



Update Guide

for Version 11.0.x.x or 11.1.x.x to 11.2



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

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

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

August 2018

Contents

Introduction	5
Update Path	5
Running in Mixed Mode	5
Entropy=log2 flag Reset After Update	5
Update Preparation Tasks	6
General	6
Task 1 - Review Core Ports and Open Firewall Ports	6
Task 2- Back Up Malware Analysis Configuration File to Another Directory	6
Task 3 - Stop Data Capture and Aggregation	7
Azure Hosts	9
Task 4 - (Conditional) Azure Host Update Preparation Requirements	9
Endpoint Insights	10
Task 5 - (Conditional) Back Up Existing Custom Meta Data Mappings before Applying 11.2	
Update to Endpoint Host	10
Reporting Engine	10
Task 6 - Configure Reporting Engine for Out-of-the-Box Charts	10
Respond	10
Task 7 - (Conditional) Restore Respond Service Custom Keys	10
Task 8 - Back Up Customized Respond Service Normalization Scripts	10
Update Tasks	12
Apply Updates from the Hosts View (Web Access)	12
Task 1. Populate Local Repo or Set Up an External Repo	12
Task 2. Apply Updates from the Hosts View to Each Host	13
Apply Updates from the Command Line (No Web Access)	16
Update or Install Legacy Windows Collection	17
Post Update Tasks	18
General	19
Task 1 - Start Data Capture and Aggregation	19
Task 2 - Set Up Context Menu Actions User Permissions	20
NW Server	22

Task 3 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File	22
(Conditional) Task 4 - Reconfigure PAM Radius Authentication	22
Endpoint Insights	23
Task 5 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed	23
Task 6 - Restore Backed Up Endpoint Custom Meta Data Mappings	23
Event Stream Analysis	24
(Conditional) Task 7 - Reconfigure the “Suspected Command and Control Communication By Domain” Aggregation Rule for Automated Threat Detection	24
Respond	25
Task 8 - Get the Latest Version of the Aggregation Rule Schema and Restore any Respond Service Custom Keys	25
Task 9 - Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts	26
Task 10 - Add Respond Notification Settings Permissions	26
Task 11 - Update Default Incident Rule Group By Values	27
NetWitness UEBA	28
Task 12 - Install NetWitness UEBA	28
Appendix A. Troubleshooting Version Installations and Updates	29
Appendix B. Populate Local Repo	36
Appendix C. Set Up External Repo	38
Revision History	41

Introduction

RSA NetWitness® Platform 11.2.0.0 provides fixes for all products in the Platform. The components of the Platform are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, Security sever, and Source server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, UEBA, Warehouse Connector, and Workbench.

Note: The Reporting Engine is installed on the NW Server host, Workbench is installed on the Archiver host, Warehouse Connector can be installed on the Decoder host or Log Decoder host.

The instructions in this guide apply to both physical and virtual hosts (including AWS and Azure Public Cloud) unless stated to the contrary.

Update Path

The following update paths are supported for NetWitness Platform 11.2.0.0:

- 11.0.x to 11.2.0.0
- 11.1.x to 11.2.0.0
- 10.6.6.x to 11.2.0.0

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents. See the *RSA NetWitness Platform 10.6.6.x to 11.2 Physical Host Upgrade Guide* and *RSA NetWitness Platform 10.6.6.x to 11.2 Virtual Host Upgrade Guide* for instructions on how to upgrade 10.6.6.x to 11.2.0.0.

Running in Mixed Mode

Running in mixed mode occurs when some services are updated to the latest version and some services are on older versions. See "Running in Mixed Mode" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for further information.

Entropy=log2 flag Reset After Update

If your Entropy=log2 flag is set to false (Entropy="log2=false") in 11.0.x.x , NetWitness resets this flag to true (Entropy="log2=true") after you upgrade to 11.2 to align for all sources to include packets and NetWitness Endpoint Insights. If desired, you can set the flag back to false to retain the log10 calculation: Entropy="log2=false".

Update Preparation Tasks

Complete the following tasks to prepare for the update to NetWitness Platform 11.2.0.0. These tasks are organized by the following categories.

[General](#)

[Azure Hosts](#)

[Endpoint Insights](#)

[Reporting Engine](#)

[Respond](#)

General

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.2.0.0.

Caution: Make sure that the new ports are implemented and tested before updating so that update does not fail due to missing ports.

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5672	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

Task 2- Back Up Malware Analysis Configuration File to Another Directory

1. Make a backup of the following file to another, safe directory.
`/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`
 You need to retrieve your custom parameter values from this backup after you update the Malware Analysis host to 11.2.0.0. The update creates a new configuration file with all the parameters set to the default values.
2. Delete the following file.
`/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`

Task 3 - Stop Data Capture and Aggregation



Stop Network Capture

1. Log in to NetWitness Platform 11.0.x and go to **ADMIN > Services**.
The Services view is displayed.
2. Select each **Decoder** service.

The screenshot displays the NetWitness Platform 11.1.0.0 interface. The top navigation bar includes tabs for RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the Services view is selected. The breadcrumb trail shows 'Change Service' > 'S5Decoder - Decoder' > 'System'. The toolbar contains buttons for 'Upload Packet Capture File', 'Stop Capture', 'Host Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content area is divided into four sections: 'Decoder Service Information', 'Appliance Service Information', 'Decoder User Information', and 'Host User Information'.

Decoder Service Information		Appliance Service Information	
Name	S5Decoder (Decoder)	Name	S5Decoder (Host)
Version	11.1.0.0	Version	11.1.0.0
Memory Usage	2858 MB (2.54% of 110 GB)	Memory Usage	25964 KB (0.02% of 110 GB)
CPU	1%	CPU	0%
Running Since	2018-Feb-08 02:32:47	Running Since	2018-Feb-06 22:14:56
Uptime	11 hours 23 minutes 46 seconds	Uptime	1 day 15 hours 41 minutes 38 seconds
Current Time	2018-Feb-08 13:56:33	Current Time	2018-Feb-08 13:56:34

The bottom of the interface shows the RSA | NETWITNESS SUITE logo and the version number 11.1.0.0.

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

Stop Log Capture

1. Log in to NetWitness Platform 11.0.x and go to **ADMIN > Services**.
The Services view is displayed.


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

The screenshot shows the RSA NetWitness Platform ADMIN interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are sub-tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The main content area displays two side-by-side panels: 'Log Decoder Service Information' and 'Appliance Service Information'. Both panels show details for the S5EndPtLogHyb1783 service, including Name, Version (11.1.0.0), Memory Usage, CPU usage, Running Since, Uptime, and Current Time. Below these panels, there are sections for 'Log Decoder User Information' and 'Host User Information'. The bottom of the interface shows the RSA NETWITNESS SUITE logo and the version 11.1.0.0.

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

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

Stop Aggregation

1. Log in to NetWitness Platform 11.0.x and go to **ADMIN > Services**.
2. Select the **Broker** service.
3. Under  (actions), select **View > Config**.
4. The **General** tab is displayed.

The screenshot shows the RSA NetWitness Platform ADMIN interface with the 'SERVICES' tab selected. The 'BROKER - Broker' service is highlighted, and the 'Config' sub-tab is active. The 'General' tab is displayed, showing 'Aggregate Services' and 'System Configuration'. The 'Aggregate Services' table lists 'ip-address' with a port of 56005, a rate of 1, and a max of 7091. The 'System Configuration' table shows 'Compression' set to 0 and 'Port' set to 50003. On the right, the 'Aggregation Configuration' panel shows settings for 'Aggregate Hours' (0), 'Aggregate Interval' (60000), 'Aggregate Max Sessions' (5000000), and 'Service Heartbeat' (300). A tooltip is visible over the 'Stop Aggregation' button, stating 'Stop consuming session from the list of attached services.' The bottom of the interface shows the user 'admin', language 'English (United States)', and time 'GMT+00:00'.

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

Azure Hosts

Task 4 - (Conditional) Azure Host Update Preparation Requirements

Review your Azure Host deployment for the following three conditions and complete the tasks under these conditions if required.

- If you have an 11.0.0.0 Azure base image on the host (even you updated the host to 11.1.0.x), create a Centos-Base repo.

Caution: If the `libgudev1-219-30.el7_3.9.x86_64` RPM does not exist, do not complete the following steps.

1. SSH to the NW Server host.
 2. Run the following command from the NW Server Host `root` directory.

```
yum remove libgudev1-219-30.el7_3.9.x86_64
```
 3. Create a Centos-Base repo as described in step 6 in the **CentOS 7.0+** procedure (<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-upload-centos#centos-70>).
 4. Run the following command strings from the NW Server Host `root` directory.

```
yum clean all  
yum install WALinuxAgent  
sudo systemctl enable waagent
```
 5. Delete the CentOS-base repo.
- If the update path is 11.0.0.x to 11.2, populate the Repo with additional packages.
Contact Customer Support (<https://community.rsa.com/docs/DOC-1294>) for the `nw-azure-11.1-extras.zip` file).
 1. SSH to the NW Server host.
 2. Go to the `root` directory of the On the NW Server host.
 3. Run the following command strings to extract the Azure zip file.

```
mkdir -p /var/lib/netwitness/common/repo/11.2.0.0/OS/other+  
unzip nw-azure-11.1-extras.zip -d  
/var/lib/netwitness/common/repo/11.2.0.0/OS/other
```
 4. If you use an External Repo,
 - If you use an External Repo to apply updates, update the External Repo with the additional packages.
 1. After you set up the 11.2.0.0 content on the external repo, go to the `<base-directory>11.2.0.0/OS/other` of the external repo.
 2. Run the following command string to extract the Azure zip file from the external repo `11.2.0.0/OS` directory.

```
unzip nw-azure-11.1-extras.zip -d /<base-directory>11.2.0.0/OS/other
```
 3. Run the following command from the external repository's `11.2.0.0/OS` directory.

```
createrepo
```

Endpoint Insights

Task 5 - (Conditional) Back Up Existing Custom Meta Data Mappings before Applying 11.2 Update to Endpoint Host

In 11.2, RSA enhanced the Endpoint meta data mappings to align with the current Unified Data Model (UDM) changes. When you apply the 11.2 update your Endpoint Insights host, it clears the existing custom mapping to avoid overriding the newly added default meta data mappings. If you want to use the existing custom metadata mapping, RSA recommends that you back up the existing custom mappings before you update the Endpoint Insights host to 11.2. To back up:

1. Run the `get-custom` API through `nw-shell`. The list of custom mappings is displayed.
2. Copy the custom mappings manually to a safe directory.

For more information, see *Endpoint Insights Configuration Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Reporting Engine

Task 6 - Configure Reporting Engine for Out-of-the-Box Charts

For Out-of-the-Box charts to run after the update, you must configure the default data source on the Reporting Engine Configuration page before you perform the update. If you do not perform this task, you must manually set up the data source after the update. For more information on Reporting Engine data sources, see the *NetWitness Platform 11.2 Reporting Engine Configuration Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Respond

Task 7 - (Conditional) Restore Respond Service Custom Keys

If you added custom keys in `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` for use in the `groupBy` Clause in 11.0, copy and save the custom keys in a file.

Task 8 - Back Up Customized Respond Service Normalization Scripts

RSA re-factored Respond service normalization scripts are stored in the `/var/lib/netwitness/respond-server/scripts` directory in 11.2.0.0. You need to back them up in 11.0.x before you update to 11.2.0.0 so you can restore them in 11.2.0.0 as described in the [Respond Post Update Tasks](#).

1. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
2. Back up the following files:
 - `data_privacy_map.js`
 - `normalize_alerts.js`
 - `normalize_core_alerts.js`

```
normalize_ecat_alerts.js  
normalize_ma_alerts.js  
normalize_wtd_alerts.js  
utils.js
```

3. (Conditional) If you have any custom logic added in 11.0.x or any previous release, copy and save this logic from the backed up scripts so you can restore it in 11.2.0.0.

Update Tasks

Complete the following tasks to update NetWitness Platform 11.0.x.x or 11.1.x.x to 11.2.0.0.

There are two methods you can use to apply version updates to a host.

Note: If you plan to use an update repository (repo) for NetWitness Platform 11.2.0.0 that is different from the repo you have set up now for 11.0.x.x or 11.1.x.x, refer to [Appendix C. Set Up External Repo](#) for instructions.

- [Apply updates from the Host view \(Web Access\)](#)
- [Apply update from the command line \(No Web Access\)](#)

Apply Updates from the Hosts View (Web Access)

There are two tasks you must complete to apply updates from the Hosts view:

- Task 1. Populate Local Repo or Set Up an External Repo - make sure that you have the latest version updates .
- Task 2. Apply updates from the Hosts View to each host.

Task 1. Populate Local Repo or Set Up an External Repo

When you set up your NW Server in 11.2.0.0, you select the Local Repo or an external repo. The Hosts view retrieves version updates from the repo you selected.

If you selected the Local Repo, you do not need to set it up, but you must make sure that it is populated with the latest version updates. See [Appendix B. Populate Local Repo](#) for instructions on how populate it with version update.

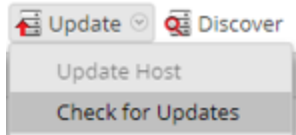
If you selected an External Repo, you must set it up. See [Appendix C. Set Up External Repo](#) for instructions on how to set up an external repo.

Task 2. Apply Updates from the Hosts View to Each Host

The Hosts view displays the software version updates available in your Local Update Repository and you choose and apply the updates you want from the Host view.

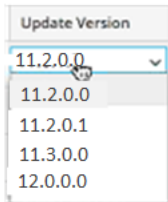
This procedure tells you how to update a host to a new version of NetWitness Platform.

1. Log in to NetWitness Platform.
2. Go to **ADMIN > HOSTS**.
3. (Conditional) Check for the latest updates.




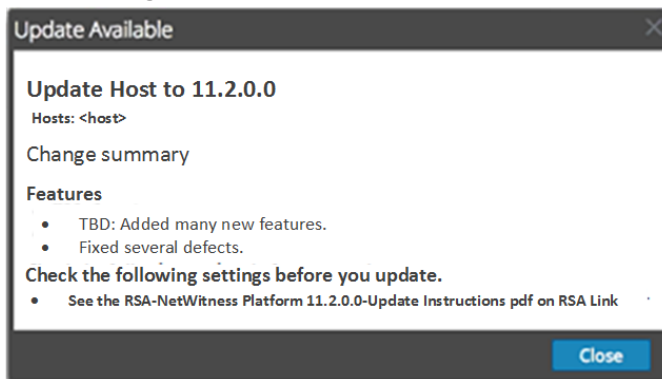
4. Select a host or hosts.
You must update the NW Server to latest version first. You can update the other hosts in any sequence you prefer, but RSA recommends that you follow the guidelines in "Running in Mixed Mode" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for further information.
Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected hosts.

5. Select the version you want to apply from the **Update Version** column.



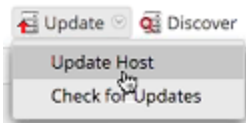
If you:

- Want to update more than one host to that version, after you update the NW Server host, select the checkbox to the left of the hosts. Only currently supported update versions are listed.
- Want to view a dialog with the major features in the update and information on the updates click the information icon () to the right of the update version number. The following is an example of this dialog.

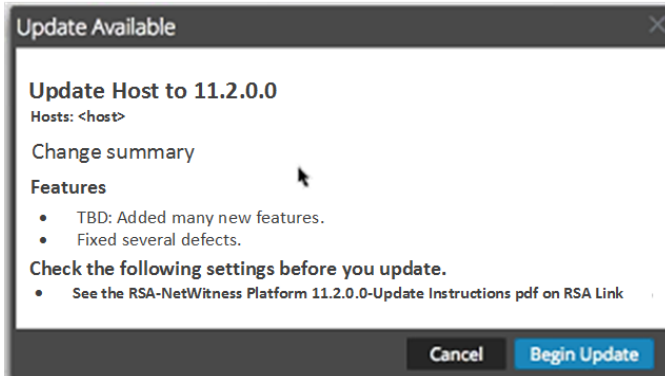


- Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show **Update Available**. By default, only supported updates for the selected host are displayed.

6. Click **Update > Update Host** from the toolbar.



A dialog is displayed with information on the selected update. Click **Begin Update**.



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

- Stage 1 - **Downloading update packages** - downloads the repository artifacts to the NW Server applicable to the services on the host you chose.
 - Stage 2 - **Configuring update packages** - configures update files in to correct format.
 - Stage 3 - **Update in progress** - updates host to new version.
7. When you see **Update in progress**, refresh the browser.
This may send you to the NetWitness Log In screen. If this happens, log in and navigate back to the Host view.
After the host is updated, NetWitness Platform prompts you to **Reboot Host**.
8. (Conditional - For Host with Unity Storage Only) If the host (for example, the Network Decoder host) has Unity storage configured with PowerPath on 11.1.x.x , and the Powerpath version installed is EMCPower.LINUX.6.3.0.b049, SSH to the host and submit the following commands to install the new PowerPath version (that is, DelleMCPower.LINUX.6.4.0.b095).
- ```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DelleMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
9. Click **Reboot Host** from the toolbar.  
NetWitness Platform shows the status as **Rebooting...** until the host comes back online. After the host comes back online, the **Status** shows **Up-to-Date**. Contact Customer Care if the host does not come back online.

**Note:** 1.) If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates. 2.) If you have Unity storage, check the PowerPath status and verify the it can see the Unity device.

## Apply Updates from the Command Line (No Web Access)

If your RSA NetWitness Platform deployment does not have Web access, complete the following procedure to apply a version update.

1. Download .zip update package for the version you want (for example, `netwitness-11.2.0.0.zip`) from RSA Link to a local directory.
2. SSH to the NW Server host.
3. Make a `tmp/upgrade/<version>` staging directory for the version you want (for example, `tmp/upgrade/11.2.0.0`).  
`mkdir -p /tmp/upgrade/11.2.0.0`
4. Unzip the package into the staging directory you created (for example, `tmp/upgrade/11.2.0.0`).  
`cd /tmp/upgrade/11.2.0.0`  
`unzip /tmp/upgrade/11.2.0.0/netwitness-11.2.0.0.zip`
5. Initialize the update on the NW Server.  
`upgrade-cli-client --init --version 11.2.0.0 --stage-dir /tmp/upgrade/`
6. Apply the update to the NW Server.  
`upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.2.0.0`
7. Log in to NetWitness Platform and reboot the NW Server host in the Host View.
8. Apply update to each non-NW Server host.  
`upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.2.0.0`  
 The update is complete when the polling is completed.
9. (Conditional) If the host (for example, the Network Decoder host) has Unity storage configured with PowerPath on 11.1.x.x , and the Powerpath version installed is EMCPower.LINUX.6.3.0.b049, SSH to the host and submit the following commands to install the new PowerPath version (that is, DelleMCPower.LINUX.6.4.0.b095).  
`systemctl stop nwdecoder`  
`umount -R /var/netwitness/decoder`  
`yum update DelleMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm`
10. Log in to NetWitness Platform and reboot the host in the Host View.  
 You can verify the version applied to the host with the following command:  
`upgrade-cli-client --list`

**Note:** 1.) If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates. 2.) If you have Unity storage, check the PowerPath status and verify the it can see the Unity device.



## Update or Install Legacy Windows Collection

---

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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

## Post Update Tasks

---

Complete the following tasks after you update to NetWitness Platform 11.2.0.0.

- [General](#)
- [NW Server](#)
- [Endpoint Insights](#)
- [Event Stream Analysis](#)
- [Respond](#)
- [NetWitness UEBA](#)



## General

These tasks apply to all NetWitness Platform 11.2.0.0 customers.



### Task 1 - Start Data Capture and Aggregation

Restart network and log capture and aggregation after updating to 11.2.0.0.



#### Start Network Capture

1. In the **NetWitness Platform** menu, select **ADMIN > Services**.  
The Services view is displayed.
2. Select each **Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture** .

#### Start Log Capture


1. In the **NetWitness Platform** menu, select **ADMIN > Services**.  
The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture** .

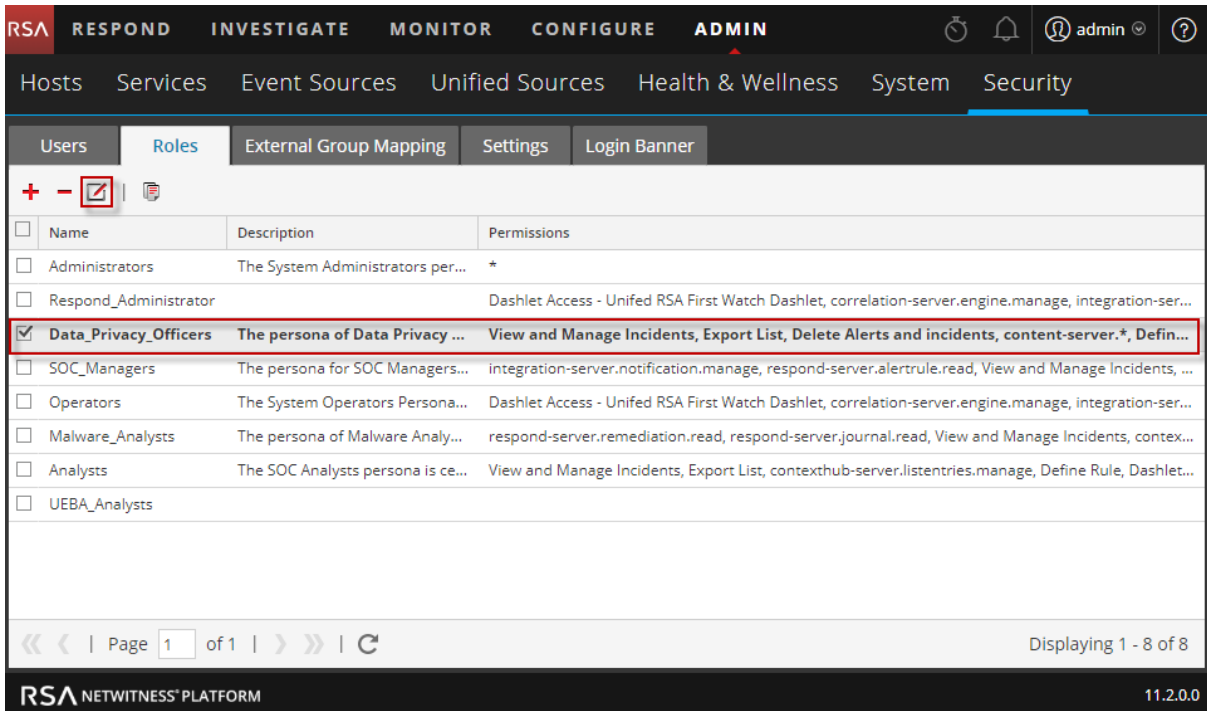
#### Start Aggregation

1. In the **NetWitness Platform** menu, select **ADMIN > Services**.  
The Services view is displayed.
2. For each Concentrator and Broker service.
  - a. Select the service.
  - b. Under  (actions), select **View > Config**.
  - c. In the toolbar, click  **Start Aggregation** .

## Task 2 - Set Up Context Menu Actions User Permissions

Complete the following steps for **Analysts**, **SOC Managers**, **Data Privacy Officers** roles to set up their Context Menu Actions. You must complete these steps for the **Analysts**, **SOC Managers**, and **Data Privacy Officers** roles.

1. In the **NetWitness Platform** menu, select **ADMIN > Security > Roles**.
2. Double-click on the user role (for example, **Data Privacy Officers**), or click to select the user and click  (Edit ).



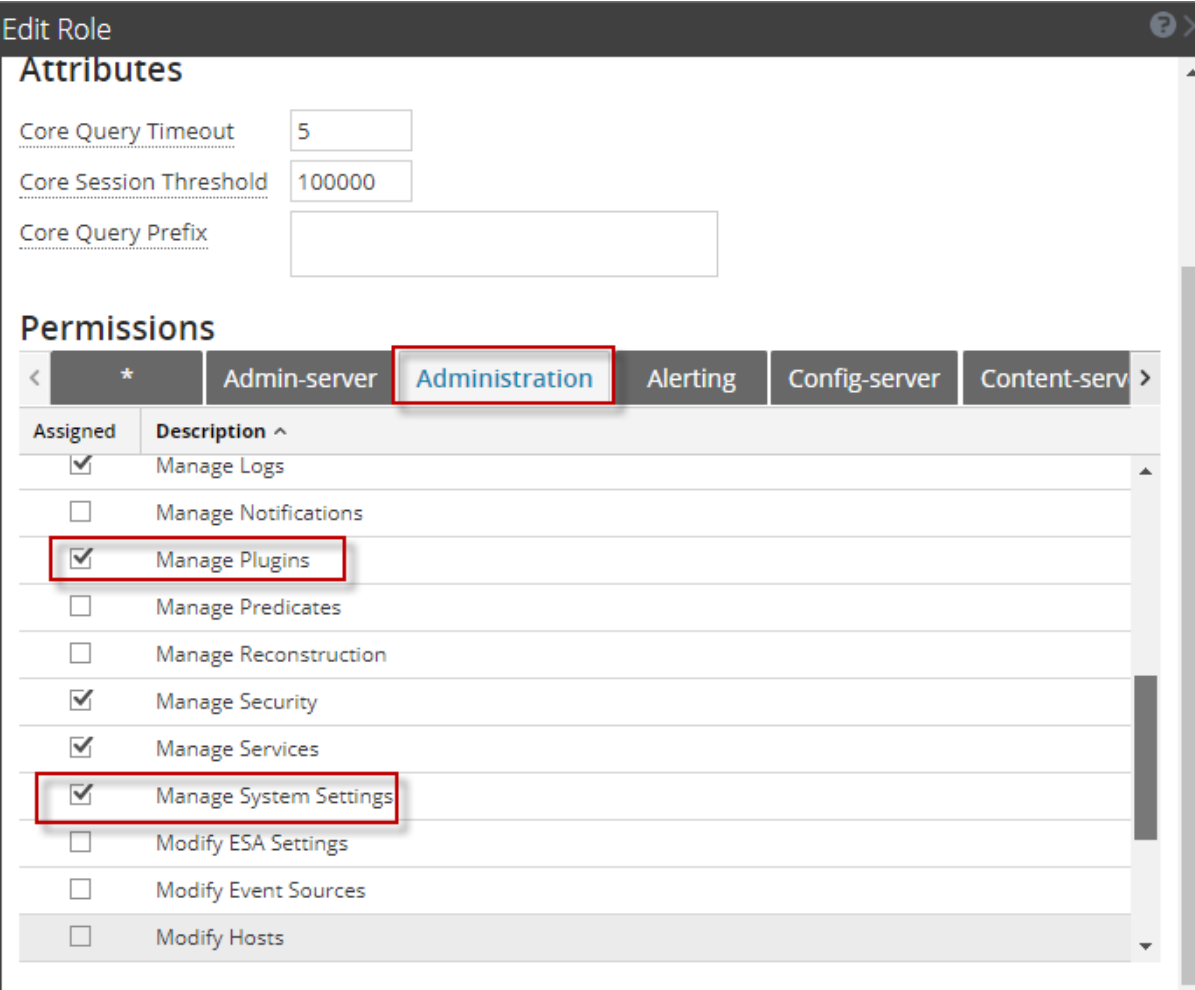
The screenshot shows the NetWitness Platform Admin console. The top navigation bar includes tabs for RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the 'Security' sub-tab is selected. Below the navigation bar, there are tabs for Users, Roles, External Group Mapping, Settings, and Login Banner. The 'Roles' tab is active, and a table lists various roles. The 'Data\_Privacy\_Officers' role is selected and highlighted with a red box. The role's permissions are listed as 'View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.\*, Defin...'. The table also includes columns for Name, Description, and Permissions.

| Name                                                      | Description                       | Permissions                                                                                           |
|-----------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Administrators                   | The System Administrators per...  | *                                                                                                     |
| <input type="checkbox"/> Respond_Administrator            |                                   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input checked="" type="checkbox"/> Data_Privacy_Officers | The persona of Data Privacy ...   | View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.*, Defin...       |
| <input type="checkbox"/> SOC_Managers                     | The persona for SOC Managers...   | integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, ... |
| <input type="checkbox"/> Operators                        | The System Operators Persona...   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input type="checkbox"/> Malware_Analysts                 | The persona of Malware Analy...   | respond-server.remediation.read, respond-server.journal.read, View and Manage Incidents, contex...    |
| <input type="checkbox"/> Analysts                         | The SOC Analysts persona is ce... | View and Manage Incidents, Export List, contexthub-server.listentries.manage, Define Rule, Dashlet... |
| <input type="checkbox"/> UEBA_Analysts                    |                                   |                                                                                                       |

Page 1 of 1 | Displaying 1 - 8 of 8

RSA NETWITNESS PLATFORM 11.2.0.0

3. In the **Edit Role** view under **Permissions**, check the **Manage Logs**, **Manage Plugins**, and **Manage System Settings** check boxes and click **Save**.



**Edit Role**

**Attributes**

Core Query Timeout: 5

Core Session Threshold: 100000

Core Query Prefix:

**Permissions**

< \* Admin-server **Administration** Alerting Config-server Content-serv >

| Assigned                            | Description ^          |
|-------------------------------------|------------------------|
| <input checked="" type="checkbox"/> | Manage Logs            |
| <input type="checkbox"/>            | Manage Notifications   |
| <input checked="" type="checkbox"/> | Manage Plugins         |
| <input type="checkbox"/>            | Manage Predicates      |
| <input type="checkbox"/>            | Manage Reconstruction  |
| <input checked="" type="checkbox"/> | Manage Security        |
| <input checked="" type="checkbox"/> | Manage Services        |
| <input checked="" type="checkbox"/> | Manage System Settings |
| <input type="checkbox"/>            | Modify ESA Settings    |
| <input type="checkbox"/>            | Modify Event Sources   |
| <input type="checkbox"/>            | Modify Hosts           |

4. Complete steps 1 through 3 for the **Analysts** and **SOC Managers** roles in addition to **Data Privacy Officers**.


## NW Server

### Task 3 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File

**Problem:** When a user updates from 11.0.0.0 to 11.2.0.0, if they have global auditing set up, audit log templates are not getting updated in Logstash output conf file.

**Workaround:** If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click save to apply the latest Audit log configuration.

If you had global auditing configured in 11.0.x, you must complete the following procedure to apply the latest Global Auditing configuration.

1. In the **NetWitness Platform** menu, select **ADMIN > System > Global Notifications**.  
The **Global Notifications** view is displayed.
2. Click the **Servers** tab, select any syslog server.
3. Click  (edit icon) and click **Save**.

### (Conditional) Task 4 - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.0.x.x using the `pam_radius` package, you must reconfigure it in 11.2.0.0 using the `pam_radius_auth` package to achieve better performance. See “Configure PAM Login Capability” in the *RSA NetWitness® Platform 11.2 System Security and User Management Guide* for instructions. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## Endpoint Insights

### Task 5 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

You must reconfigure the Legacy Endpoint recurring feed due to the change in Java version. Complete the following step to fix this problem.

1. Import the NetWitness Endpoint CA certificate into the NetWitness Platform Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness Endpoint Integration Guide* to import the certificate.  
Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

### Task 6 - Restore Backed Up Endpoint Custom Meta Data Mappings

RSA recommends not to override any 11.2 default mappings unless required. If you backed up 11.1.x.x custom mappings, before updating to 11.2, review the list of custom mappings, and restore only those mappings that are not already in the default, using the `set-custom API` through `nw-shell`.

To modify any mappings, see *Endpoint Insights Configuration Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## Event Stream Analysis

These tasks apply to NetWitness Platform 11.2.0.0 customers using Event Stream Analysis.

### (Conditional) Task 7 - Reconfigure the “Suspected Command and Control Communication By Domain” Aggregation Rule for Automated Threat Detection

In 11.0, the “Suspected Command & Control Communication By Domain” aggregation rule Group By condition “Domain by Suspected C&C” was not functioning as expected and had to be changed to “Domain” to aggregate alerts and enable incidents to be created for “Suspected C&C.” The “Domain by Suspected C&C” condition works correctly in 11.2.0.0 and should be used as the Group By condition for the “Suspected Command & Control Communication By Domain” aggregation rule (known as incident rule in 11.2.0.0).

If you changed the “Suspected Command & Control Communication By Domain” aggregation rule Group By condition to “Domain” for 11.0, you will need to change it back to “Domain by Suspected C&C” for 11.2.0.0.

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules**.
2. In the Incident Rules list, locate the Suspected Command & Control Communication by Domain rule and click the link in the NAME field to open it.
3. In the Incident Rule Details view Grouping Options section, set the Group By field to Domain for Suspected C&C and click Save.

For more information, see the NetWitness Platform Automated Threat Detection Guide and the “Configure ESA Analytics” section of the NetWitness Platform ESA Configuration Guide. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.



## Respond

### Task 8 - Get the Latest Version of the Aggregation Rule Schema and Restore any Respond Service Custom Keys

Complete the following procedure to get the latest version of the Aggregation Rule Schema and restore any Respond service custom keys.

1. Delete the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file.
2. Restart the Respond server to get the latest version of the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file.  
`systemctl restart rsa-nw-respond-server`
3. If you added custom keys in `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.0, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys that you previously saved as an Update Preparation task.

**Note:** New Group By fields have been added to Respond in 11.2.0.0. The new Group By fields will not be visible in the NetWitness Platform user interface if you do not get the latest version of the file from the server.

## Task 9 - Get the Latest Version of the Respond Service Normalization Scripts and Restore any Customized Respond Service Normalization Scripts

RSA re-factored Respond service normalization scripts in the `/var/lib/netwitness/respond-server/scripts` directory in 11.2.0.0. You must replace the old versions.

Before the update to 11.2.0.0, you backed up the following files from the `/var/lib/netwitness/respond-server/scripts` directory.

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

Complete the following procedure to get the latest version of the normalization scripts.

1. After backing up the files listed above, delete the `/var/lib/netwitness/respond-server/scripts` directory and its contents.
2. Restart the Respond server.  
`systemctl restart rsa-nw-respond-server`
3. (Conditional ) Edit the new files to include any custom logic from the 11.0 scripts that were backed up.

**Note:** The following files changed with the 11.2.0.0 release:

```
normalize_alerts.js
aggregation_rule_schema.json
```

## Task 10 - Add Respond Notification Settings Permissions

**Note:** If you already configured these permissions in 11.1, you can skip this task.

Respond Notification Setting permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (**CONFIGURE > Respond Notifications**), which enable them to send email notifications when incidents are created or updated.

To access these settings, you will need to add additional permissions to your existing built-in NetWitness Platform user roles. You will also need to add permissions to your custom roles. See the “Respond Notification Settings Permissions” topic in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## Task 11 - Update Default Incident Rule Group By Values

Four of the default incident rules now use “Source IP Address” as the Group By value:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

To update the default rules, change the Group By value of the above default rules to “Source IP Address.”

**Note:** If you already updated the Group By values for the default rules listed above in 11.1, you do not have to do it again.

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules** and click on the rule that you want to update in the **Name** column. The **Incident Rule Details** view is displayed.
2. In the **GROUP BY** field, select the new Group By value from the drop-down list.
3. Click **Save** to update the rule.

To aggregate NetWitness Endpoint alerts based on the Detector IP Address, complete the following steps to clone the default NetWitness Endpoint incident rule and change the Group By IP address.

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules**. The **Incident Rules List** view is displayed.
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**. You will receive a message that you successfully cloned the selected rule.
3. Change the Name of the rule to an appropriate name, such as High Risk Alerts: NetWitness Endpoint Detector IP.
4. In the **GROUP BY** field, remove **Source IP Address** and add **Detector IP Address**. It is important that Detector IP Address is the only Group By value listed.
5. Click **Save** to create the rule.

For detailed information, see the *NetWitness Platform Respond Configuration Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

## NetWitness UEBA

### Task 12 - Install NetWitness UEBA

NetWitness UEBA is a new feature as of NetWitness® Platform 11.2.

See:

*RSA NetWitness Platform 11.2 Physical Host Installation Guide* for instructions for installation on a physical host.

*RSA NetWitness Platform 11.2 Virtual Host Installation Guide* for instructions for installation on a virtual host.

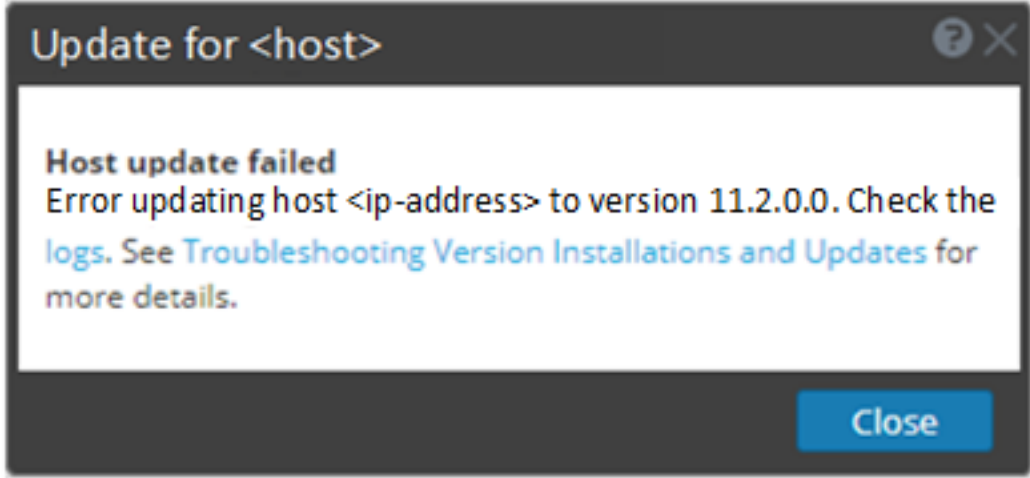
*RSA NetWitness UEBA User Guide* for information about UEBA.

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

6. Select **Manage System Settings** and **Manage Plugins**.

## Appendix A. Troubleshooting Version Installations and Updates

This section describes the error messages displayed in the **Hosts** view when it encounters problems updating host versions and installing services on hosts in the **Hosts** view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact Customer Support (<https://community.rsa.com/docs/DOC-1294>).

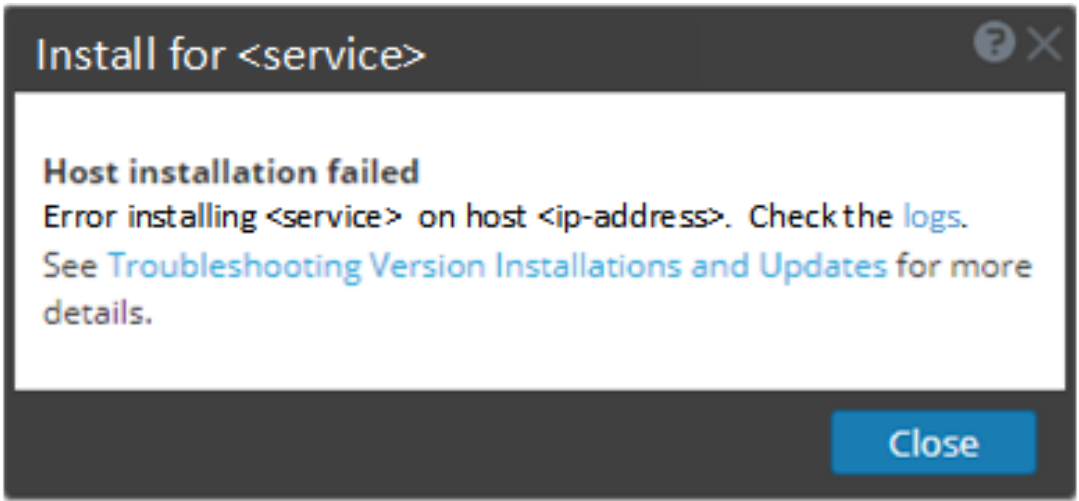
|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Message | <p><b>Host Update Failed</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Problem       | <p>When you select an update version and click <b>Update &gt; Update Host</b>, the download process is successful, but the update process fails.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Solution      | <ol style="list-style-type: none"> <li>1. Try to apply the version update to the host again.<br/>Often this is all you need to do.</li> <li>2. If you still cannot apply the new version update: <ol style="list-style-type: none"> <li>a. Monitor the following logs on NW Server as it progresses (for example, run the <code>tail -f</code> command from the command line): <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out </pre> The error appears in one or more of these logs. </li> <li>b. Try to resolve the issue and reapply the version update. <ul style="list-style-type: none"> <li>• Cause 1 - <code>deploy_admin</code> password has expired.<br/>Solution - Reset your <code>deploy_admin</code> password .</li> </ul> </li> </ol> </li> </ol> |

Complete the following steps to resolve Cause 1.

1. In the NetWitness Suite menu, select **ADMIN > Security > Users** tab.
2. Select the `deploy_admin` and click **Reset Password**.
3. (Conitional) If NetWitness Suite does not allow you to expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
  - a. Reset `deploy_admin` to use a new password.
  - b. On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.  
`/opt/rsa/saTools/bin/set-deploy-admin-password`
- Cause 2 -The `deploy_admin` password was changed on NW Server host but not changed on non-NW Server hosts.

Complete the following step to resolve Cause 2.

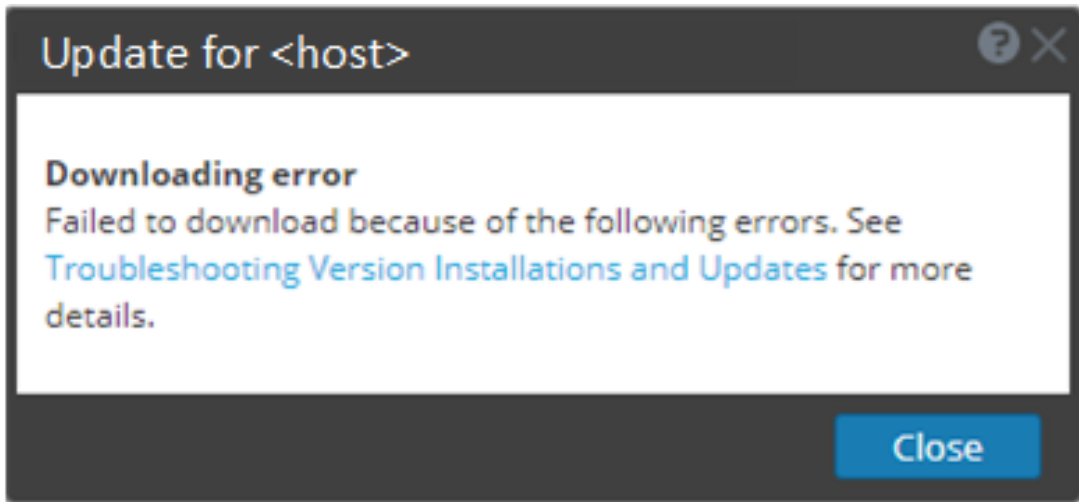
- On all non-NW Server hosts on 11.x , run the following command using the matching `deploy_admin` password from NW Server host.  
`/opt/rsa/saTools/bin/set-deploy-admin-password`
3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (<https://community.rsa.com/docs/DOC-1294>).

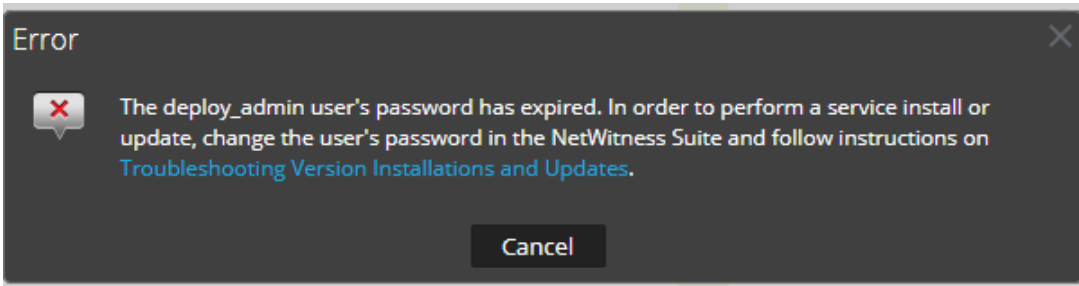
|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Message | <p><b>Host Installation Failed</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Problem       | <p>When you select a host and click <b>Install</b> the install service process fails.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Solution      | <ol style="list-style-type: none"> <li>1. Try to install the service again.<br/>Often this is all you need to do.</li> <li>2. If you still cannot install the service: <ol style="list-style-type: none"> <li>a. Monitor the following logs on NW Server as it progresses (for example, submit the <code>tail -f</code> command string from the command line'): <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out </pre> The error appears in one or more of these logs. </li> <li>b. Try to resolve the issue and reinstall the service. <ul style="list-style-type: none"> <li>• Cause 1 - Entered the wrong <code>deploy_admin</code> password in the <code>nwsetup-tui</code>.<br/>Solution - Retrieve your <code>deploy_admin</code> password.<br/>Complete the following steps to resolve Cause 1. <ol style="list-style-type: none"> <li>1. In the NetWitness Suite menu, select <b>ADMIN &gt; Security &gt; Users</b> tab.</li> <li>2. Select the <code>deploy_admin</code> and click <b>Reset Password</b>.</li> <li>3. (Conitional) If NetWitness Suite does not allow you to expired <code>deploy_admin</code> password in the <b>Reset Password</b> dialog, complete the following steps. <ol style="list-style-type: none"> <li>a. SSH to the NW Server host. <pre> security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name </pre> </li> </ol> </li> </ol> </li> </ul> </li> </ol> </li> </ol> |

```
platform.deployment.password -quiet
```


- b. SSH to the host that failed installation/orchestration.
  - c. Run the `nwsetup-tui` again using correct `deploy_admin` password.
- Cause 2 -The `deploy_admin` password has expired.  
Complete the following step to resolve Cause 2.
  1. In the NetWitness Suite menu, select **ADMIN > Security > Users** tab.
  2. Select the `deploy_admin` and click **Reset Password**.
  3. (Conditional) If NetWitness Suite allows you enter the expired `deploy_admin` password in the **Reset Password** dialog, complete the following steps.
    - a. Enter the expired `deploy_admin` password.
    - b. Uncheck the Force password change on next login checkbox.
    - c. Click **Save**.
  4. (Conditional) If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the Reset Password dialog, complete the following steps.
    - a. Reset `deploy_admin` to use a new password.
    - b. On all the NW Server host and all other hosts on 11.x, run the following command using the new `deploy_admin` password.  
`/opt/rsa/saTools/bin/set-deploy-admin-password`
    - c. On the host that failed installation/orchestration, run the `nwsetup-tui` and use the new `deploy_admin` password.
3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support (<https://community.rsa.com/docs/DOC-1294>).



|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Message | <p><b>Downloading Error</b></p>                                                                                                                                                                                                                                                                                                                                                  |
|               | <p><b>Problem</b></p> <p>When you select an update version and click <b>Update &gt;Update Host</b>, the download starts but fails to complete.</p>                                                                                                                                                                                                                                                                                                                 |
|               | <p><b>Cause</b></p> <p>Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.</p>                                                                                                                                                                                                                                                                                               |
|               | <p><b>Solution</b></p> <ol style="list-style-type: none"><li>1. Try to download it again.</li><li>2. If the download still fails, try to download it outside of NetWitness Suite as described in <a href="#">Apply Updates from the Command Line (No Web Access)</a>.</li><li>3. If you still cannot download the update file, contact Customer Support (<a href="https://community.rsa.com/docs/DOC-1294">https://community.rsa.com/docs/DOC-1294</a>).</li></ol> |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Message | <p><b>deploy_admin User's Password Has Expired</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Cause         | <p>The <code>deploy_admin</code> user password has expired.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Solution      | <p>Reset your <code>deploy_admin</code> password.</p> <ol style="list-style-type: none"> <li>1. In the NetWitness Suite menu, select <b>ADMIN &gt; Security &gt; Users</b> tab.</li> <li>2. Select the <b>deploy_admin</b> and click <b>Reset Password</b>. <ul style="list-style-type: none"> <li>• If NetWitness Suite allows you to enter the expired <code>deploy_admin</code> password in the <b>Reset Password</b> dialog, complete the following steps. <ol style="list-style-type: none"> <li>a. Enter the expired <code>deploy_admin</code> password.</li> <li>b. Uncheck the <b>Force password change on next login</b> checkbox.</li> <li>c. Click <b>Save</b></li> </ol> </li> <li>• If NetWitness Suite does not allow you to enter the expired <code>deploy_admin</code> password in the <b>Reset Password</b> dialog. <ol style="list-style-type: none"> <li>a. On the NW Server host and all other hosts on 11.x , run the following command using the new <code>deploy_admin</code> password.<br/> <code>/opt/rsa/saTools/bin/set-deploy-admin-password</code></li> <li>b. On the host that failed installation/orchestration, run the <code>nwsetup-tui</code> and use the new <code>deploy_admin</code> password.</li> </ol> </li> </ul> </li> </ol> |

|                      |                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Error Message</b> | <p>The <code>/var/log/netwitness/orchestration-server/orchestration-server.log</code> has an error similar to the following error:</p> <pre>API Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException Exception::Version '11.0.0.n' is not supported</pre> |
| <b>Problem</b>       | <p>After you update the NW Server host to 11.1, the only update path for the non-NW Server hosts is 11.1. If you try to update any non-NW Server host to an 11.0.0.n patch (for example from 11.0.0.0 to 11.0.0.3), you will get this error.</p>                                                          |
| <b>Solution</b>      | <p>You have two options:</p> <ul style="list-style-type: none"><li>• Update the non-NW Server host to 11.1, or</li><li>• Do not update the non-NW Server host (keep it at its current version).</li></ul>                                                                                                 |

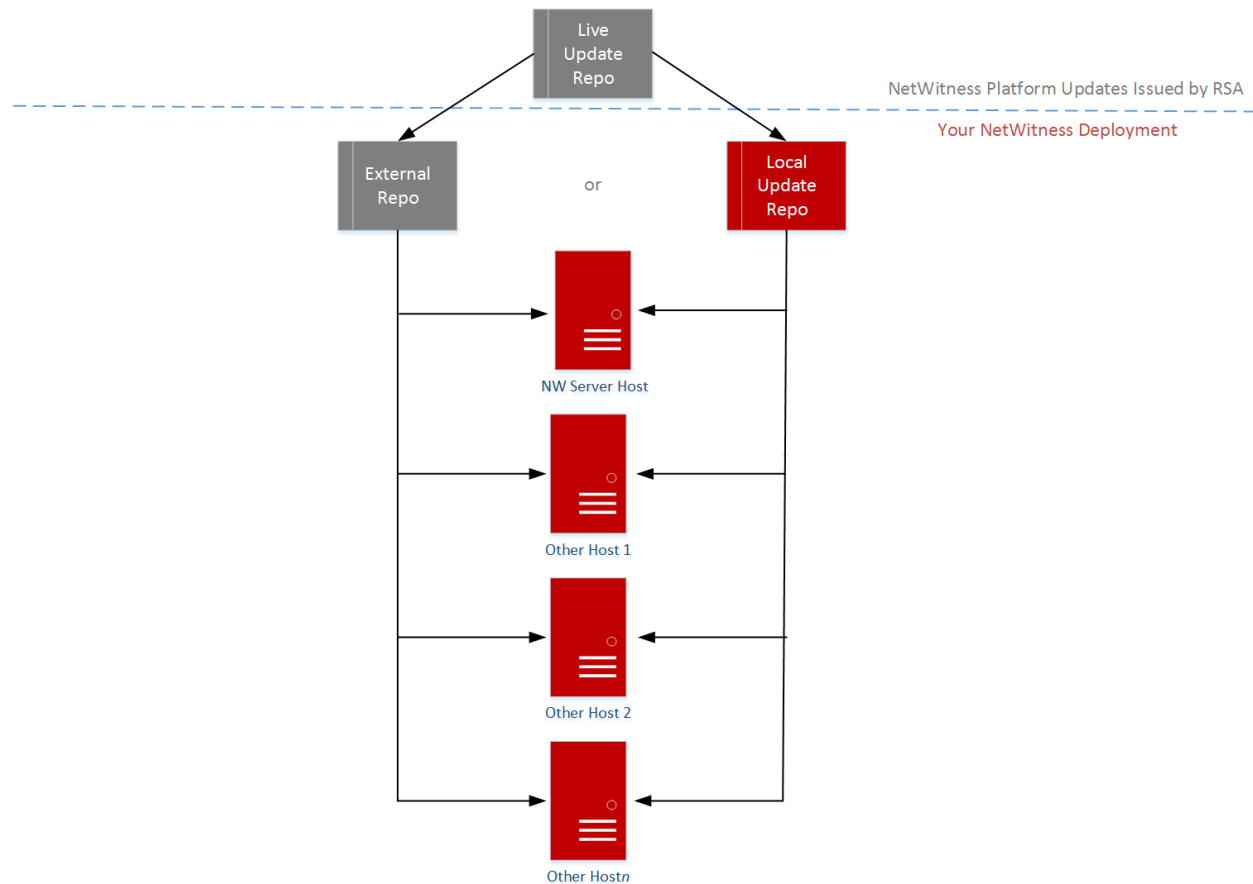
|                      |                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Error Message</b> | <p>You receive a message in the User Interface to reboot the host after you update and reboot the host offline.</p>  |
| <b>Cause</b>         | <p>You cannot use CLI to reboot the host. You must use the User Interface.</p>                                                                                                                           |
| <b>Solution</b>      | <p>Reboot the host in the Host View in the User Interface.</p>                                                                                                                                           |

## Appendix B. Populate Local Repo

NetWitness Platform sends version updates to the Local Update Repository from the Live Update Repository. Access to the Live Update Repository requires and uses the Live Account credentials configured under **ADMIN > SYSTEM > Live**. In addition, you must check the **Automatically download information about new updates every day** checkbox under **ADMIN > SYSTEM > Updates** to populate the Local Repo daily.

The following diagram illustrates how you obtain version updates if your NetWitness Platform deployment has Web Access.

**RSA** NetWitness Platform® 11.x.x.x Version Update Workflow – Web Access



**Note:** When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 7 system packages and the RSA Production packages. This download of over 2.5 GB of data takes an indeterminate amount of time depending on your NW Server Internet connection and the traffic of the RSA Repository. It is not mandatory to use the Live Update Repository. Alternatively you can use an External Repo as described in [Set Up an External Repository with RSA and OS Updates](#).

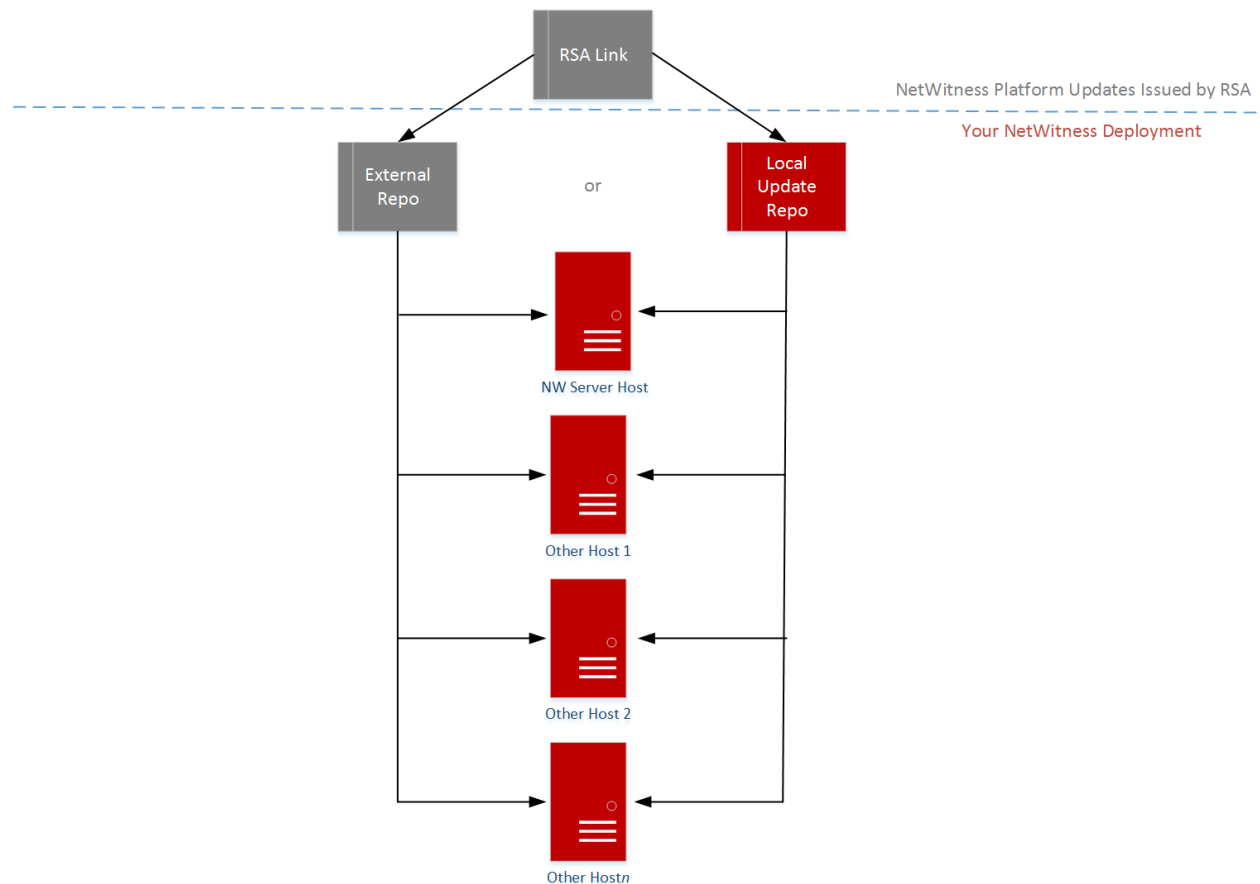
To connect to the Live Update Repository, go to the ADMIN > System view, select **Live Services** in the options panel and make sure that credentials are configured (**Connection** light should be green). If it is not green, click **Sign In** and connect.

**Note:** If you need to use proxy to reach out to the Live Update Repository, you can configure the Proxy Host, Proxy Username, and Proxy Password. For more information see "Configure Proxy for NetWitness Platform" in the *NetWitness Platform 1.1 System Configuration Guide*.

See [Apply Updates from the Command Line \(No Web Access\)](#) if your NetWitness Platform deployment does not have Web Access.

The following diagram illustrates how you obtain version updates if your NetWitness Platform deployment does not have Web Access.

**RSA** NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access



## Appendix C. Set Up External Repo

Complete the following procedure to set up an external repository (Repo).

**Note:** 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step if you have an external repo and you want to override it.
  - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
    - a. Create the `/etc/netwitness/platform/repobase` file.
 

```
vi /etc/netwitness/platform/netwitness/repobase
```
    - b. Edit the `repobase` file so that the only information in the file is the following URL.
 

```
https://nw-node-zero/nwrpmrepo
```
    - c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
  - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
    - a. Create the `/etc/netwitness/platform/repobase` file.
 

```
vi /etc/netwitness/platform/netwitness/repobase
```
    - b. Edit the `repobase` file so that the only information in the file is the following URL.
 

```
https://<webserver-ip>/<alias-for-repo>
```
    - c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.  
The instructions are in the [Apply Updates from the Command Line \(No Web Access\)](#).
2. Set up the external repo.
  - a. Log in to the web server host
  - b. Create directory to host the NW repository (`netwitness-11.2.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, `/var/netwitness` is the web-root, run the following command string.
 

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
  - c. Create the 11.2.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
 

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0
```
  - d. Create the OS and RSA directories under `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
 

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```
  - e. Unzip the `netwitness-11.2.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.2.0.0` directory.
 

```
unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0
```

Unzipping `netwitness-11.2.0.0.zip` results in two zip files (`OS-11.2.0.0.zip` and `RSA-11.2.0.0.zip`) and some other files.

f. Unzip the:

1. `OS-11.2.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
```

The following example illustrates how the Operating System (OS) file structure appears after you unzip the file.















|                                                                                                                                                           |                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|  <a href="#">Parent Directory</a>                                        | -                      |
|  <a href="#">GeoIP-1.5.0-11.el7.x86_64.rpm</a>                           | 20-Nov-2016 12:49 1.1M |
|  <a href="#">HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm</a> | 03-Oct-2017 10:07 4.6M |
|  <a href="#">Lib_Utils-1.00-09.noarch.rpm</a>                            | 03-Oct-2017 10:05 1.5M |
|  <a href="#">OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm</a>                  | 20-Nov-2016 14:43 502K |
|  <a href="#">OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm</a>              | 20-Nov-2016 14:43 15K  |
|  <a href="#">PyYAML-3.11-1.el7.x86_64.rpm</a>                            | 19-Dec-2017 12:30 160K |
|  <a href="#">SDL-1.2.15-14.el7.x86_64.rpm</a>                            | 25-Nov-2015 10:39 204K |
|  <a href="#">acl-2.2.51-12.el7.x86_64.rpm</a>                            | 03-Oct-2017 10:04 81K  |
|  <a href="#">adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm</a>      | 13-Feb-2018 05:10 706K |
|  <a href="#">alsa-lib-1.1.3-3.el7.x86_64.rpm</a>                        | 10-Aug-2017 10:52 421K |
|  <a href="#">at-3.1.13-22.el7_4.2.x86_64.rpm</a>                       | 25-Jan-2018 17:56 51K  |
|  <a href="#">atk-2.22.0-3.el7.x86_64.rpm</a>                           | 10-Aug-2017 10:53 258K |
|  <a href="#">attr-2.4.46-12.el7.x86_64.rpm</a>                         | 03-Oct-2017 10:04 66K  |

2. `RSA-11.2.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

The following example illustrates how the RSA version update file structure appears after

you unzip the file.

|                                                                                                                                                        |                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|  <a href="#">Parent Directory</a>                                     | -                      |
|  <a href="#">MegaCli-8.02.21-1.noarch.rpm</a>                         | 03-Oct-2017 10:07 1.2M |
|  <a href="#">OpenIPMI-2.0.19-15.el7.x86_64.rpm</a>                    | 03-Oct-2017 10:07 173K |
|  <a href="#">bind-utils-9.9.4-51.el7_4.2.x86_64.rpm</a>               | 22-Jan-2018 09:03 203K |
|  <a href="#">bzip2-1.0.6-13.el7.x86_64.rpm</a>                        | 03-Oct-2017 10:07 52K  |
|  <a href="#">cifs-utils-6.2-10.el7.x86_64.rpm</a>                     | 10-Aug-2017 11:14 85K  |
|  <a href="#">device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm</a> | 25-Jan-2018 17:56 134K |
|  <a href="#">dnsmasq-2.76-2.el7_4.2.x86_64.rpm</a>                    | 02-Oct-2017 19:36 277K |
|  <a href="#">elasticsearch-5.6.9.rpm</a>                              | 17-Apr-2018 09:37 32M  |
|  <a href="#">erlang-19.3-1.el7.centos.x86_64.rpm</a>                  | 03-Oct-2017 10:07 17K  |
|  <a href="#">fineserver-4.6.0-2.el7.x86_64.rpm</a>                    | 27-Feb-2018 09:11 1.3M |
|  <a href="#">htop-2.1.0-1.el7.x86_64.rpm</a>                          | 14-Feb-2018 19:23 102K |
|  <a href="#">i40e-zc-2.3.6.12-1dkms.noarch.rpm</a>                    | 04-May-2018 11:08 399K |
|  <a href="#">ipmitool-1.8.18-5.el7.x86_64.rpm</a>                     | 10-Aug-2017 12:41 441K |
|  <a href="#">iptables-services-1.4.21-18.3.el7_4.x86_64.rpm</a>       | 08-Mar-2018 09:20 51K  |
|  <a href="#">ixgbe-zc-5.0.4.12-dkms.noarch.rpm</a>                    | 04-May-2018 11:08 374K |

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

g. (Conditional - For Azure) Follow these steps for Azure update.

- i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
- ii. `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
- iii. `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
- iv. `createrepo .`
- h. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.2.0.0 Setup program (`nwsetup-tui`) prompt.



## Revision History

---

| Revision | Date      | Description           | Author |
|----------|-----------|-----------------------|--------|
| 1.0      | 15-Aug-18 | Release to Operations | IDD    |
| 1.1      | 4-Sep-18  | Post-RTO updates.     | IDD    |

