RSA NETWITNESS® PLATFORM

AWS Upgrade Guide

for RSA NetWitness® Platform 10.6.6.x to 11.4

Contents

Introduction

The instructions in this guide apply to the upgrade of AWS for RSA NetWitness Platform 10.6.6.x to 11.4 exclusively.For instructions on how to upgrade your 10.6.6.x physical hosts to 11.4. See the *RSA NetWitness Platform Physical Host Upgrade Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.This document assumes that the appliances are in AWS cloud.

NetWitness Platform 11.4 is a major release that affects all products in the NetWitness Platform suite. The components of the suite are the NetWitness Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoit Log Hybrid, Endpoint Broker, User Entity Behavior Analytics , Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, and Workbench.

CentOS6 to CentOS7 Upgrade

NetWitness Platform 11.4 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.4 platform environment is improved to accommodate current and future physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Platform 11.4 Upgrade Path

The supported upgrade path for RSA NetWitness® Platform 11.4 is Security Analytics 10.6.6.x. If you are running a version of NetWitness Platform that is prior to 10.6.6.x, you must update to 10.6.6.x before you can upgrade to 11.4. For more information, see the *RSA Security Analytics 10.6.6 Update Guide* on RSA Link.

> **Caution:** There is a known issue if you have Active Directory users configured in 10.6.6.x. You have two options to address this issue:
> • Apply the 10.6.4.2 patch before you back up your data for the 11.4 upgrade.

> **Note:** If you are updating from 11.0 to 11.4, see *Update Guide for Version 11.1 to 11.4* on RSA link.

Hardware, Deployments, Services, and Features Not Supported in 11.4

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.4.

- RSA All-in-One (AIO) Appliance

- Multiple NetWitness Server Deployment

- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.0.)

- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.4, your custom policy is not present. Instead for version 11.4, there is an OOTB Context hub Server Monitoring Policy in the user interface.

- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.

- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Platform 11.4, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.0, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.4.x is removed.

> **Caution:** If you have not used Incident Management in 10.6.4.x, carefully consider whether or not to upgrade to version 11.0.

The following guidelines help you determine whether or not to upgrade your ESA hosts to 11.4.

In your 10.6.4.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.0.

  - Multiple ESA hosts configured to use Incident Management – The system continues to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.4.x, you can upgrade to version 11.0.

- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.0.

> **Note:** If you have not used Incident Management in 10.6.4.x, you cannot view the 10.6.4.x ESA alerts in the 11.0 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.0 that will allow Respond to view them. For more information for instructions on how to run the script, see the *ESA Alert Migration Instructions for 10.6.4.x to 11.0* knowledge base article (https://community.rsa.com/docs/DOC-81680) in RSA Link .

User Attribute and Role Changes Affecting Investigate

The following changes affect how NetWitness Platform 11.3 handles user and role attributes in the Investigate component.

- User Attributes
  When you upgrade to 11.4, the user attributes (query prefix, session timeout, and query threshold) available in SA 10.6.6.x no longer exist. The same attributes are available at the role level for use.

- User and Role Attributes (Query Prefix) is not applicable to Investigate Event Analysis. The user and role attributes, most importantly the query prefix, do not apply to the new Investigate Event Analysis. Any user can modify the URL in browser to access data that should be restricted from viewing even when query prefix is applied.

RSA NetWitness Suite® 11.0 AWS Upgrade Workflow
Phase 1 – Upgrade SA Server, ESA, and Malware
Phase 2 – Upgrade All Other Hosts
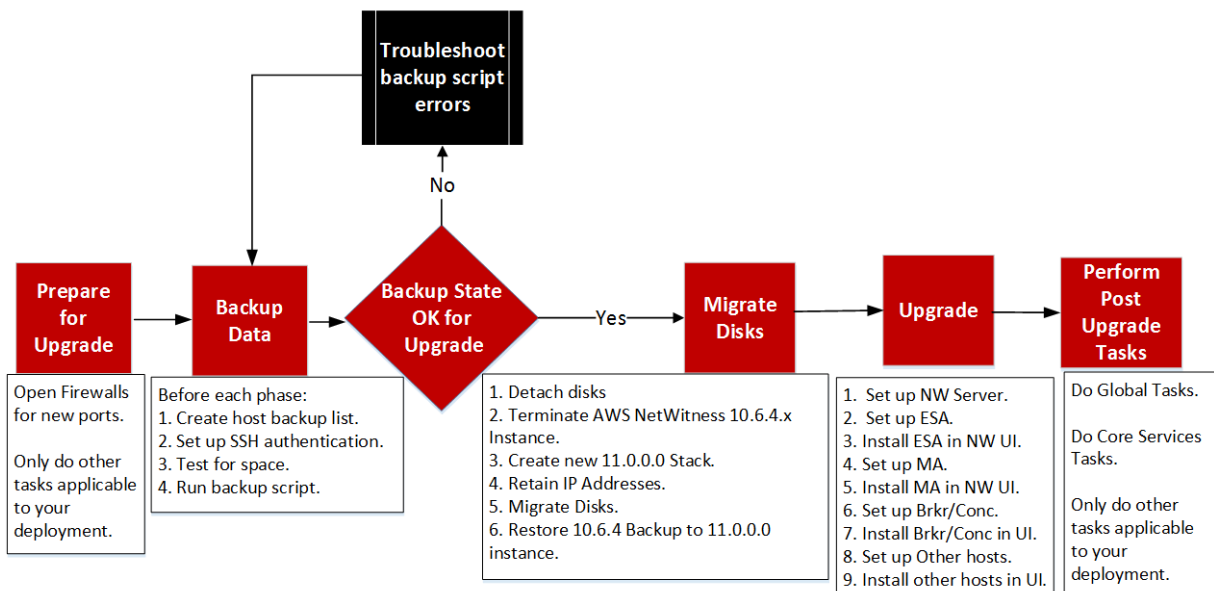
Contact Customer Support

Refer to the Contact RSA Customer Support page (https://community.rsa.com/docs/DOC-1294) in RSA Link for instructions on how to get help on RSA NetWitness Platform 11.4.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Platform 11.4. These tasks are organized by the following categories.

- General

- Event Stream Analysis (ESA)

- Reporting Engine

- Respond

- Warehouse Connector

- Other

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

General

Task 1 - Review Core Ports and Open Firewall Ports

The following tables list new ports in 11.4.

> **Caution:** Make sure that the new ports are implemented and tested before upgrading so that upgrade does not fail due to missing ports.

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 27017	MongoDB
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
NW Hosts	NW Server	TCP 15671	RabbitMQ Management UI

ESA Host

Source Host	Destination Host	Destination Ports	Comments
NW Server, NW Endpoint, ESA Secondary	ESA Primary	TCP 27017	MongoDB

Endpoint Log Hybrid

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

All NetWitness Platform core ports are listed in the "Network Architecture and Ports" topic in the *Deployment Guide* in case you need to reconfigure NetWitness Platform services and firewalls.

Task 2 - Record Your 10.6.6.x `admin user` Password

Record your 10.6.6.x `admin user` password. You will need it to complete the upgrade.

Task 3 - Create a Backup of the `/etc/fstab` File

Copy the `/etc/fstab` file from all the physical hosts and into your local machine (backup host or remote machine).

> **Note:** You need this file to restore a physical host with external storage mounts.

Task 4 - Make Sure Password Strength Settings Check Boxes Are Set in 10.6.6.x

The check box to the left of the **Password Strength Settings** in the **Administration** > **Security** > **Settings** tab must be set in 10.6.6.x or these settings will not be migrated to 11.4.

Complete the following task to make sure that the Password Strength Settings check boxes are set in 10.6.6.x.

1. In Security Analytics 10.6.6.x, go to the **Administration** > **Security** > **Settings** tab.

2. Make sure that all of the check boxes to the left of the **Password Strength Settings** are set. If they are not, set them and click **Apply**.

The following example shows all check boxes as set (required in 10.6.6.x before upgrading to 11.4).
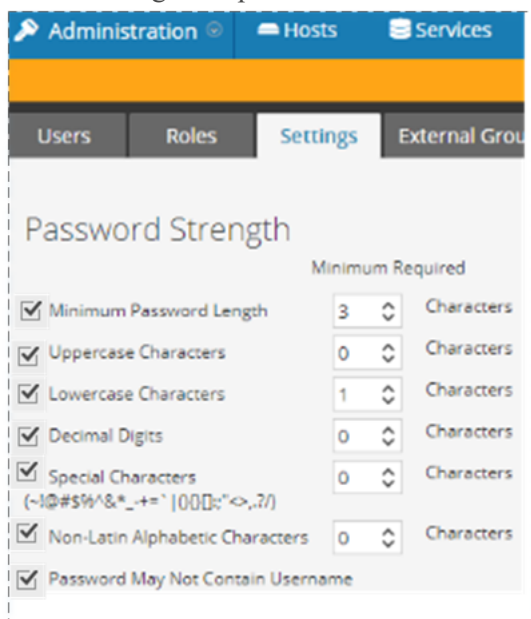
Task 5 (Conditional) - Extract 10.6.x Public Key Infrastructure (PKI) Certificates

Before you upgrade to from 10.6.6.x to 11.4, complete the following procedure to extract the existing 10.6.x PKI keystores that contain server certificates with private keys, and the truststores that contain the trusted CA certificates.

1. Download the `rsa-nw-pki-migration-10.6.6.zip` file from **RSA Link** > **RSA NetWitness Platform** > **Downloads** > **RSA NetWitness LOGS & NETWORK** > **Version 11.4**.

2. Extract the `pki-migration-1.0.jar` file from the `rsa-nw-pki-migration-10.6.6.zip` file.

3. SSH to the 10.6.6.x Security Analytics Server host and log in with the root credentials.

4. Copy the `pki-migration-1.0.jar` file into `/tmp` folder.

5. Run the following command strings to extract the certificates.
   ```
   cd /tmp
   java -jar pki-migration-1.0.jar
   extract
   ```
   This :

   - Creates the `rsa-pki-migration-tool-<yyyy-MM-dd-hh-mm>` directory under the `tmp` directory.

   - Extracts output files into the `/tmp/rsa-pki-migration-<yyyy-MM-dd-hh-mm>` directory.

   - Creates a keystore (for example, `<keystore-x>.p12`) for each server certificate. The keystore is encrypted with **netwitness** as the password.

- Creates a certificate file (for example, `<certificate-X>.cer`) for each trusted CA certificate in truststore.

> **Note:** Refer to the line in the console output to find the storage location of the
>
> - server certificate (`<keystore-X>.p12`). For Example:
>
> ```
> The Entry le-056cdfb6-7577-4287-a791-64fbf999ff2d is a Private Key Entry
> Storing the entry le-056cdfb6-7577-4287-a791-64fbf999ff2d into store at /tmp/rsa-pki-migration-tool-2019-03-04-13-48/keystore-2.p12
> ```
>
> - trusted CA certificate (`<certificate-x>.cer`). For example
>
> ```
> The Entry srv3-server3-ca-2917457683755998433032433135284559 9851 is a Certificate Key Entry
> Writing certificate Entry srv3-server3-ca-2917457683755998433032433135284559 9851 into file /tmp/rsa-pki-migration-tool-2019-03-04-13-48/certificate-
> 4.cer
> ```
>
> This process does not modify the original keystores and trusted CA certificates of 10.6.6.x. You can run these steps multiple times, if required.

6. Open any keystore and display its contents to verify that the extracted keystores and the trusted CA certificates are correct.

```
cd rsa-pki-migration-tool-<yyyy-MM-dd-hh-mm>
ls -ltrh
 Openssl x509 -in <certificate-X>.cer -inform DER
```

The certificate in displayed in PEM (Base64) format. For example:

```
-----BEGIN CERTIFICATE-----
MIIDZTCCAk2gAwIBAgIQZ4o94d5AiLBC4sPXgDYXpTANBgkqhkiG9w0BAQUFADBF
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IsZAEZFgNwa2kxFzAV
BgNVBAMTDnBraS1TRVJWRVIxLUNBMB4XDTE1MDgwNzA2MTU1MVoXDTIwMDgwNzA2
MjU1MVowRTEVMBMGCgmSJomT8ixkARkWBWxvY2FsMRMwEQYKCZImiZPyLGQBGRYD
cGtpMRcwFQYDVQQDEw5wa2ktU0VSVkVSMS1DQTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKNFzsm3rsY7OGLb5ZWVVWsfZCuO517Re3eSiHdgWgp86QdT
URTSYDuHWVLnUMmo4CVKNNF0c9nzxJZDG4b0LSL/qkUVmxAhrcw52/0edKCmROa9
auZMPgyYtXeKiA8Ak55qOn2Es3tjJAf90IsAprK1mXOH9cs24Fdtm7ahNCqy1569
cxeBC0ykr/xYhU+AkBFd4uvlA8Bf6ll+70UeUdu3f04XMhYk4VTPF5gI5DNhZgMp
DQi93Bj/nY3MaQ4Woz4r3TFbIVZwe4kRW+FAD5gWundA4O1QfQZQAQi+1cy6pbl5
nyi0C9ktEsQ1Ru+mhChOKEjhV9Q5pHaZsdpxfXsCAwEAAaNRME8wCwYDVR0PBAQD
AgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFNFlTRzf8QR77KIn4I5kjvzG
WUIbMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQCNdbUNknKp
9FDj3nJRFXPXw8kStBIQwqS4WfyPzHmxCAzmDUreN/9YVqNniJhII0KLzesgFj12
FeJ6R1mps4e5IHMKNrOTr+WCnG/ipDOucn2MHol4InLP4FeapVOPXs7E7IiR5iQR
cwW4Iag6LcFAoIwW5gOxnV93Etb2e1VnQHxXWMhtaGnSuHgFudm/WHcZFGWfwX9T
22w4Hf8L4qNmP9w97Cq+Vu/emamdO2eIzPgKZJPu4B6oeKxUp6/QwUXCUYHZNRcj
qJ+la1VnMeDWH+VrZtZf1SeMiAh6qObwk6sXxQyKAuB8vlvG4svPIFrqlT4KpRXQ
3lAXU6iWqYZP
-----END CERTIFICATE-----
```

```
keytool -list -keystore <keystore-X>.p12 -storetype PKCS12 - storepass
netwitness
```

The following is an example of the output.

```
Keystore type: PKCS12
Keystore provider: <XXXXX>
```

7. Exit the keystore.

```
exit
```

You can use:

- One of the `.p12` keystore files as a server certificate. Refer to the command output to find `.p12` file that corresponds to the server certificate you must use.

- The extracted certificate files (.cer) as trusted CA certificates.

For instructions on how to configure PKI authentication, see the "*System Security and User Management Guide*".

Event Stream Analysis (ESA)

Task 6 (Conditional) - Record Any String Array Type Meta Keys on the Event Stream Analysis Service

If you added any string array type meta keys to the Event Stream Analysis service for your ESA correlation rules in 10.6.6.x or earlier, record these meta keys so you can verify that they exist after upgrade to 11.4.

To record your 10.6.6.x string array type meta keys before the 11.4 upgrade:

1. In Security Analytics 10.6.6.x:

    a. Go to the **Administration** > **Services** view.

    b. Select the Event Stream Analysis service.

    c. Click (actions) > **View** > **Explore**.

2. In the **Explore** view node list, select **Workflow** > **Source** > **netgenAggregationSource**.

3. In the **ArrayFieldNames** list, make a note of any string array type meta keys added to the Event Stream Analysis service so you can verify that they are on the ESA Correlation service after the upgrade.

Respond

Task 7 - Check Aggregation Rules Match Conditions for "Domain" or "Domain for Suspected C&C"

Make a note of any Incident Management aggregation rules that have match conditions using Domain or Domain for Suspected C&C in the drop-down list in the rule builder. You will need to add back these conditions after you upgrade to 11.4 as described in the "Respond" Post Upgrade Tasks later in this document.

Complete the task for each aggregation rule.

1. In Security Analytics 10.6.6.x, go to **Incidents** > **Configure** > **Aggregation Rules** tab and edit the rules to view the matching conditions.

2. In the **Match Conditions** section, look for **Domain** or **Domain for Suspected C&C** listed in the drop-down lists for the conditions.

3. Make a note of the rule name and the entire condition that uses **Domain** or **Domain for Suspected C&C**, including operators and values.

Task 8 - Set Data Retention Run Interval to ≥ 24 Hours

In Security Analytics 10.6.6.x, the Data Retention run interval does not have any minimum value check. In 11.3, RSA added a validation check to make sure that it is run at least every 24 hours. When you upgrade to 11.3 and later, if this value is less than 24 hours, the Respond service will not start.

Complete the following task to ensure that the Respond service starts after upgrading to 11.4.

1. In Security Analytics 10.6.6.x, go to **ADMIN** > **Services**.

2. Select the **Incident Management** service, and then select > **View** > **Explore**.

3. In the Incident Management **Explore** view, go to `Service` > `Configuration` > `dataRetentionConfiguration`.

4. Make sure that the `FrequencyInHours` parameter is $\geq$ **24**.
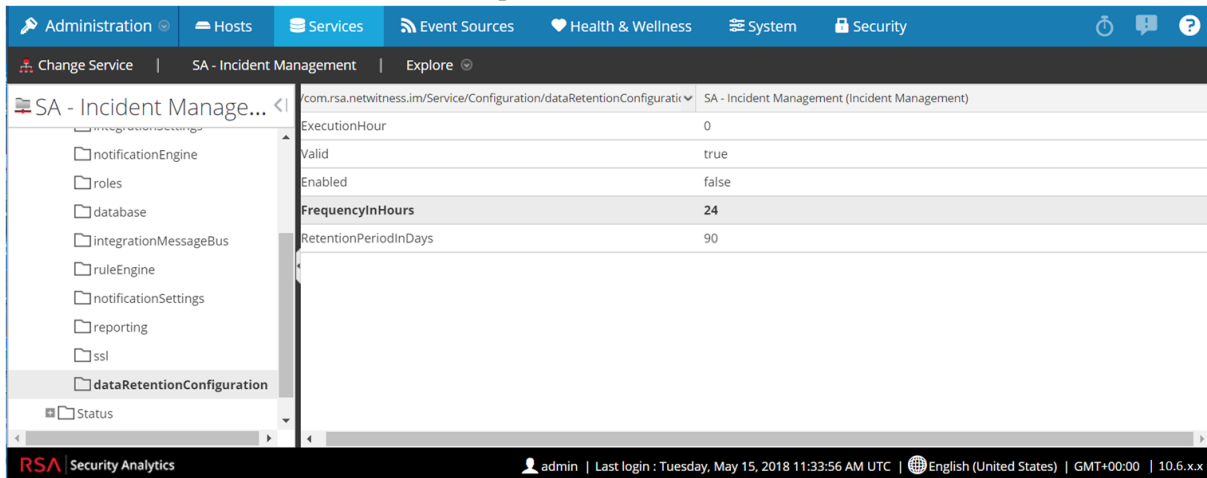
Reporting Engine

(Conditional) Task 9 - Unlink External Storage

If the Reporting Engine has external storage, such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports, complete the following task to unlink the storage.

> **Note:** In these steps:
> `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
> `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.

2. Stop the Reporting Engine service.
   ```
   stop rsasoc_re
   ```

3. Switch to `rsasoc` user.
   ```
   su rsasoc
   ```

4. Change to the Reporting Engine the home directory.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```

5. Unlink the `resultstore` directory mounted to external storage.
   ```
   unlink /externalStorage/resultstore
   ```

6. Unlink the `formattedReports` directory mounted to external storage.
   ```
   unlink /externalStorage/formattedReports
   ```

Warehouse Connector

(Conditional) Task 10 - Copy `keytab` files in `root` or `etc` Directory Stored in Other Directory

Complete the following task to copy the `keytab` files in the `root` or `etc` directory if it is stored in another directory.

1. Record the absolute path of NFS mount directory and the `keytab` file.
   You need this information to restore the Warehouse Connector after upgrade.

2. Unmount the NFS directory.

   a. SSH to the Warehouse Connector and log in with `root` credentials.

   b. Submit the following command to unmount the NFS directory.
   ```
   umount <NFS-absolute-path>
   ```

Other Tasks

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.6.x is the first step in upgrading from 10.6.6.x releases to 11.4.0.0.

> **Note:** It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to make sure that these certificate files are backed up. Your custom certificate files will be automatically restored during the upgrade process. After upgrading to 11.4.0.0, the custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types

> **Caution:** 1) These services are not supported in the 10.6.6.x backup and upgrade process.
> - IPDB
> - All in One servers
> - Malware Analysis Co-Located on the NetWitness Server
> - Standalone Warehouse Connector
> 2) There is a known issue if you have Active Directory users configured in 10.6.6.x. You have two options to address this issue:
> • Apply the 10.6.6.2 patch before you back up your data for the 11.4 upgrade.
> • If you failed to apply the 10.6.6.2 patch, you can apply the 11.0.0.1 patch immediately after you upgrade to 11.4.

The following types of hosts can be backed up and are automatically restored during the upgrade process:

- **NetWitness Server** (may include Malware Analysis, NetWitness Respond, Health and Wellness, and Reporting Engine)

- **Archiver**

- **Broker**

- **Event Stream Analysis** (including Context Hub and NetWitness Respond database)

- **Concentrator**

- **Log Decoder**

- **Packet Decoder**

- **Virtual Log Collector**

The following types of files are automatically backed up but must be restored manually after the upgrade process:

- PAM configuration files: For information about restoring the PAM configuration files, see "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.4.0.0", in the "Global" section of the Post Upgrade Tasks.

- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files, you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "

(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of Post Upgrade Tasks.

> **Note:** If you have problems during the backup or upgrade processes and you lose data, you can recover the data and start the process again. For information about recovering lost data, see "Recover Data After System Failure" in the *System Maintenance Guide*.

The following diagram shows the high-level task flow of the steps you perform to back up your hosts.

Set up an external host.	→	Create a list of hosts to back up.	→	Set up authentication.	→	Check backup requirements for specific types of hosts.	→	Check for adequate space.	→	Back up your host Systems.
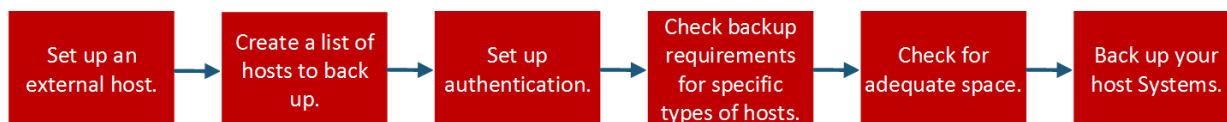
Task 1 - Set up an External Host for Backing up Files

You must set up an external host to use for backing up files. The host must be running Centos 6 with connectivity through SSH to the NetWitness Platform stack of hosts.

Make sure that the host names for systems to be backed up are resolvable on the backup host machine, either by DNS or listed in the `/etc/hosts` file.

> **Note:** These scripts are designed to run on CentOS 6 only. You must execute these scripts on CentOS 6 machines.

There are several scripts that you run during the backup process. You must download the zip file that contains the scripts (`nw-backup-v4.3.sh` or later) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your NetWitness Servers and host systems to be backed up.

- `ssh-propagate.sh`: Automates sharing keys between systems you are backing up and the backup host system so that you are not prompted for passwords multiple times.

- `nw-backup.sh`: Performs the backup of your hosts.

> **Note:** The backup scripts do not support backing up data for STIG-hardened hosts.

Task 2 - Create a List of Hosts to Back up

The script that you use to back up your files depends on the `all-systems` and `all-systems-master-copy` files, which contain a list of hosts that you want to back up. The `all-systems-master-copy` file contains a list of all your hosts. The `all-systems` file is used for each backup session, and contains only those hosts which are being backed up for a particular session. You must run the `get-all-systems.sh` script to generate these files. RSA recommends that you back up your hosts in groups, and not all at once. The recommended order and grouping of hosts for backup sessions is shown in the following diagram:
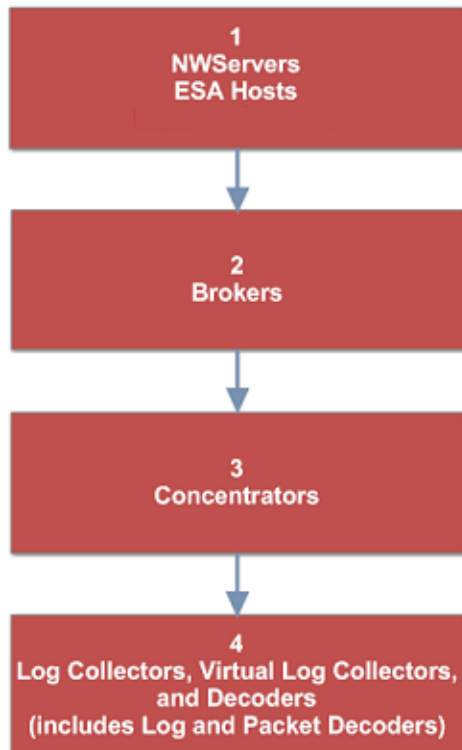
Limit each backup session to five hosts to make sure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference, and then manually edit the `all-systems` file to contain specific hosts.

To generate the `all-systems` and `all-systems-master-copy` files:

1. From the host on which you are running the backup process, make the `get-all-systems.sh` script executable by running the following command:

   `chmod u+x get-all-systems.sh`

2. At the root level, run the following script:

   `./get-all-systems.sh <IP-Address-of-NetWitness-Admin-Server>`

   You will be prompted for the password for each host system once per host.
   This script saves the `all-systems` file and the `all-systems-master-copy` file to `/var/netwitness/database/nw-backup/`.

3. Validate that the `all-systems` and `all-systems-master-copy` files were generated and that they contain the right hosts.

4. Edit the `all-systems` file to contain only the systems you are backing up. You can do this by using the `all-systems-master-copy` file as a reference, and then opening the `all-systems` file in an editor (such as vi) and modifying it to include only the systems you want to back up.

> **Note:** If you use vi, be sure to include the path to the location of the `all-systems` file.

Here is an example of an `all-systems-master-copy` file:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.6.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.6.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

And here is an example of an `all-systems` file based on the `all-systems-master-copy` file that could be used in the first backup session:

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
```

Troubleshooting Information

- Be sure to save copies of the `all-systems` and `all-systems-master-copy` files in a safe location.

  Follow these recommendations:

  - Do not edit the `all-systems-master-copy` file.
  - If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure to remove pre-existing entries from the file so that the file contains only those hosts that are currently being backed up.

    For more information, see [Post Backup Tasks](#).

- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.

- The `get-all-systems.sh` script generates a list of hosts that were defined in the NetWitness Platform user interface. Make sure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to NetWitness Platform, you use the NetWitness Platform user interface to Msure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.

- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the NetWitness Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the NetWitness Server. (Any Windows Legacy Collectors or AWS Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)

- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

RSA recommends that you run the `ssh-propagate.sh` script to automate sharing keys between the backup host and the host systems.

> **Note:** If you have SSH keys that are protected with pass phrases, you can use `ssh-agent` to save time. For more information, refer to the man page for `ssh-agent`.

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:

   ```
   chmod u+x ssh-propagate.sh
   ```

2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:

   ```
   ssh-propagate.sh <path-to-all-systems-file>
   ```

3. You are prompted for the password once per host, but you will not need to enter it repeatedly later during the backup process.

Task 4 - Check for Backup Requirements for Specific Types of Hosts

After you create the `all-systems` file to use for backup, you must check to see if any of the hosts listed in the file have requirements that must be met before you run the backup process.

For All Host Types

Perform the following steps for all host types:

1. On the NetWitness Server, place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to make sure that these certificate files are backed up. Your custom certificate files that are placed in this directories will be automatically restored during the upgrade process. After upgrading to 11.4.0.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`.

   You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the NetWitness Server and run the following command strings to perform the conversions listed.

   Convert a DER file (.crt .cer .der) to PEM
   ```
   openssl x509 -inform der -in certificate.cer -out certificate.pem
   ```
   Convert a PEM file to DER
   ```
   openssl x509 -outform der -in certificate.pem -out certificate.der
   ```
   Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)
   ```
   openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
   ```

```
certificate.crt -certfile CACert.crt
```
Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM
```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Note:** Add the following qualifier to the command string to:
> `-nocerts` convert private keys exclusively.
> `-nokeys` convert certificates exclusively.

2. Manually record any custom configurations made to CentOS 6 (for example, driver customizations) for restoration after you update to CentOS 7. Custom configurations to CentOS 6 are not automatically backed up and restored.

For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for Decoder, Concentrator, or Broker hosts, stop data capture and aggregation on all the systems that you are backing up. For instructions, refer to Appendix B. Stopping and Restarting Data Capture and Aggregation

Log Collectors (LC) and Virtual Log Collectors (VLCs): Run `prepare-for-migrate.sh`

> **Caution:** This task stops log collection so you must perform this step immediately before you upgrade to minimize the loss of event collection. Complete this task in accordance with the backup and upgrade tasks in this guide.

Prerequisites

You need the following information before you prepare LCs and VLCs for upgrade.

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.

- If you set the password for `logcollector` user for RabbitMQ , you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.

2. Submit the following command string.

   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```

   This command:

   - Stops the Puppet Agent service.

   - Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.4.0.0.

- Stops all the collection protocols in the Log Collector service.

- Saves the list of Plugin accounts and RabbitMQ accounts.

- Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.

- Waits until the Log Collector queues are empty.

- Stops the Log Collector service.

- Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

The `prepare-for-migrate.sh` script:

- Sends informational, warning, and error messages to the console.

- Saves a session log in the `/var/log/backup/` directory.

You must fix any of the following errors and resume the preparation. Contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

- Log Collector queues with events but without consumers are found.

- Unable to stop the Puppet Agent service.

- Unable to stop a collection protocol in the Log Collector service.

- Unable to block event publishers to the RabbitMQ server.

- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.

- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting

For Integrations with Web Threat Detection, Archer Cyber Incident & Breach Response or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.6.x host, on the NetWitness Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.4.0.0 upgrade, you can restore RabbitMQ user accounts.

To get a list of RabbitMQ usernames and passwords, run the following command:

`rabbitmqctl list_users >> /root/rabbitmq_users.txt`

To restore RabbitMQ user accounts, refer to *Task 2 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL* in Post Upgrade Tasks.

For Bluecoat Event Sources

Bluecoat ProxySG event sources use FTPS protocol to upload log files to the Log Collector (LC) and Virtual Log Collector (VLC). The event source documentation contains the steps to configure VSFTPD service on the LC and VLC.

- If key material exists in `/root/vsftpd/` directory in 10.6.6.x, this material area will be backed up and restored. **If the material was in another location, you must back it up and restore it manually.**

- If the `/etc/vsftpd/vsftpd.conf` file exits in 10.6.6.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to make sure that you provide adequate space for the backup so that the backup captures all your data.

To check for adequate disk space:

1. Make the backup script executable by running the following command:
   ```
   chmod u+x nw-backup.sh
   ```

2. Run the following command at the root directory level:
   ```
   ./nw-backup.sh -t
   ```
   The output displays the amount of disk space that is required for the backup.

   > **Note:** The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-d` option by using `-D`. Using the `-D` option will show how much space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

The following figure shows an example of the output from using the `-t` option.

```
************************* NW-BACKUP SCRIPT - TEST MODE *************************
* *  RSA nw-backup script is running in test mode where in it will only verify the disk space required for successful backup.
----------------------------------------------------------------------
CONTENT options currently selected:
----------------------------------------------------------------------

    Backup IPDB?          'no'            Backup Yum Repo?        'no'
    Backup Malware Analysis repository? 'no'   Backup SA Colo MA?   'no'
    Backup Reporting Engine repository? 'no'   Backup /var/log?     'no'
    Backup ESA DB?        'yes'           Backup Context Hub?     'yes'
    Backup SMS RRD?       'yes'


Checking that the environment is configured for proper execution of script...
Backup path configured...        [ OK ]   Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence...         [ OK ]
Check for all-systems file...    [ OK ]
Dated backup dir...              [ OK ]   Backup directory: /var/netwitness/database/nw-backup/2017-09-18
Logging to /var/netwitness/database/nw-backup/rsa-nw-backup-2017-09-18.log

Testing SSH connectivity to saserver
SSH connectivity...              [ OK ]
Calculating size of backup for saserver
Disk space required for saserver backup is 1.91GB
Check Backup Storage Space @ lab-cos6-RF:/var/netwitness/database/nw-backup
Space Required 1.91GB vs. Space Available 11.66GB
Backup Storage Space...          [ OK ]
Total Execution Time : 0 d 0 h 0 m 19 s


Disk space check test completed with no errors.
[root@lab-cos6-RF ~]#
```

Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.4.0.0.

> **Note:** The script will stop services as it runs. However, you can stop services manually before you run the script if needed.

When you run the backup script, you can choose from several options that are described in the following sections.

Usage:
```
./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>
```

General Options

`-u : This option is required for upgrading to 11.4. Enables the upgrade flag to run backup for upgrading to 11.4. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) - COPY`

```
-b <path to write backups> : path to the location for storing backup files on
a backup server. For upgrading to 11.4, please use the default location!
Default: (/var/netwitness/database/nw-backup)
```

> **Note:** Do **not** change the backup path in upgrade (-u) mode.

Advanced Content Selection Options

```
-c : back up Colocated Malware Analysis on SA servers. Default: (no)
```

```
-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)
```

```
-m : back up Malware Analysis File Repository. Default: (no)
```

```
-r : back up Reporting Engine Report Repository (automatically set if -u is
used). Default: (no)
```

```
-v : back up system logs (/var/log). Default: (no)
```

```
-y : back up YUM Web Server & RPM Repository. Default: (no)
```

```
-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)
```

```
-C : If set: DISABLES back up of Context-Hub configuration and database.
Default: (not-set)
```

```
-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)
```

Test Options

```
 -t : performs script test run for disk space check only. Services are not
stopped and excludes execution of backup. Can be combined with (-d) or (-D)
and other flags. Default: (-t)
```

For example, the command:
```
./nw-backup.sh
```
would run the backup with options as set in the Header of the script itself.
OR, the command:
```
./nw-backup.sh -ue /mnt/external_backup
```
would run a normal backup using the backup path defined in the script, with the following options:

```
-u : enables the upgrade flag to run backup for upgrading to 11.4. It also
enables disk space check (-d), backing up reporting engine reports (-r) and
stores backup content locally (-l). Default: (no)
```

```
-e : Copy the backup files to external mount point, mounted on /mnt/external_
backup
```

```
For Help: ./nw-backup.sh –h
```

When you run the script, the following text is displayed at the top of the script:

> **Caution:** `RSA nw-backup script backs up configuration files, data, and logs on`
> `the options provided in the script. It tars the content, with options to`
> `store the backup files on the backup server, move or copy them to external`
> `storage on a mount point (USB/NFS/SMB), or SCP them back to the target host.`
> `This backup script has been qualified on the following versions of Security`
> `Analytics:`
> `10.6.6.x`
> `Use of this script on any other versions of the product may not give`
> `expected results and may not be supported by RSA Customer Service.Note: All`
> `non-RSA custom files, scripts, Cronjobs and other important files should be`
> `placed in /root, /home/'user', OR /etc to be included in the backup.`

To run the backup script to back up your hosts:

1. Make sure that the `all-systems` file contains only the hosts to back up. For information, see [Task 2 - Create a List of Hosts to Back up](#).

2. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`

3. Begin the backup process by running the following command at the root directory level:
   `./nw-backup.sh -u <additional options as needed>`

   > **Note:** You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.4.0.0.

   When the text "`Backup completed with no errors`" is displayed, the backup has completed successfully.

   A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:
   `rsa-nw-backup-2017-03-15.log`

4. When the backup has completed, to make sure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:
   `tar -tzvf hostname-ip-address-backup.tar.gz`
   The following archive files are created:
   For all hosts:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `tar checksum` files
   `<hostname-IPaddress>-network.info.txt`
   For NetWitness Servers:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `<hostname-IPaddress>-mongodb.tar.gz`
   `tar checksum` files
   `<hostname-IPaddress>-network.info.txt`
   For ESA Hosts:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `<hostname-IPaddress>-mongodb.tar.gz`
   `<hostname-IPaddress>-controldata-mongodb.tar.gz`
   `tar checksum` files
   `<hostname-IPaddress>-network.info.txt`

The archived files are located in the `/var/netwitness/database/nw-backup` directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

Post Backup Tasks

Task 1 - Save a Copy of the `all-systems` File and the Backup Tar files

Make copies of the `all-systems` file, the `all-systems-master-copy` file, and the backup tar files and put the copies in a secure location. You cannot regenerate these files after you upgrade the NetWitness Server (specifically the Admin service) to 11.4.0.0.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.4.0.0 upgrade process. Before you begin the upgrade process, you must make sure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

The following files are generated on all hosts by the backup scripts:

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

In addition to the files listed above, the following files will be generated on NetWitness Server and ESA hosts:

- `<hostname>-<host IP address>-mongodb.tar.gz`
- `<hostname>-<host IP address>-mongodb.tar.gz.sha256`

The backup script will also generate the following `controldata-mongodb.tar.gz` files.

> **Note:** The backup script copies the following files from all ESA hosts to the NetWitness Server host's backup path .

- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz`
- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256`

(Conditional) Task 3 - For Multiple ESA Hosts, Copy `mongodb tar` files to Primary ESA Host

If you have multiple ESA host systems in your enterprise, copy the following two files from each ESA host to the `/opt/rsa/database/nw-backup/` directory on the Primary ESA host system (the host that has the ContextHub service running on it) :

- `<hostname>-<host-IP-address>-mongodb.tar.gz`

- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Task 4 - Ensure All Required Backup Files are on Each Host

Before you upgrade to 11.4.0.0, make sure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

> **Note:** The default paths for backup files are:
> - NetWitness Server hosts:`/var/netwitness/database/nw-backup`
> - ESA hosts:`/opt/rsa/database/nw-backup`
> - Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

- `all-systems-master-copy`

- `<hostname>-<host-IP-address>-backup.tar.gz`

- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`

- `<hostname>-<host-IP-address>-root.tar.gz`

- `<hostname>-<host-IP-address>-root.tar.gz.sha256`

- `<hostname>-<host-IP-address>-network.info.txt`

- `<hostname>-<host-IP-address>-mongodb.tar.gz`

- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz`

- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256`

Required Files for ESA Hosts

- `all-systems-master-copy`

- `<hostname>-<host-IP-address>-backup.tar.gz`

- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`

- `<hostname>-<host-IP-address>-root.tar.gz`

- `<hostname>-<host-IP-address>-root.tar.gz.sha256`

- `<hostname>-<host-IP-address>-network.info.txt`

- `<hostname>-<host-IP-address>-mongodb.tar.gz`

- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Required Files for All Other Hosts

- `all-systems-master-copy`

- `<hostname>-<host-IP-address>-backup.tar.gz`

- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`

- `<hostname>-<host-IP-address>-root.tar.gz`

- `<hostname>-<host-IP-address>-root.tar.gz.sha256`

- `<hostname>-<host-IP-address>-network.info.txt`

> **Note:** The following files are located in the `<hostname>-<host-IP-address>-`
> `backup.tar.gz` tar on all hosts:
> `appliance_info`
> `service_info`

> **Note:** The paths to the location of the backup and restore files for iptables, NAT
> configurations, user accounts, and crontab entries are shown in the following list:
> **Backup paths:**
> `BUPATH=/opt/rsa/database/nw-backup` for the ESA Correlation Engine
> `BUPATH=/var/lib/rsamalware/nw-backup` for the Malware Service
> `BUPATH=/var/netwitness/database/nw-backup` for all other services
> **Restore locations:**
> `BUPATH/restore/etc/sysconfig` for Iptable rules
> `BUPATH/restore/etc/sysconfig` for NAT configurations
> `BUPATH/restore/etc` for Crontab entries
> `BUPATH/restore/etc` for User Accounts (users are located in the `passwd` file, and
> groups are located in the `group` file. These are not restored during the upgrade process
> but can be restored manually.
> `BUPATH/restore/etc/ntp.conf` for NTP configurations (must be restored using the
> NetWitness Platform UI)

Migrate Disk Drives from 10.6.6.x to 11.4

These instructions tell you how to upgrade virtual hosts from 10.6.6.x to 11.4.

> **Caution:** 1.) Run the backup immediately before you upgrade hosts for each phase so that the data is not out-dated.
> 2.) This guide applies to AWS host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Platform 11.0 Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

There are five tasks you must complete to migrate from 10.6.6.x to 11.4:

Task 1 - Backup the 10.6.6.x EC2 appliance

(Optional) Task 2 - Run the backup script to take backup data of 10.6.6.x instance

Task 3 - Stop the instances and detach volumes from 10.6.6.x instances

Task 4 - Note the IP addresses of 10.6.6.x instances and then terminate the EC2 instances

Task 5 - (IP retention) Create 11.4 instances using 11.4 AMI.

Task 6 - Attach volumes to the corresponding 11.4 instance

Task 7 - Restore backup data in 10.6.6.x to 11.4 Instances (Data Restoration)

Task 8 Run nwsetup-tui script

Task 1 - Backup the 10.6.6.x EC2 appliance

Select the 10.6.6.x EC2 Instance and navigate to Actions. Click Image and then select Create Image.
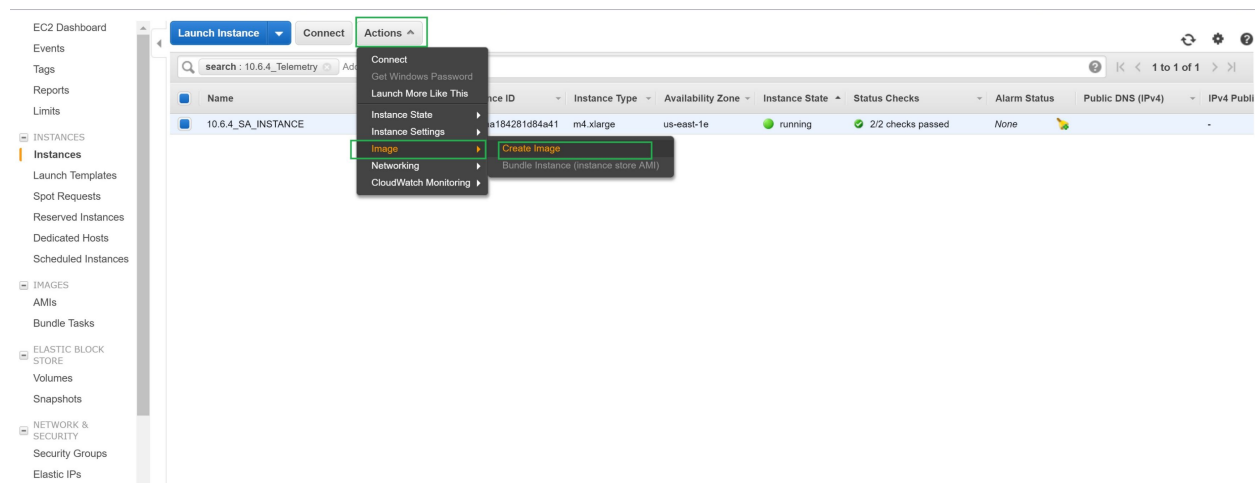
(Optional) Task 2 - Run the backup script to take backup data of 10.6.6.x instance

Note: If you have not taken a backup of the 10.6.6.x instance, follow these steps, otherwise skip to Task 3 - Stop the instances and detach volumes from 10.6.6.x instances.

If the stack contains Log Collector then prepare **Log Collector** for the migration:

1. Navigate to `/opt/rsa/nwlogcollector/nwtools/` and run the below command:

`sh prepare-for-migrate.sh --prepare`

2. Download backup scripts from GitHub: https://github.rsa.lab.emc.com/asoc/nw-backup (maintenance-11.0) and place it anywhere in a computer running an RPM-based Linux distribution (RHEL or CentOS for example) with a large amount of free hard drive space. In many cases the SA server will suffice. Now, navigate to `scripts` directory inside 'nw-backup-master' and run the following commands:

`./get-all-systems.sh <SA server-IP>`

`./ssh-propagate.sh <path-to-backup-directory/all-systems>`

`./nw-backup.sh -u`

Its safe to copy a backup of the tar balls created at `/var/netwitness/database`, in some safe location (not mandatory).

Before starting the restore process, if you have ESA deployment then copy the files `<hostname>-<IP>-controldata-mongodb.tar.gz` & `<hostname>-<IP>-controldata-mongodb.tar.gz.sha256` from the location `/opt/rsa/database/nw-backup` of ESA VM to `/var/netwitness/database/nw-backup/` of SA VM.

```
root@ip-172-24-184-59 ~]# ./nw-backup.sh -u
----------------------------------------------------------------
Starting execution of NW-BACKUP script in UPGRADE backup mode
----------------------------------------------------------------
WARNING: For UPGRADE backups, services must be stopped and all externally mounted disks (DACs) must be unmounted.
         If you prefer to stop the services and unmount the external partions manually, exit out of the script by typing
         (CTRL-C) within 30 seconds, otherwise the services will be automatically stopped, all externally mounted
         filesystems will be unmounted, and the script will proceed with the UPGRADE backup process.

NOTE: The easiest way to remount and restart the services on a host is to perform a reboot of the host.

The script will continue in 30 seconds...


------------------------------------------------------------------------------
OUTPUT options currently selected:
------------------------------------------------------------------------------
    Path to files on backup system:        '/var/netwitness/database/nw-backup'
    Copy backup files locally to each system?  'yes'
    Performing backup in upgrade mode?         'yes'
------------------------------------------------------------------------------
CONTENT options currently selected:
------------------------------------------------------------------------------
    Backup IPDB?            'no'              Backup Yum Repo?        'no'
    Backup Malware Analysis repository? 'no'  Backup SA Colo MA?      'no'
    Backup Reporting Engine repository? 'yes' Backup /var/log?        'no'
    Backup ESA DB?         'yes'             Backup Context Hub?     'yes'
    Backup SMS RRD?        'yes'
------------------------------------------------------------------------------


Checking that the environment is configured for proper execution of script...
OS Version...              [ OK ]
Backup path configured...       [ OK ]   Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence...        [ OK ]
Check for all-systems file...   [ OK ]
Created backup dir...           [ OK ]   Backup directory: /var/netwitness/database/nw-backup/2017-12-08
SA Version check ...            [ OK ]
**************************** NW-BACKUP SCRIPT - UPGRADE MODE ****************************
******** UPGRADE IS ONLY SUPPORTED FOR SA VERSION 10.6.4.0 AND HIGHER*************** *
*   RSA nw-backup script backs up configuration files, data, and logs based        * *
*   on the options provided in the script.  It tars the content and leaves a       * *
*   copy of tars on the host for consumption by the upgrade process.  It also      * *
*   provides an option to back up the tars to an external mount point (USB/NFS).   * *
*                                                                                  * *
*      NOTE: The following systems and services are NOT supported for restore      * *
*      for the 11.0.0.0 upgrade:                                                   * *
*                - Malware-Analysis (Co-located on SA server)                      * *
*                - IPDB Extractor (Co-located on SA Server & Standalone)           * *
*                - Warehouse Connector (Standalone)                                * *
*                - All-in-one Servers                                              * *
*                                                                                  * *
*   Note: All non-RSA custom files, scripts, Cronjobs and other important files    * *
*   should be placed in /root, /home/'user', OR /etc to be included in the backup. * *
*************************************************************************************** *
```

Task 3 - Stop the instances and detach volumes from 10.6.6.x instances

> **Note:** If detach fails, do a forced detach on the volume.

Select the 10.6.6.x EC2 instance and navigate to Actions and then click Stop.
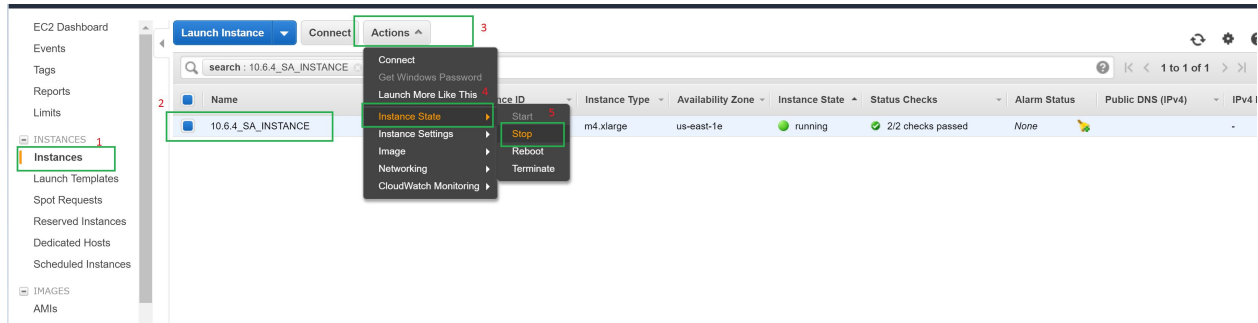
Click on Volumes and then select the 10.6.6.x instance volumes to detach Actions and then select Detach Volume.
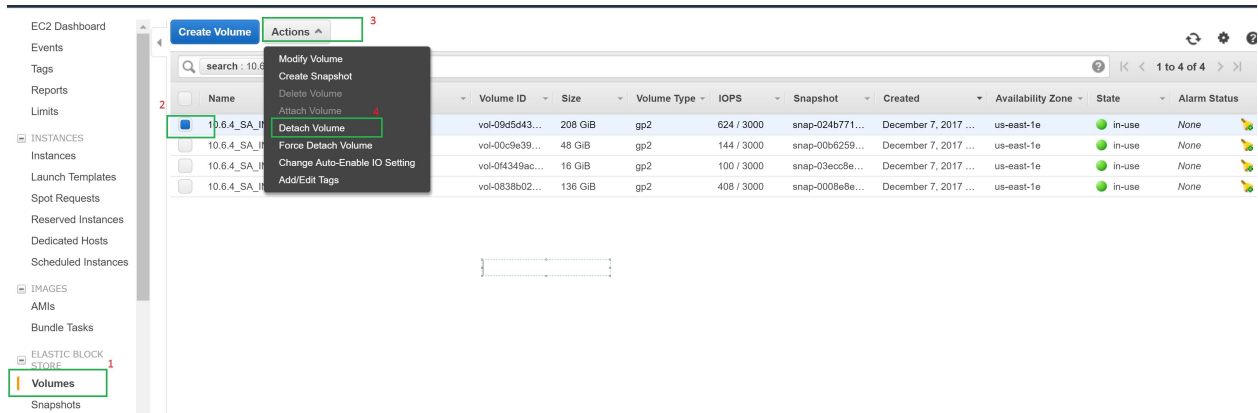
Task 4 - Note the IP addresses of 10.6.6.x instances and then terminate the EC2 instances

> **Note:** Termination is required to free the IP address.

1. Click on Instances and then select the Instance.

2. Click Actions and navigate to Instance State.

3. Click Terminate
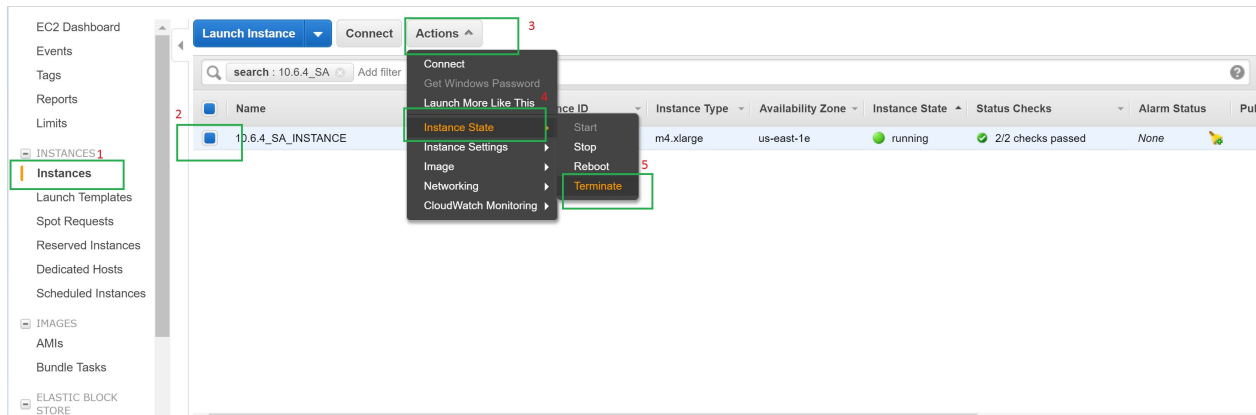
Task 5 - (IP retention) Create 11.4 instances using 11.4 AMI.

1. During the creation of EC2 instance, provide the IP address from task 4. Click on AMIs and select 11.x AMI.

> **Note:** Refer to the *AWS Deployment Guide for version 11.0* for installing RSA NetWitness Platform11.0.0.0

2. Click Actions and then click Launch.
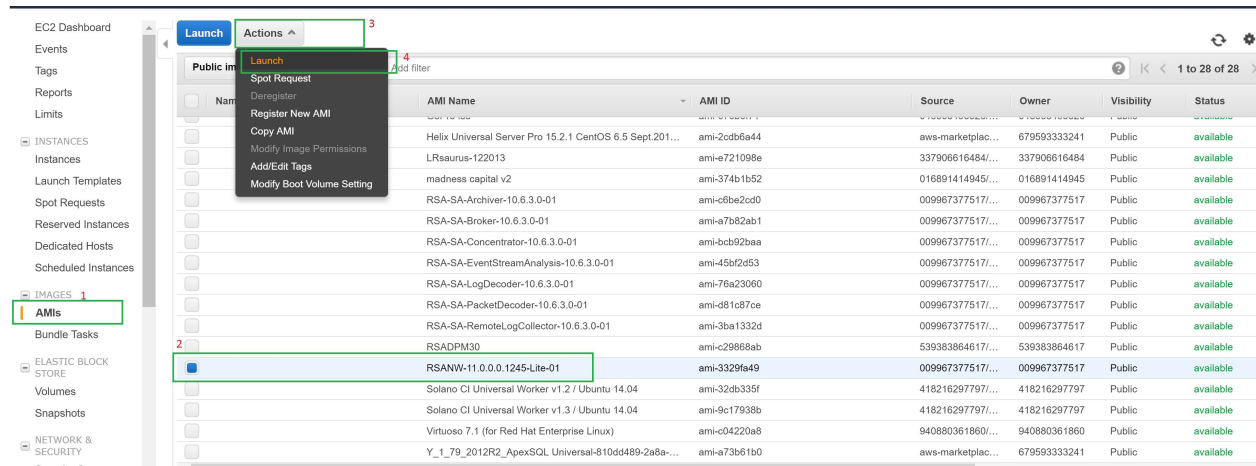
3. Assign the retained IP for the appropriate instances (IP retention). For example, If 10.6.1.x SA instance IP is 172.24.184.63 . Then assign the same IP(172.24.184.63) for 11.4 Instance.
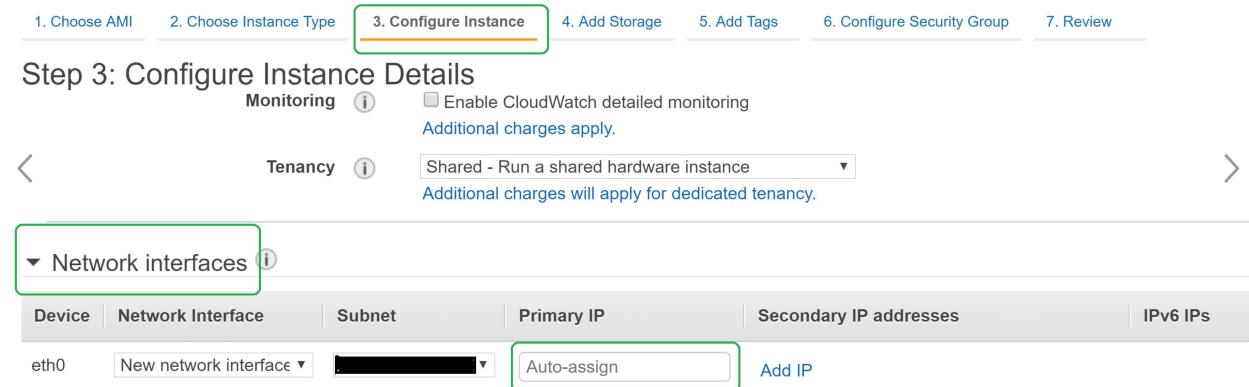
Note: To deploy components other than NW, select the image (RSANW-11.4.0.0.14000-Lite) which is available under community AMIs section.

Task 6 - Attach volumes to the corresponding 11.4 instance

After NW 11.4 instance is deployed, stop the 11.0 instance and attach the available 10.6.1.x volumes (except the 'OS disk') to 11.4 instances.

1. Click on Volumes.

2. Select the 10.6.6.x instance volume to attach.

3. Click Actions and then select Attach Volume.
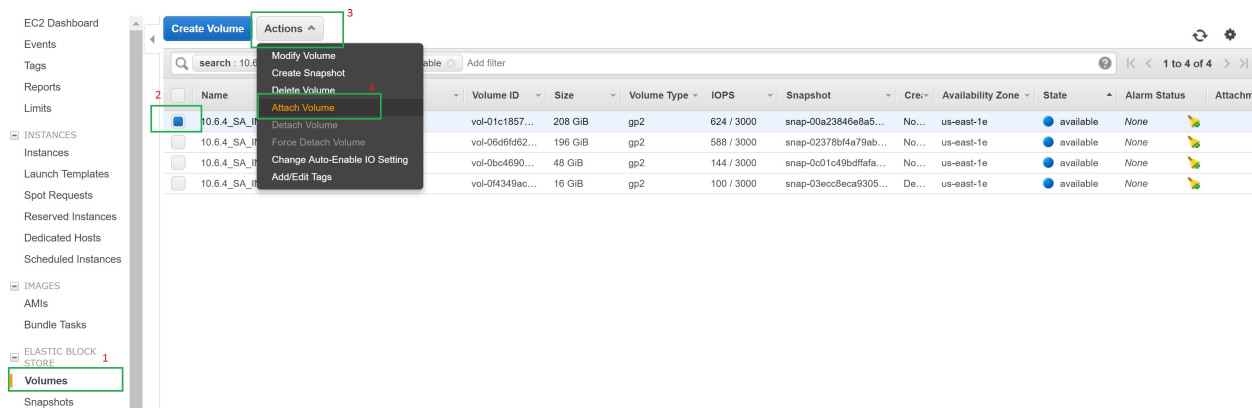
4. Enter the 11.4 instance ID to which the volume has to be attached.

Attach Volume   ✕

Volume	ⓘ	vol-011574048a0c11e43 (LD-10.6.4_Nilotpal_3) in us-east-1e
Instance	ⓘ	LogDecoder in us-east-1e
Device	ⓘ	

i-0fdd23599a84d5120 (LogDecoder-10-Nilotpal) (running)

i-0ae427387a3b3ba93 (ML-QE-11.1-DO-LOGDECODER-127049) (running)

i-06ee9052c56db18c7 (ML-QE_11.0_LogDecoder_CET_01) (running)
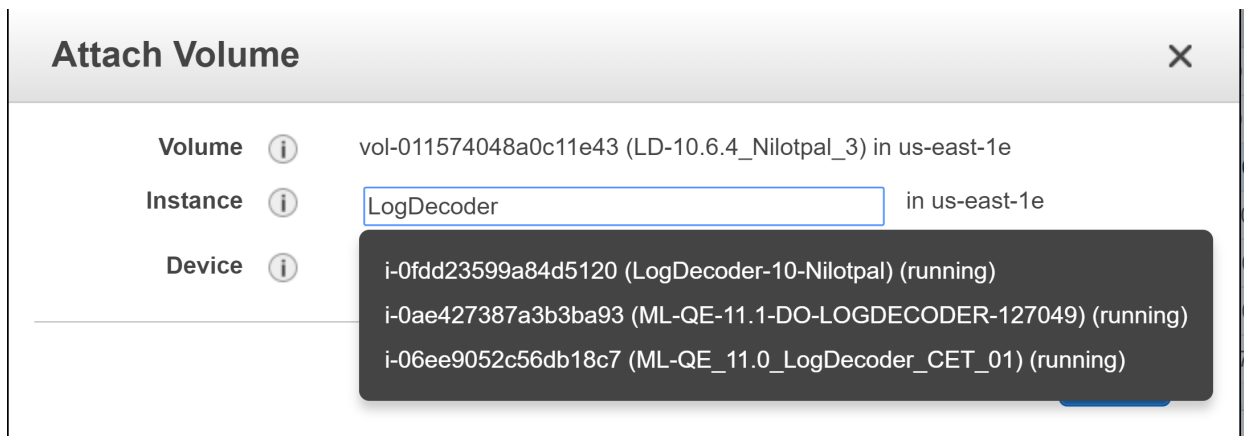
5. Power ON all the 11.4 instances once all the disks are attached.

Task 7 - Restore backup data in 10.6.6.x to 11.4 Instances (Data Restoration)

Execute the following steps for copying the backup data on SA, LD/LC, PD, Concentrator, Archiver, Broker:

1. Create a directory under `/tmp/` by the name `nwhome`.

2. Mount `VolGroup00-nwhome` on `/tmp/nwhome/` and make sure `/var/netwitness/database/` directory is present.

`mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/`

3. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`.

4. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`

`umount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/`

Follow these steps for **ESA**:

1. Create a directory under `/tmp/` by the name `apps`.

2. Mount `VolGroup01-apps` temporarily on `/tmp/apps/`

`mount /dev/mapper/VolGroup01-apps /tmp/apps/`

3. Copy nw-backup directory from here to `/var/netwitness`

`cp -r /tmp/apps/database/nw-backup /var/netwitness`

4. Unmount VolGroup01-apps from `/tmp/apps/`

`umount /tmp/apps`

5. Add the following entries in `/etc/fstab` for `mounts`:(Disk Mounting) and then run `mount -a`

For SA:

```
/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
defaults,noatime,nosuid 1 2
```

For LogDecoder/LogCollector:

```
/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb xfs
defaults,noatime,nosuid 1 2
```

For PacketDecoder:

```
dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb xfs
defaults,noatime,nosuid 1 2
```

For Concentrator:

```
/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb xfs
defaults,nosuid,noatime 1 2
```

```
/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb xfs
defaults,noatime,nosuid 1 2
```

For Archiver:

```
/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
defaults,nosuid,noatime 1 2
```

```
/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
defaults,nosuid,noatime 1 2
```

For Broker:

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
defaults,nosuid,noatime 1 2
```

6. Then run mount command
   ```
   mount -a
   ```

Task 8 Run nwsetup-tui script

> **Note:** Please provide appropriate host names for all the 11.4 instances after launching. (for 10.6.6.x instance names refer all-systems-master-copy file, which contains 10.6.6.x instance names with IP address)

Execute the command to set the hostname: `hostnamectl set-hostname <hostname>`

Login to SA Sever CLI and run `nwsetup-tui` script for rest of the process completion.

Run 'nwsetup-cli' on rest of the components for Bootstrap and Orchestration. For more information, refer to the [Set Up Virtual Hosts in 11.4](#) section.

Set Up Virtual Hosts in 11.4

There two phases to set up your 11.4 virtual stack that you must complete in the order shown.

- Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

> **Note:** For Event Stream Analysis, if you had C2 modules enabled in 10.6.6.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.3 and will not be available until the warm up completes.

- Phase 2 - Set Up The Rest of the Component Hosts

Phase 1 - Set Up NW Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts

Task 1 - Set Up 11.4 NetWitness Server

Follow the instructions under Set Up 11.4 NW Server Host.

Task 2 - Setup 11.4 ESA

> **Caution:** If you had C2 modules enabled in 10.6.4.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.0 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.4 Non-NW Server Host to set up your ESA hosts.

1. Set up your primary ESA host through the Setup program and install **ESA Primary** on the host in the user interface on the **Admin Hosts** view.

> **Note:** If you have multiple ESA hosts in your enterprise, you must upgrade the ESA Primary host, where all the `mongodb` (Mongo Database) backup tar files are located, first, before you upgrade ESA Secondary hosts.

2. (Conditional) If you have a secondary ESA host, set it up through the Setup program and install **ESA Secondary** on the host in the user interface on the **Admin Hosts** view.

Task 3 - Set Up 11.4 Malware Analysis

Follow the instructions under Set Up 11.4 Non-NW Server Host.

Task 4 - Set Up 11.4 Broker or Concentrator

Follow the instructions under Set Up 11.0 Non-NW Server Host.

> **Note:** If you do not have a Broker, upgrade your Concentrator hosts. The 11.4 NW Server cannot communicate with 10.6.6.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Set Up The Rest of the Component Hosts

See Appendix B. Stopping and Restarting Data Capture and Aggregation for instructions on how to stop and restart data capture and aggregation when upgrading the Decoder, Concentrator, and Log Collection hosts.

Decoder and Concentrator Hosts

1. Stop data capture and aggregation.

2. Complete the steps in Set Up 11.4 Non-NW Server Host.

3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the *Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh* in the **Backup Instructions**.

2. Stop data capture on the Log Decoder.

3. Complete the steps in Set Up 11.4 Non-NW Server Host.

4. Restart data capture on Log Decoder.

> **Note:** After you upgrade, you will restart log collection after completing the Task 33 - Update Incident Rules Identified in the Domain Matching Conditions Upgrade Preparation Task in the **Post Upgrade Tasks**

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described in the *Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh*.

2. Back up your 10.6.6.x VLC by editing the `all-systems` file on host where you performed the backup.

    a. Make sure your `all-systems` file contents has this information before you perform this step.
    ```
    vlc,<host-name>,<IP-address>,<UUID>,10.6.6.0
    ```

    b. Run the following command to create backup.
    ```
    ./nw-backup.sh -u
    ```
    See Backup Instructions for detailed procedures on how to back up the host.

3. Make sure the backup host contains the VLC backup in the following format.
    ```
    <hostname>-<IPaddress>-root.tar.gz
    <hostname>-<IPaddress>-root.tar.gz.sha256
    ```

```
<hostname>-<IPaddress>-backup.tar.gz
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```

4. Power off the 10.6.6.x VLC so that a new 11.4 VM can be created with the same network configuration.

5. Deploy a fresh Non-NW Server host using the 11.0 NetWitness Platform ova.

6. Connect to the VM console of the new VLC.

7. Update the network configuration to be the same as the 10.6.6.x VLC.
   This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.6.x VLC backup file.

> **Note:** Make sure IPv6 is disabled.

a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings.
   Contents of `ifcfg-eth0` should be as follows.
   ```
   TYPE=Ethernet
   DEFROUTE=yes
   NAME=eth0
   UUID=<uuid>
   DEVICE=eth0
   DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
   DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
   BOOTPROTO=static
   IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
   NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
   GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
   NM_CONTROLLED=no
   ONBOOT=yes
   ```

b. Submit the following command string.
   ```
   systemctl restart network.service
   ```

8. Create the backup directory.
   ```
   # mkdir –p /var/netwitness/database/nw-backup/
   ```

9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new VLC in the `/var/netwitness/database/nw-backup` directory.

10. Complete the steps 2 through 12 inclusive in Set Up 11.4 Non-SA Server Host for the rest of the NetWitness Platform components . Make sure that you select **Log Collector** for the service in step 12.

Set Up 11.4 NW Server Host

Make sure that you have backed up 10.6.6.x data for the SA Server host. **You must follow the instructions in** Backup Instructions **to back up the host.**

> **Caution:** Run the backup immediately before upgrading the SA Server to 11.4 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.4.

Complete the following steps to set up the 11.4 NW Server host.

1. Power on the NW Server VM and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

> **Note:** 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press the Enter key to register your command response and move to the next prompt.
> 2.) The Setup program adopts the color scheme of the desktop or console you use access the host.

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                      92%

            <Accept >                    <Decline>
```

2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

> **Caution:** If you choose the wrong host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.4 NW Server Host to correct this error.
>
> ```
>    You must setup an NW Server before setting up
>    any other NetWitness Platform components.
>
>    Is this the host you want for your 11.4
>    NW Server?
>
>         < Yes >        < No  >
> ```

3. Tab to **Yes** and press **Enter**.
   Choose No if you already upgraded the NW Server to 11.4.
   The Install or Upgrade prompt is displayed.

```
NetWitness Platform 11.3 Install or Upgrade
 Specify if you are installing NetWitness
 for the first time or upgrading from a
 previous version:

  1  Install (Fresh Install)
  2  Upgrade (From Previous Vers.)
  3  Recover (Reinstall)
  4  Install (Warm/Standby)



      <  OK  >        < Exit >
```
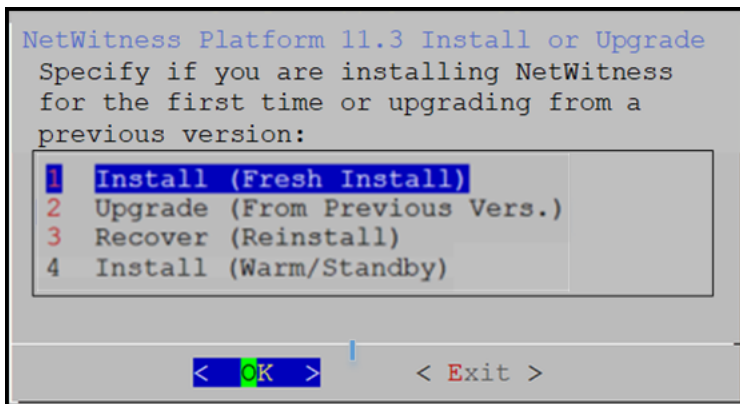
The backup path is displayed.

> **Caution:** The backup path in the following prompt must be the same as the path in which your backup is stored. For example, the backup script assigns **/var/netwitness/database/nw-backup** as the default path. If you used the default backup path during backup and did not change it subsequently, you must keep **/var/netwitness/database/nw-backup** as the path in the following prompt.

4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.

```
             Path for Previous Version Backup
   The upgrade process needs the directory path in which
   the data from your previous version was backed up so
   it can restore this data after you upgrade to
   NetWitness Platform 11.3.


   /var/netwitness/database/nw-backup


        <  OK  >           <Cancel>
```
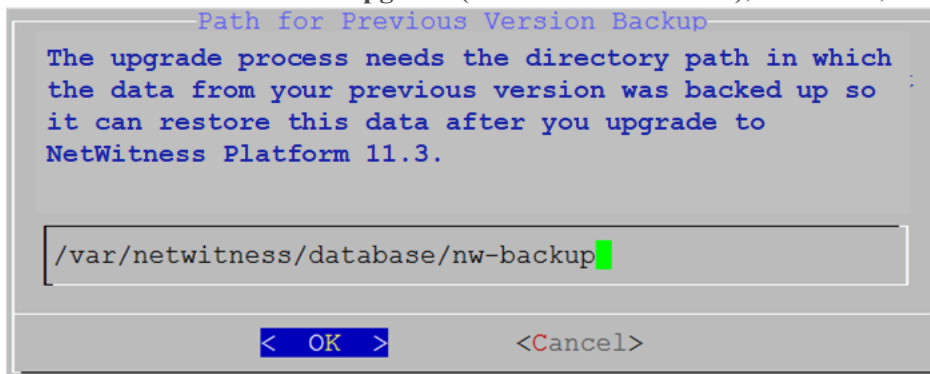
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.

The Master Password prompt is displayed.
The following list of characters are supported for Master Password and Deployment Password:

- Symbols : ! @ # % ^ + ,

- Numbers :0-9

- Lowercase Characters : a-z

- Uppercase Characters : A-Z

No ambiguous characters are supported for Master Password and Deployment Password (for example: space { } [ ] ( ) / \ ' " ` ~ ; : . < > -.
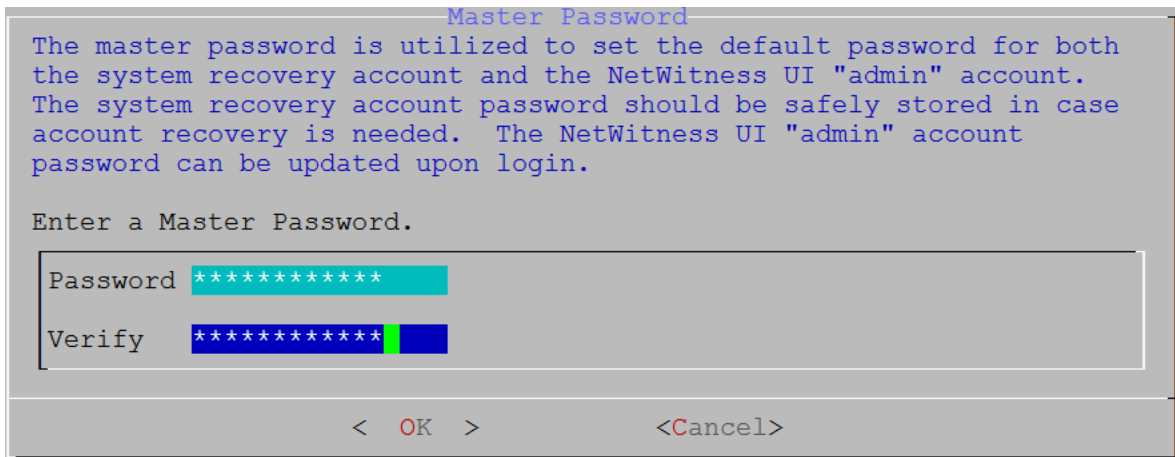
```
                    ┌──────Master Password──────────────────────────────────┐
  The master password is utilized to set the default password for both
  the system recovery account and the NetWitness UI "admin" account.
  The system recovery account password should be safely stored in case
  account recovery is needed.  The NetWitness UI "admin" account
  password can be updated upon login.

  Enter a Master Password.
  ┌──────────────────────────────────────────────────────────────────┐
  │ Password ************                                             │
  │                                                                  │
  │ Verify   ************                                            │
  └──────────────────────────────────────────────────────────────────┘

              <  OK  >                    <Cancel>
```

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. The Deployment Password prompt is displayed.

```
                    ┌──────Deployment Password──────────────────────────────┐
  The Deployment password is used when deploying NetWitness
  hosts.  It needs to be safely stored and available when
  deploying additional hosts to your NetWitness Platform.

  Enter a Deploy Password.
  ┌──────────────────────────────────────────────────────────────────┐
  │ Password *********                                               │
  │                                                                  │
  │ Verify   *********                                               │
  └──────────────────────────────────────────────────────────────────┘

              <  OK  >                <Cancel>
```

7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. The Update Repo prompt is displayed.

```
                ┌──────NetWitness Platform Update Repository──────────────┐
  The NetWitness Platform Update Repository contains all the
  RPMs needed to build and maintain all the NetWitness Platform
  components.  All components managed by the NW Server need
  access to the Repository.

  Do you want to connect to:
  ┌──────────────────────────────────────────────────────────────────┐
  │    1   The Local Repo on the NW Server                           │
  │    2   An External Repo (on an externally-managed server)        │
  │                                                                  │
  │                                                                  │
  │                                                                  │
  └──────────────────────────────────────────────────────────────────┘

            <  OK  >                   < Exit >
```

You must use the same repo that you used for the NW Server hosts for all hosts.

8. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL.

```
NetWitness Platform 11.3 External Update Repo URL
Enter the base URL of the external update
repositories:

  [█                                              ]

        <   OK   >            <Cancel>
```
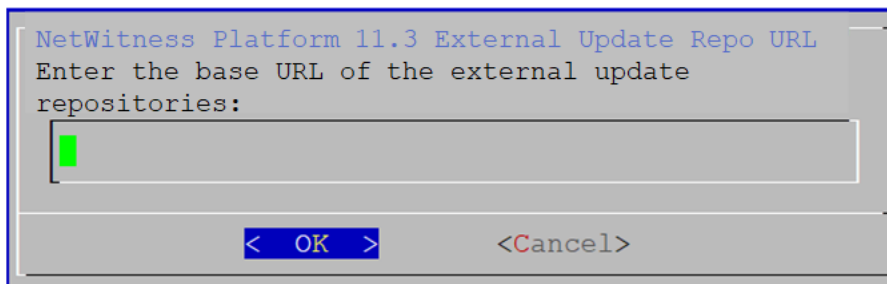
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the*Hosts and Services Getting Started Guide for Version 11.4* for instructions. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

9. Enter the base URL of the NetWitness Platform external repo and click **OK**.
   The disable or use standard firewall configuration prompt is displayed.

```
        ┌──────Disable Firewall──────┐
        Do you need to apply custom
        firewall rules to this host?
        ("No" enforces the standard
        NetWitness firewall rule set to
        the host)

             < Yes >      < No   >
```

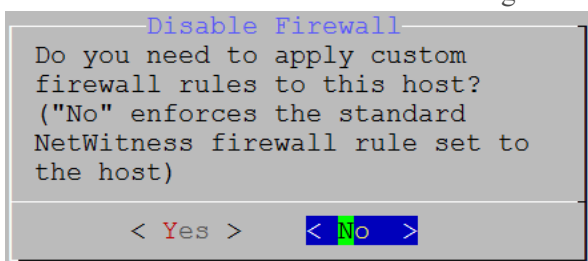10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

   - If you select Yes, confirm your selection.

```
   Warning: you chose to disable the default NetWitness
   firewall configuration which means you must set up
   firewall rules manually.

   Select "Yes" to confirm that you will set up firewall
   rules manually.

              < Yes >            < No  >
```

   - If you select No, the standard firewall configuration is applied.

The start upgrade prompt is displayed.

```
┌──────────────── Start Install/Upgrade ────────────────┐
│ All the required information has been gathered.        │
│                                                        │
│ Select "1 Upgrade Now" to start the installation       │
│ on this host.                                          │
│ ┌────────────────────────────────────────────────────┐ │
│ │        1  Upgrade Now                               │ │
│ │        2  Restart                                   │ │
│ │                                                    │ │
│ └────────────────────────────────────────────────────┘ │
│                                                        │
│        <  OK  >              < Exit >                  │
└────────────────────────────────────────────────────────┘
```
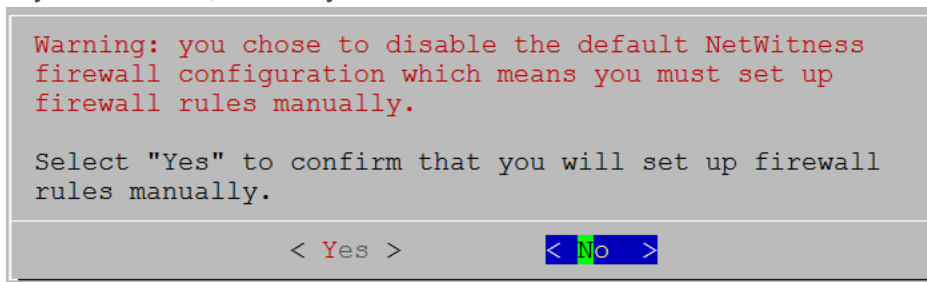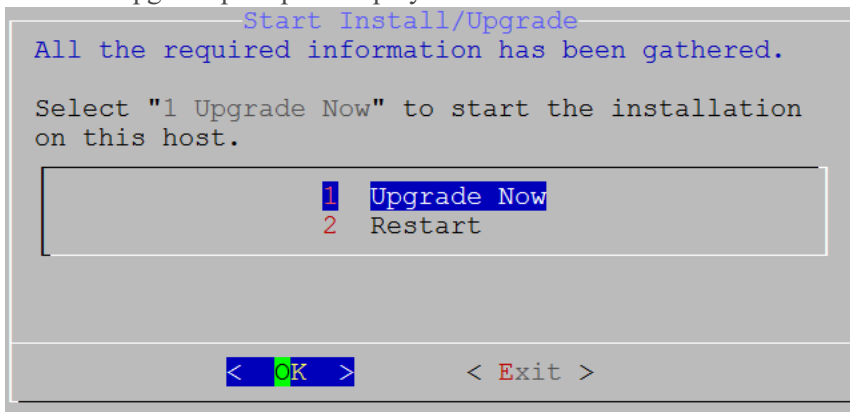
11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.

    When "Installation complete" is displayed, you have upgraded the 10.6.6.x SA Server to the 11.3 NW Server.

    > **Note:** Ignore the hash code errors similar to the errors shown in the following screen shot that are displayed when you initiate the `nwsetup-tui` command. Yum does not use MD5 for any security operations so they do not affect the system security.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
      (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```
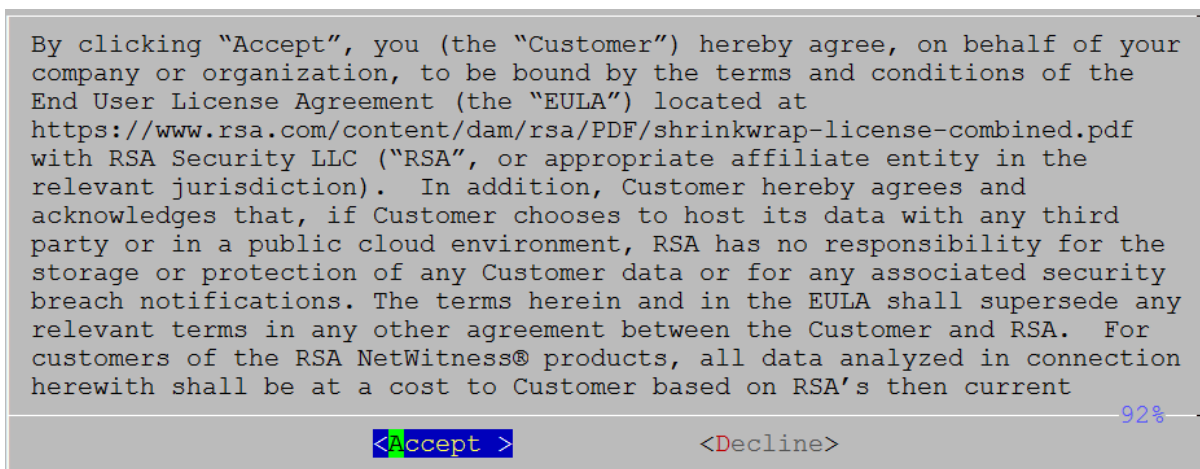
Set Up 11.4 Non-NW Server Host

Make sure that you Back up your 10.6.6.x data for the host. You must follow the instructions in Backup Instructions to back up the host.

> **Caution:** Run the backup immediately before upgrading the host to 11.4 so that the data is as recent as possible.
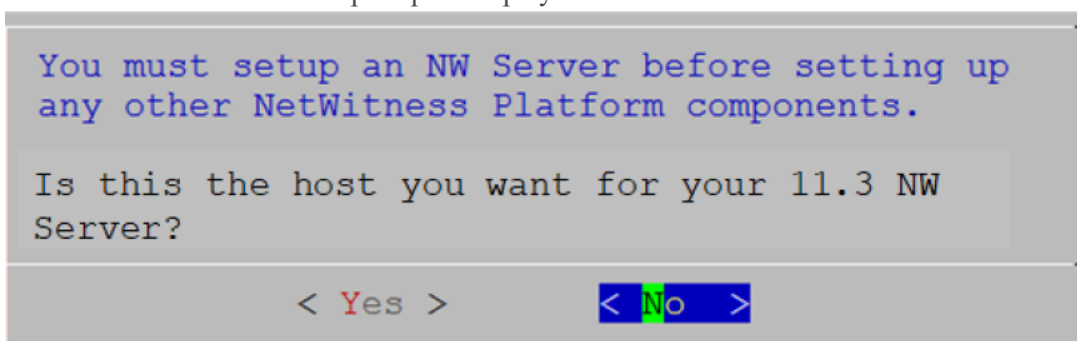
Complete the following steps to set up an 11.4 Non-NW Server host.

1. **Power On** the non-NW Server VM and run the `nwsetup-tui` command.
    This initiates the Setup program and the EULA is displayed.

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                    92%
            <Accept >                    <Decline>
```

2. Tab to **Accept** and press **Enter**.
   The "Is this the NW Server" prompt is displayed.

```
You must setup an NW Server before setting up
any other NetWitness Platform components.

Is this the host you want for your 11.3 NW
Server?

            < Yes >              < No  >
```
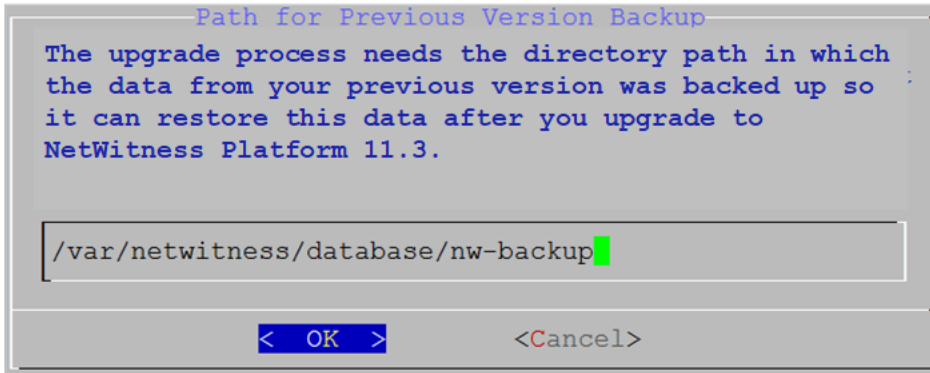
> **Caution:** If you choose the wrong the host for the NW Server and complete the upgrade, you must
> repeat steps 1 through 11 of Set Up 11.3 NW Server Host to correct this error.

3. Tab to **No** and press **Enter**.
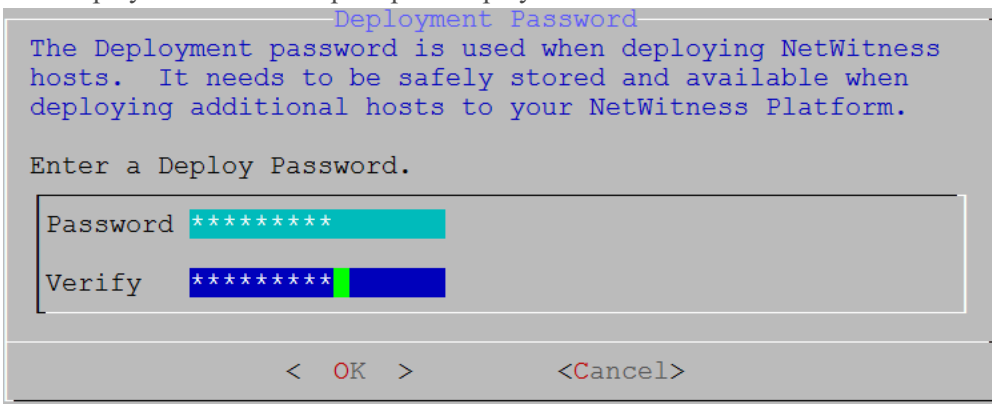   The Install or Upgrade prompt is displayed.

```
NetWitness Platform 11.3 Install or Upgrade
  Specify if you are installing NetWitness
  for the first time or upgrading from a
  previous version:

        1   Install (Fresh Install)
        2   Upgrade (From Previous Vers.)
        3   Recover (Reinstall)

            <  OK  >          < Exit >
```
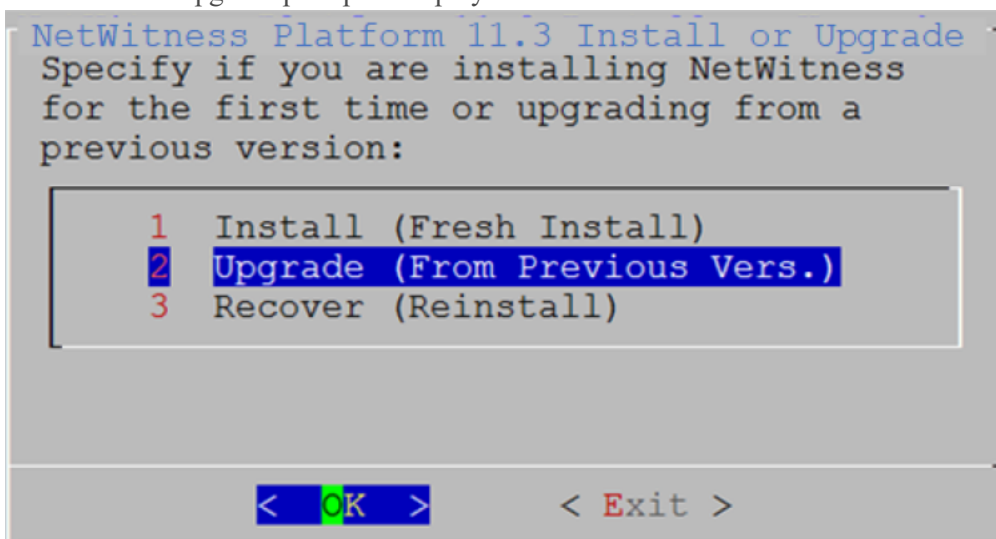
4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.
The backup path prompt is displayed.

```
┌──────────Path for Previous Version Backup──────────┐
│                                                     │
│   The upgrade process needs the directory path in which │
│   the data from your previous version was backed up so  │
│   it can restore this data after you upgrade to         │
│   NetWitness Platform 11.3.                             │
│                                                         │
│  ┌────────────────────────────────────────────────┐    │
│  │/var/netwitness/database/nw-backup▌             │    │
│  └────────────────────────────────────────────────┘    │
│                                                         │
│        <   OK   >            <Cancel>                   │
└─────────────────────────────────────────────────────┘
```
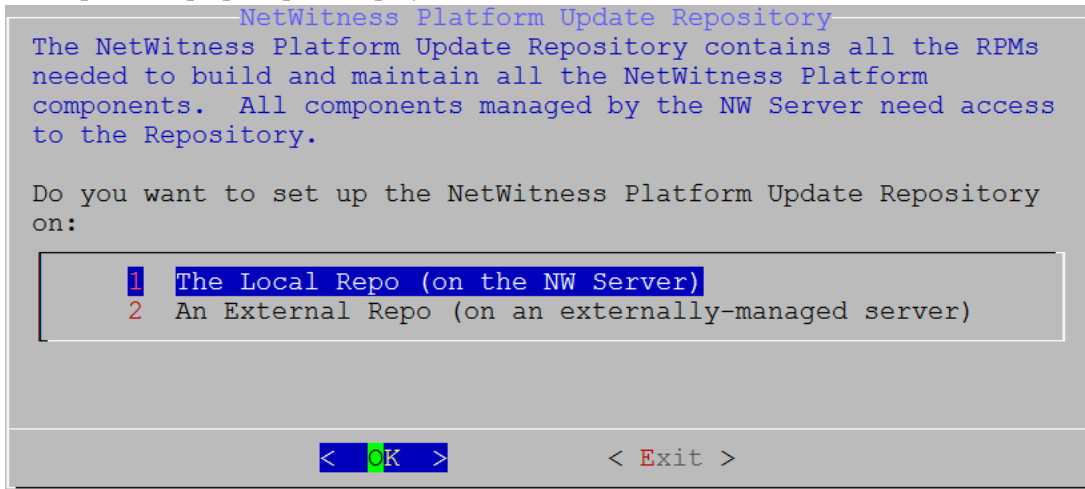
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.
The Deployment Password prompt is displayed.

```
┌──────────────────Deployment Password──────────────────┐
│  The Deployment password is used when deploying NetWitness │
│  hosts.  It needs to be safely stored and available when   │
│  deploying additional hosts to your NetWitness Platform.   │
│                                                            │
│  Enter a Deploy Password.                                  │
│  ┌──────────────────────────────────────────────────┐     │
│  │Password ********                                  │     │
│  │                                                   │     │
│  │Verify   ********▌                                 │     │
│  └──────────────────────────────────────────────────┘     │
│                                                            │
│           <   OK   >            <Cancel>                   │
└──────────────────────────────────────────────────────────┘
```

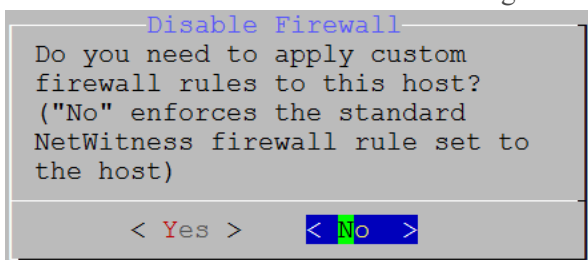**Note:** You must use the same deployment password that you used when you upgraded the NW Server.

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
   The Update Repo prompt is displayed.

```
┌─────────────────NetWitness Platform Update Repository─────────────────┐
│  The NetWitness Platform Update Repository contains all the RPMs      │
│  needed to build and maintain all the NetWitness Platform             │
│  components.  All components managed by the NW Server need access      │
│  to the Repository.                                                    │
│                                                                        │
│  Do you want to set up the NetWitness Platform Update Repository       │
│  on:                                                                   │
│                                                                        │
│    ┌───────────────────────────────────────────────────────────────┐ │
│    │ 1  The Local Repo (on the NW Server)                          │ │
│    │ 2  An External Repo (on an externally-managed server)         │ │
│    │                                                                │ │
│    └───────────────────────────────────────────────────────────────┘ │
│                                                                        │
│            <  OK  >                    < Exit >                        │
└────────────────────────────────────────────────────────────────────────┘
```

7. Use the down and up arrows to select **1 The Local Repo on the NW Server**, tab to **OK**, and press **Enter**.

8. The NW Server IP Address is displayed.

```
┌────────NW Server IP Address────────┐
│ Please Enter the IP address of     │
│ the 11.3 NW Server. The NW         │
│ Server must be routable from       │
│ this instance for installation     │
│ to continue.                       │
│  ┌──────────────────────────────┐  │
│  │ <IP-address>                 │  │
│  └──────────────────────────────┘  │
│                                    │
│      <  OK  >      <Cancel>        │
└────────────────────────────────────┘
```
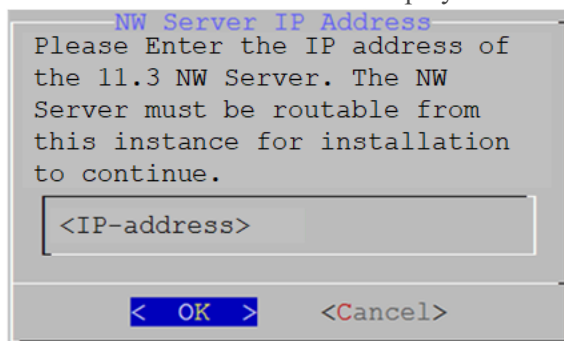
9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.
   The disable or use standard firewall configuration prompt is displayed.

```
┌────────Disable Firewall────────┐
│ Do you need to apply custom    │
│ firewall rules to this host?   │
│ ("No" enforces the standard    │
│ NetWitness firewall rule set to│
│ the host)                      │
│      < Yes >      < No  >       │
└────────────────────────────────┘
```

10. Tab to **No**, and press Enter to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- If you select **Yes**, confirm your selection.

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

            < Yes >                < No  >
```

- If you select **No**, the standard firewall configuration is applied.

The start upgrade prompt is displayed.

```
            Start Install/Upgrade
  All the required information has been gathered.

  Select "1 Upgrade Now" to start the installation
  on this host.

                    1  Upgrade Now
                    2  Restart



            <  OK  >           < Exit >
```
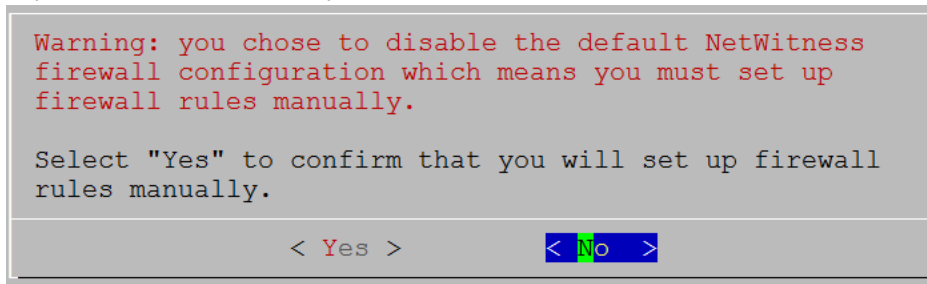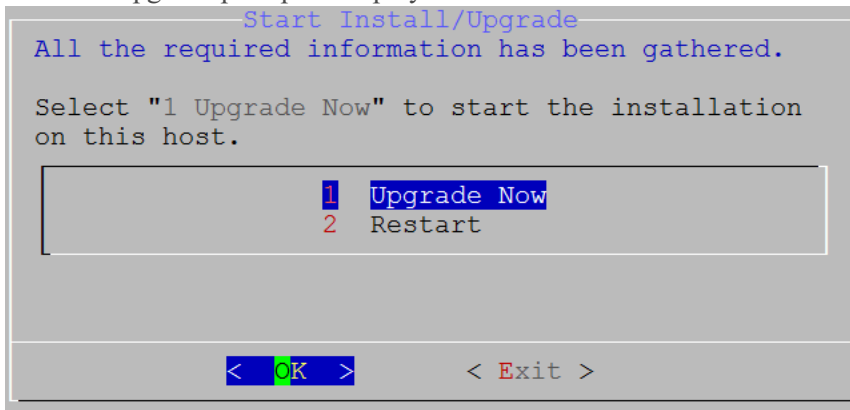
11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.
    When "Installation complete" is displayed, you have upgraded the host to the 11.4.

Once 'nwsetup-cli' script ran successfully on all the components, follow the below steps to complete NW 11.3 Upgrade or Migration:

1. Log into NetWitness Platform. (Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Platform Login screen)

2. Click ADMIN > Hosts. The New Hosts dialog is displayed with the Hosts view grayed out in the background. Note: If the New Hosts dialog is not displayed, click Discover in the Hosts view toolbar.

3. Click on the host in the New Hosts dialog and click Enable. The New Hosts dialog closes and the host is displayed in the Hosts view.

4. Select that host (for example, ESA Primary) and click The Install Services dialog is displayed.

e. Select the appropriate service (for example, **ESA Primary**) and click **Install**.
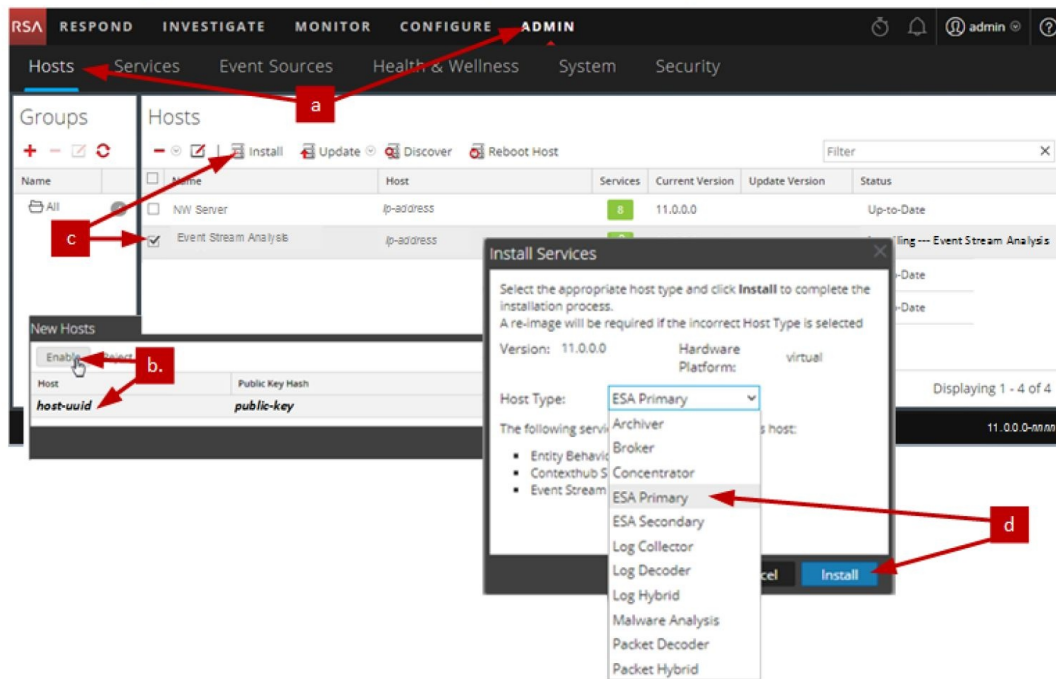
Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.4 Legacy Windows Collection Guide* on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

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

Post Upgrade Tasks

You must complete the following tasks after you upgrade your hosts from 10.6.6.x to 11.4. These tasks are organized by the following categories.

- General

- Event Stream Analysis

- Investigate

- Log Collection

- Log Decoder and Decoder

- Malware Analysis

- Reporting Engine

- Respond

- Warehouse

- RSA Archer® Cyber Incident & Breach Response

- RSA NetWitness® Endpoint

- RSA NetWitness® UEBA

- NetWitness Platform Integrations

- Other

Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

General

General tasks apply to all customers regardless of the NetWitness Components you deploy.

Task 1 - Remove Backup-Related Files from Host Local Directories

> **Caution:** 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.4 before you remove the backup-related files from the local directories on your 11.4 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.4, you must remove:

- The backup files from the local directories on the hosts.

- All the files from `nw-backup` and `restore` directories on the hosts.

Host	Backup Path	Restore Path
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
All Other Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Task 2 - Make Sure Port 15671 Is Configured Correctly

Port 15671 is new in 11.x, but you do not need to open a firewall for this port. Make sure that port 15671, and all ports, are configured as shown in the "Network Architecture and Ports" topic in the *Deployment Guide*.

(Optional) Task 3 - Reissue Certificates for Your Hosts

In 11.4.0.0, RSA introduced a `cert-reissue` command line command and its arguments to reissue host certificates. After you update all your hosts to 11.4, you should reissue certificates for all of them as soon as possible to avoid having them expire. If the certificates expire, this places your NetWitness deployment in a bad security state. Refer to the *System Security and User Management Guide* for instructions on how to use the `cert-reissue` command.

(Conditional) Task 4 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.6.x, you must reinstate them in 11.4. See "Add a Role and Assign Permissions" in the *System Security and User Management Guide*.

(Conditional) Task 5 - If NetWitness Platform Has No Web Access, Upload Response `.bin` File Again (License Server)

If your NetWitness Deployment does not have Internet access, after you upgrade to 11.4, you must upload the response `.bin` file again to view the license information in the **ADMIN** > **System** > **Licensing** view in the NetWitness Platform User Interface. See "Upload an Offline Capability Response to NetWitness Platform" in the *Licensing Management Guide* for instructions.

Task 6 - Migrate Active Directory (AD)

The first time you log into the NetWitness Platform 11.4 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Platform 11.4 with your `admin user` credentials.

2. Go to **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.

External Authentication Migration

10.6.x authentication providers and external role mappings are not migrated. To migrate these settings click on **Migrate** button.
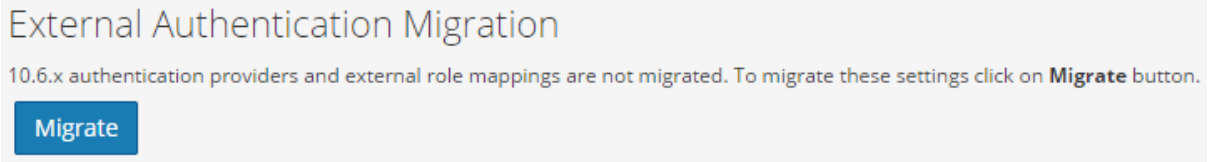
Migrate

3. Click **Migrate**.
   The migration is complete and the dialog closes.

Task 7 - Modify Migrated AD Configuration to Upload Certificate

If you authenticated through Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.6.x, you must modify the migrated AD configuration to upload the Active Directory server certificate.

Complete the following procedure to modify the migrated AD configuration to upload the certificate.

1. Log in to **NetWitness Platform** 11.4, go to **ADMIN** > **Security** and click the **Settings** tab.

2. Under **Active Directory Settings**, select an AD configuration and click ✎ .
   The Edit Configuration dialog is displayed.

3. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.

4. Click **Save**.

Task 8 - Reconfigure Pluggable Authentication Module (PAM) in 11.4

You must reconfigure PAM after you upgrade to 11.4. See "Configure PAM Login Capability" in the *System Security and User Management Guide* for instructions.

You can refer to your 10.6.6.x PAM configuration files in the **/etc** directory in the your 10.6.6.x backup data for guidance.

Task 9 - Restore NTP Servers

You must use the NetWitness Platform 11.4 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *System Configuration Guide* for detailed instructions on how to add NTP servers.

Task 10 - Restore Licenses for Environments without FlexNet

Operations-On Demand Access

If your environment does not have access to FlexNet Operations-On Demand, you need to re-download your NetWitness Platform licenses. Refer to "Step 1. Register the NetWitness Server" in the *Licensing Management Guide* for instructions on how to re-download licenses.

(Conditional) Task 11 - If You Disabled Standard Firewall Config - Add Custom IPtables

During the upgrade, you have the option of using these rules or disabling them. If you disabled them, follow these instructions as a baseline to create user-managed firewall rule sets on all the hosts for which you disabled the standard firewall configuration.

> **Note:** You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the restore folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.

2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```

3. Reload the `iptables` and `ip6tables` services.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditional) Task 12 - Specify SSL Ports If You Never Set Up Trusted Connections

Complete this task only if you never set up Trusted Connections. You would not have set up Trusted Connections if you:

- Used the base ISO image for 10.3.2 or earlier.
- Updated the system using RPMs exclusively to get to 10.6.6.x.

NetWitness Platform 11.4 cannot communicate with the Core services if you are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. Log in to **NetWitness Platform** and go to **ADMIN** > **Services**.

2. Select each core service and change the ports from Non-SSL to SSL ports.

Service	Non-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

3. Click ✎ (Edit icon) from the SERVICES view toolbar.
   The Edit Service dialog is displayed.

4. Change the port from Non-SSL to SSL as shown in the table and click **Save** (for example, change the Broker port from 50003 to 56003).

Task 13 (Conditional) Reconfigure Public Key Infrastructure (PKI) Certificates

If you had PKI keystores that contained server certificates with private keys and the truststores that contain the trusted CA certificates, you must reconfigure after you upgrade to 11.4. For instructions on how to configure PKI authentication, see the "*System Security and User Management Guide*".

Event Stream Analysis (ESA)

Task 14 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.6.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.4.

1. Log in to **NetWitness Platform** and go to **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Network data and C2 for Logs, require a whitelist named "**domains_whitelist**".

2. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:

   a. Go to **ADMIN** > **Services**, select the Context Hub service, in the action commands ( ) drop-down menu, click **View** > **Config** > **Lists** tab.

    b.   Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *ESA Configuration Guide*.

Task 15 (Conditional) Verify String Array Type Meta Keys on the ESA Correlation Service

If you added any string array type meta keys to the Event Stream Analysis service for your ESA correlation rules in 10.6.6.x or earlier, verify that they appear on the ESA Correlation service in 11.4.

1. Follow the "Configure Meta Keys as Arrays in ESA Correlation Rule Values" procedure in the *ESA Configuration Guide* to verify if the string array type meta keys that were added before the upgrade are on the ESA Correlation service. Add any missing string array type meta keys.

2. Do not remove any meta keys from the multi-valued parameter on the ESA Correlation service. In NetWitness Platform 11.4, the ESA rules from Live use meta keys with array syntax and they depend on these meta keys to work correctly. Removing values from the multi-valued list can cause the ESA Rule Deployments to fail.

Task 16 (Conditional) Update RSA Live ESA Rules with Meta Type Changes from String to Array

The following table lists the ESA rules from RSA Live that had meta key type changes from String to Array in NetWitness Platform 11.4.

Rule #	Rule Name	Array Type Meta Keys in 11.4
1	RIG Exploit Kit	threat_category
2	AWS Critical VM Modified	alert
3	Multiple Successful Logins from Multiple Diff Src to Same Dest	host.src and host.dst
4	Multiple Successful Logins from Multiple Diff Src to Diff Dest	host.src and host.dst
5	Multiple Failed Logins from Multiple Diff Sources to Same Dest	host.src and host.dst
6	Multiple Failed Logins from Multiple Users to Same Destination	host.src and host.dst
7	User Login Baseline	host.src and host.dst

1. If you:

   - Deployed these rules before version 11.4:

     a. Note any rule parameters that you have changed so you can adjust the rules for your environment.

     b. Download the updated rules from RSA Live.

     c. Reapply any changes to the default rule parameters and deploy the rules. (For instructions, see "Download RSA Live ESA Rules" in the *Alerting with ESA Correlation Rules User Guide*.)

   - Are deploying these rules for the first time in version 11.4, follow the customization directions with the ESA rule descriptions. Rules 3 to 7 in the above table require that the Context Hub lists for `User_Whitelist`, `Host_Whitelist` and `IP_Whitelist` to be added as enrichments to ESA. (See "Configure Context Hub List as an Enrichment Source" in the *Alerting with ESA Correlation Rules User Guide*.)

2. Deploy the ESA rule deployment that contains these rules. (See "ESA Rule Deployment Steps" in the *Alerting with ESA Correlation Rules User Guide*.)

Task 17 (Conditional) - Verify ESA Rule Deployment

After you upgrade to 11.4, verify your ESA rule deployments. For every ESA host, a new deployment is created in the format "<ESA Host name> – ESA Correlation".

1. Make sure that a new deployment was created.

2. Make sure that the new deployment contains an ESA Correlation service, data sources, and rules for all previous deployments on that ESA host.

3. Make sure that the ESA Correlation service has status of "Deployed".

For a detailed example, see the *ESA Configuration Guide*. For Deployment information, see "ESA Rule Deployment Steps" in the *Alerting with ESA Correlation Rules User Guide*. For troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.

Investigate

Task 18 - Make Sure Customized User Roles Have `Investigate-server` Permissions for Event Analysis Access

After you upgrade to 11.4.0.0, any customized user role does not have `investigate-server.*` permission enabled by default. Complete the following procedure to make sure that the appropriate user roles have permission to access Event Analysis.

1. Log in to NetWitness Platform 11.4.0.0 with your `Admin user` credentials and go to **ADMIN** > **Security**.

2. Click the **Roles** tab.

3. Select the roles that need `investigate-server.*` permissions and click (Edit icon).

4. Select the **Investigate-server** tab under under **Permissions**.

5. If the **investigate-server** checkbox is not set, set it for the Roles that require Event Analysis access.

6. Click **Save**.

Log Collection

Task 19 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.4 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *Log Collection Configuration Guide* for instructions.

Update Log Collector Service RabbitMQ User Account Password

If the `logcollector` service RabbitMQ user account password was changed, you must reenter it after the 11.4 upgrade.

1. Log in to **NetWitness Platform** and go to **ADMIN** > **Services**.

2. Select the Log Collector service.

3. Click [gear icon] (Actions) > **View** > **Explore**.

4. Right click `event-broker` > **Properties** .

5. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.
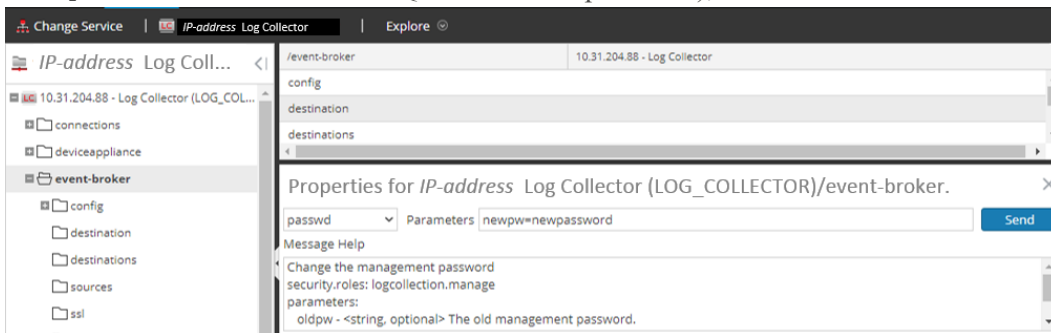
Task 20 - (Conditional) Update SSHD Configuration after Upgrade with Older Windows and UNIX SFTP Agents

This task applies if you have Log Collection, Log Collector (LC) and or Virtual Log Collector (VLC), with File Collection event sources.

If all the event sources:

- Resume collection after upgrade, you do not need to do anything.

- Do not resume collection after the upgrade, you may have to restore Cipher, MACs and Key Exchange Algorithms to the SSHD configuration from the original LC/VLC. Change the

---

`/etc/ssh/sshd_config` file.

1. Make the following changes to `/etc/ssh/sshd_config` file.

    a. If the `KexAlgorithms` line:

       ○ Exists, append "`,diffie-hellman-group1-sha1`" to the file.

       ○ Does not exist, add "`KexAlgorithms +diffie-hellman-group1-sha1`" line.

    b. If the `Ciphers` line:

       • Exists, append "`,aes128-cbc`" to the file.

       • Does not exist, add the "`Ciphers +aes128-cbc`" line to the file.

2. Restart SSHD service.

3. If collection still fails, edit the `/etc/systemd/system/sshd.service.d/sshd-opts-managed.conf` file and change "`OWB_ALLOW_NON_FIPS=on`" to "`OWB_FIPS_MODE=off`" in the Environment line and restart SSHD service.

4. If collection still fails, contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294).

Task 21 - Enable FIPS Mode

> **Note:** This task is optional for Upgrades from 10.6.6.x with FIPS enabled for Log Collectors, Log Decoders and Network Decoders)

FIPS is enabled on all services except Log Collector, Log Decoder, and Decoder. FIPS cannot be disabled on any services except Log Collector, Log Decoder, and Decoder.

Log Decoder and Decoder

(Conditional) Task 23 - Enable Metadata for GeoIP2 Parser

By default, the GeoIP2 parser generates less metadata than the GeoIP parser did. After updating to 11.4, if you require any of the additional metadata, you must enable them (once only) for each Decoder. This can also be altered post-upgrade. Note that the `isp` and `org` meta fields usually produce an equivalent value to `domain`.

To enable metadata:

1. Go to **ADMIN** > **Services**.

2. In the **Administration services** view, select a Log Decoder or a Decoder.

3. Click the settings icon (⚙️ ⊙) and select **View** > **Config**. The Parsers Configuration panel is displayed, from which you can select **GeoIP2** to enable the desired metadata.

For more information about GeoIP2 parsers, see the "GeoIP2 and GeoIP Parsers" topic in the *Decoder and Log Decoder Configuration Guide*.

Malware Analysis

Task 24 - Enable Threat - Malware Indicators Dashboard

In 11.3, the 10.6.6.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.6.x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.4.

2. Set datasource for new dashlets.
   See "Dashlets" in RSA Link (https://community.rsa.com/docs/DOC-81463) for a description of Dashlets in the context of NetWitness Platform.

> **Note:** After upgrading to 11.4, both the Threat-Indicators and the Threat-Malware Indicators dashboards can be displayed in the User Interface. If this is the case, disable the Threat-Indicators dashboard, and enable the Threat-Malware Indicators report charts and dashboard. For information about disabling dashboards, see the "Managing Dashboards" topic in the *NetWitness Getting Started Guide*.

Reporting Engine

(Conditional) Task 25 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the backup you made prior to the upgrade. The Backup script backs up the 10.6.6.x CA certificates into the `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts` directory.

Complete the following procedure to restore the CA certificates in 11.4.

1. SSH to the NW Server host.

2. Export the CA certificates.
   `keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file`

3. Copy the CA PEM file into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 26 - Restore External Storage for Reporting Engine

If you have external storage for the Reporting Engine (such as SAN or NAS for storing reports), you must restore the mount you unlinked before the upgrade. See "Reporting Engine: Add Additional Space for Large Reports" in the *Reporting Engine Configuration Guide* for instructions.

Respond

Task 27 - Restore Respond Service Custom Keys

In 10.6.6.x, if you added custom keys for use in the **groupBy** clause, the `alert_rules.json` file was modified. The `alert_rules.json` file contains aggregation rule schema. RSA moved the `alert_rules.json` file to the following new location:
`/var/lib/netwitness/respond-server/scripts`

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.
   This directory is where the `alert_rules.json` file is restored from the 10.6.6.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.4.
   This is the new file for 11.4.

3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 28 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.4 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
 If you customized these scripts in 10.6.6.x, you must:

1. Go to the to the `/opt/rsa/im/scripts` directory.
   This directory is where the following Respond service normalization scripts are restored from the 10.6.6.x backup.
   `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`

2. Copy any custom logic from the 10.6.6.x scripts.

3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Platform 11.4 stores the re-factored scripts.

4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.6.x scripts.

5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
    The `alert_rules.json` file contains aggregation rule schema.

Task 29 - Add Respond Notification Settings for Custom Roles

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*.

Task 30 - Manually Configure Respond Notification Settings

The Incident Management notification settings in NetWitness Platform 10.6.6.x are different from the Respond notification settings available in 11.4, so your existing 10.6.6.x settings will not migrate to 11.4.

NetWitness Respond notification settings enable email notifications to be sent to SOC Managers and the Analyst assigned to an incident when an incident is created or updated.

To manually configure the Respond Notification Settings, go to **CONFIGURE** > **Respond Notifications.** See the "Configure Respond Email Notification Settings" procedure in the *NetWitness Respond Configuration Guide*.

Notification Servers from 10.6.6.x will not display in the Email Server drop-down list. The email servers must be edited and saved in the Global Notification Servers panel (**ADMIN** > **System** > **Global Notifications** > **Server** tab).

1. Log in to **NetWitness Platform** and go to **CONFIGURE** > **Respond Notifications**.
   The Respond Notifications Settings view is displayed. Notice that the email notification servers do not appear in the EMAIL SERVER drop-down list.

2. Click the **Email Server Settings** link.
   You will see the Global Notifications panel.

3. Click the **Servers** tab.

4. For each of your email notification servers:

   a. Select the Email notification server and click (Edit icon).
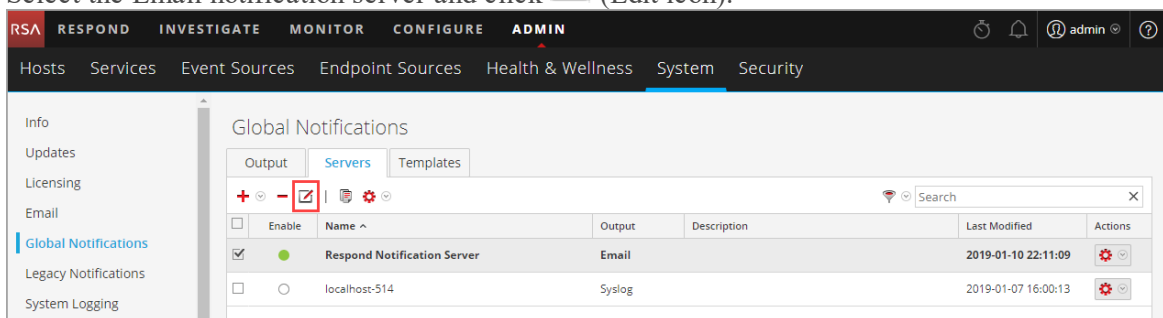
b. In the Define Email Notification Server dialog, click **Save**.

5. Go back to **CONFIGURE** > **Respond Notifications**. Your servers will appear in the **EMAIL SERVER** drop-down list.
Custom Incident Management notification templates cannot be migrated to 11.4. No custom templates are supported in 11.4.

Task 31 - Update Default Incident Rule Group By Values

The following 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: ESA**

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

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

The **High Risk Alerts: NetWitness Endpoint** default incident rule now uses Host Name as the Group By value. If you have NetWitness Endpoint you can use this rule. Change the Group By value of the default NetWitness Endpoint rule to "Host Name."

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 File Hash, complete the following steps to clone the default NetWitness Endpoint incident rule and change the Group By value.

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 File hash.

4. In the **GROUP BY** field, remove the previous Group By value and add **File MD5 Hash**. It is important that File MD5 Hash is the only Group By value listed.

5. Click **Save** to create the rule.

For detailed information, see the *Respond Configuration Guide*.

Task 32 - Add Group By Field to Incident Rules

The **Group By** field is not required in 10.6.6, but it is required in 11.3 and later. After you upgrade to 11.4, some incident rules will not have a **Group By** field, so you must add them to the rules or the rules will not work and they will not create incidents.

Complete the following steps for each incident rule:

1. Log in to NetWitness Platform.

2. Go to **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.

3. In the Group By field, verify that a Group By value is selected. If not, select a Group By value.

4. Click **Save** to update the rule.

   For information about incident rules, see the *NetWitness Respond Configuration Guide*.

Task 33 - Update Incident Rules Identified in the Domain Matching Conditions Upgrade Preparation Task

Modify the incident rules that you identified in the Task 7 - Check Aggregation Rules Match Conditions for "Domain" or "Domain for Suspected C&C" upgrade preparation task, which contained Domain or Domain for Suspected C&C in the matching conditions in rule builder.

For each rule that you previously identified:

1. Log in to **NetWitness Platform**, go to **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.

2. In the **Match Conditions** section, in the blank fields, select **Domain** and **Domain for Suspected CC** in the drop-down list and then select the conditions that you previously identified in the pre-upgrade tasks.

3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*.

Warehouse

Task 34 - Restore `keytab` Files, Mount NFS, Install Service

1. Restore the `keytab` files from `<backup-path>/restore` directory.

2. Restore the Kerberos Realm Configuration from the `<backup-path>/restore/etc/krb5.conf` into `/etc/krb5.conf`.

3. (Conditional) If you perform the upgrade from a Non - FIPS environment and the `isCheckValidationRequired` parameter is not enabled in the destination, to configure the SFTP destination:

   a. SSH to the Warehouse Connector host and submit the following commands:
      ```
      cd /root/.ssh/
       mv id_dsa id_dsa.old
      OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_dsa.old -
      out id_dsa
      ```
      You are prompted for the pass phrase.

   b. Enter the Encryption password.

   c. Run the following command.
      ```
      chmod 600 id_dsa
      ```

4. Install the Warehouse Connector.
   See the *Warehouse Connector Configuration Guide* for instructions.

Task 35 - Refresh Warehouse Connector Lockbox and Start Stream

> **Note:** If the streams have auto start turned on in 10.6.6.x, there will be a small delay before you will see the Warehouse Connector service in the NetWitness Platform User Interface.

1. Refresh the Lockbox of Warehouse Connector.

2. SSH to the Warehouse Connector and log in with root credentials.

3. Restart the service.
   ```
   service nwwarehouseconnector restart
   ```

4. (Conditional) If the auto start was not enabled in 10.6.6.x, you must start the stream manually after the service restarts.

Task 36 - Update Hive Version

After you update to 11.4, you must update to the Hive version that is compatible with the 11.4 Warehouse (either Hive version 0.12 or version 1.0).

- Hive Version 0.12
  SSH to the NW Server and run the following command.
  ```
  rpm -ivh rsa-nw-hive-jdbc-0.12.0-1.x86_64.rpm
  ```

- Hive Version 1.0

  SSH to the NW Server and run the following command.

  `rpm -ivh rsa-nw-hive-jdbc-1.0.0-1.x86_64.rpm`

RSA Archer Cyber Incident & Breach Response

Task 37 - Reconfigure RSA Archer Cyber Incident & Breach Response Integration

For information on how to reconfigure RSA Archer Cyber Incident & Breach Response for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*.

RSA NetWitness® Endpoint

Task 38 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   > **Note:** In NetWitness Platform 11.4, the virtual host is `/rsa/system`. For 10.6.6.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.

3. SSH to the NW Server and log in with `root` credentials.

4. Submit the following command to add all certificates to the truststore.
   `orchestration-cli-client --update-admin-node`

5. Submit the following command to restart the RabbitMQ server.
   `systemctl restart rabbitmq-server`
   The NetWitness Endpoint account should automatically be available on RabbitMQ.

6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Task 39 - 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 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.

(Optional) Task 40 - Install Endpoint Log Hybrid and Endpoint Agents

See:

RSA NetWitness Platform 11.4 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Platform 11.4 Virtual Host Installation Guide for instructions for installation on a virtual host.

RSA NetWitness® UEBA

Task 41 - Install NetWitness UEBA

NetWitness UEBA is new a new feature as of NetWitness Platform 11.4.

See:

RSA NetWitness Platform 11.4 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Platform 11.4 Virtual Host Installation Guide for instructions for installation on a virtual host.

RSA NetWitness UEBA User Guide for information about NetWitness UEBA.

NetWitness Platform Integrations

(Conditional) Task 42 - For Integrations with Web Threat Detection, RSA Archer® Cyber Incident & Breach Response or NetWitness Endpoint.

If you integrate with Web Threat Detection, Archer Cyber Incident & Breach Response or NetWitness Endpoint, you must configure Mutually Authenticated SSL on each integrated system so that the application can authenticate itself when connecting to the RabbitMQ message bus.

> **Note:** Use the RabbitMQ usernames and passwords that were obtained when you backed up your 10.6.6.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Platform by logging into the host and running the following `rabbitmqctl` command.
   ```
   > rabbitmqctl add_user <username> <password>
   ```

2. Set permissions for users by running the following command (use the username from step 1).
   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"
   ```

For example:

```
> rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*", ".*", ".*"
```

Appendix A. Troubleshooting

This section describes problems that you may encounter during the upgrade with solutions. In most cases, NetWitness Platform creates log messages when it encounters these problems.

> **Note:** If you cannot resolve any upgrade issue using the following troubleshooting solutions, contact Customer Support (https://community.rsa.com/docs/DOC-1294)

This section has troubleshooting documentation for the following services, features, and processes.

- 11.4 Setup Program (nwsetup-tui)
- Backup
- Event Stream Analysis
- General
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

11.4 Setup Program (`nwsetup-tui`)

Problem	Host Setup Program (`nwsetup-tui`) exits and creates the following error message in `/var/log/netwitness/bootstrap/launch/`
	`security-server/security-server.log:`
	`<yyyy-mm-dd hh:mm:ss,nnn> [ main] ERROR`
	`SystemOperation|Service startup failed. Running in safe mode`
	`org.h2.jdbc.JdbcSQLException: The database is read only [90097-193]`
	` at org.h2.message.DbException.`
	`getJdbcSQLException(DbException.java:345) ...`
	`at org.springframework.jdbc.datasource.`
	`AbstractDriverBasedDataSource.getConnection`
	`(AbstractDriverBasedDataSource.java:159)`
	`at`
	`com.rsa.asoc.security.upgrade.legacy.`
	`MigrationDatabase.<init>(MigrationDatabase.java:113)`

Cause	The H2 database needs write permission to complete the host setup.

Solution	From the NW Server command line, provide write permission to `H2.db`, restart the NW Server, and restart nwsetup-tui Setup Program.
	
	`chmod o+w /var/lib/netwitness/uax/db/platform.h2.db`
	`systemctl restart rsa-nw-security-server.service`
	`nwsetup-tui`

Backup (`nw-backup` script)

Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the the *RSA NetWitness® Platform Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *to find all RSA NetWitness Platform 11.x documents.*

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.4 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESAPrimary host and log in.
	
	2. In the `/opt/rsa/esa/conf/wrapper.conf` file, replace the following line:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	with:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	
	3. Submit the following command to restart ESA .
	`systemctl restart rsa-nw-esa-server`
	
	Note: If you have multiple ESA hosts and you encounter that same problem, repeat steps 1 through 3 inclusive on each secondary ESA host.

General

Logs referred to in this section are posted to `/var/log/install/install.log` on the NW Server Host.

Message	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.` `AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Platform sees the Service Management Service (SMS) as down after successful upgrade even though the service is running.
Solution	Restart SMS service using below command. `systemctl restart rsa-sms`

Message	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt`
	`is nGB`
	
	`<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed`
	`on /opt. The available disk space nGB is less than the recommended`
	`minimum disk space of 10GB.`

Cause	Low or insufficient disk space allocated for the SMS service.
Solution	RSA recommends that you provide a minimum of 10 GB of disk space for the SMS service to run optimally.

Problem	After you run the Setup Program for a non-NW Server host, you must go in to the UI, enable the host, and install the service on the host from the Hosts View. If you see "Install error <u>View Details</u>" in the **Status** column of the Hosts view, the host lost connectivity due to network issues.
Solution	Re-install the service on the host from the Hosts view.

Log Collector Service (`nwlogcollector`)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Platform and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Message	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness Platform and configure the Lockbox as described in the"Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents..

Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Platform and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the *Log Collection Configuration Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Problem	You have prepared a Log Collector for upgrade and no longer want to upgrade at this time.
Cause	Delay in upgrade.
Solution	Use the following command string to revert a Log Collector that has been prepared for upgrade back to resume normal operation. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the sa.log. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.6 to 11.4.
Solution	1. SSH to the NW Server. 2. Submit the following command. `orchestration-cli-client --update-admin-node`

Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Message	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Appendix B. Stopping and Restarting Data Capture and Aggregation

RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.4. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

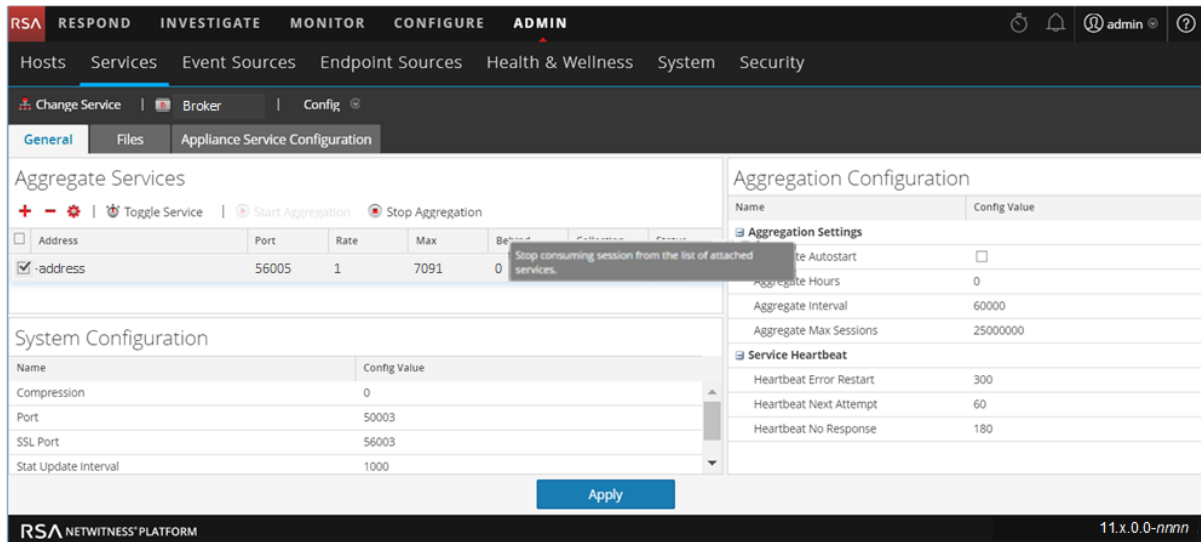1. Log in to NetWitness Platform and go to **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Decoder** service.

    Stop Capture

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 Platform and go to **ADMIN** > **Services**.
   The Services view is displayed.

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

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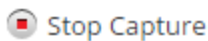
3. Under (actions), select **View** > **System**.

4. In the toolbar, click Stop Capture .

Stop Aggregation

1. Log in to NetWitness Platform

2. Go to **ADMIN** > **Services**.

3. Select the **Broker** service.

4. Under (actions), select **View** > **Config**.

5. The **General** tab is displayed.

6. Under **Aggregated Services** click .

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.4.

Start Packet Capture

To start packet capture:

1. Login to **NetWitness Platform**.

2. Go to **ADMIN** > **Services**.

   The Services view is displayed.

3. Select each **Decoder** service.

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

5. In the toolbar, click .

Start Log Capture

To 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 Aggregation

1. Log in to **.**NetWitness Platform.

2. Go to **ADMIN** > **Services**.

3. Select the **Broker** service.

4. Under (actions), select **View** > **Config**.

5. The **General** tab is displayed.

6. Under **Aggregated Services** click .

Revision History

Revision	Date	Description	Author
1.0	10-Apr-19	GA	IDD