RSA NETWITNESS® SUITE

Update Guide

for Version 11.0.x to 11.1

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

License Agreement

Third-Party Licenses

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.

June 2018

Contents

Introduction

RSA NetWitness® Suite11.1.0.0 provides fixes for all products in the suite. The components of the suite are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, and Security sever), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, 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 Suite 11.1.0.0:

- 11.0.0.0 to 11.1.0.0
- 11.0.0.1 to 11.1.0.0
- 11.0.0.2 to 11.1.0.0
- 10.6.5.x to 11.1.0.0

  Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

  See the *RSA NetWitness Suite 10.6.5.x to 11.1 Physical Host Upgrade Guide* and *RSA NetWitness Suite 10.6.5.x to 11.1 Virtual Host Upgrade Guide* for instructions on how to upgrade 10.6.5.x to 11.1.0.0.

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 Suite 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 11.1 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 Suite 11.1.0.0. These tasks are organized by the following categories.

General

Reporting Engine

Respond

General

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.1.0.0.

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 11.1.0.0. 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

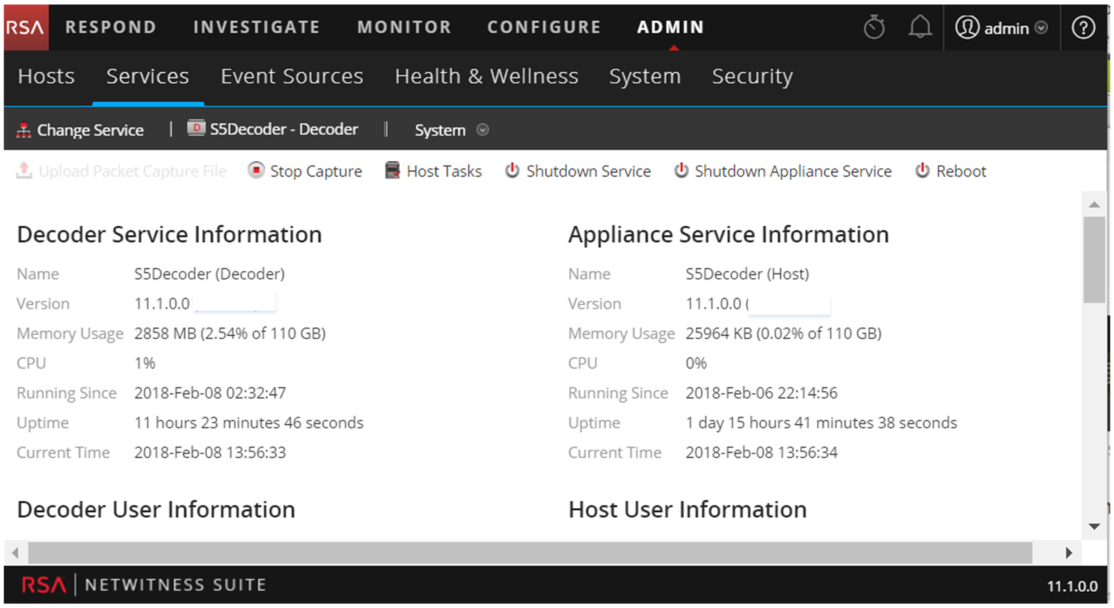
Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite 11.0.x and go to **ADMIN** > **Services**.

   The Services view is displayed.

2. Select each **Decoder** service.



Decoder Service Information

Name	S5Decoder (Decoder)
Version	11.1.0.0 [redacted]
Memory Usage	2858 MB (2.54% of 110 GB)
CPU	1%
Running Since	2018-Feb-08 02:32:47
Uptime	11 hours 23 minutes 46 seconds
Current Time	2018-Feb-08 13:56:33

Appliance Service Information

Name	S5Decoder (Host)
Version	11.1.0.0 ([redacted]
Memory Usage	25964 KB (0.02% of 110 GB)
CPU	0%
Running Since	2018-Feb-06 22:14:56
Uptime	1 day 15 hours 41 minutes 38 seconds
Current Time	2018-Feb-08 13:56:34

Decoder User Information

Host User Information

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

4. In the toolbar, click ● Stop Capture .

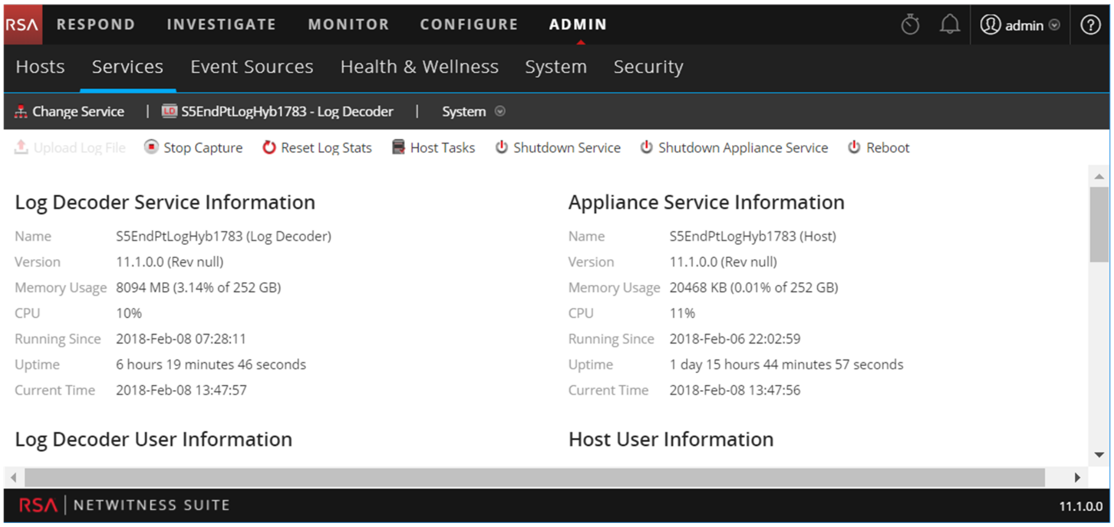
Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite 11.0.x and go to **ADMIN** > **Services**.

   The Services view is displayed.

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



RSA RESPOND INVESTIGATE MONITOR CONFIGURE **ADMIN** admin

Hosts | Services | Event Sources | Health & Wellness | System | Security

Change Service | S5EndPtLogHyb1783 - Log Decoder | System

Upload Log File | Stop Capture | Reset Log Stats | Host Tasks | Shutdown Service | Shutdown Appliance Service | Reboot

Log Decoder Service Information

Name	S5EndPtLogHyb1783 (Log Decoder)
Version	11.1.0.0 (Rev null)
Memory Usage	8094 MB (3.14% of 252 GB)
CPU	10%
Running Since	2018-Feb-08 07:28:11
Uptime	6 hours 19 minutes 46 seconds
Current Time	2018-Feb-08 13:47:57

Appliance Service Information

Name	S5EndPtLogHyb1783 (Host)
Version	11.1.0.0 (Rev null)
Memory Usage	20468 KB (0.01% of 252 GB)
CPU	11%
Running Since	2018-Feb-06 22:02:59
Uptime	1 day 15 hours 44 minutes 57 seconds
Current Time	2018-Feb-08 13:47:56

Log Decoder User Information

Host User Information

RSA | NETWITNESS SUITE 11.1.0.0

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

4. In the toolbar, click ● Stop Capture .

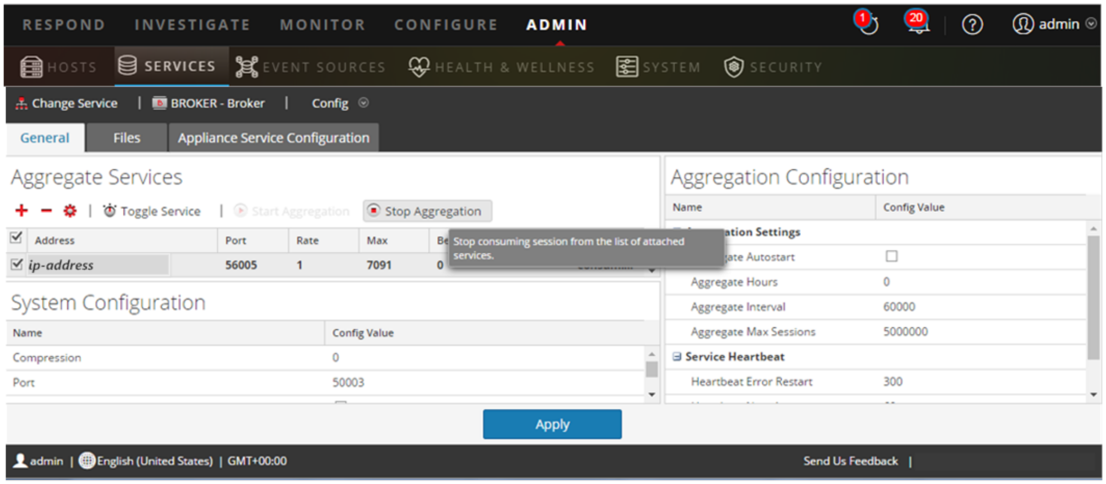
Stop Aggregation

1. Log in to NetWitness Suite 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.



RESPOND INVESTIGATE MONITOR CONFIGURE **ADMIN** 1 20 admin

HOSTS | SERVICES | EVENT SOURCES | HEALTH & WELLNESS | SYSTEM | SECURITY

Change Service | BROKER - Broker | Config

General | Files | Appliance Service Configuration

Aggregate Services

+ − ⚙ | Toggle Service | Start Aggregation | Stop Aggregation

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

Stop consuming session from the list of attached services.

System Configuration

Name	Config Value
Compression	0
Port	50003

Aggregation Configuration

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

Apply

admin | English (United States) | GMT+00:00 Send Us Feedback |

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

Task 4 - Make Sure That `deploy_admin` User Credentials Are Still Valid (Not Expired)

You must have valid (not exipred) `deploy_admin` user credentials to update to 11.1.

Part I. Verify Expiration Status of `deploy_admin` User Credentials

Complete the following procedure to determine if the `deploy_admin` user credentials have expired.

1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab.
2. Make sure that the `deploy_admin` has not expired.
   - If they are still valid, you can proceed with the update.
   - If they have expired , complete Part II of this task.

(Conditional) Part II. Reset Expired `deploy_admin` User Credentials

Complete the following procedure to reset expired `deploy_admin` user credentials.

1. Select the `deploy_admin` and click **Reset Password**.
2. (Conditional) If NetWitness Suite allows you to 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**.
3. (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.

Reporting Engine

Task 5 - 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 Suite11.1 Reporting Engine Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

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

Respond

Task 6 - (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 7 - 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 11.1.0.0. You need to back them up in 11.0.x before you update to 11.1.0.0 so you can restore them in 11.1.0.0 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 11.1.0.0.

Task 8 - (Conditional - For Azure Stack)

Populate the Repo with the additional packages.

1. If using a local repository, extract the Azure Zip from the following steps on the Admin server:

a. Run as root: `mkdir -p /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

b. Unzip to the above directory: `unzip nw-azure-11.1-extras.zip -d /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

2. If you are using external repo, follow these steps:

a. After setting up the 11.1.0.0 content on the external repo, unzip the nw-azure-11.1-extras.zip to the external repo directory's <base-directory>11.1.0.0/OS/other folder.

b. Run createrepo from the external repository's 11.1.0.0/OS directory.

Update Tasks

Complete the following tasks to update NetWitness Suite 11.0.x.x to 11.1.0.0.

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 Suite 11.1.0.0 that is different from the repo you have set up now for 11.0.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 11.1.0.0, 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.

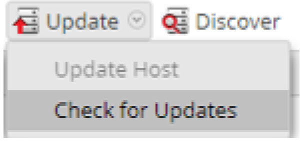
If you selected an External Repo, you must set it up. See Appendix C. Set Up External Repo for instructions on how to set up an external repo.

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

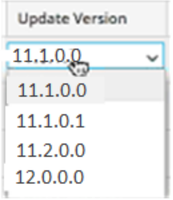
The Hosts view displays the software version updates available in your Local Update Repository and you choose and apply the updates you want from the Host view.

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

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



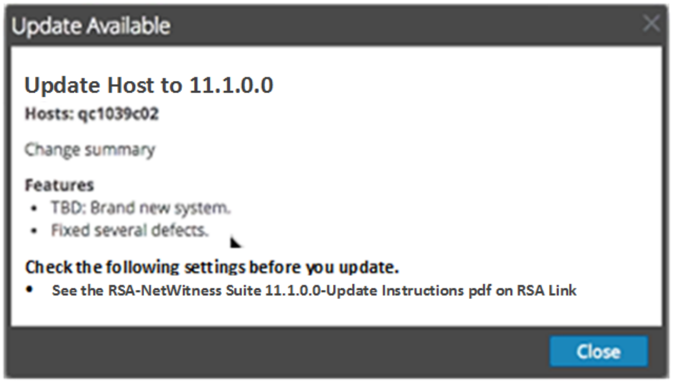
4. Select a host or hosts.
   You must update the NW Server to latest version first. You can update the other hosts in any sequence you prefer, but RSA recommends that you follow the guidelines in "Running in Mixed Mode" in the *RSA NetWitness Suite Hosts and Services Getting Started Guide* for further 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.



Update Available

Update Host to 11.1.0.0

Hosts: qc1039c02

Change summary

Features

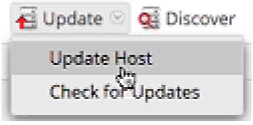
- TBD: Brand new system.
- Fixed several defects.

Check the following settings before you update.

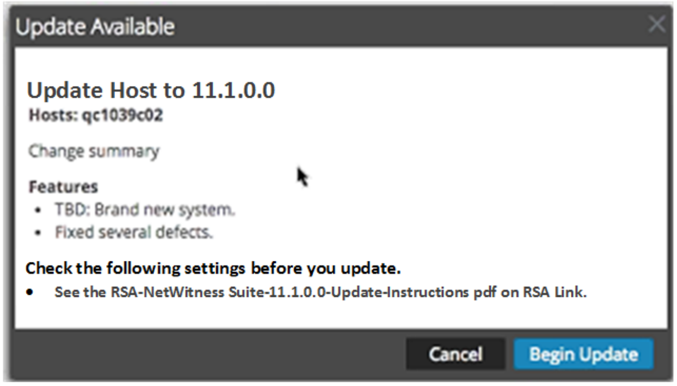
- See the RSA-NetWitness Suite 11.1.0.0-Update Instructions pdf on RSA Link

- 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**.



Update Available

Update Host to 11.1.0.0

Hosts: qc1039c02

Change summary

Features

- TBD: Brand new system.
- Fixed several defects.

Check the following settings before you update.

- See the RSA-NetWitness Suite-11.1.0.0-Update-Instructions pdf on RSA Link.

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 Suite prompts you to **Reboot Host**.

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

   NetWitness Suite 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: 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.

Apply Updates from the Command Line (No Web Access)

If your RSA NetWitness Suite 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-11.1.0.0.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/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Unzip the package into the staging directory you created (for example, `tmp/upgrade/11.1.0.0`) .
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Initialize the update on the NW Server.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Apply the update to the NW Server.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Log in to NetWitness Suite 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 11.1.0.0
   ```
   The update is complete when the polling is completed.
9. Log in to NetWitnesss Suite 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
   ```

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness Legacy Windows Collection Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 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 Suite 11.1.0.0.

- General
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Respond

General

These tasks apply to all NetWitness Suite 11.1.0.0 customers.

Task 1 - Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.1.0.0.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Suite** 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

To start log capture:

1. In the **NetWitness Suite** 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

To start aggregation:

1. In the **NetWitness Suite** 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 .

NW Server

Task 2 - (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 11.1.0.0, 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 Suite** 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 3 - 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 11.1.0.0 using the `pam_radius_auth package` to achieve better performance. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite 11.1 System Security and User Management Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint

Task 4 - 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.

- Import the NetWitness Endpoint CA certificate into the NetWitness Suite 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 11.1 Endpoint Integration Guide* to import the certificate.
  Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® Endpoint Insights

(Optional) Task 5 - Install Endpoint Hybrid or Endpoint Log Hybrid

See:

RSA NetWitness Suite 11.1 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Suite 11.1 Virtual Host Installation Guide for instructions for installation on a virtual host.

Event Stream Analysis

These tasks apply to NetWitness Suite 11.1.0.0 customers using Event Stream Analysis.

(Conditional) Task 6 - 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 11.1.0.0 and should be used as the Group By condition for the “Suspected Command & Control Communication By Domain” aggregation rule (known as incident rule in 11.1.0.0).

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 11.1.0.0.

1. Log in to NetWitness Suite 11.1.0.0.
2. Go to **CONFIGURE** > **Incident Rules**.
3. 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.
4. 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 Suite Automated Threat Detection Guide and the “Configure ESA Analytics” section of the NetWitness Suite ESA Configuration Guide. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

Task 7 - (Conditional) 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 11.1.0.0. The new Group By fields will not be visible in the NetWitness Suite user interface if you do not get the latest version of the file from the server.

Task 8 - 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 11.1.0.0. You must replace the old versions.

Before the update to 11.1.0.0, 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 11.1.0.0 release:
> ```
> normalize_alerts.js
> normalize_core_alerts.js
> normalize_ma_alerts.js
> ```

Task 9 - Add Respond Notification Settings Permissions

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 Suite 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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 10 - Update Default Incident Rule Group By Values

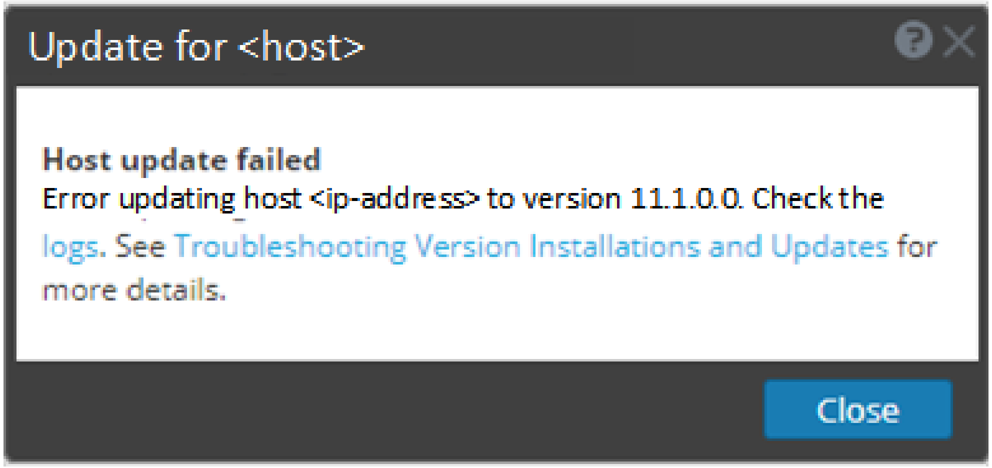
Four of the default incident rules now use “Source IP Address” as the Group By value. To update the default rules, change the Group By value of the following default rules to “Source IP Address”:

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

1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update. The Incident Rule Details view is displayed.
2. In the **Group By** field, select the new Group By value.
3. Click **Save** to update the rule.

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	 **Host update failed** Error updating host <ip-address> to version 11.1.0.0. Check the logs. See Troubleshooting Version Installations and Updates for more details.
Problem	When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails.

Solution	1. **Try to apply the version update to the host again**.
	Often this is all you need to do.
	2. If you still cannot apply the new version update:
	a. Monitor the following logs on NW Server as it progresses (for example, use submit the `tail -f` command string from the command line'):
	`/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`
	The error will appear in one or more of these logs.

b. Try to resolve the issue and reapply the version update.

- Cause 1 - `deploy_admin` password has expired.
  Solution - Reset your `deploy_admin` password .
  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
     ```

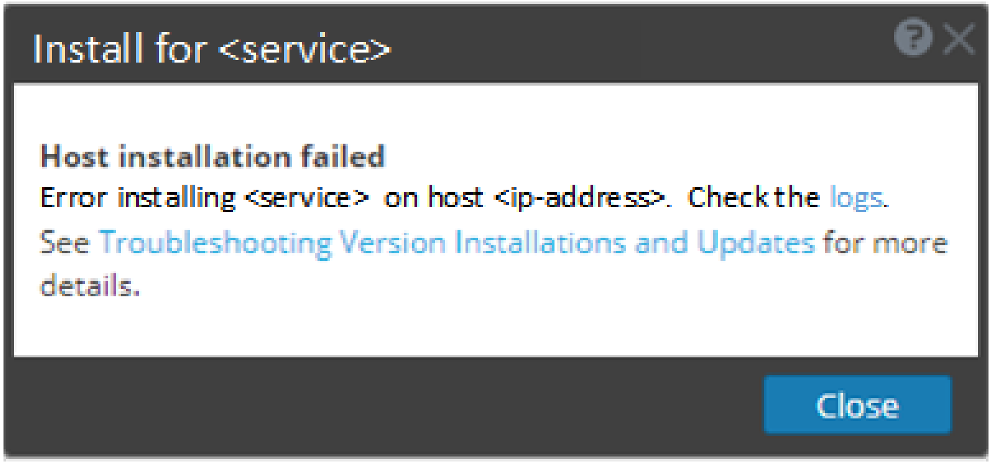
- Cause 2 -The `deploy_admin` password was changed on NW Server host but not changed on non-NW Server hosts.
  Complete the following step to resolve Cause 2.

  ■ 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



Install for <service>

Host installation failed

Error installing <service> on host <ip-address>. Check the logs.
See Troubleshooting Version Installations and Updates for more details.

Problem

When you select a host and click **Install** the install service process fails.

Solution

1. **Try to install the service again.**.

   Often this is all you need to do.

2. If you still cannot install the service:

   a. Monitor the following logs on NW Server as it progresses (for example, submit the `tail -f` command string from the command line'):

   ```
   /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
   ```

   The error will appear in one or more of these logs.

   b. Try to resolve the issue and reinstall the service.

   - Cause 1 - Entered the wrong`deploy_admin` password in the nwsetup-tui.

     Solution - Retrieve your `deploy_admin` password.

     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. SSH to the NW Server host.
   ```
   security-cli-client --get-config-prop --prop-
   hierarchy
   nw.security-client --prop-name
   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**.

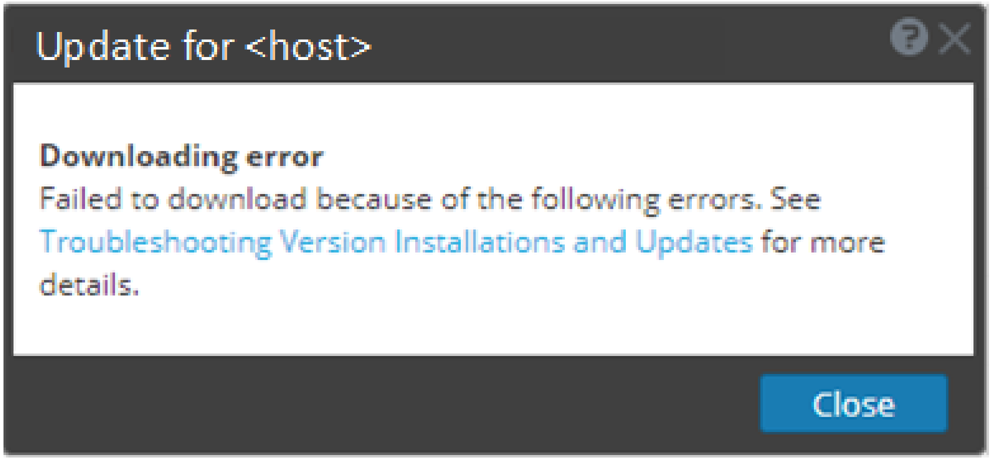
  4. (Conditional) If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the Reset Password dialog, complete the following steps.

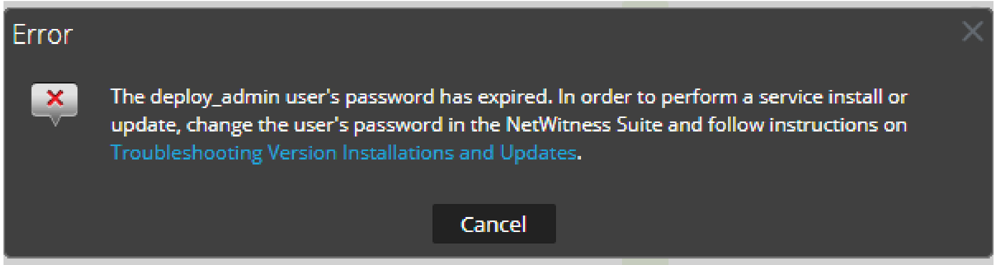
     a. Reset `deploy_admin` to use a new password.

     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	 **Downloading error** Failed to download because of the following errors. See Troubleshooting Version Installations and Updates for more details.
Problem	When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete.
Cause	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
Solution	1. Try to download it again. 2. If the download still fails, try to download it outside of NetWitness Suite as described in Apply Updates from the Command Line (No Web Access). 3. If you still cannot download the update file, contact Customer Support (https://community.rsa.com/docs/DOC-1294).

Error Message	 Error The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on Troubleshooting Version Installations and Updates.
Cause	The `deploy_admin` user password has expired.
Solution	Reset your `deploy_admin` password password. 1. In the NetWitness Suite menu, select **ADMIN** > **Security** > **Users** tab. 2. Select the **deploy_admin** and click **Reset Password**. • If NetWitness Suite allows you to 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** • If NetWitness Suite does not allow you to enter the expired `deploy_admin` password in the **Reset Password** dialog. a. On 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` b. On the host that failed installation/orchestration, run the nwsetup-tui and use the new `deploy_admin` password.

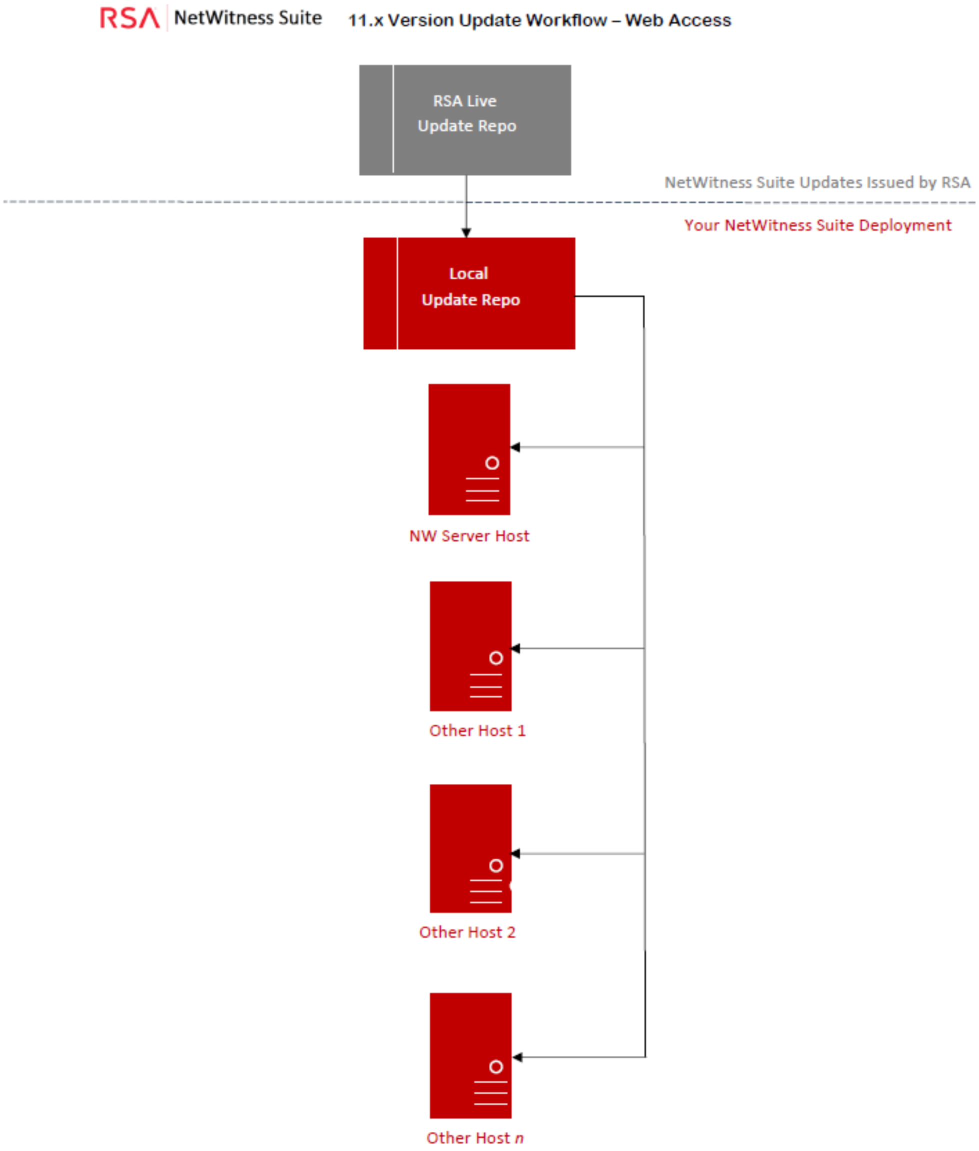
Error Message	The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error: `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgument Exception::Version '11.0.0.n' is not supported`
Problem	After you update 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.

Solution	You have two options: • Update the non-NW Server host to 11.1, or • Do not update the non-NW Server host (keep it at its current version).

Appendix B. Populate Local Repo

NetWitness Suite 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 Suite deployment has Web Access.


RSA NetWitness Suite
11.x Version Update Workflow – Web Access
RSA Live Update Repo
NetWitness Suite Updates Issued by RSA
Your NetWitness Suite Deployment
Local Update Repo
NW Server Host
Other Host 1
Other Host 2
Other Host *n*

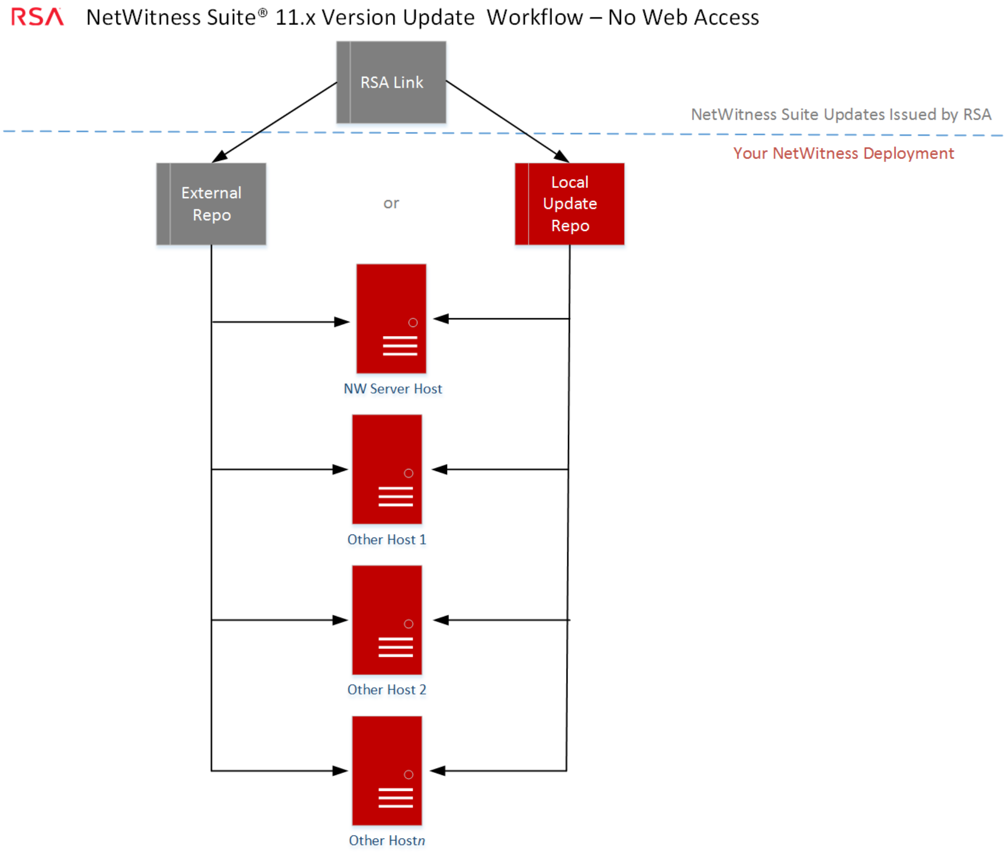
Note: When you make the initial connection with the Live Update Repository, you will be accessing all the CentOS 7 system packages and the RSA Production packages. This download of over 2.5GB of data will take an indeterminate amount of time depending on your NW Server Internet connection and the traffic 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 Repo."

To connect to the Live Update Repository, Navigate to the **ADMIN > SYSTEM** view, select **Live** in the options panel and ensure 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. Refer to "Configure Proxy forNetWitness Suite" in the *NetWitness Suite 1.1 System Configuration Guide*.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

See "Apply Updates from Command Line" if your NetWitness Suite deployment does not have Web Access.

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


RSA
NetWitness Suite® 11.x Version Update Workflow – No Web Access
RSA Link
NetWitness Suite Updates Issued by RSA
Your NetWitness Deployment
External Repo
or
Local Update Repo
NW Server Host
Other Host 1
Other Host 2
Other Hostn

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.
     See for the instructions.
   - 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" under topic.
2. Set up the external repo.
   a. Log in to the web server host
   b. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo`under `web-root` of the web server. For example, /var/netwitness is the web-root, submit the following command string.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>
   ```
   c. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0
   ```

d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

e. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.

```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

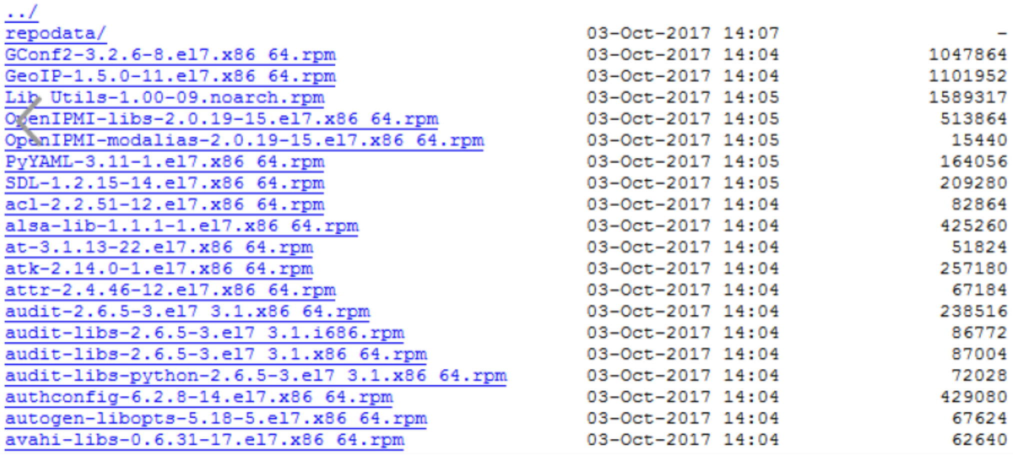
Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.

f. Unzip the:

1. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
```

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

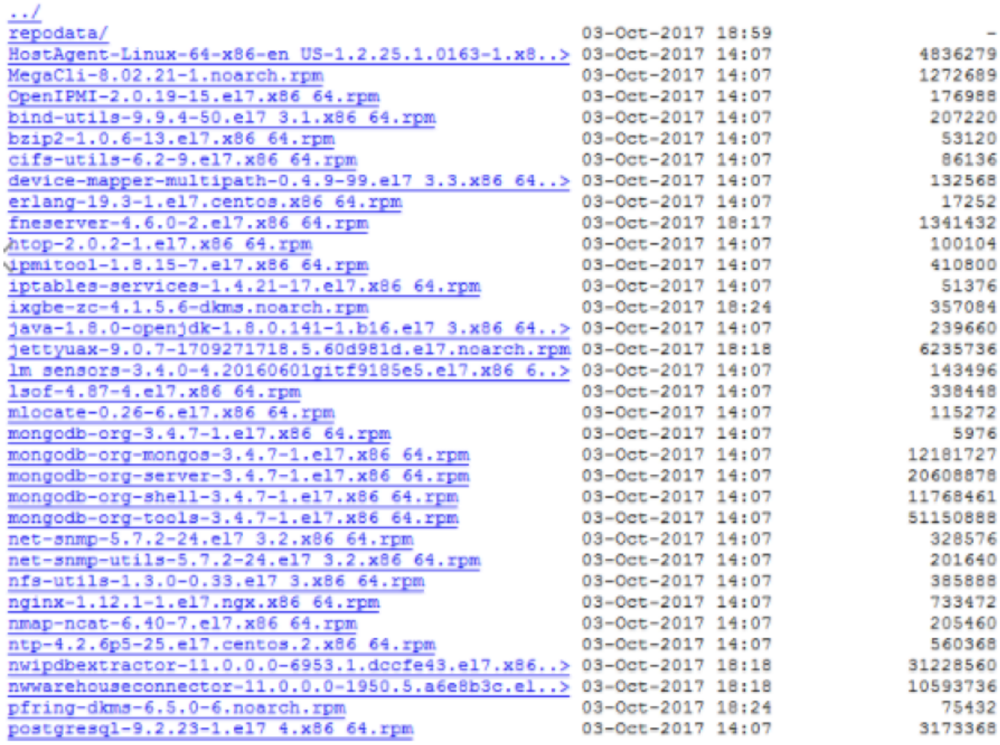


```
../
repodata/                                        03-Oct-2017 14:07                   -
GConf2-3.2.6-8.el7.x86_64.rpm                    03-Oct-2017 14:04             1047864
GeoIP-1.5.0-11.el7.x86_64.rpm                    03-Oct-2017 14:04             1101952
Lib_Utils-1.00-09.noarch.rpm                     03-Oct-2017 14:05             1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm           03-Oct-2017 14:05              513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm       03-Oct-2017 14:05               15440
PyYAML-3.11-1.el7.x86_64.rpm                     03-Oct-2017 14:05              164056
SDL-1.2.15-14.el7.x86_64.rpm                     03-Oct-2017 14:05              209280
acl-2.2.51-12.el7.x86_64.rpm                     03-Oct-2017 14:04               82864
alsa-lib-1.1.1-1.el7.x86_64.rpm                  03-Oct-2017 14:04              425260
at-3.1.13-22.el7.x86_64.rpm                      03-Oct-2017 14:04               51824
atk-2.14.0-1.el7.x86_64.rpm                      03-Oct-2017 14:04              257180
attr-2.4.46-12.el7.x86_64.rpm                    03-Oct-2017 14:04               67184
audit-2.6.5-3.el7_3.1.x86_64.rpm                 03-Oct-2017 14:04              238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm              03-Oct-2017 14:04               86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm            03-Oct-2017 14:04               87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm     03-Oct-2017 14:04               72028
authconfig-6.2.8-14.el7.x86_64.rpm               03-Oct-2017 14:04              429080
autogen-libopts-5.18-5.el7.x86_64.rpm            03-Oct-2017 14:04               67624
avahi-libs-0.6.31-17.el7.x86_64.rpm              03-Oct-2017 14:04               62640
```

2. `RSA-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA` directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

The following example illustrates how the RSA version update file structure will appear after you unzip the file.



```
../
repodata/                                          03-Oct-2017 18:59                   -
HostAgent-Linux-64-x86-en US-1.2.25.1.0163-1.x8..> 03-Oct-2017 14:07             4836279
MegaCli-8.02.21-1.noarch.rpm                       03-Oct-2017 14:07             1272689
OpenIPMI-2.0.19-15.el7.x86 64.rpm                  03-Oct-2017 14:07              176988
bind-utils-9.9.4-50.el7 3.1.x86 64.rpm             03-Oct-2017 14:07              207220
bzip2-1.0.6-13.el7.x86 64.rpm                      03-Oct-2017 14:07               53120
cifs-utils-6.2-9.el7.x86 64.rpm                    03-Oct-2017 14:07               86136
device-mapper-multipath-0.4.9-99.el7 3.3.x86 64..> 03-Oct-2017 14:07              132568
erlang-19.3-1.el7.centos.x86 64.rpm                03-Oct-2017 14:07               17252
fneserver-4.6.0-2.el7.x86 64.rpm                   03-Oct-2017 18:17             1341432
htop-2.0.2-1.el7.x86 64.rpm                        03-Oct-2017 14:07              100104
ipmitool-1.8.15-7.el7.x86 64.rpm                   03-Oct-2017 14:07              410800
iptables-services-1.4.21-17.el7.x86 64.rpm         03-Oct-2017 14:07               51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm                   03-Oct-2017 18:24              357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7 3.x86 64..> 03-Oct-2017 14:07              239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm 03-Oct-2017 18:18             6235736
lm sensors-3.4.0-4.20160601gitf9185e5.el7.x86 6..> 03-Oct-2017 14:07              143496
lsof-4.87-4.el7.x86 64.rpm                         03-Oct-2017 14:07              338448
mlocate-0.26-6.el7.x86 64.rpm                      03-Oct-2017 14:07              115272
mongodb-org-3.4.7-1.el7.x86 64.rpm                 03-Oct-2017 14:07                5976
mongodb-org-mongos-3.4.7-1.el7.x86 64.rpm          03-Oct-2017 14:07            12181727
mongodb-org-server-3.4.7-1.el7.x86 64.rpm          03-Oct-2017 14:07            20608878
mongodb-org-shell-3.4.7-1.el7.x86 64.rpm           03-Oct-2017 14:07            11768461
mongodb-org-tools-3.4.7-1.el7.x86 64.rpm           03-Oct-2017 14:07            51150888
net-snmp-5.7.2-24.el7 3.2.x86 64.rpm               03-Oct-2017 14:07              328576
net-snmp-utils-5.7.2-24.el7 3.2.x86 64.rpm         03-Oct-2017 14:07              201640
nfs-utils-1.3.0-0.33.el7 3.x86 64.rpm              03-Oct-2017 14:07              385888
nginx-1.12.1-1.el7.ngx.x86 64.rpm                  03-Oct-2017 14:07              733472
nmap-ncat-6.40-7.el7.x86 64.rpm                    03-Oct-2017 14:07              205460
ntp-4.2.6p5-25.el7.centos.2.x86 64.rpm             03-Oct-2017 14:07              560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..> 03-Oct-2017 18:18            31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..> 03-Oct-2017 18:18            10593736
pfring-dkms-6.5.0-6.noarch.rpm                     03-Oct-2017 18:24               75432
postgresql-9.2.23-1.el7 4.x86 64.rpm               03-Oct-2017 14:07             3173368
```

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>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/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 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD
1.1	12-Mar-17	Change to note at the start of the Update Tasks concerning an external repository.	IDD
1.2	12-Apr-18	Added "Task 4 - Make Sure That `deploy_admin` User Credentials Are Still Valid (Not Expired)" to the Update Preparation Tasks.	IDD
1.3	31-May-18	Added note to Introduction on Resetting of Entropy=log2 flag in 11.1.	IDD
1.4	11-Jun-18	Fixed directory path in Appendix C. Set Up External Repo (from `/etc/platform/repobase` to `/etc/netwitness/platform/repobase` .	