



# SA and RE Consolidation Tool Guide



Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

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

## **Trademarks**

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

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

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

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

## **Third-Party Licenses**

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

## **Note on Encryption Technologies**

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

## **Distribution**

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

March 2019

# Contents

---

<b>Overview of Consolidation Tool</b> .....	<b>5</b>
Prerequisites .....	5
Back Up Commands .....	5
SSH Propagate Commands .....	5
Tool Location .....	6
Tool Contents .....	6
<b>SA Server Consolidation</b> .....	<b>7</b>
Using the Tool .....	7
Option 1 – Consolidation of Hosts and Services .....	8
Option 2 – Consolidation of Users and Roles .....	9
Option 3 – Consolidation of Custom/Identity feeds .....	9
Option 4 – Exit .....	10
Security Analytics User Interface View Post Consolidation .....	10
Hosts View .....	11
Services View .....	12
Users View .....	12
Roles View .....	13
Custom Feeds View .....	13
Post Consolidation Task for Security Analytics .....	13
Troubleshooting Scenarios for SA Server Consolidation .....	14
<b>Reporting Engine Consolidation</b> .....	<b>15</b>
Prerequisites for Reporting Engine Data Consolidation: .....	16
Using the Tool .....	17
(Mandatory) Option 1 – Transfer Configs from Instances .....	18
(Mandatory) Option 2 – Consolidate Configurations .....	20
(Optional) Option 3 – Consolidate Data .....	20
(Mandatory) Option 4 – Post Consolidation .....	21
(Optional) Option 5 – Cleanup .....	22
(Optional) Option 6 – Exit .....	23
Manual Steps for RE Consolidation .....	23
Reporting Engine User Interface View Post Consolidation .....	26
Rules Page .....	27

Reports Page .....	27
Charts Page .....	28
Alerts Page .....	28
Lists Page .....	28
OOTB View .....	29
Post Consolidation Task for Reporting Engine .....	29
Troubleshooting Scenarios for Reporting Engine .....	30
<b>Contact Customer Care .....</b>	<b>31</b>

# 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 <b>groups</b> 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.

```
[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 1** to begin the SA Server consolidation process.

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

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

```
-----
SA SERVER CONSOLIDATION
-----
To start with SA Server Consolidation, Source and Target SA IP would be required.
Source SA IP : 10.43.21.140
Target SA IP : 10.43.21.140

Please choose what you wish to consolidate
1. Consolidation of Hosts & Services
2. Consolidation of Users & Roles
3. Consolidation of Custom/Identity feeds
4. Exit
```

## 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.

```
-----
SA SERVER CONSOLIDATION
-----
To start with SA Server Consolidation, Source and Target SA IP would be required.
Source SA IP :
Target SA IP :

Please choose what you wish to consolidate
1. Consolidation of Hosts & Services
2. Consolidation of Users & Roles
3. Consolidation of Custom/Identity feeds
4. Exit
```



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](#)

```
-----
Consolidation of Hosts & Services
-----
2019-03-05 09:27:00,479 [main] INFO com.rsa.netwitness.consolidation.NwConsolidator - **** Source Node ( ) is going to stop all require services ****
2019-03-05 09:27:06,938 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - [Stopping puppetmaster: [ OK ]]
2019-03-05 09:27:06,944 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - service puppetmaster stop - Done!
2019-03-05 09:27:09,455 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - [Shutting down mcollective: [ OK ]]
2019-03-05 09:27:09,456 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - service mcollective stop - Done!
2019-03-05 09:27:13,935 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - [Stopping puppet agent: [ OK ]]
2019-03-05 09:27:13,935 [main] INFO com.rsa.netwitness.consolidation.utilities.CommonOperations - service puppet stop - Done!
```

## 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.

```
-----
SA SERVER CONSOLIDATION
-----
To start with SA Server Consolidation, Source and Target SA IP would be required.
Source SA IP : 
Target SA IP : 

Please choose what you wish to consolidate
1. Consolidation of Hosts & Services
2. Consolidation of Users & Roles
3. Consolidation of Custom/Identity feeds
4. Exit
2
```

2. All the Users and Roles data is consolidated.

```
-----
Consolidation of Users and Roles
-----
jettyshv stop/waiting
jettyshv stop/waiting
tar: Removing leading '/' from member names
Starting Jetty in Source Node
jettyshv start/running, process 26384
sa-source.tar                               100% 40MB 40.0MB/s 00:01
Copied the required backup from SOURCE node
2019-03-05 09:33:51,599 [main] INFO com.rsa.netwitness.SAConsolidation - ***** Started users and roles consolidation *****
2019-03-05 09:34:58,066 [main] INFO com.rsa.netwitness.SAConsolidation - ##### Users [2] already available in targeted node ip [ ] #####
2019-03-05 09:34:59,067 [main] WARN com.rsa.netwitness.SAConsolidation - User [custom] already exists with login [custom]
2019-03-05 09:34:58,068 [main] WARN com.rsa.netwitness.SAConsolidation - User [Administrator] already exists with login [admin]
2019-03-05 09:34:58,068 [main] INFO org.springframework.context.annotation.AnnotationConfigApplicationContext - Closing org.springframework.context.annotation.AnnotationConfigApplicationContext
ntext856f521c6: startup date [Tue Mar 05 09:34:07 UTC 2019]: root of context hierarchy
2019-03-05 09:34:58,069 [main] INFO com.rsa.netwitness.SAConsolidation - ##### Completed merging users to targeted node ip [ ] #####
2019-03-05 09:34:59,069 [main] INFO com.rsa.netwitness.SAConsolidation - ***** Completed users and roles consolidation *****
Please wait , Restarting Jetty service !
```

## 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.

```

-----
SA SERVER CONSOLIDATION
-----
To start with SA Server Consolidation, Source and Target SA IP would be required.
Source SA IP : 10.43.21.140
Target SA IP : 10.43.21.140

Please choose what you wish to consolidate
1. Consolidation of Hosts & Services
2. Consolidation of Users & Roles
3. Consolidation of Custom/Identity feeds
4. Exit
3
    
```

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

```

-----
Consolidation of Custom/Identity feeds
-----
* Note: Consolidation of Hosts and Services has to be done before running Feeds
* In case of conflicting feed names in Source and Target the Source feeds will be appended with Source Host-Name
-----
Do you wish to continue?
y
Stopping Jetty in Target and copying the database
jettyshv stop/waiting
Stopping Jetty in Source and copying the database
jettyshv stop/waiting
tar: Removing leading '/' from member names
Starting Jetty in Source Node
jettyshv start/running, process 8709
sa-source.tar                               100% 489MB 16.9MB
Copied the required backup from SOURCE node
2019-03-05 09:50:24,069 [main] INFO com.rsa.netwitness.CustomFeed - ***** Completed feeds merge to targeted node ip [10.43.21.140] *****
Please wait , Restarting Jetty service !
start: Job is already running: jettyshv
    
```

### Option 4 – Exit

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

```

-----
SA SERVER CONSOLIDATION
-----
To start with SA Server Consolidation, Source and Target SA IP would be required.
Source SA IP : 10.43.21.140
Target SA IP : 10.43.21.140

Please choose what you wish to consolidate
1. Consolidation of Hosts & Services
2. Consolidation of Users & Roles
3. Consolidation of Custom/Identity feeds
4. Exit
4
    
```

**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:



## Services View

Name	Licensed	Host	Type	Version	Actions
ArchiverS - Archiver	✓	ArchiverS	Archiver	10.6.6.0	[Settings] [Refresh]
ArchiverS - Workbench	✓	ArchiverS	Workbench	10.6.6.0	[Settings] [Refresh]
con - Concentrator	✓	con	Concentrator	10.6.6.0	[Settings] [Refresh]
concentrator - Concentrator	✓	concentrator	Concentrator	10.6.6.0	[Settings] [Refresh]
decoder - Decoder	✓	decoder	Decoder	10.6.6.0	[Settings] [Refresh]
esa - Event Stream Analysis	✓	esa	Event Stream Analysis	10.6.6.0	[Settings] [Refresh]
LDLC - Log Collector	✓	LDLC	Log Collector	10.6.6.0	[Settings] [Refresh]
LDLC - Log Decoder	✓	LDLC	Log Decoder	10.6.6.0	[Settings] [Refresh]
NWAPPLIANCE17339 - Log Collector	✓	NWAPPLIANCE17339	Log Collector	10.6.6.0	[Settings] [Refresh]
NWAPPLIANCE17339 - Log Decoder	✓	NWAPPLIANCE17339	Log Decoder	10.6.6.0	[Settings] [Refresh]
NWAPPLIANCE24678 - Decoder	✓	NWAPPLIANCE24678	Decoder	10.6.6.0	[Settings] [Refresh]
NWAPPLIANCE27791 - Concentrator	✓	NWAPPLIANCE27791	Concentrator	10.6.6.0	[Settings] [Refresh]
remoteLC - Log Collector	✓	remoteLC	Log Collector	10.6.6.0	[Settings] [Refresh]

## Users View

Username	Name	Email Address	Roles	External	Description
Analyst	analyst	analyst@abc.com	Analysts	no	
Kaushal	KK	kk@abc.com	Analysts, Data_Privacy_Officers	no	KK
Source1	Source1	test@abc.com	Data_Privacy_Officers	no	
Test	test	test@abc.com	Operators	no	Test
Tst	kk	r@a.com	Malware_Analysts	no	kk
admin	Administrator		Administrators	no	System Administrator
customs1	customs1	customs1@rsa.com	custom_source	no	
ian	ian	ian@rsa.com	Analyst_ian	no	ian
norm	Norman	norm@rsa.com	SystemAdministrator	no	
test1admin	test1admin	test1admin@test1ad...	Administrators, test1admin	no	User_test1admin
test2alert	test2alert	test2alert@test2alert...	Malware_Analysts, test2alert	no	
test3incidents	test3incidents	test3incidents@test3i...	test3incidents	no	asd
test4malware	test4malware	test4malware@test4...	test4malware_live	no	
test5reports	test5reports	test5reports@test5re...	Operators, test5reports	no	
tony	tony	tony@rsa.com	PrincipalThreatAnalyst	no	

## Roles View

Name	Description	Permissions
Analysts	The SOC Analysts persona is ce...	Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Export List, Define Rule, Navigate Events, Delete Jobs, Dashboard Access - Reporting Recent Report Dashboard, Search Live Resources...
Operators	The System Operators Persona...	Dashboard Access - Unified RSA First Watch Dashboard, Dashboard Access - Live Updated Resources Dashboard, Modify ESA Settings, View Health & Wellness Stats Browser, Manage SA Email, Manage SA Notification...
SOC_Managers	The persona for SOC Managers...	Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Export List, Define Rule, Navigate Events, Delete Jobs, View Event Sources, Dashboard Access - Reporting Recent Report Dashl...
Malware_Analysts	The persona of Malware Analy...	Access Investigation Module, Download Malware File(s), View and Manage Incidents, Navigate Events, Initiate Malware Analysis Scan, Manage List from Investigation, Context Lookup, Navigate Values, ...
Data_Privacy_Officers	The persona of Data Privacy Of...	Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Export List, Delete Alerts and Incidents, Define Rule, Navigate Events, Delete Jobs, Dashboard Access - Reporting Recent Repo...
Administrators	The System Administrators per...	View and Manage Incidents, Export List, Delete Alerts and Incidents, Define Rule, View Event Sources, Dashboard Access - Reporting Recent Report Dashboard, Search Live Resources, View Rules, Access View...
custom_source	target custom source	View and Manage Incidents, Export List, Delete Alerts and Incidents, Define Rule, Delete Jobs, Search Live Resources, Access View, View Reports, Context Lookup, Manage Live Feeds, Manage Jobs, View...
PrincipalThreatAnalyst	target PrincipalThreatAnalyst	Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Export List, Delete Alerts and Incidents, Define Rule, Navigate Events, Delete Jobs, Dashboard Access - Reporting Recent Repo...
Custom		Configure Incident Management integration, Modify ESA Settings, View and Manage Incidents, View Health & Wellness Stats Browser, Delete Alerts and Incidents, Manage SA Email, Manage SA Notifica...
custom1		Access Live Module, View Rules, View Alerts, Manage Rules, Access Alerting Module, Manage Live System Settings
Analyst_lan	source2 analyst lan	Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Export List, Delete Alerts and Incidents, Define Rule, Navigate Events, Delete Jobs, View Event Sources, Dashboard Access - Re...
test1admin	test1admin	Modify ESA Settings, View Health & Wellness Stats Browser, Manage SA Email, Manage SA Notifications, Manage SA Predicates, Manage SA Security, Manage SA Logs, View Rules, C...
test2alert		Configure Incident Management integration, Modify ESA Settings, View and Manage Incidents, View Health & Wellness Stats Browser, Delete Alerts and Incidents, Manage SA Email, Manage SA Notifica...
test3incidents		Configure Incident Management integration, Download Malware File(s), Deploy Live Resources, View and Manage Incidents, Delete Alerts and Incidents, Manage Alert Handling Rules, Initiate Malware...
test4malware_live	test4malware_live	Download Malware File(s), Define RE Alert, Deploy Live Resources, Manage RE Alerts, Initiate Malware Analysis Scan, View Live Resource Details, Search Live Resources, Access Live Module, Export RE ...
test5reports	Test5reports	Dashboard Access - Unified RSA First Watch Dashboard, Export List, Define Rule, Delete Jobs, Dashboard Access - Reporting Recent Report Dashboard, Access View, View Reports, Manage Jobs, View Schedules, Defin...
wq		Access Administration Module
All_permissions		Dashboard Access - Unified RSA First Watch Dashboard, View and Manage Incidents, Delete Alerts and Incidents, Manage SA Notifications, Manage SA Predicates, Navigate Events, View Event Sources, Dashlet...

## Custom Feeds View

Name	Trigger	Created	Last Run Time	Status	Progress
SAcsvAdhoc	Once	2019-01-15 13:12:14	2019-01-23 08:20:36	Completed	<div style="width: 100%;"></div>
csvAdhocGroup	Once	2019-01-15 13:14:56	2019-01-21 08:33:42	Completed	<div style="width: 100%;"></div>
SAcsvXmlAdhoc	Once	2019-01-15 13:15:51	2019-01-23 08:23:56	Completed	<div style="width: 100%;"></div>
stixRec	Starting at 2019-Jan-15 16:29, every 4 minutes	2019-01-15 16:29:44	2019-03-14 10:07:37	Completed	<div style="width: 100%;"></div>
csvAdhoc	Once	2019-01-15 16:41:20	2019-01-23 08:26:50	Completed	<div style="width: 100%;"></div>
csvRec	Starting at 2019-Jan-15 16:44, every 2 minutes	2019-01-15 16:44:29	2019-03-14 10:09:03	Completed	<div style="width: 100%;"></div>
stixRec	Starting at 2019-Jan-15 16:50, every minute	2019-01-15 16:50:05	2019-03-14 10:09:28	Completed	<div style="width: 100%;"></div>
SAcsvRec	Starting at 2019-Jan-21 08:34, every minute	2019-01-21 08:34:57	2019-03-14 10:09:30	Completed	<div style="width: 100%;"></div>
SAIDEPRec	Starting at 2019-Jan-21 09:33, every 2 minutes	2019-01-21 09:33:23	2019-03-14 10:09:23	Completed	<div style="width: 100%;"></div>
SAIDEPAdhoc	Once	2019-01-21 09:34:04	2019-01-23 08:26:11	Completed	<div style="width: 100%;"></div>
IDEPRec	Starting at 2019-Jan-21 09:39, every 2 minutes	2019-01-21 09:39:51	2019-03-14 10:09:51	Completed	<div style="width: 100%;"></div>
IDEPAdhoc	Once	2019-01-21 09:40:25	2019-01-21 09:40:25	Completed	<div style="width: 100%;"></div>
TestCsvRec	Starting at 2019-Jan-31 09:18, every minute	2019-01-31 09:18:09	2019-03-14 10:10:09	Completed	<div style="width: 100%;"></div>
TestStixRec	Starting at 2019-Jan-31 09:19, every minute	2019-01-31 09:19:07	2019-03-14 10:10:07	Completed	<div style="width: 100%;"></div>
SAstixAdhoc	Once	2019-02-27 10:13:58	2019-02-27 10:13:58	Completed	<div style="width: 100%;"></div>
csvXmlAdhoc	Once	2019-02-27 10:20:24	2019-02-27 10:20:24	Completed	<div style="width: 100%;"></div>
stixAdhoc	Once	2019-02-27 10:24:49	2019-02-27 10:24:49	Completed	<div style="width: 100%;"></div>

**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 <code>ssh-propagate</code> 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 <code>ssh-propagate</code> 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/ras/soc/reporting-engine/statusdb** and **/home/rsasoc/ras/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/ras/soc/reporting-engine/statusdb** = 2GB

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

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

10.1.1.2: space used by **/home/rsasoc/ras/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.

```
Please select what you wish to consolidate
1. SA Server Consolidation
2. Reporting Engine Consolidation
3. Exit 2
```

### (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.

```

-----
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
1

```

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

```

Please specify the number of hosts (apart from target) you want to consolidate : 2
Please Enter Host details
IP : 10.43.21.140
IP : 10.43.21.140

Do you want to pull ['rule', 'reports', 'subreports', 'charts', 'alerts', 'lists']
for host [10.43.21.140] Y/N : y

Host 10.43.21.140 needs : 37.34MB

Do you want to pull ['rule', 'reports', 'subreports', 'charts', 'alerts', 'lists']
for host [10.43.21.140] Y/N : y

```

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.

```

[root@SA re_consolidate]# cd consolidate/
[root@SA consolidate]# ll
total 15228
drwxr-xr-x. 14 root root    4096 Feb 19 10:03 10.43.21.140
drwxr-xr-x. 14 root root    4096 Feb 19 10:04 10.43.21.140
drwxr-xr-x. 13 root root    4096 Feb 19 10:02 10.43.21.140

```

## (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.

```
-----
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
_
```

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.

```
[root@SA re_consolidate]# cd consolidate/
[root@SA consolidate]# ll
total 15228
drwxr-xr-x. 14 root root    4096 Feb 19 10:03 10.43.25.149
drwxr-xr-x. 14 root root    4096 Feb 19 10:04 10.43.25.149
drwxr-xr-x. 13 root root    4096 Feb 19 10:02 10.43.25.149
-rw-r--r--.  1 root root 15574283 Feb 19 10:02 RE-Consolidation-config.log
drwxr-xr-x. 11 root root    4096 Feb 19 10:02 reporting-engine
[root@SA consolidate]#
```

## (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.

```

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

```

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

```

/var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_1_20190219094408
10:33:52,644 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_1_20190219094408/content.history is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_1_20190219094408/content.history
10:33:52,693 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_1_20190219094408/contentid.permissions copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_1_20190219094408/contentid.permissions
10:33:52,751 INFO CopyAndMergeResultstoreDirectory:175 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_1_20190219094408/ALERT_1_20181130083744 is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_1_20190219094408/ALERT_1_20181130083744
10:33:52,752 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_1_20190219094408/result.props is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_1_20190219094408/result.props
10:33:52,752 INFO CopyAndMergeResultstoreDirectory:110 - Copied
10:33:52,753 INFO CopyAndMergeResultstoreDirectory:92 - Started copy FROM : /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_2_20190219094408 TO /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_2_20190219094408
10:33:52,769 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_2_20190219094408/content.history is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_2_20190219094408/content.history
10:33:52,827 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_2_20190219094408/contentid.permissions copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_2_20190219094408/contentid.permissions
10:33:52,911 INFO CopyAndMergeResultstoreDirectory:175 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_2_20190219094408/ALERT_1_20190110141927 is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_2_20190219094408/ALERT_1_20190110141927
10:33:52,912 INFO CopyAndMergeResultstoreDirectory:171 - /var/netwitness/database/re_consolidate/consolidate/10.63.21.149/resultstore/EXEC_ALERTDEF_2_20190219094408/result.props is copied to /var/netwitness/database/re_consolidate/consolidate/reporting-engine/resultstore/EXEC_ALERTDEF_2_20190219094408/result.props
10:33:52,912 INFO CopyAndMergeResultstoreDirectory:110 - Copied
10:33:52,912 INFO Consolidate:199 - -----Data Copying/Merging complete for 3 instances
10:33:52,912 INFO Consolidate:202 - The 'reporting-engine' directory is created at /var/netwitness/database/re_consolidate/consolidate/reporting-engine. Please follow the post consolidation steps now either via script or go through the documentation.

```

### (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 reporting-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.

```

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

```

### (Optional) Option 6 – Exit

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

```

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

```

## 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 <code>rsa-nw-consolidator.sh</code> script and choose Option 1 of Reporting Engine .

Option	Menu	Equivalent Manual Steps
2	Consolidate Configuration	<ol style="list-style-type: none"><li>1. Obtain the <code>RSA-RE-Consolidation.jar</code> from from tool bin folder.</li><li>2. Place the jar in <code>/var/netwitness/database/re_consolidate/</code></li><li>3. Run the command: <code>cd /var/netwitness/database/re_consolidate/</code></li><li>4. Run the script <code>java -jar RSA-RE-Consolidation.jar -repository consolidate/</code> <b>Note:</b>Before running the <code>java -jar</code>, make sure all the directories of the RE instances are available at <code>/var/netwitness/database/re_consolidate/consolidate</code> directory. And are renamed appropriately with the IP of the specific instance.</li></ol>



Option	Menu	Equivalent Manual Steps										
3	Consolidate data	<p>This is a manual step. After you complete the above mentioned manual step, you must trigger the jar as follows:</p> <table border="1"> <thead> <tr> <th data-bbox="553 369 813 422">Command</th> <th data-bbox="813 369 1419 422">Action Performed</th> </tr> </thead> <tbody> <tr> <td data-bbox="553 422 813 659"> <pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1&gt;</pre> </td> <td data-bbox="813 422 1419 659">Consolidates the data from IP1 only.</td> </tr> <tr> <td data-bbox="553 659 813 1360"> <pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2&gt;</pre> </td> <td data-bbox="813 659 1419 1360"> <p>Consolidates the data from IP1 and IP2.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p> <p>To calculate the space required, perform the following:</p> <pre>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</pre> <p><b>Note 1:</b> Make sure you have this space available in the partition /home/rsasoc/</p> <p><b>Note 2:</b> Make sure you have enough space available in the partition /var/netwitness/</p> </td> </tr> <tr> <td data-bbox="553 1360 813 1646"> <pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2, host&gt;</pre> </td> <td data-bbox="813 1360 1419 1646"> <p>Consolidates the data from IP1, IP2 and target or host machine.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p> </td> </tr> <tr> <td data-bbox="553 1646 813 1843"> <pre>java -jar RSA-RE-Consolidation-1.0.jar -data</pre> </td> <td data-bbox="813 1646 1419 1843">Consolidates the data from host or target machine i.e 127.0.0.1.</td> </tr> </tbody> </table>	Command	Action Performed	<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1&gt;</pre>	Consolidates the data from IP1 only.	<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2&gt;</pre>	<p>Consolidates the data from IP1 and IP2.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p> <p>To calculate the space required, perform the following:</p> <pre>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</pre> <p><b>Note 1:</b> Make sure you have this space available in the partition /home/rsasoc/</p> <p><b>Note 2:</b> Make sure you have enough space available in the partition /var/netwitness/</p>	<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2, host&gt;</pre>	<p>Consolidates the data from IP1, IP2 and target or host machine.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p>	<pre>java -jar RSA-RE-Consolidation-1.0.jar -data</pre>	Consolidates the data from host or target machine i.e 127.0.0.1.
Command	Action Performed											
<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1&gt;</pre>	Consolidates the data from IP1 only.											
<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2&gt;</pre>	<p>Consolidates the data from IP1 and IP2.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p> <p>To calculate the space required, perform the following:</p> <pre>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</pre> <p><b>Note 1:</b> Make sure you have this space available in the partition /home/rsasoc/</p> <p><b>Note 2:</b> Make sure you have enough space available in the partition /var/netwitness/</p>											
<pre>java -jar RSA-RE-Consolidation-1.0.jar -data &lt;IP1, IP2, host&gt;</pre>	<p>Consolidates the data from IP1, IP2 and target or host machine.</p> <p><b>Note:</b> Make sure you have enough space before executing this option.</p>											
<pre>java -jar RSA-RE-Consolidation-1.0.jar -data</pre>	Consolidates the data from host or target machine i.e 127.0.0.1.											

Option	Menu	Equivalent Manual Steps
		<div style="border: 1px solid black; padding: 2px; display: inline-block;">host</div>
4	Post Consolidation	<p>Perform the post consolidation using the following commands:</p> <ol style="list-style-type: none"> <li>1. Stop RE service using the command <code>rsasoc_re</code>.</li> <li>2. Rename the existing reporting-engine directory from <code>/home/rsasoc/rsa/soc/reporting-engine</code> to <code>/home/rsasoc/rsa/soc/reporting-engine_old</code>. This takes a backup of the host and target RE data.</li> <li>3. Copy the reporting-engine directory from <code>/var/netwitness/database/re_consolidate/consolidate/reporting-engine</code> to <code>/home/rsasoc/rsa/soc/reporting-engine</code></li> <li>4. Change the primary and secondary owner of the new reporting-engine directory using the command <code>#chown -R rsasoc:rsasoc /home/rsasoc/rsa/soc/reporting-engine</code></li> <li>5. Start the reporting-engine service using the command <code>rsasoc_re</code>. Wait for RE service to be up and running.</li> <li>6. Stop <code>rsasoc_re</code></li> <li>7. Delete the <code>/home/rsasoc/rsa/soc/reporting-engine/conf</code> directory.</li> <li>8. Rename <code>/home/rsasoc/rsa/soc/reporting-engine/conf</code> to <code>renameToconfAfter1stStartStop</code> to <code>/home/rsasoc/rsa/soc/reporting-engine/conf</code>.</li> <li>9. Start <code>rsasoc_re</code> and check if RE service is up and running.</li> <li>10. Stop <code>jettysrv</code></li> <li>11. Start <code>jettysrv</code></li> </ol>
5	Cleanup	<code># rm -rf /var/netwitness/database/re_consolidate /consolidate/reporting-engine</code>
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.

The screenshot shows the 'Rules' page in the Reports application. The 'Groups' sidebar on the left lists two groups: '10.31.1.212' with 43 items and '10.63.21.160' with 183 items. The main 'Rules' table displays a list of rules with columns for Name, Type, Group, Date Modified, and Actions. The rules listed include 'a\_ip\_src', 'Accounts Created', 'Accounts Disabled', 'Accounts Modified', 'Ad Servers by Bandwidth', 'Alert Eth Src', 'Alert Eth Src(1)', 'Alert IDs by Profiled Source IP', 'Alert001', 'Alertkk', 'Alertkk(1)', 'Alertkk(1)(1)', 'Alertkk(10)', 'Alertkk(2)', 'Alertkk(3)', 'Alertkk(4)', and 'Alertkk(5)'. The page is on Page 1 of 8, displaying 1-30 of 235 items.

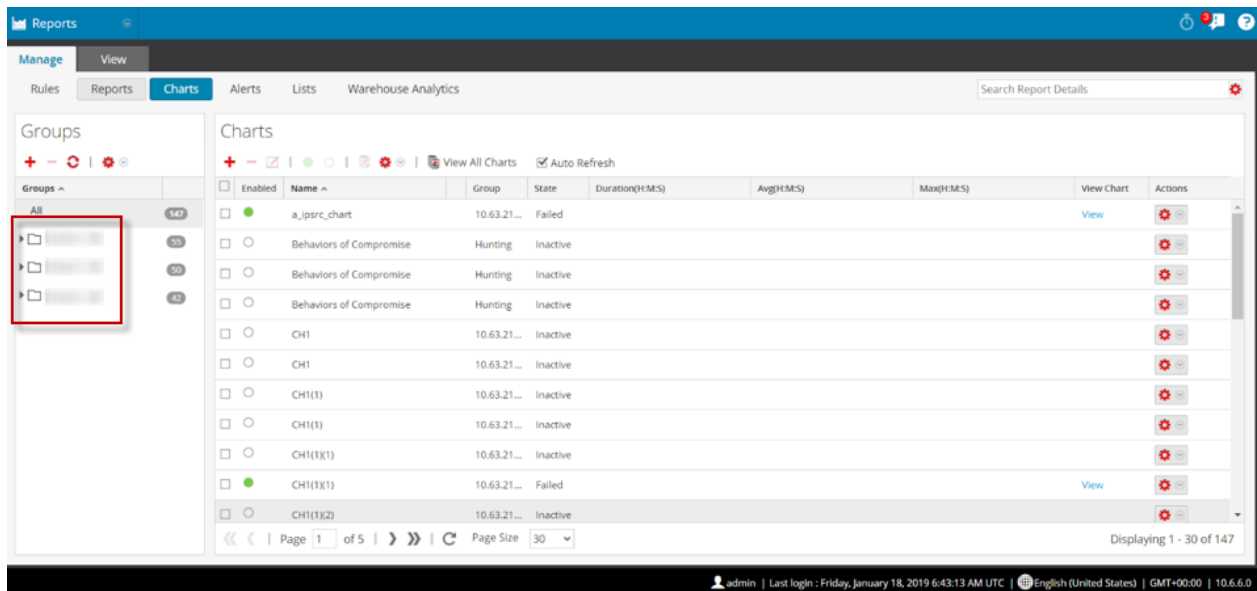
## Reports Page

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

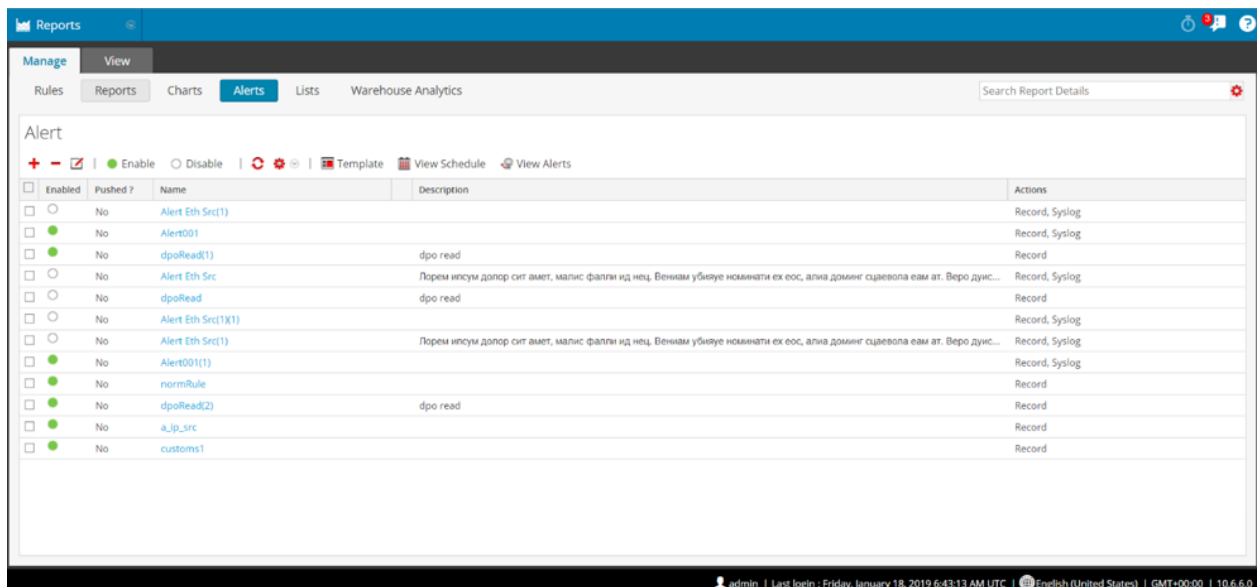
The screenshot shows the 'Reports' page in the Reports application. The 'Groups' sidebar on the left lists several groups. The main 'Reports' table displays a list of reports with columns for Name, Group, Date Modified, # Schedules, and Actions. The reports listed include 'a-Report-a\_ip\_src', 'Iterative reports', 'malAnalyst', 'malAnalyst', 'malAnalyst', 'Report-Expert', 'Report-Iterative Rule', 'Report-Test', 'Report-test1', 'Report-Test1', and 'Report-username'. The page is on Page 1 of 2, displaying 1-30 of 44 items.

## Charts Page

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

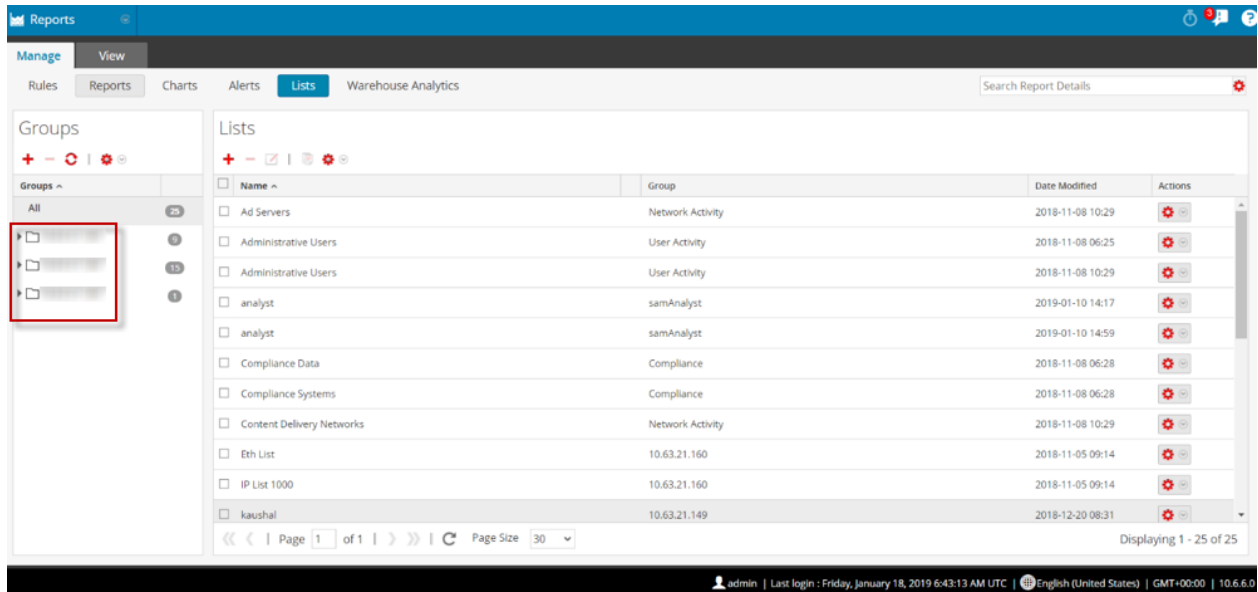


## Alerts Page



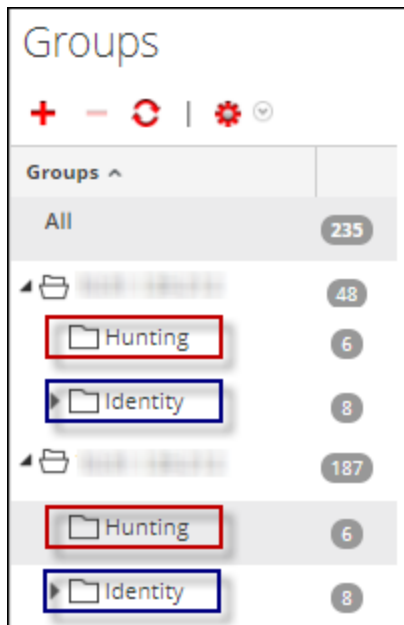
## Lists Page

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, " <b>Authentication failed</b> " error message is displayed shown	Re-run <code>ssh-propagate</code> 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>).