RSA NETWITNESS® PLATFORM

Azure Upgrade Guide

for Version 10.6.6.x to 11.2

Contents

Introduction

The instructions in this guide apply to the upgrade of Azure for RSA NetWitness Platform 10.6.6.x to 10.6.6.x to 11.2 exclusively. See the *RSA NetWitness Platform Physical Host Upgrade Guide* for instructions on how to upgrade your 10.6.6.x physical hosts to 11.2. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents. This document assumes that the appliances are in Azure cloud.

NetWitness Platform 11.2 is a major release that affects all products in the NetWitness Platform in Azure. The components of the suite are the NetWitness Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Entity Behavior Analytics, Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, and Workbench.

CentOS6 to CentOS7 Upgrade

NetWitness Platform 11.2 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.2 platform environment has been improved greatly 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 11.2 Upgrade Path

The supported Upgrade path for RSA NetWitness® Platform 11.2 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 11.2. See the *RSA Security Analytics 10.6.6 Update Guide* (https://community.rsa.com/docs/DOC-85119) on RSA Link.

For updating from RSA NetWitness® Platform 11.0.0.0 to RSA NetWitness® Platform 11.2.0.0, please see the *Update Guide from 11.0.x to 10.6.6.x to 11.2Guide*.

Hardware, Deployments, Services, and Features Not Supported in 11.2

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.2.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- IPDB service
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.2.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.2.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.2, your custom policy is not present. In its place, there is the out-of-the-box Context hub Server Monitoring Policy in the user interface, which is specific for version 11.2.
- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)
- Malware Analysis
- Packet Decoder

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Platform 11.2, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.2, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.6.x has been removed.

Caution: If you do not use Incident Management in 10.6.6.x, carefully consider whether or not to upgrade to version 11.2.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.2.

In your 10.6.6.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.2.

- Multiple ESA hosts configured to use Incident Management – The system will continue to aggregate alerts centrally. If the system is correctly sized and operating as intended in 10.6.6.x, you can upgrade to version 11.2.

- 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 11.2.

Upgrade Phases

RSA recommends that you stagger host upgrades as described in this section. The update to CentOS7 and the need of a physical or iDRAC access cause the 11.2 upgrade to take more time than most upgrades.

> **Caution:** If you stagger the upgrade, you:
> • must upgrade the hosts in Phase 1 first, in the order shown.
> • may not have all the features operational until you update your entire deployment.
> • will not have service administrative features available until you upgrade all the hosts in your deployment.

Phase 1

You perform Phase 1 first and you must upgrade the hosts in the following order:

1. Security Analytics Server host

2. Event Stream Analysis hosts

3. Broker hosts (if you do not have a Broker, upgrade your Concentrator hosts)
   The 11.2 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

Upgrade the rest of your hosts.

In Phase 2, (other than Log Collection hosts with downstream event destinations) there is no technical reason to upgrade your hosts in the following order. RSA recommends that you follow the order in Phase 2 to reduce:

- functionality loss during investigation.

- downtime that results in the loss of packet and log capture.

1. Concentrator hosts

2. Archiver hosts

3. Log Collection hosts - Log Collectors on Log Decoder hosts (LDs), Virtual Log Collectors (VLCs) and Legacy Windows Collectors (LWCs)
   Before you upgrade a log collection host , you must prepare it for the upgrade. Part of this preparation ensures that no event data remains in the queues. This requires you to keep the downstream destinations of event data (Log Collectors, Virtual Log Collectors and Log Decoders) up and functioning properly.

If you have event data destinations downstream from the Log Decoder, you must prepare and upgrade log collectors in the following order.

a. LDs (one LD at a time)

b. VLCs and LWCs

If you do not have event data destinations, downstream from the Log Decoder, you can prepare and upgrade multiple LDs, VLCs, and LWCs together.

4. All other hosts

See "Running in Mixed Mode" under "The Basics" in the RSA 11.2 *NetWitness Platform Hosts and Services Getting Started Guide* for:

● Functionality gaps encountered while running in this mode.

● Examples of staggered upgrades.

Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.2 and some are still on 10.6.x. This happens when you upgrade to 11.2 in phases.

> **Note:** You must follow the host upgrade sequence as shown in Upgrade Phases to ensure complete Investigate functionality. The 11.2 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.0 to access the Event Analysis View.

After you upgrade all services to 11.2, when an analyst conducts an investigation, Role-Based Access Control (RBAC) of downloads works consistently to limit access to restricted data.

In mixed mode (that is, some services are upgraded to 11.2 and some are still on 10.6.x), when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads.

If the `sdk.packets` setting has not been disabled on the 10.6.x services, analysts with SDK meta and roles permissions in place to restrict viewing and reconstructing an event's content can download the PCAP of an event that has content restrictions. Other types of downloads appear to download, then generate errors due to insufficient permissions, and the data is still protected.

During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.2, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NetWitness Server is on version 11.2 connected to services at a lower version.

Connecting Service Version	Affected View	User Role	Can See	Can Download Successfully	Can Download with Errors
11.2 Broker -> 10.x Concentrator	Events View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst		PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload
	Event Reconstruction View	Admin			Files archive is downloaded but cannot unzip
11.2 Broker -> 11.2 Concentrator	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items		Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Reconstruction View				
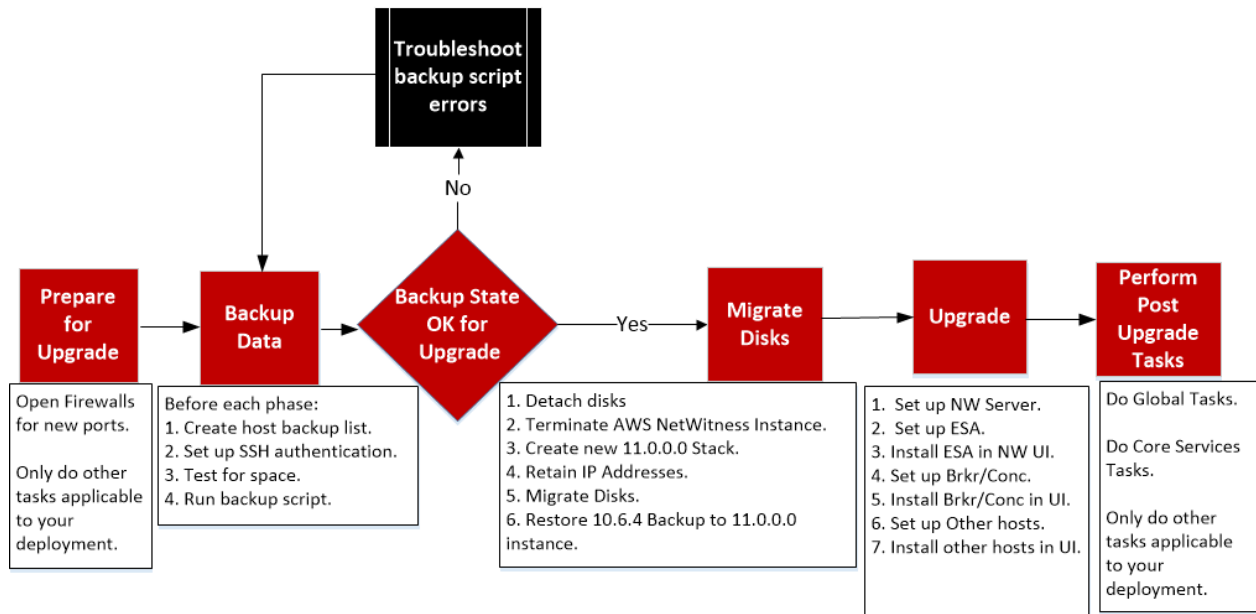
Contact Customer Support

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 11.2.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Platform 11.2. These tasks are organized by the following categories.

- Global
- Reporting Engine
- Respond and Incident Management

Global

You must complete these tasks regardless of how you deploy NetWitness Platform and which components you use.

Task 1 - Review Core Ports and Open Firewall Ports

The following table lists new ports in 11.2.

> **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

ESA Host

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

All NetWitness Platform core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® Platform Deployment Guide* in case you need to reconfigure NetWitness Platform services and firewalls. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

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 `/etc/fstab` File

Copy the `/etc/fstab` file from all VMs to your local machine (backup host or remote machine).

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

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

> **Note:** You can skip this task if you do not want to migrate the password strength setting to 11.2.

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 11.2.

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 the required check boxes to the left of the **Password Strength Settings** are set and click **Apply**.
   The following example shows the required check boxes as set (required in 10.6.6.x before upgrading to 11.2).
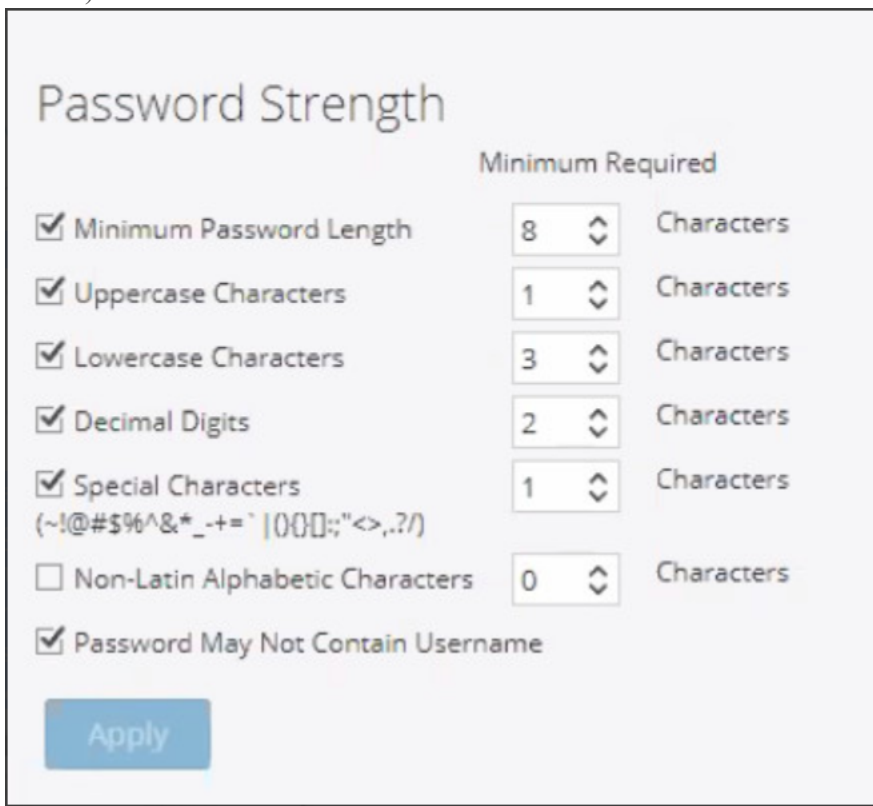
Reporting Engine

(Conditional) Task 5 - Unlink External Storage

If the Reporting Engine has external storage [such as Storage Area Network (SAN) or Network Attached Storage (NAS) for storing reports] you must perform the follow steps to unlink the storage.

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`

Respond

Task 6- Set Data Retention Run Interval to ≥ 24 Hours

In Security Analytics 10.6.x , the Data Retention run interval does not have any minimum value check. In 11.2, RSA added a validation check to make sure that it is run at least every 24 hours. When you upgrade to 11.2, if this value is less than 24 hour, the Respond service will not start.

Complete the following task to ensure that the Respond service starts after upgrading to 11.2.

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

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

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

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

Upgrade Preparation Tasks
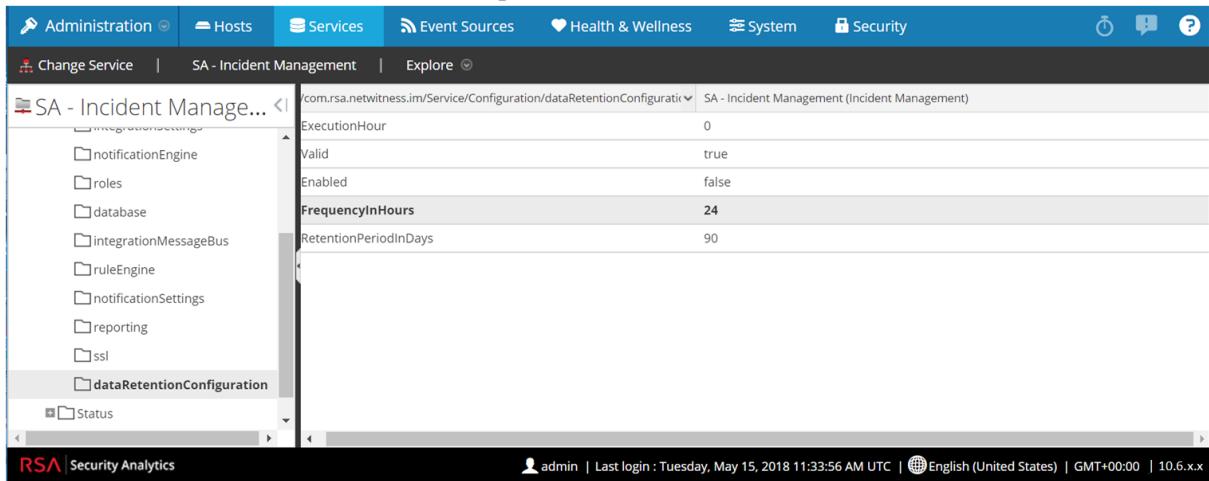
Backup Instructions

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 11.2.0.0.

> **Note:** It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.2.0.0, your 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

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** (including Local LogCollector and Warehouse Connector, if installed)

- **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, refer to "Task 5 - Reconfigure Plugable Authentication Module (PAM) in 11.2.0.0", 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. |
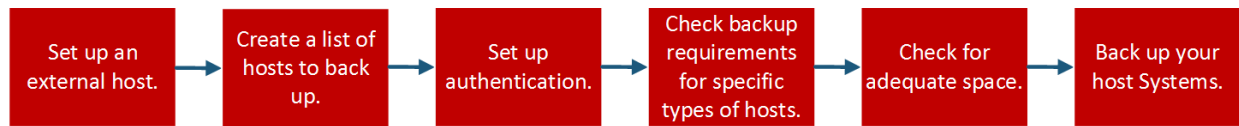
The following sections describe each of these tasks:

- Task 1 - Set up an External Host for Backing up Files

- Task 2 - Create a List of Hosts to Back up

- Task 3 - Set up Authentication Between Backup and Target Hosts

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

- Task 5 - Check for Adequate Space for the Backup

- Task 6 - Back up Your Host Systems

- Post Backup Tasks

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.

Ensure that the host names for the 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-v3.0.zip`) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Click the **RSA NetWitness Logs & Packets 11.2 Backup Script (nw-backup-v3.0.sh)** link and 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 the 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 the 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 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:

```
1
NWServers
ESA Hosts
```

```
2
Brokers
```

```
3
Concentrators
```

```
4
Log Collectors, Virtual Log Collectors,
```
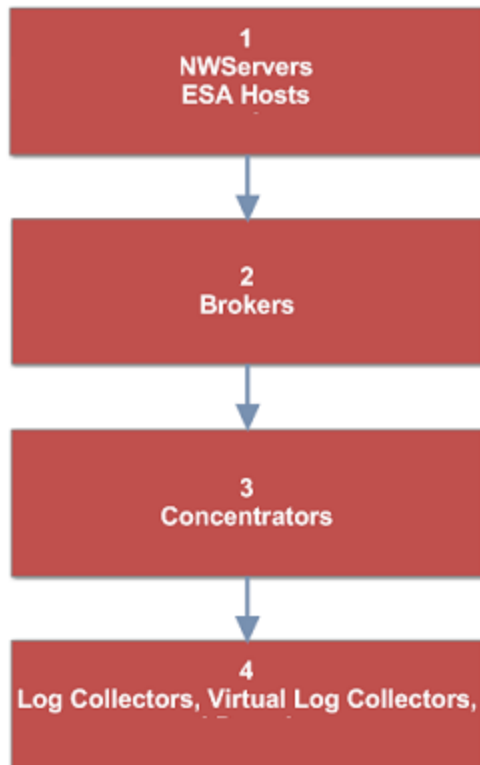
Limit each backup session to five hosts to ensure that you do not run out of space for the backup files. You create `all-systems` files for your backup sessions by using the `all-systems-master-copy` file as a reference and then manually editing the `all-systems` file to contain specific hosts.

To generate the `all-systems` and the `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 `get-all-systems.sh` 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,10.6.4.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.4.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.4.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.4.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.4.0
```

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,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
```

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 Upgrade 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. Ensure 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 ensure 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 Azure 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 again 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 ensure 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 11.2.0.0, 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 Concentrator, or Broker Hosts: Stop Data Capture and Aggregation

In addition to the tasks described in For All Host Types, for 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 11.2.0.0.

   - 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 11.2.0.0 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 ensure 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.

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 11.2.0.0.

> **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 -u -l -x -e <external-mnt> -b <backup file path>
```

General Options

-u : This option is required for upgrading to 11.2. Enables the upgrade flag to run backup for upgrading to 11.2. 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 11.0, 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 11.2. 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:
> 10.6.3.x and 10.6.4.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. Ensure that the `all-systems` file contains only the 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 11.2.0.0.

   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 ensure 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 11.2.0.0.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.2.0.0 upgrade process. Before you begin the upgrade process, you must ensure 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`

Task 3 - (Conditional) 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 11.2.0.0, ensure 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`

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 11.2

These instructions tell you how to upgrade Azure NetWitness VMs from 10.6.6.x to 11.2.0.0 on Azure Cloud Platform.

Prerequisites:

- Download and install the latest version of Azure PowerShell from https://github.com/Azure/azure-powershell/releases on a Windows machine.

- Upload the same latest version of Azure modules in automation account. [https://docs.microsoft.com/en-us/azure/automation/automation-update-azure-modules]

> **Note:** Azure PowerShell 4.4.1 was used for qualification.

> **Note:** Both versions of VMs must be on the same Virtual Network and Resource Group for the migration.

> **Caution:** 1) You cannot perform the migration if you have a snapshot for your VM.
> 2). Run the backup immediately before you upgrade hosts for each phase so that the data is not outdated.
> 3.) This guide applies to virtual host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Platform Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.
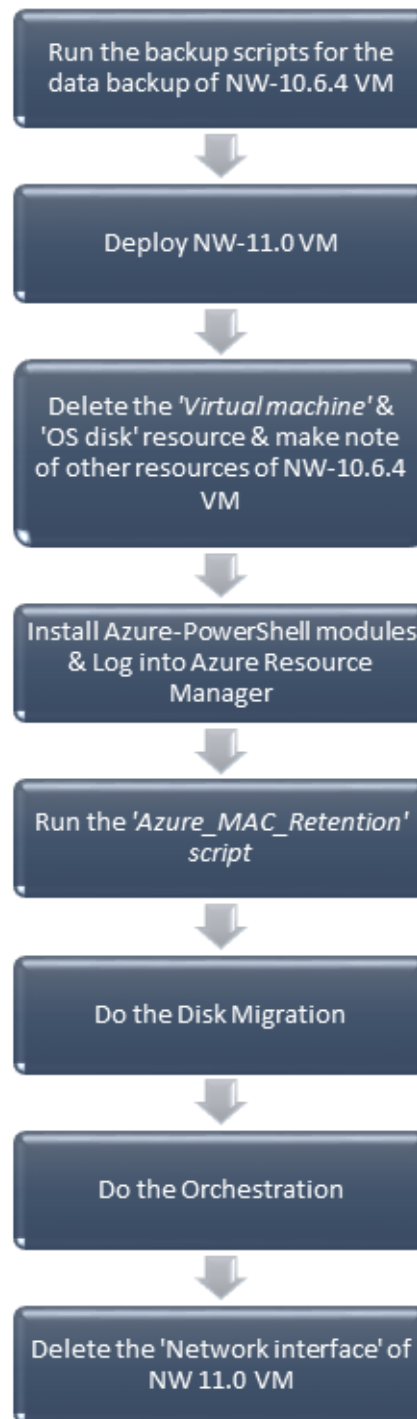
Complete the following tasks to migrate your Virtual Machine (VM) deployment disk drives from 10.6.6.x to 11.2:

Task 1 - Deploy NW 11.2 VM

Task 2 - Delete Virtual Machine and OS disk resource of NW 10.6.6 VM

Task 3 - Install Azure PowerShell modules on a local Windows machine

Task 4 - IP Retention: Run the PowerShell script

Task 1 - Deploy NW 11.2 VM

1. Deploy NW 11.2 VMs. [Refer to the Azure deployment guide for v 10.6.6.x to 11.2.

2. Power OFF all the NW 10.6.6 and 11.2 VMs.

3. In the Azure Portal, navigate to Virtual machines.

4. Click on the <Name_of_the_VM>.

5. Click Overview and then click Stop.

Task 2 - Delete Virtual Machine and OS disk resource of NW 10.6.6 VM

Note the other resources like Data disks and Network Interface.

1. Delete the 'Virtual machine' and the 'OS disk' (usually disk1 of VM) resource of NW 10.6.6 VM and make a note of these Network interface and Data disks.

> **Note:** Delete only these 2 resources and retain all other resources of NW 10.6.6 VMs like 'Network interface', 'Network security group' and 'Data disks') and make a note of these 'Network interface' and 'Data disks'.

2. In the Azure Portal, navigate to All resources. Select the Name_of_NW_10.6.6_VM.

3. Click Delete.

Task 3 - Install Azure PowerShell modules on a local Windows machine

Install the Azure PowerShell modules on a local Windows machine and Login to Azure Resource Manager.

Navigate to Azure PowerShell on the Windows machine where you have installed the Azure PowerShell modules and log in to Azure Resource Manager using the below command

> **Note:** Make sure you have followed the steps mentioned in the Prerequisites section above before executing the below command.

```
Login-AzureRmAccount
```

Login using the Azure credentials in the window that appears.
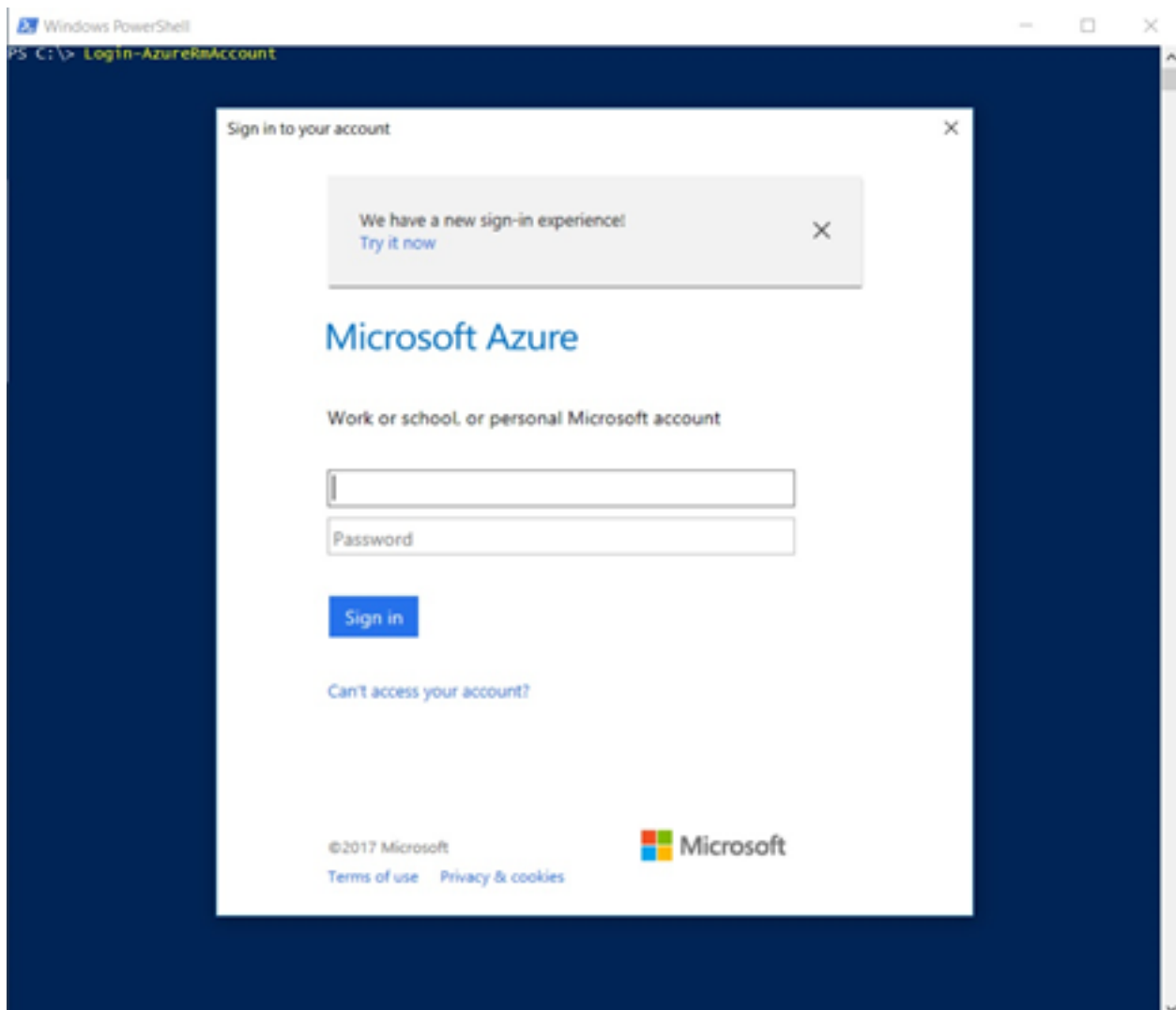
Task 4 - IP Retention: Run the PowerShell script

Run the PowerShell script for MAC retention for all NW Components. MAC address and IP retention:

MAC address and IP are bound to the 'Network interface' resource of a VM.

The Azure portal doesn't allow us to

- Specify an existing network interface to add when creating the VM

- Create a VM with multiple network interfaces

- Specify a name for the network interface (the portal creates the network interface with a default name)

This can be achieved using the Azure PowerShell. [https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm]

Click here to download and run the script by providing the requested parameters on the Windows machine installed with Azure PowerShell to retain the 'Network interface' from NW 10.6.6 VM to 11.2 VM.

You should be able to see NW 10.6.6 VM's NIC attached to 11.2 VM under 'Networking' settings after successful execution of the script.
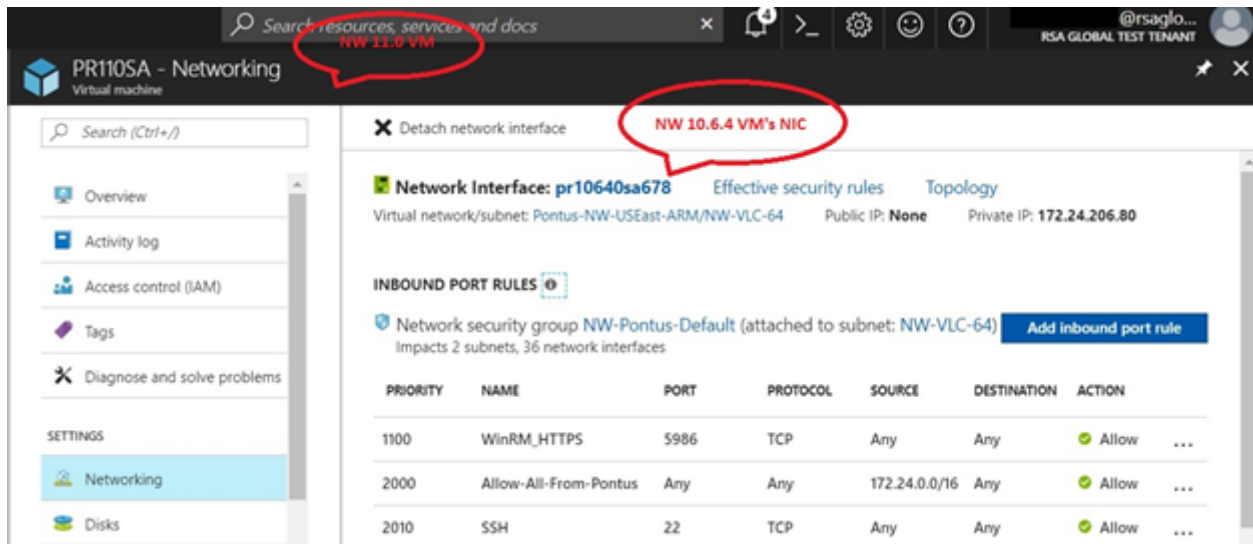
Task 5 - Perform Disk Migration

Add all the disks (except the 'OS disk') of NW 10.6.6 VM to the corresponding NW 11.2 VM under the 'Disks' settings.

In Azure Portal, navigate to Virtual machines and then Name_of_the_11.2_VM. Click **Disks** and then click + **Add data disk**. Select all disks of corresponding NW-10.6.6 VM which you had noted down earlier in the dropdown list that appears.

Click **Save**.
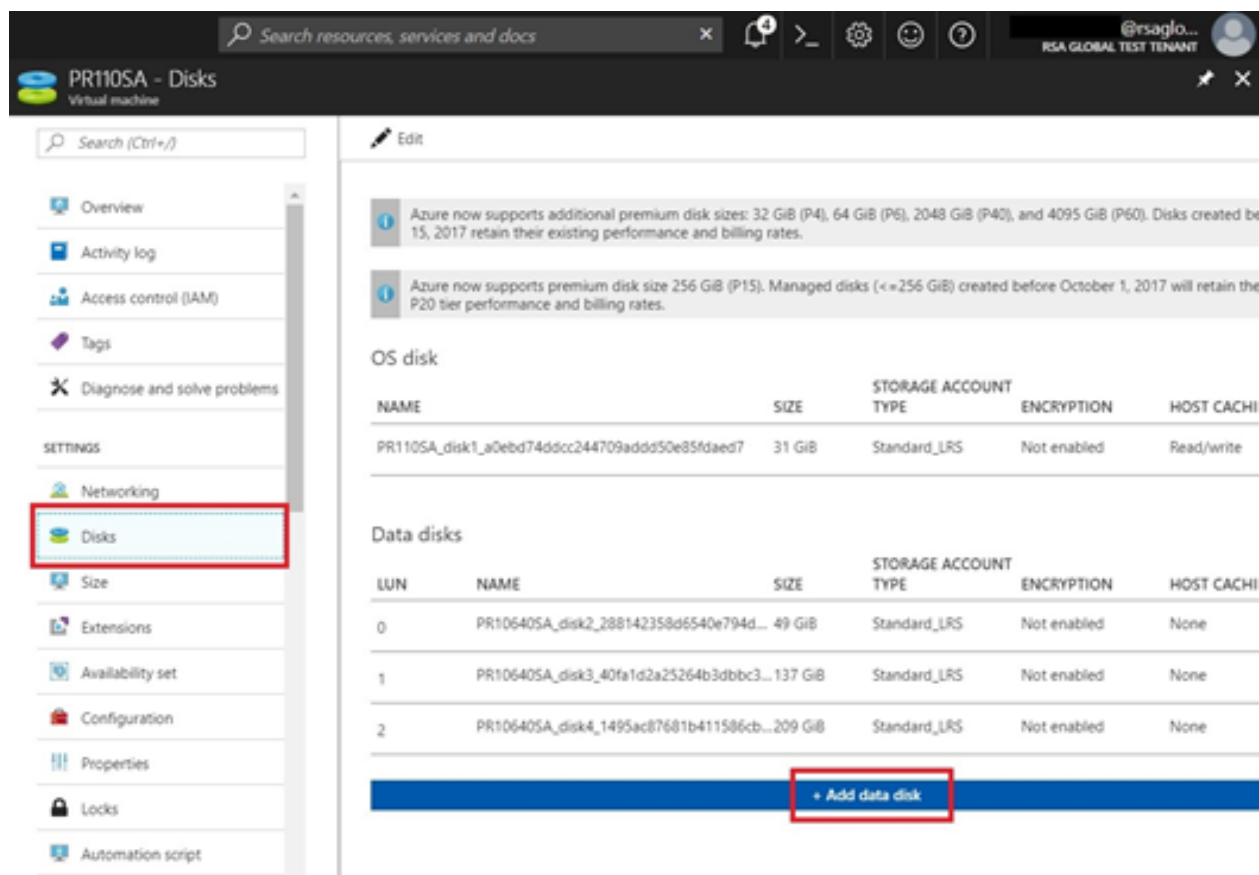
Power ON the NW 11.2 VM and login with the credentials provided during VM deployment and set the root password as netwitness.

Task 6 - Data Restoration

Copy NW 10.6.6 VM's backed up data (nw-backup) to NW 11.2 VM.

> **Note:** Do the Data Restoration for SA Server first followed by other components

For SA, LD/LC, Virtual Log Collector, Concentrator, Archiver, Broker:

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

2. Mount `VolGroup00-nwhome` on `/tmp/nwhome/`.

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

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

`cp -R /tmp/nwhome/* /var/netwitness/`

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

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

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/
```

Perform disk mounting by running the below commands:

For NW Server:

```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
```

```
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Add below entries for these mounts in `/etc/fstab`:

```
/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:

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
```

```
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
```

```
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb
```

```
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
```

```
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
```

```
mount /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
```

Add below entries for these mounts in `/etc/fstab`:

```
/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 Virtual LogCollector:

```
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
```

Add below entry for these mounts in `/etc/fstab`:

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

For Concentrator:

```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
```

Add below entries for these mounts in `/etc/fstab`:

```
/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:

```
mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
```

Add below entries for these mounts in `/etc/fstab`:

```
/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:

```
mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
```

Add below entry for these mounts in `/etc/fstab`:

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

Task 7 - Delete all NW 11.2 Deployment 'Network interface' Resources

1. In Azure Portal, go to All resources.
2. Click on <Name_of_NW_11.2_Network_interface> and select Delete.

Set Up Virtual Hosts in 11.2

There two phases to set up your 11.2 virtual stack that you must complete in the order shown.

- Phase 1 - Set Up NW Server, Event Stream 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 11.2 and they 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, and Broker or Concentrator Hosts

Task 1 - Set Up 11.2 NetWitness Server

Follow the instructions under Set Up 11.2 NW Server Host.

Task 2 - Setup 11.2 ESA

> **Caution:** 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 11.2 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.2 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 11.2 Broker or Concentrator

Follow the instructions under Set Up 11.2 Non-NW Server Host.

> **Note:** If you do not have a Broker, upgrade your Concentrator hosts. The 11.2 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.

Concentrator Hosts

1. Stop data capture and aggregation.

2. Complete the steps in Set Up 11.2 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.

2. Stop data capture on the Log Decoder.

3. Complete the steps in Set Up 11.2 Non-NW Server Host.

4. Restart data capture on Log Decoder.

> **Note:** After you upgrade, you will restart log collection after completing the Task 12 - Reset Stable System Values for Log Collector after Upgrade 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 11.2 VM can be created with the same network configuration.

5. Deploy a fresh Non-NW Server host using the 11.2 NetWitness Suite 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 11.2 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 11.2 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 11.2 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 11.2.

Complete the following steps to set up the 11.2 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 11.2 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 11.2 NW
>  Server?
>
>         < Yes >          < No  >
> ```

3. Tab to **Yes** and press **Enter**.
   Choose No if you already upgraded the NW Server to 11.2.
   The Install or Upgrade prompt is displayed.

```
┌NetWitness Platform 11.2 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 >
└───────────────────────────────────────────┘
```
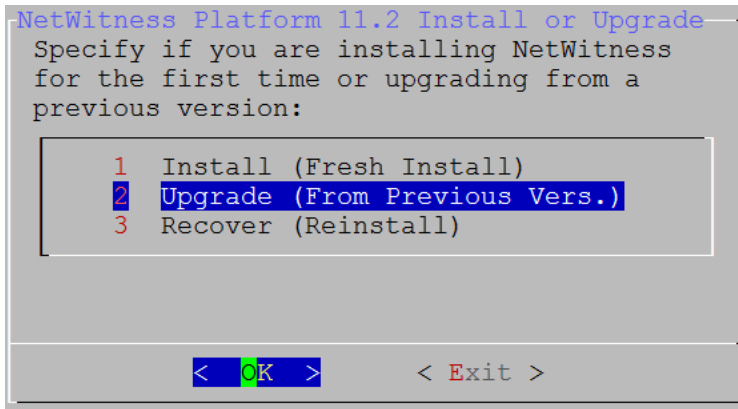
The backup path is displayed.

> **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 11.2.

  Enter the Backup directory path.
  ┌────────────────────────────────────────────────┐
  │ /var/netwitness/database/nw-backup              │
  └────────────────────────────────────────────────┘

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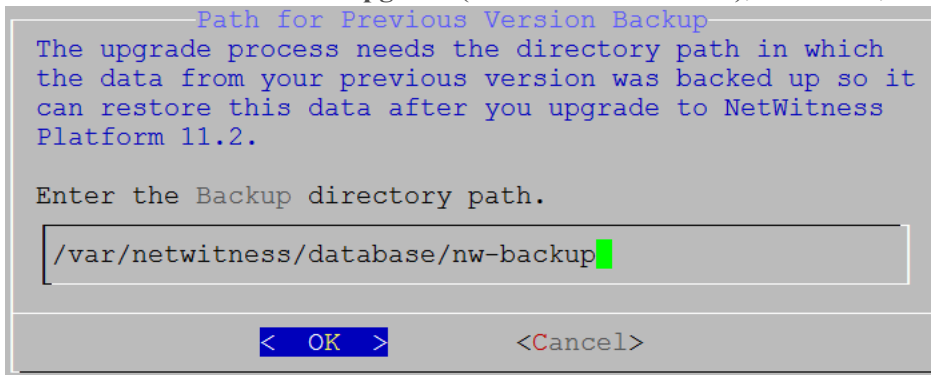
5. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.

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 { } [ ] ( ) / \ ' " ` ~ ; : . < > -).
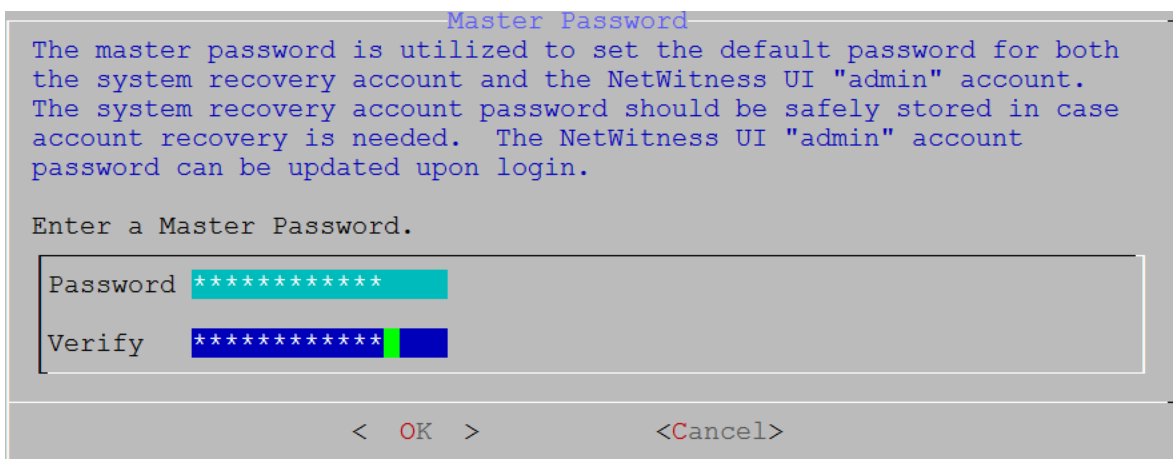
```
                        ┌────────── Master Password ──────────┐
                        │ The master password is utilized to set the default password for both │
                        │ the system recovery account and the NetWitness UI "admin" account.    │
                        │ The system recovery 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.
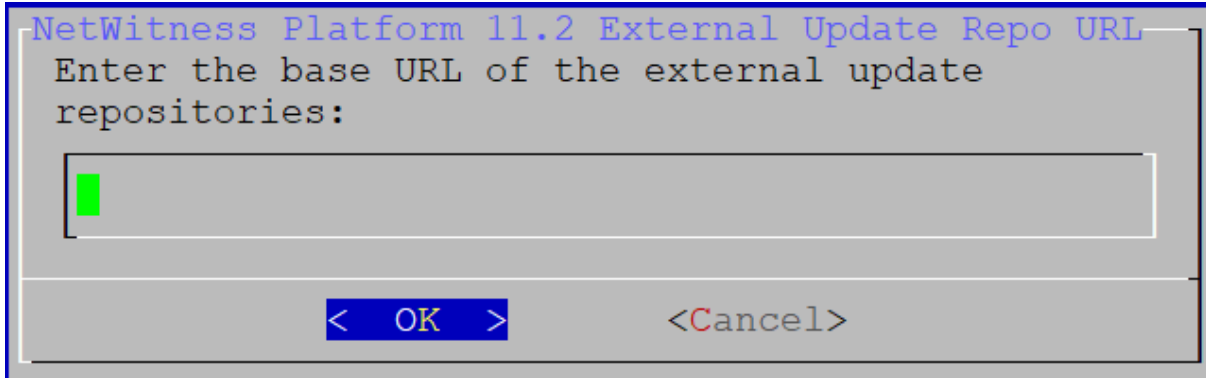
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite 11.2 Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

9. Enter the base URL of the NetWitness Platform external repo and click **OK**.
    The disable or use standard firewall configuration prompt is displayed.
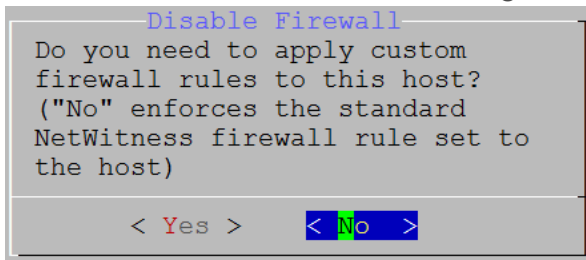
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

    - If you select Yes, confirm your selection.

    - 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 >                     │
└──────────────────────────────────────────────────────────────┘
```
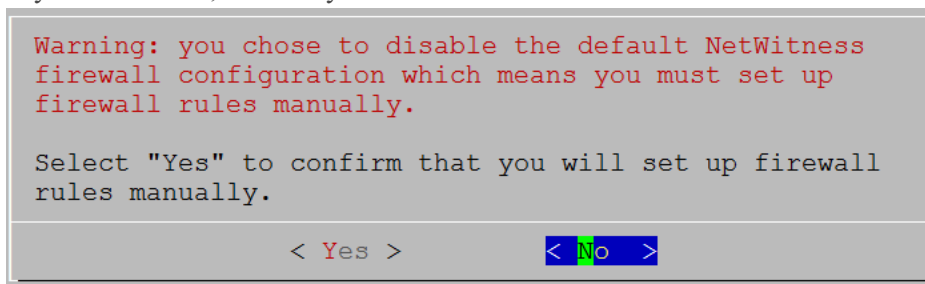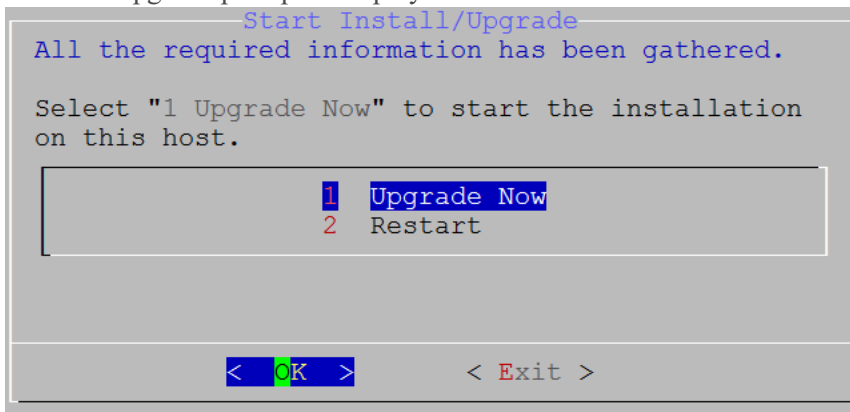
11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.

    When "Installation complete" is displayed, you have upgraded the 10.6.6.x SA Server to the 11.2 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 11.2 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 11.2 so that the data is as recent as possible.

Complete the following steps to set up an 11.2 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 11.2 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 11.2 NW Server Host to correct this error.

3. Tab to **No** and press **Enter**.

   The Install or Upgrade prompt is displayed.

```
NetWitness Platform 11.2 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 >
```
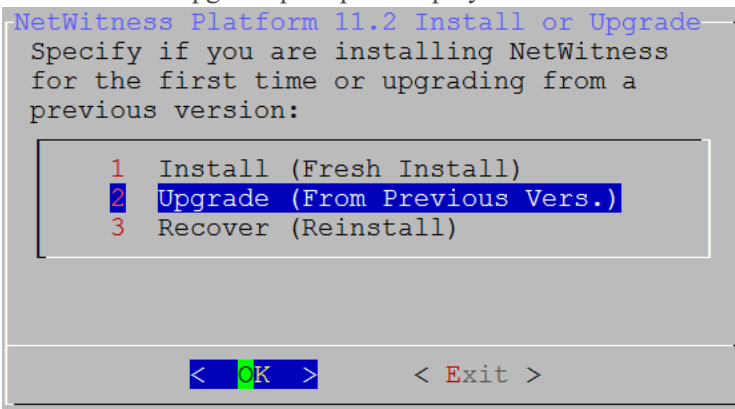
4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.
   The backup path prompt is displayed.
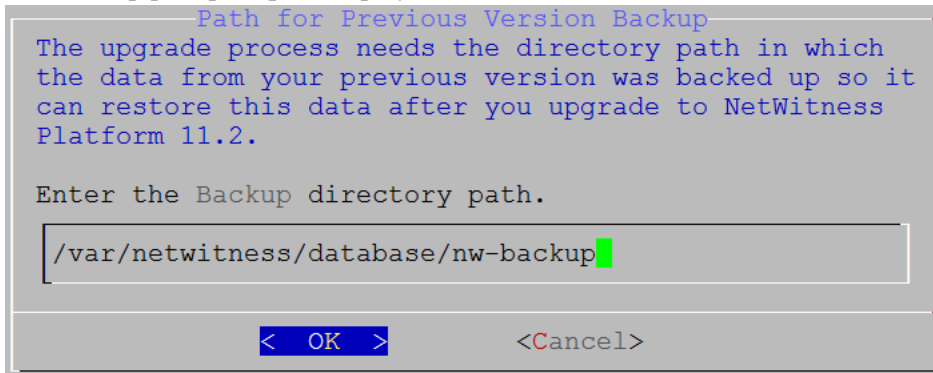
```
┌────────────Path for Previous Version Backup────────────┐
│ The upgrade process needs the directory path in which   │
│ the data from your previous version was backed up so it │
│ can restore this data after you upgrade to NetWitness    │
│ Platform 11.2.                                           │
│                                                          │
│ Enter the Backup directory path.                         │
│ ┌──────────────────────────────────────────────────┐   │
│ │ /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 >                   │
└──────────────────────────────────────────────────────────┘
```
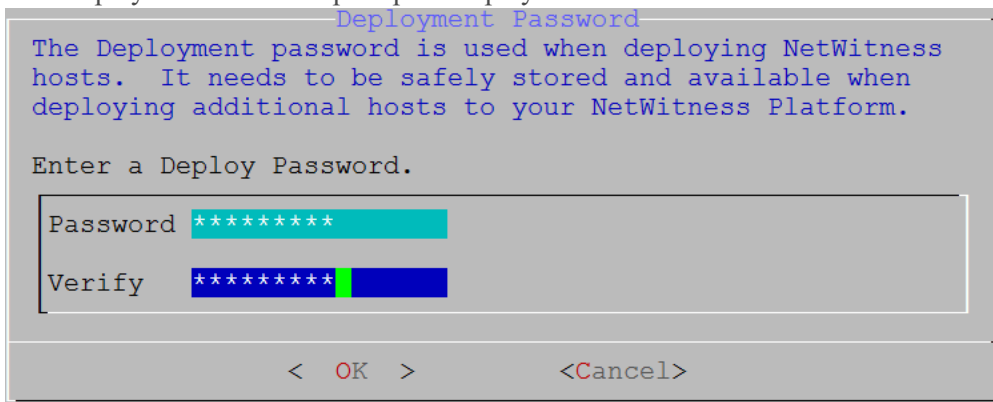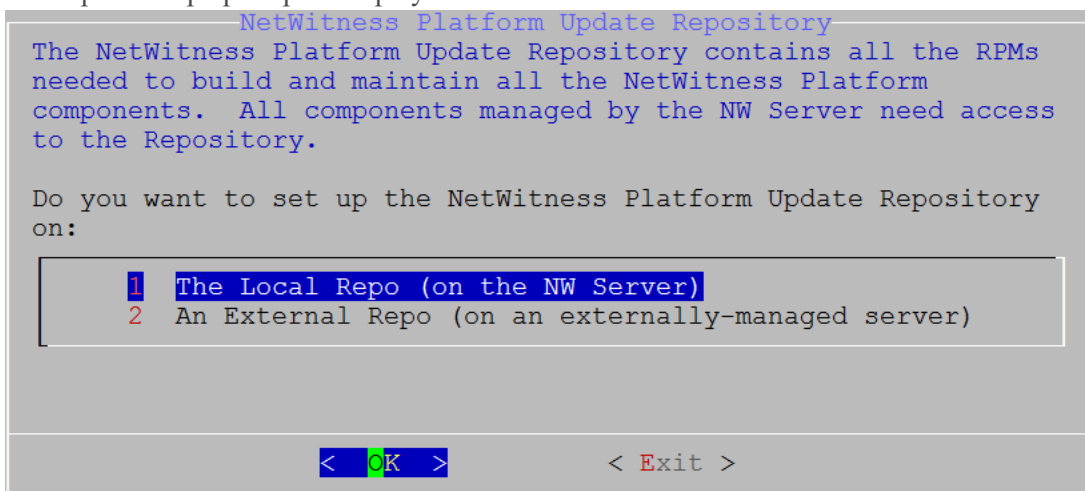
7. Use the down and up arrows to select the **2 The Local Repo (on the NW Server)**, tab to **OK**, and press **Enter**.

8. Enter the base URL of the NetWitness Platform external repo and click **OK**.
The NW Server IP Address is displayed.

```
┌──NW Server IP Address──┐
│ Please Enter the IP address of  │
│ the 11.2 NW Server.  The NW     │
│ Server must be routable from    │
│ this instance for installation  │
│ to continue.                    │
│ ┌─────────────────────────────┐ │
│ │ <IP-address>                │ │
│ └─────────────────────────────┘ │
│                                 │
│    <  OK  >      <Cancel>        │
└─────────────────────────────────┘
```
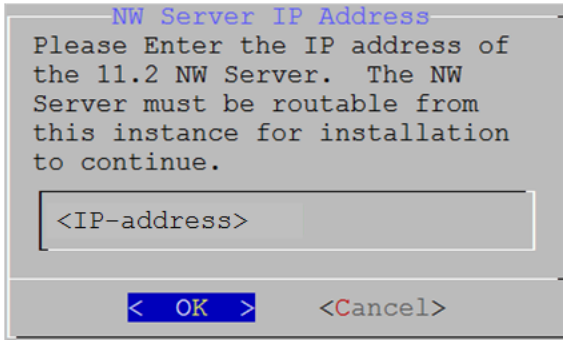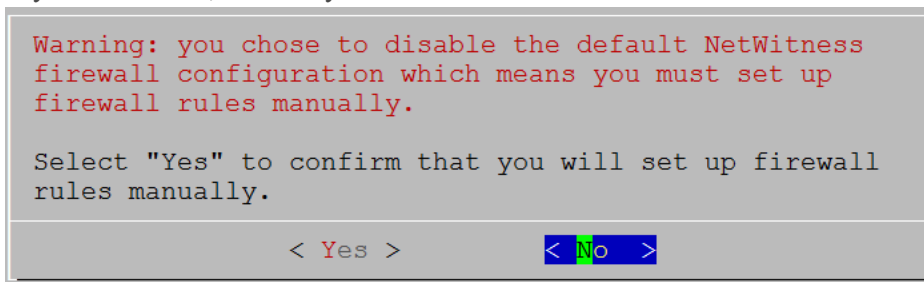
9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.
The disable or use standard firewall configuration prompt is displayed.
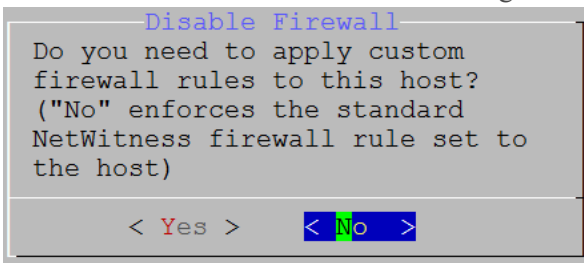
```
┌──Disable Firewall──┐
│ Do you need to apply custom  │
│ firewall rules to this host? │
│ ("No" enforces the standard  │
│ NetWitness firewall rule set to │
│ the host)                    │
│                              │
│   < Yes >      < No  >       │
└──────────────────────────────┘
```
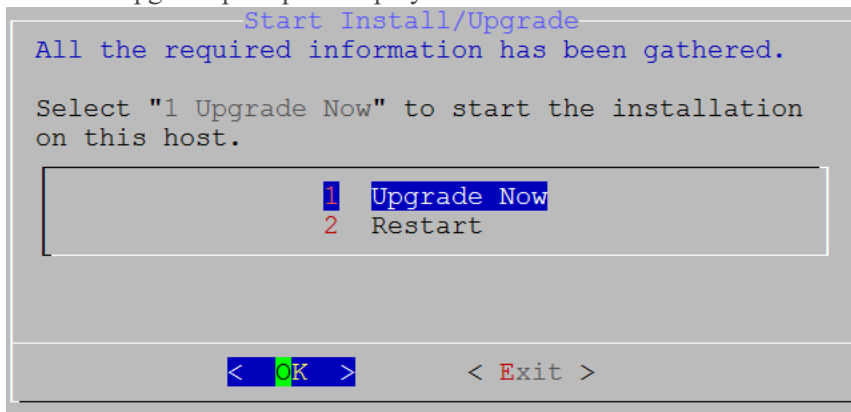
10. Tab to **No**, and press Enter to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- 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 11.2.

12. Install the service on this host:

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

    b. 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.

    c. 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.

    d. Select that host (for example, **Event Stream Analysis**) and click Install ⊙
       The **Install Services** dialog is displayed.

e. Select the appropriate service (for example, **ESA Primary**) and click **Install**.
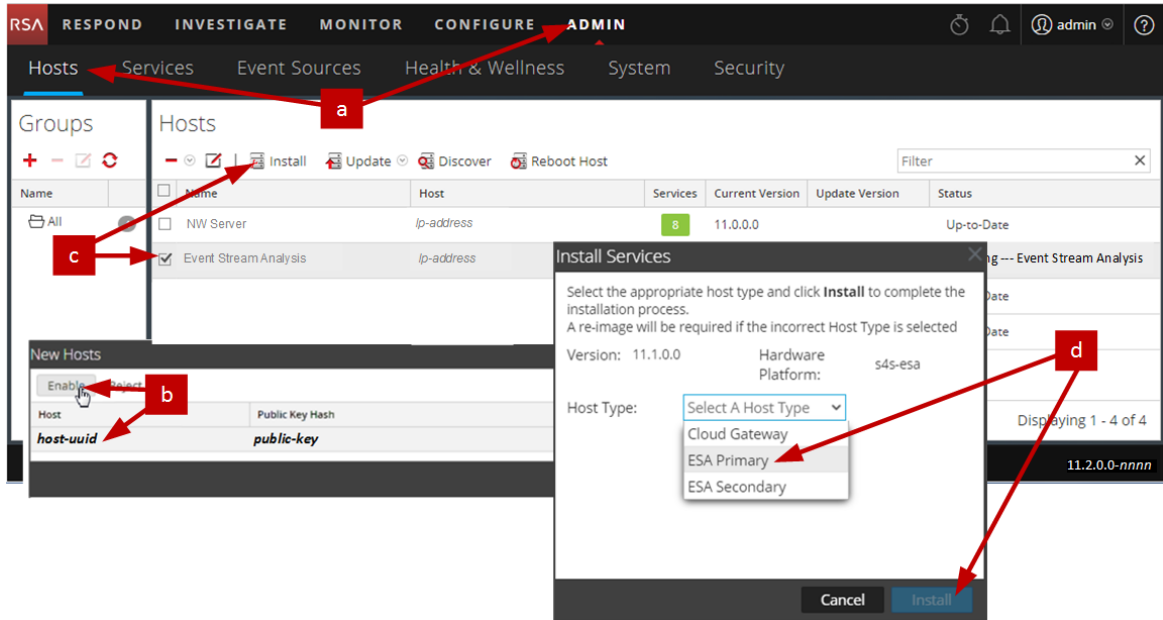
You have completed the upgrade of the non-NW Server host in NetWitness Platform

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.2 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

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.6.x to 11.2. These tasks are organized by the following categories.

- Global

- NetWitness Endpoint
  RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, and 4.4 only for NetWitness Platform 11.2.

- Event Stream Analysis

- Log Collection

- Reporting Engine

- Respond

- NetWitness SecOps Manager

- Security

Global Tasks

Task 1 - 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 15671, and all ports, are configured as shown in the "Network Architecture and Ports" topic in the *RSA NetWitness® Platform Deployment Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Task 2 - 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 11.2 before you remove the backup-related files from the local directories on your 11.2 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.2, 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
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 3 - Restore NTP Servers

You must use the NetWitness Platform 11.2 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 *RSA NetWitness® Platform 11.2 System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Task 4 - 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 *RSA NetWitness Suite Licensing Management Guide* for instructions on how to re-download licenses. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Task 5 - Remap Virtual NW Server License to 10.6.6.x MAC Address

If you are upgrading a Security Analytics server running on a virtual machine, change the 11.2 NW Server virtual host to the 10.6.6.x MAC address to retain licensing. Refer to "Licensing: Step 1. Register the NetWitness Server" in the *RSA NetWitness Suite Licensing Management Guide* for instructions on remapping a license to a new MAC address." Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

(Conditional) Task 6 - 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 a 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 7 - 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.

NetWitness Platform 11.2 cannot communicate with the core services for these customers because they 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

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

3. Select each core service and change there ports from Non-SSL to SSL ports.

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

4. Click (Edit) from the **Services** view toolbar.
   The Edit Service dialog is displayed.

5. 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).

NetWitness Endpoint

Task 8 - 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 11.2, 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.

Event Stream Analysis Tasks (ESA)

Task 9 - 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 11.2.

1. Log in to NetWitness Platform 11.2

2. Click **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".

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

   a. Click **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 *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Platform ESA Configuration Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Task 10 - For Integrations with Web Threat Detection, Archer Cyber Incident & Breach Response or NetWitness Endpoint Configure Mutually Authenticated SSL

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>
   ```
   For example:
   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

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 ".*", ".*", ".*"
   ```

Task 11 - Enable Threat - Malware Indicators Dashboard

In 11.0, 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 11.2.

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

Log Collection

Task 12 - 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 11.0 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 *RSA NetWitness® PlatformLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Update Log Collector Service RabbitMQ User Account Password

If the logcollector service RabbitMQ user account password was changed, you must reenter it after the 11.0 upgrade.

1. Log in to NetWitness Platform.

2. Click **ADMIN > Services**.

3. Select the Log Collector service.

4. Click ⚙ ⌄ (Actions) > **View** > **Explore**.

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

6. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.
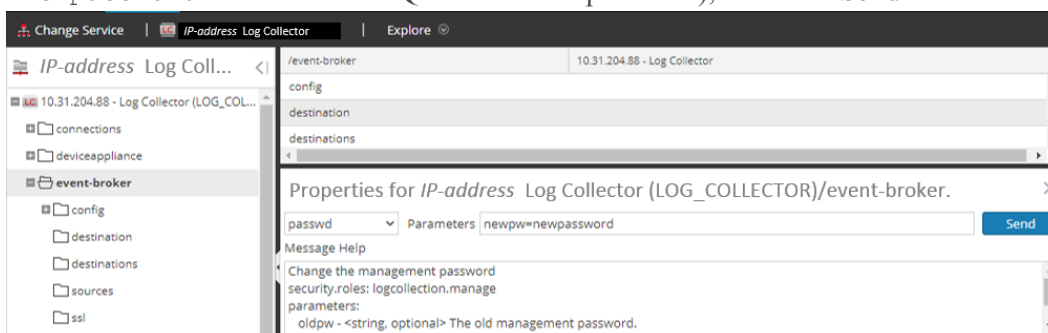
(Optional for Upgrades from 10.6.6.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 13 - Enable FIPS Mode

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. For information about how to enable FIPS for these services, see the "Sys Maintenance: Activate or Deactivate FIPS" topic in the *RSA NetWitness® PlatformSystem Maintenance Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Reporting Engine

Task 14 - Restore the CA certificates for External Syslog Servers for Reporting Engine

You must restore CA certificates after the upgrade from the back up 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 11.2.

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 into `/etc/pki/nw/trust/import` directory.

(Conditional) Task 15 - 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 *RSA NetWitness® Platform Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Respond

Task 16 - Restore Respond Service Custom Keys

In 10.6.6.x, if you added custom key 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 11.0.
   This is the new file for 11.0.

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

Task 17 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.0 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 11.0 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.

(Conditional) Task 18 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.6.x, you must reinstate them in 11.2. See *Adding Roles and Assigning Permissions for the Roles* in the *RSA NetWitness Platform Warehouse Analytics Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

NetWitness SecOps Manager

Task 19 -Reconfigure NW SecOps Manager Integration

For information on how to reconfigure NW SecOps for Event Stream Analysis, Reporting Engine, and Respond, see *RSA Archer Integration Guide*. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.
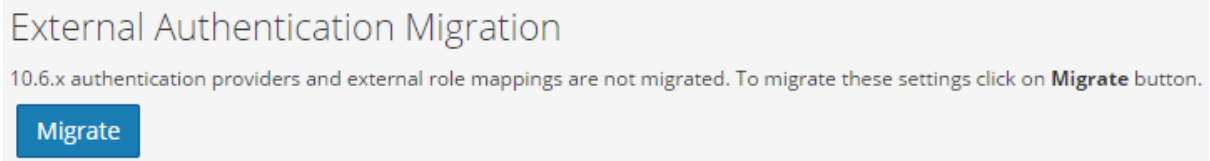
Security

Task 20 - Migrate Active Directory (AD)

The first time you log into the NetWitness Platform 11.2 User Interface, you must click on the Migrate button to complete the migration of AD.

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

2. Click **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 21 - Modify Migrated AD Configuration to Upload Certificate

If the you used a self-signed certificate in 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 certificate (either the self-signed cert or the CA cert).

Complete the following procedure to modify the migrated AD configuration to upload the certificate (either the self-signed cert or the CA cert).

1. Log in to NetWitness Platform.

2. Click **ADMIN** > **Security** and click the **Settings** tab.

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

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

5. Click **Save**.

Task 22 - Reconfigure Pluggable Authentication Module (PAM) in 11.2

You must reconfigure PAM after you upgrade to 11.2. See "Configure PAM Login Capability" in the *RSA NetWitness® Platform System Security and User Management Guide* for instructions. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

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.

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.

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

11.2 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 NetWitness Platform Logs & Network 11.x documents.*

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.2 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` *n*`GB`
	
	`<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space` *n*`GB 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 View Details" 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.

Appendix A. Troubleshooting

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 NetWitness Platform Logs & Network 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 NetWitness Platform Logs & Network 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 NetWitness Platform Logs & Network 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 11.2.
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 NetWitness Platform Logs & Network 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 11.2. 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.
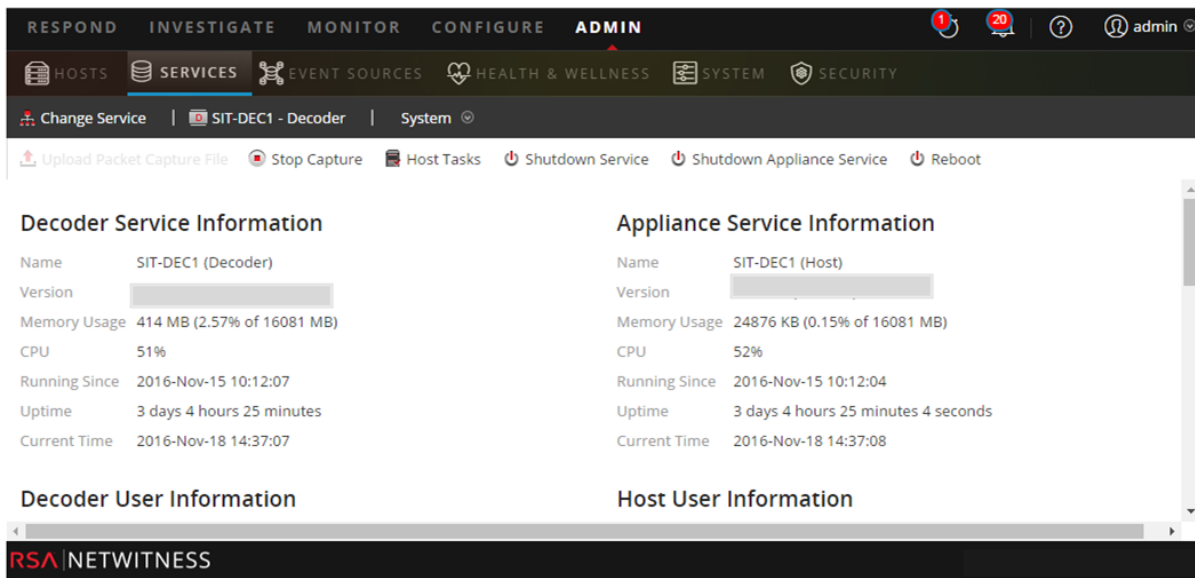
3. Under ⚙ (actions), select **View** > **System**.

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**.
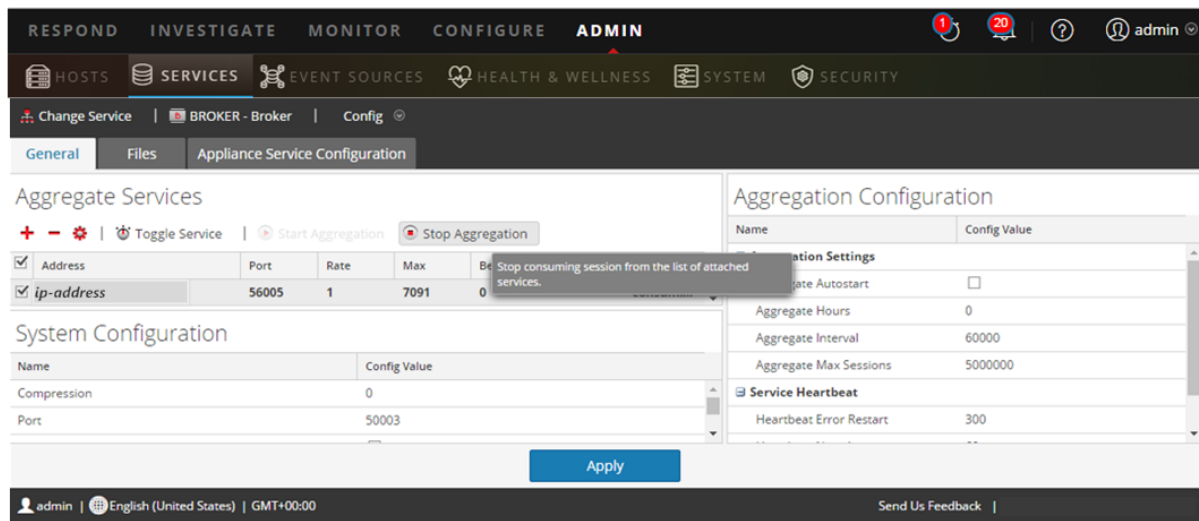   The Services view is displayed.

2. Select each **Log Decoder** service.
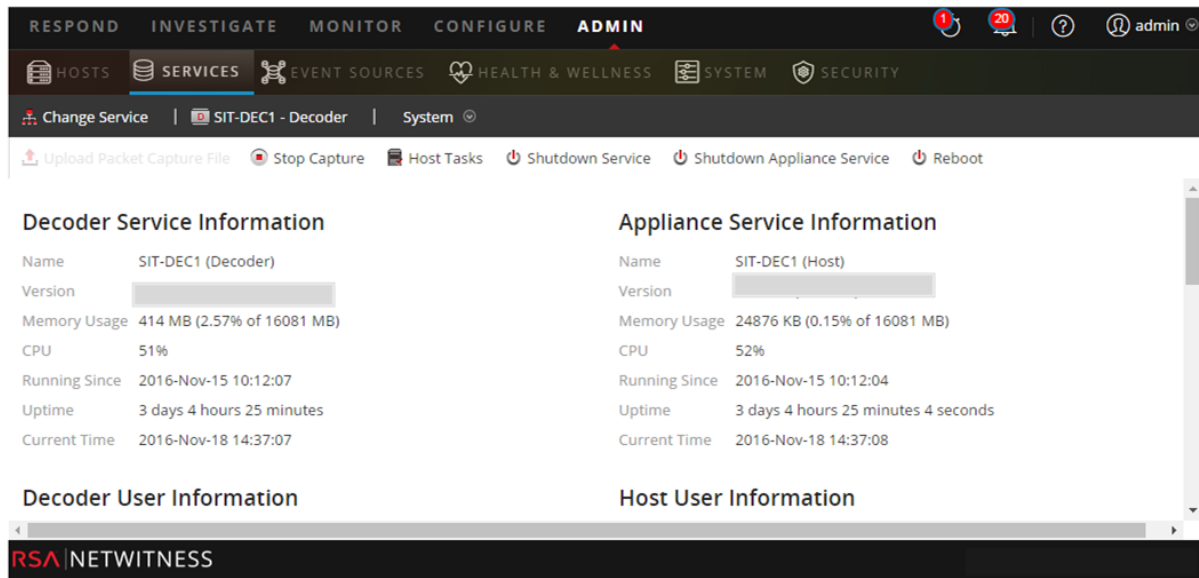
3. Under ⚙⌄ (actions), select **View > System**.

4. In the toolbar, click ⏹ Stop Capture.

Stop Aggregation

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

2. Select the **Broker** service.

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

4. The **General** tab is displayed.

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

Start Data Capture and Aggregation

Restart packet and log capture and aggregation after updating to 11.2.

Start Packet Capture

To start packet capture:

1. In the **NetWitness Platform** menu, select **ADMIN** > **Services**.
   The Services view is displayed.

2. Select each **Decoder** service.

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

4. In the toolbar, click .

Start 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

During the upgrade from 10.6.6.x to 11.2, the Broker Service is restarted and this automatically starts aggregation.

Revision History

Revision	Date	Description	Author
0.0	2-May-18	Internal Review Draft - Do not Distribute	IDD