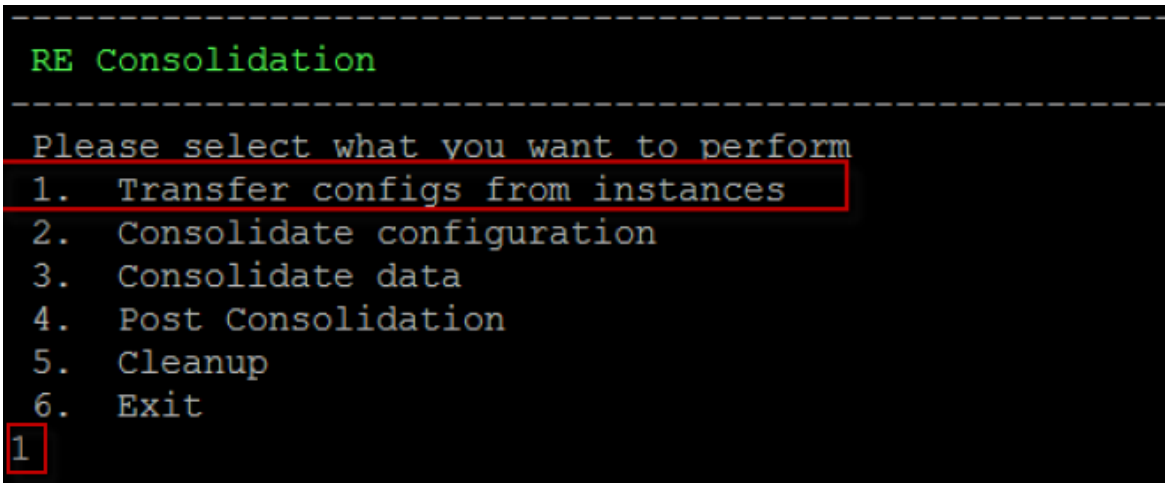


(Mandatory) Option 1 – Transfer Configs from Instances

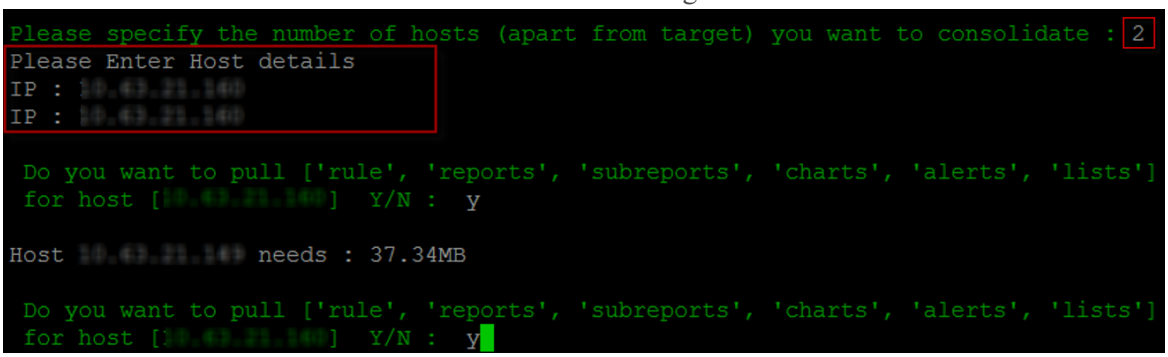
This option pulls the definition data of Rule, Report, Schedule, Alert, and List from the **/home/rsasoc/rsa/soc/reporting-engine** directory of every RE instance.

It does not pull the `resultstore` directory from these instances. The `resultstore` directory contains the previous data of RE.

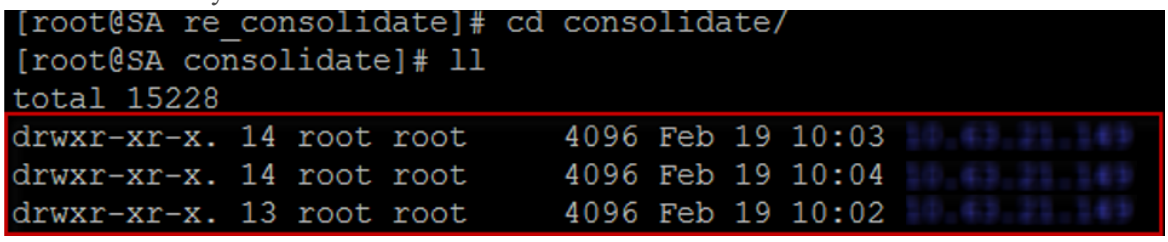
1. Under the Reporting Engine Consolidation option, select **Option 1** to begin to pull the reporting-engine directory from RE instances.



2. Enter the number of RE instances to be consolidated along with their IP addresses.

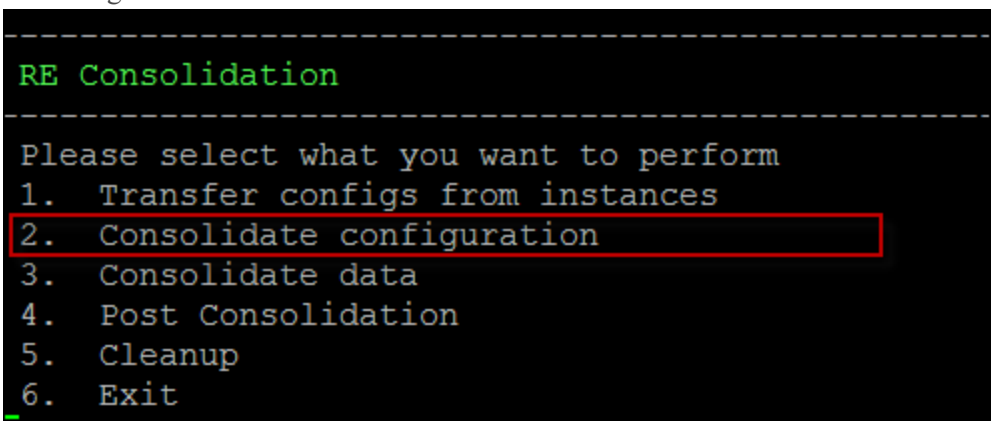


3. After the process is completed the consolidated directory displays the RE instance directory. Separate directories are created for each instance at **/home/rsasoc/rsa/soc/reporting-engine** and are named with the IP of the RE instance. For the local RE instance, the name of the directory created will always be 127.0.0.1.

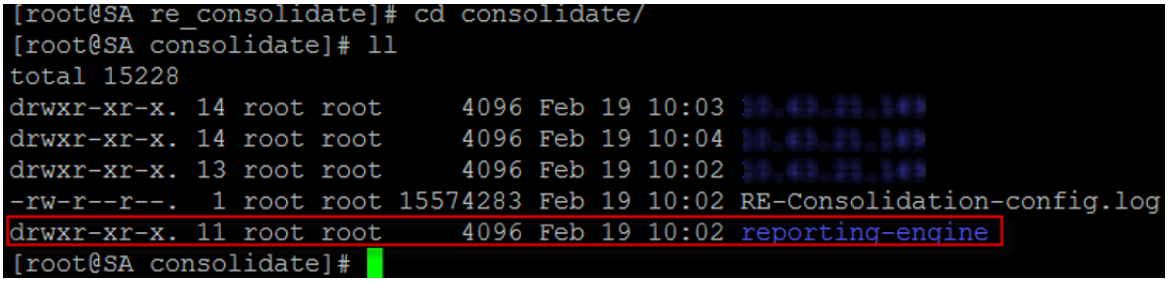


(Mandatory) Option 2 – Consolidate Configurations

1. Under the Reporting Engine Consolidation option, select **Option 2** to begin the consolidation of the configurations from all the RE instances.



2. After the process is completed a reporting-engine consolidated directory is created at **/home/rsasoc/rsa/soc/reporting-engine** which contains the configurations of all the RE instances.



(Optional) Option 3 – Consolidate Data

You must have completed the **Option 2**- Consolidate Configuration process successfully, before you start **Option 3** for data consolidation. This step consolidates the data of multiple RE instances.

To consolidate the data, manually copy the directory to the corresponding host IP directory created in Option 1.

For example:

After option 1 is completed, the following directories are created:

1. `/var/netwitness/database/re_consolidate /consolidate/10.1.1.1`
2. `/var/netwitness/database/re_consolidate /consolidate/10.1.1.2`

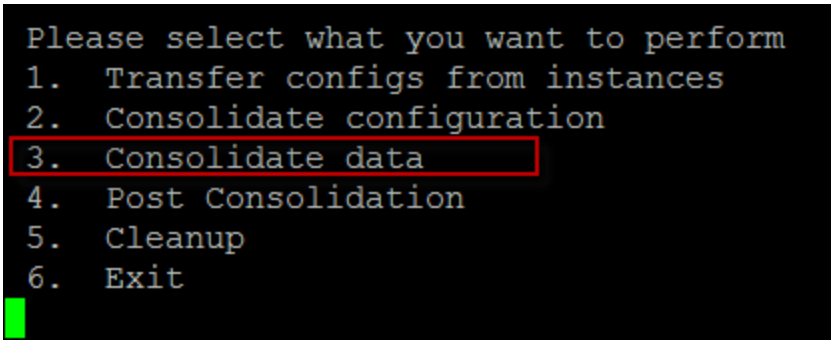
From the 10.1.1.1 host, manually copy **/home/rsasoc/rsa/soc/reporting-engine/resultstore** to **/var/netwitness/database/re_consolidate /consolidate/10.1.1.1**.

And,

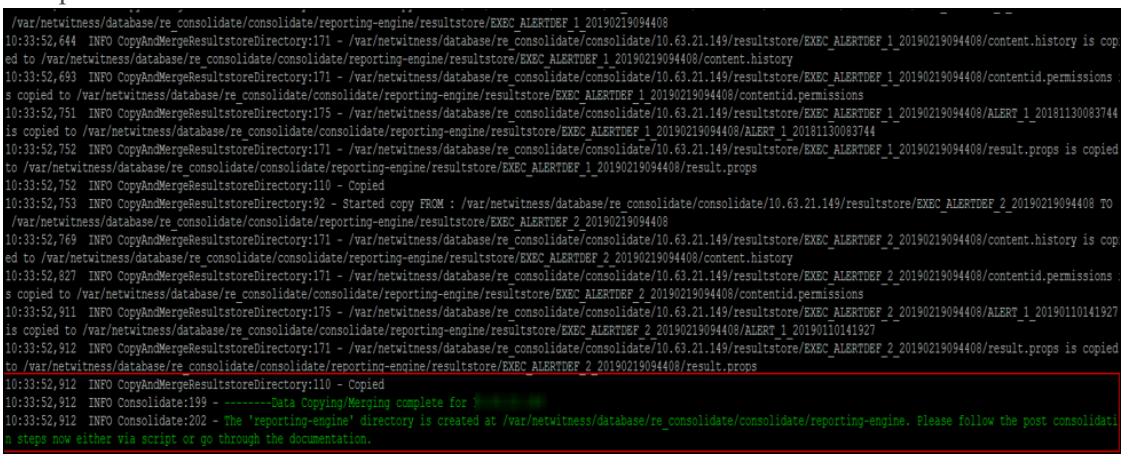
From 10.1.1.1 host, manually copy **/home/rsasoc/rsa/soc/reporting-engine/resultstore** to **/var/netwitness/database/re_consolidate/consolidate/10.1.1.2**

Note: The above process can be done either one-by-one or all instances together, depending on the space available on the target node. For single IP data consolidation, enter the RE IP one at a time.For multiple IP data consolidation, enter the RE IP's separated by comma. For example, `10.10.10.10,10.10.10.20,host` For host or target data consolidation, enter the **host** instead of an IP.

1. Under the Reporting Engine Consolidation option, select **Option 3** to consolidate the data from all the RE instances.



2. After the process is completed a message is displayed confirming the consolidation of data of the specified RE instance.



(Mandatory) Option 4 – Post Consolidation

1. Under the Reporting Engine Consolidation option, select **Option 4** to begin the post consolidation tasks on the target node.

```
------------------------------------------------------------------
 RE Consolidation
------------------------------------------------------------------
 Please select what you want to perform
 1.  Transfer configs from instances
 2.  Consolidate configuration
 3.  Consolidate data
 4.  Post Consolidation
 5.  Cleanup
 6.  Exit
4
Please make sure that data consolidation for all the nodes are performed.
Partial 'Consolidate configuration' or 'Consolidate data' cannot be done,
once the 'Post consolidation' is performed.
Do you want to continue with Post Consolidation Y/N ?
```

2. After the process is completed a message is displayed confirming the completion of the post consolidation tasks.

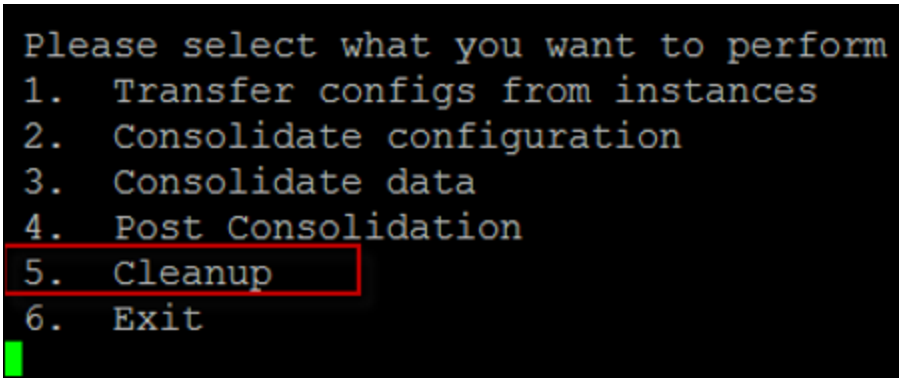
```
 Please select what you want to perform
 1.  Transfer configs from instances
 2.  Consolidate configuration
 3.  Consolidate data
 4.  Post Consolidation
 5.  Cleanup
 6.  Exit
4
Please make sure that data consolidation for all the nodes are performed.
Partial 'Consolidate configuration' or 'Consolidate data' cannot be done,
once the 'Post consolidation' is performed.
Do you want to continue with Post Consolidation Y/N ? y

PERFORMING POST CONSOLIDATION
This needs multiple service restarts
Stopping reporting-engine...
stop: Unknown instance:
creating backup of the current reporting-engine
replace reporting-engine in the RE directory
changing owner to rsasoc
restarting reporting-engine
renaming conf file.
Applying config changes this will take some time . Please wait...
copy conf file to reporing-engine folder
Starting reporting-engine
Starting jetty service
Post consolidation completed..
```

(Optional) Option 5 – Cleanup

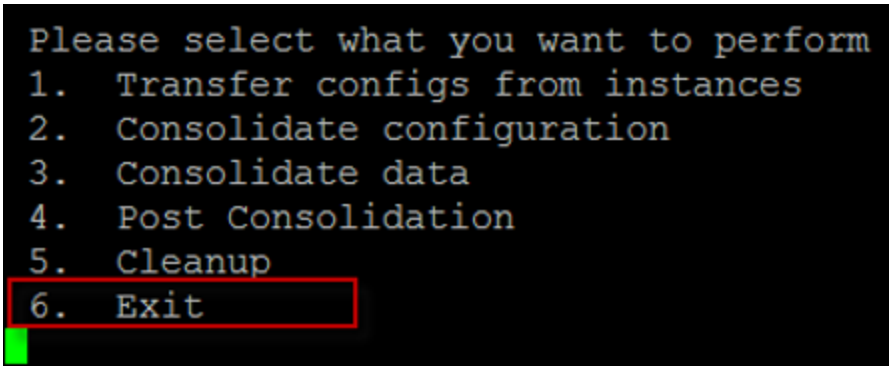
The **Option 5** deletes all the temporary directories and not the configurations that are already pulled. The **re_consolidate** directory is available to start from **Option 2**.

1. Under the Reporting Engine Consolidation option, select option 5 to clean-up the unwanted data and configurations from the target node.



(Optional) Option 6 – Exit

1. Under the Reporting Engine Consolidation option, select **Option 6** to exit the consolidation process at any time.



Manual Steps for RE Consolidation

At any point, if the consolidation tool fails and you want to run RE consolidation process manually, you can run the manual commands and complete the process.

The following table provides the equivalent commands for each option, to perform the consolidation process manually.

Option	Menu	Equivalent Manual Steps
1	**Transfer configs from instances**	**Perform this step using the `rsa-nw-consolidator.sh` script and choose Option 1 of Reporting Engine .**

Option	Menu	Equivalent Manual Steps
2	Consolidate Configuration	1. Obtain the `RSA-RE-Consolidation.jar` from from tool bin folder. 2. Place the jar in `/var/netwitness/database/re_consolidate/` 3. Run the command: `cd /var/netwitness/database/re_consolidate/` 4. Run the script `java -jar RSA-RE-Consolidation.jar -repository consolidate/` **Note**:Before running the `java -jar`, make sure all the directories of the RE instances are available at `/var/netwitness/database/re_consolidate/consolidate` directory. And are renamed appropriately with the IP of the specific instance.

<table>
<tr><th>Option</th><th>Menu</th><th>Equivalent Manual Steps</th></tr>
<tr><td>3</td><td>Consolidate data</td><td>This is a manual step. After you complete the above mentioned manual step, you must trigger the jar as follows:
<table>
<tr><th>Command</th><th>Action Performed</th></tr>
<tr><td><code>java -jar RSA-RE-Consolidation-1.0.jar -data <IP1></code></td><td>Consolidates the data from IP1 only.</td></tr>
<tr><td><code>java -jar RSA-RE-Consolidation-1.0.jar -data <IP1, IP2></code></td><td>Consolidates the data from IP1 and IP2.
Note: Make sure you have enough space before executing this option.
To calculate the space required, perform the following:
<code>total space of the /home/rsasoc/rsa/soc/reporting-engine/resultstore on IP1 instance + total space of the /home/rsasoc/rsa/soc/reporting-engine/resultstore space of IP2 instance * 2</code>
Note 1: Make sure you have this space available in the partition <code>/home/rsasoc/</code>
Note 2: Make sure you have enough space available in the partition <code>/var/netwitness/</code></td></tr>
<tr><td><code>java -jar RSA-RE-Consolidation-1.0.jar -data <IP1, IP2, host></code></td><td>Consolidates the data from IP1, IP2 and target or host machine.
Note: Make sure you have enough space before executing this option.</td></tr>
<tr><td><code>java -jar RSA-RE-Consolidation-1.0.jar -data</code></td><td>Consolidates the data from host or target machine i.e 127.0.0.1.</td></tr>
</table></td></tr>
</table>

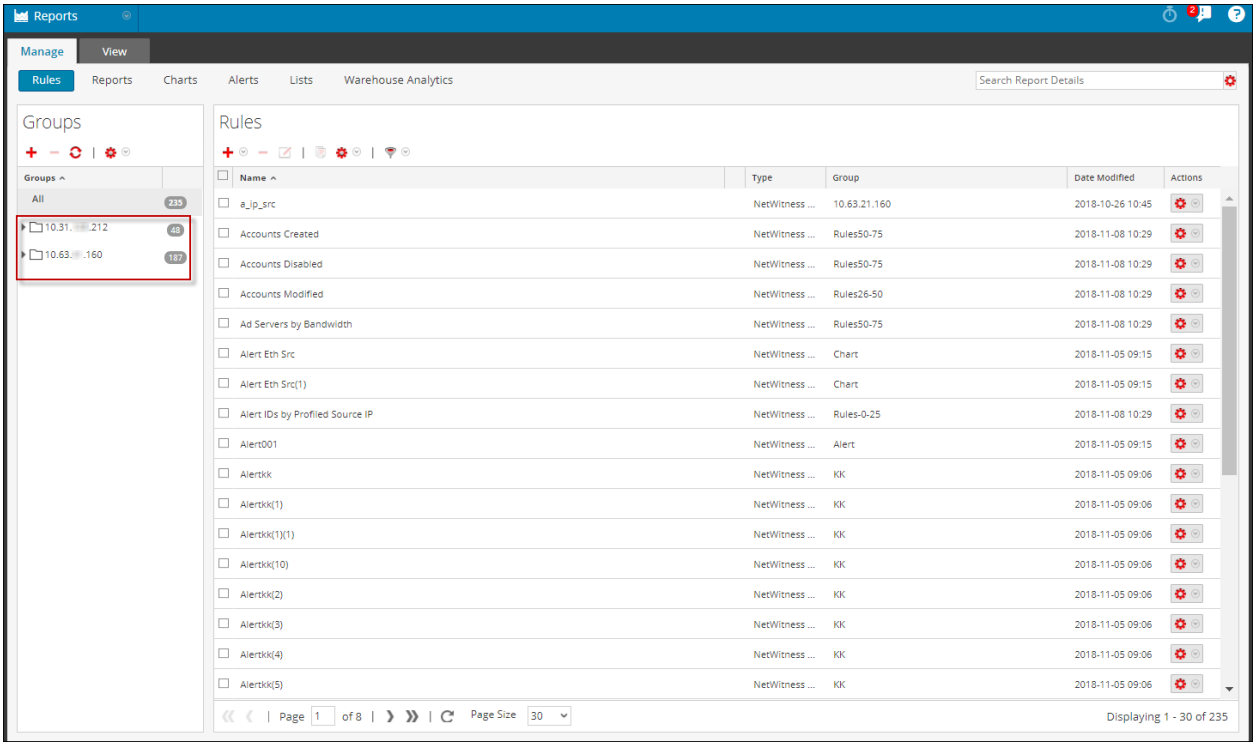
Option	Menu	Equivalent Manual Steps
		`host`
4	Post Consolidation	Perform the post consolidation using the following commands: 1. Stop RE service using the command `rsasoc_re`. 2. Rename the existing reporting-engine directory from `/home/rsasoc/rsa/soc/reporting-engine` to `/home/rsasoc/rsa/soc/reporting-engine_old`. This takes a backup of the host and target RE data. 3. Copy the reporting-engine directory from `/var/netwitness/database/re_consolidate/consolidate/reporting-engine` to `/home/rsasoc/rsa/soc/reporting-engine` 4. Change the primary and secondary owner of the new reporting-engine directory using the command `#chown -R rsasoc:rsasoc /home/rsasoc/rsa/soc/reporting-engine` 5. Start the reporting-engine service using the command `rsasoc_re`. Wait for RE service to be up and running. 6. Stop `rsasoc_re` 7. Delete the `/home/rsasoc/rsa/soc/reporting-engine/conf` directory. 8. Rename `/home/rsasoc/rsa/soc/reporting-engine/conf_renameToconfAfter1stStartStop` to `/home/rsasoc/rsa/soc/reporting-engine/conf`. 9. Start `rsasoc_re` and check if RE service is up and running. 10. Stop `jettysrv` 11. Start `jettysrv`
5	Cleanup	# rm –rf /var/netwitness/database/re_consolidate /consolidate/reporting-engine
6	Exit	Exits the consolidation process.

Reporting Engine User Interface View Post Consolidation

After you complete the RE consolidation process, the target node UI will be displayed as follows.

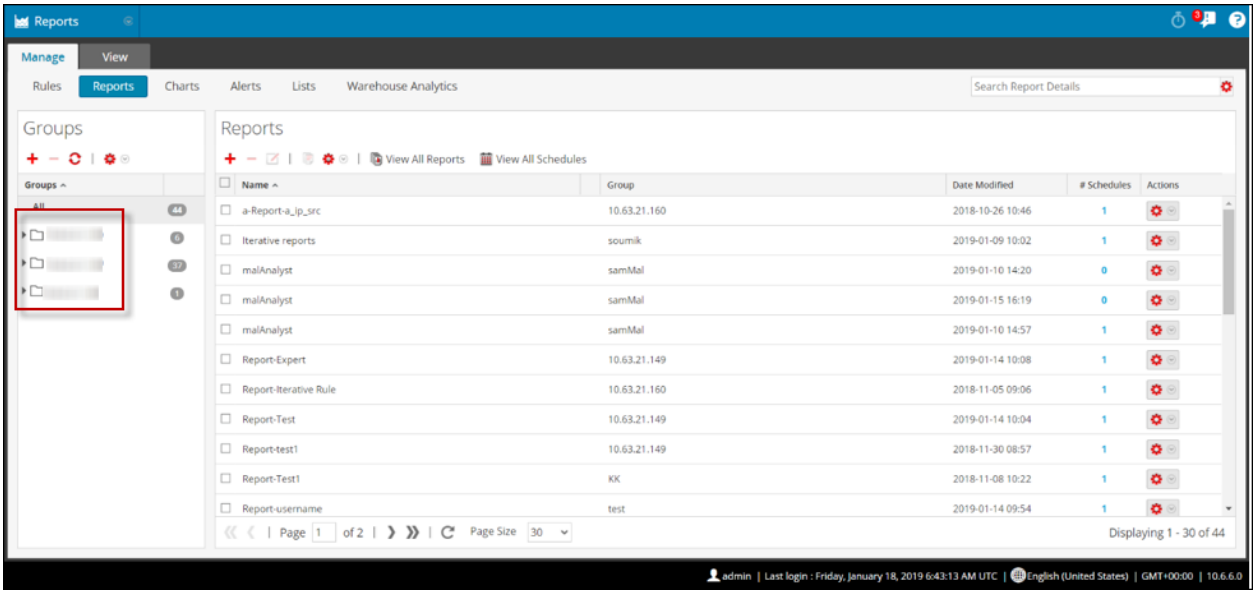
Rules Page

Displays all the consolidated rules of the RE instances in a group named after the instance IP. Target node IP is displayed as 127.0.0.1.



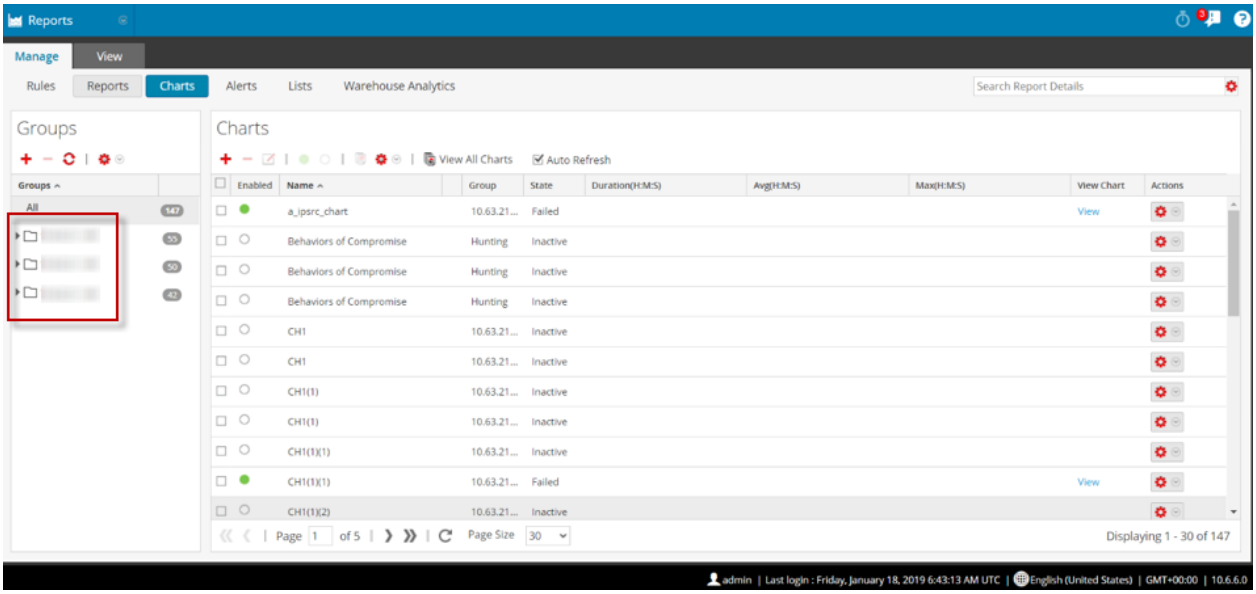
Reports Page

Displays all the consolidated reports of the RE instances in a group named after the instance IP.

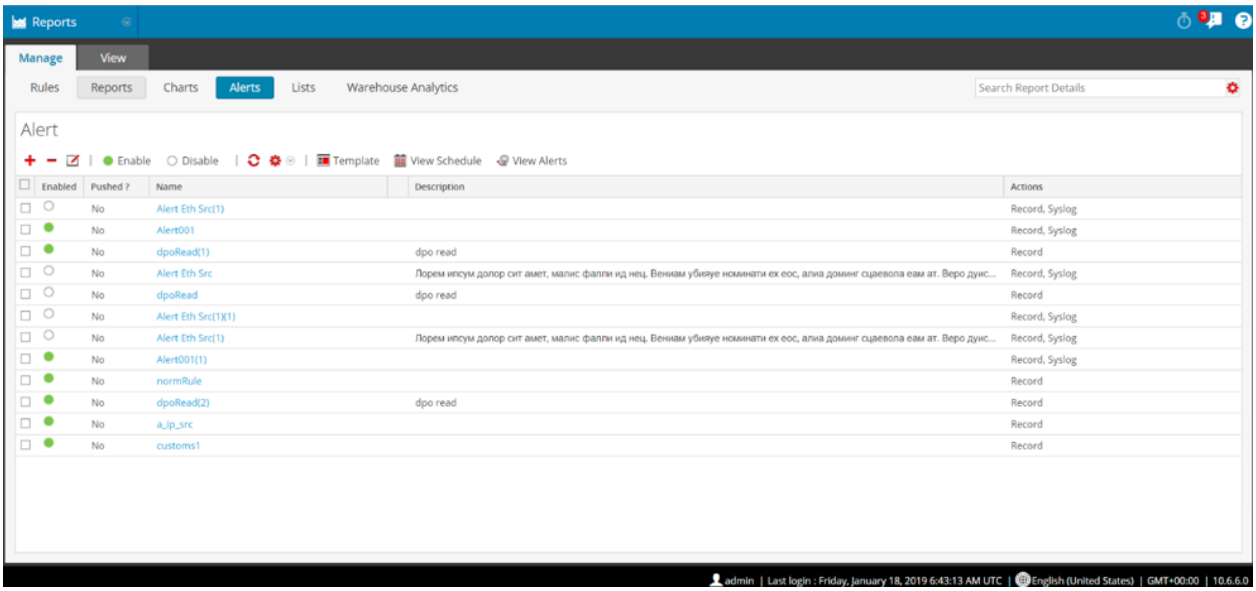


Charts Page

Displays all the consolidated charts of the RE instances in a group named after the instance IP.

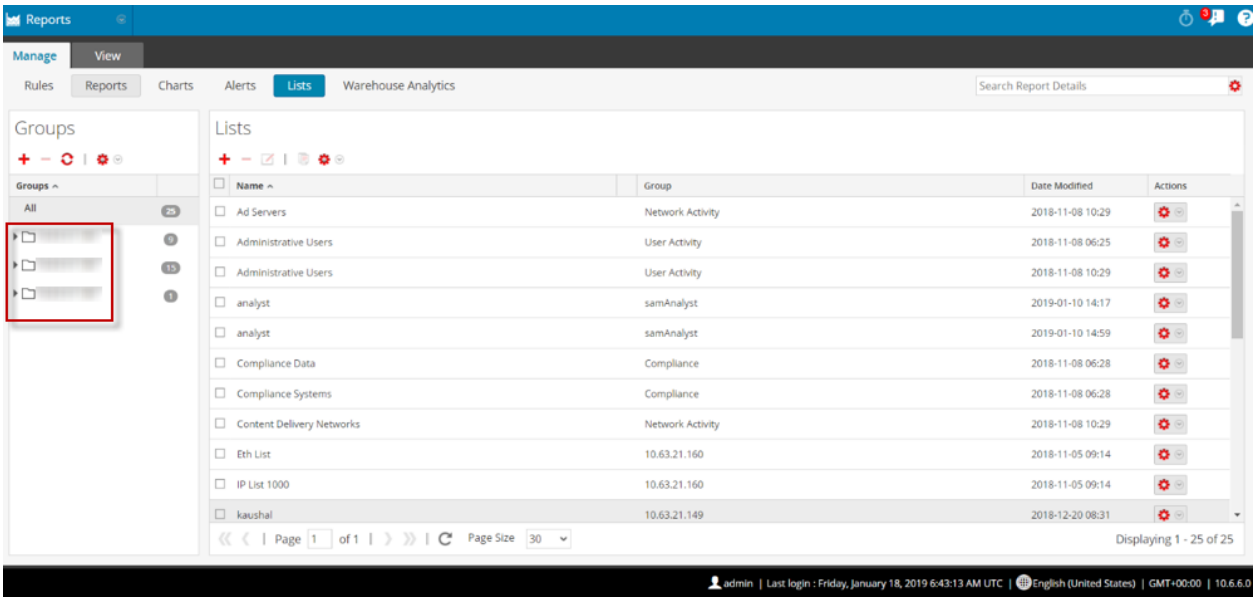


Alerts Page



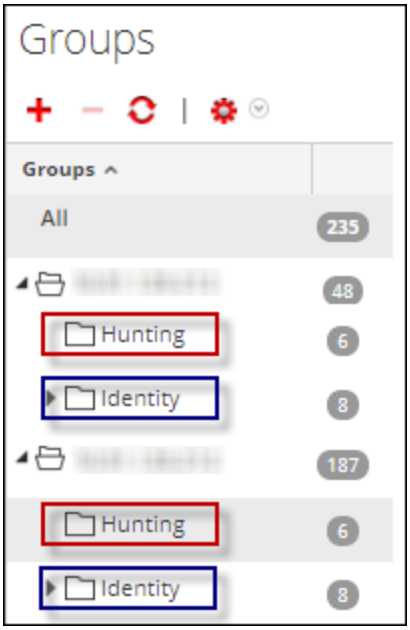
Lists Page

Displays all the consolidated lists of the RE instances in a group named after the instance IP.



OOTB View

If you have the same OOTB rules and charts across sources nodes, they appear as duplicate groups in the target node.



Post Consolidation Task for Reporting Engine

1. You must add data sources to the reporting engine. You must then configure the data source for Reports by navigating to **Reports** > **Schedules** > **Edit Schedule**.

2. The consolidated images files are located at `/home/rsasoc/rsa/soc/reporting-engine/images` on the target node and are named in IMAGE_<number>_<DateTimeStamp> format. You can rename the images file and edit the file format to .png or .jpeg, or .jpg and import them into the target RE instance.
3. The Administrator must provide the required permissions for the new RE-instance-IP groups from the SA UI.

Troubleshooting Scenarios for Reporting Engine

Problem	Solution
Unable to view the roles and permissions of the entities	Restart SA
Unable to view the data sources in the schedule page	Add the data sources
OOTB rules and charts are duplicated	Functions as designed
After entering the source or target IP, "**Authentication failed**" error message is displayed shown	Re-run `ssh-propagate` for the corresponding SA host
If authorized user is not able to see respective entities	The Administrator must provide the required permissions for the new RE-instance-IP groups from the SA UI

Contact Customer Care

When you are ready to consolidate the configuration and data, you must work with the RSA Professional Services team or Customer Support. Do not use the rsa-nw-consolidator script without assistance. For information about how to contact Customer Support, go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).