RSA NETWITNESS® SUITE

Virtual Host Upgrade Guide

for Version 10.6.5 to 11.1

Contact Information

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

Trademarks

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

License Agreement

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

November 2018

Contents

Introduction

The instructions in this guide apply to the upgrade of virtual hosts to RSA NetWitness Suite11.1 exclusively. See the *RSA NetWitness Suite Physical Host Upgrade Guide* for instructions on how to upgrade your 10.6.5.x physical hosts to 11.1. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

NetWitness Suite 11.1 is a major release that affects all products in the NetWitness Suite. The components of the suite are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, and Security sever), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.

Refer to the *RSA NetWitness Suite Getting Started Guide* to become familiar with the major changes to the 11.x User interface. Refer to the *RSA NetWitness Suite Deployment Guide* to become familiar with the major platform changes in 11.x.

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

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

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.1 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.1 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® Suite 11.1 Upgrade Path

The earliest supported Upgrade path for RSA NetWitness® Suite 11.1 is Security Analytics 10.6.5.x. If you are running a version of NetWitness Suite that is prior to 10.6.5.x, you must update to 10.6.5.x before you can upgrade to 11.1. See the *RSA Security Analytics 10.6.5 Update Guide* (https://community.rsa.com/docs/DOC-85119) on RSA Link.

Supported Host Upgrade Path

You must upgrade a host to the same host type:

- Same Series RSA Physical Appliance to Same Series RSA Physical Appliance (that is, Series 4 to Series 4, Series 5 to Series 5).
  RSA does not support third-party physical hosts in 11.1.
- On-Prem Virtual to On-Prem Virtual

Caution: The 11.1 upgrade does not support mixed-platform upgrades (for example, it does not support physical to virtual).

Hardware, Deployments, Services, and Features Not Supported in 11.1

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.1.

- 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 11.1.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.1.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.1, 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 11.1.

- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Suite 11.1, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.1, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.5.x has been removed.

Caution: If you do not use Incident Management in 10.6.5.x, carefully consider whether or not to upgrade to version 11.1.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.1.

In your 10.6.5.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.1.
- 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 10.6.5.x, you can upgrade to version 11.1.
- 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 11.1.

Note: If you did not use Incident Management in 10.6.5.x, you cannot view the 10.6.5.x ESA alerts in the 11.1 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.1 that will allow Respond to view them. See the *ESA Alert Migration Instructions* knowledge base article (https://community.rsa.com/docs/DOC-84102) in RSA Link for instructions on how to run this script.

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 11.1 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. Malware Analysis hosts
4. Broker hosts (if you do not have a Broker, upgrade your Concentrator hosts)
   The 11.1 NW Server cannot communicate with 10.6.5.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.

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.

Note: Other than Log Collection hosts with downstream event destinations, there is no technical reason to upgrade your hosts in the order shown in Phase 2.

This is the Phase 2 host upgrade order recommended by RSA.

1. Decoder hosts
2. Concentrator hosts
3. Archiver hosts
4. 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.

5. All other hosts

See "Running in Mixed Mode" under "The Basics" in the *RSA NetWitness Suite 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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.1 and some are still on 10.6.5. This happens when you upgrade to 11.1 in phases.

Note: You must follow the host upgrade sequence as shown in Upgrade Phases to ensure complete Investigate functionality. The 11.1 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.1 to access the Event Analysis View. If the Broker is not upgraded, analysts see a warning icon next to the Broker and no data aggregated to that Broker can be displayed.

After you upgrade all services to 11.1, 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 11.1 and some are still at 10.6.5), 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 be successful, then generate errors due to insufficient permissions, and the data is still protected.

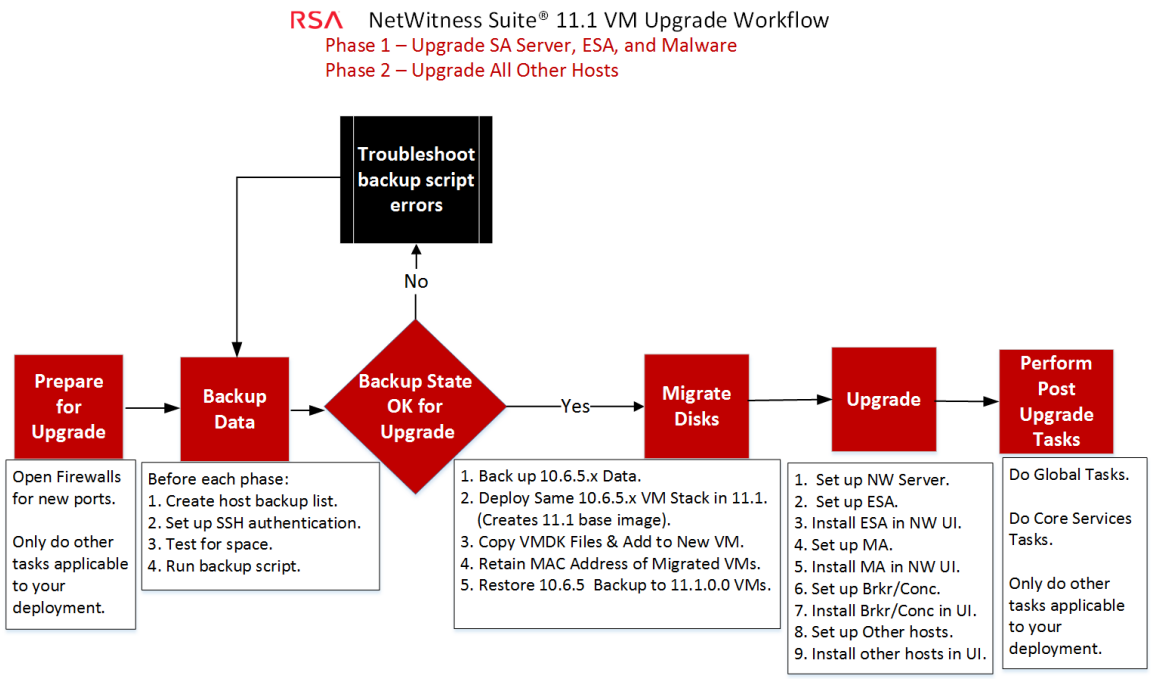
During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.1 and re-enable `sdk.packets`, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NW Server at version 11.1 is connected to services at a lower version.

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 10.6.5.x Concentrator -> 10.6.5.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst	RBAC permitted items	PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst	RBAC permitted items	PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.1 Concentrator ->11.1 Decoder/Log Decoder	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items	PCAP	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes

Connecting Service Version	Affected View	User Role With Restricted Content	Can See	Can Download Restricted Content Successfully	Can Download Restricted Content with Errors
11.1 Broker -> 11.0.0.x Concentrator -> 11.0.0.x Packet Decoder/Log Decoder	Events View	Analyst	RBAC permitted items	None	Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Reconstruction View	Analyst	RBAC permitted items	None	File archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Analysis View	Analyst	RBAC permitted items	None	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload PCAPs and logs are downloaded as zero bytes



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 Suite 11.1.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.1. These tasks are organized by the following categories.

- Global
- Respond
- Reporting Engine

Global

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

Task 1 - Review Core Ports and Open Firewall Ports

The following tables lists new ports in 11.1.

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

Endpoint Hybrid or Endpoint Log Hybrid

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

Source Host	Destination Host	Destination Ports	Comments
Endpoint Server	NW Server	TCP 27017	MongoDB

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

Task 2 - Record Your 10.6.5.x `admin user` Password

Record your 10.6.5.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.

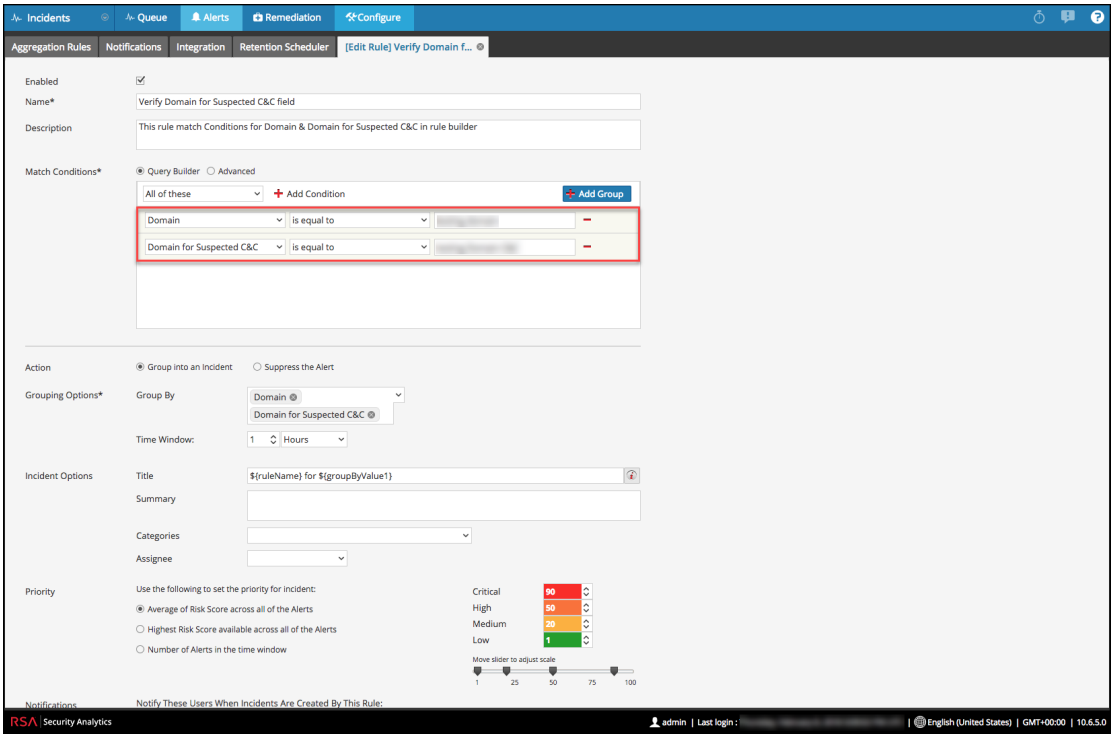
Respond

Task 4 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C”

Make a note of any Incident Management aggregation rules that have match conditions using Domain or Domain for Suspected C&C in the drop-down list in the rule builder. In NetWitness Suite 11.1, you will need to modify these rules to use Domain after you upgrade to 11.1 as described in the Respond Post Update Tasks.

Check the following for each aggregation rule:

1. In the Security Analytics 10.6.5.x menu, select **Incidents** > **Configure** > **Aggregation Rules** tab and edit the rules to view the matching conditions.
2. In the **Match Conditions** section, look for **Domain** or **Domain for Suspected C&C** listed in the drop-down lists for the conditions.



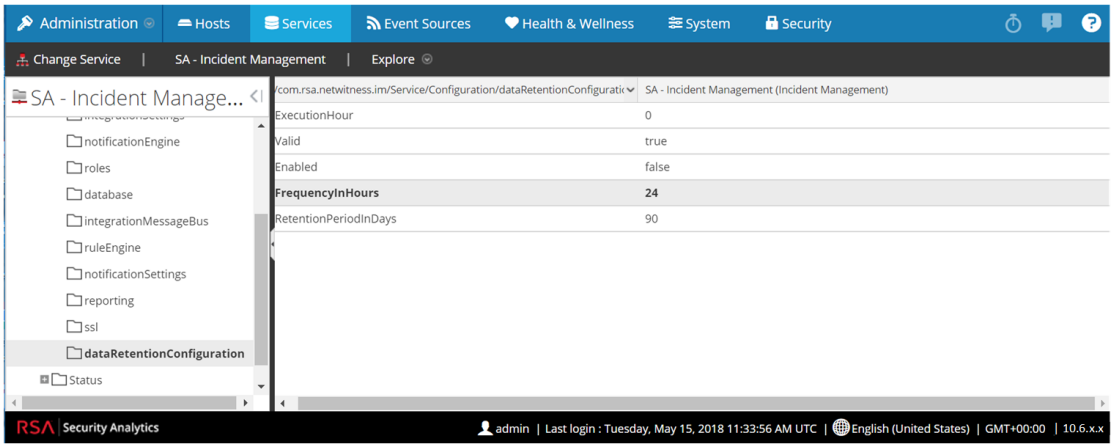
3. Make a note of the rule name and the entire condition that uses **Domain** or **Domain for Suspected C&C**, including operators and values.

Task 5 - 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 11.1, RSA added a validation check to make sure that it is run at least every 24 hours. When you upgrade to 11.1, 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  > **View** > **Explore**.
3. In the Incident Management **Explore** view, go to `Service` > `Configuration` > `dataRetentionConfiguration`.
4. Make sure that the `FrequencyInHours` parameter is ≥ **24**.



Reporting Engine

(Conditional) Task 6 - 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
   ```

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from Security Analytics 10.6.5.x releases to NetWitness Suite 11.1.

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 11.1, 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: These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the Security Analytics Server
- Standalone Warehouse Connector
- Warehouse Analytics (Datascience)

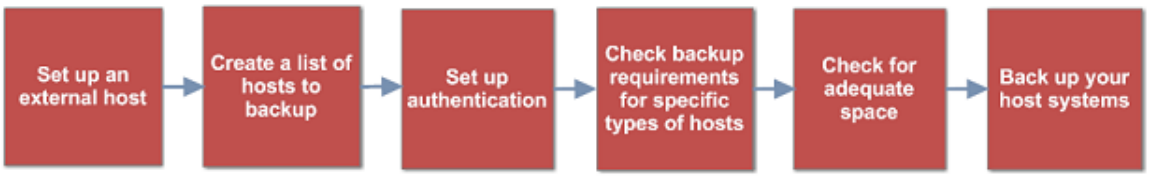
The following types of hosts can be backed up and are automatically restored during the upgrade process:

- **Security Analytics Admin Server** (may include Malware Analysis, Incident Management, Health and Wellness, and Reporting Engine)
- **Malware Analysis** (standalone)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and Incident Management database)
- **Concentrator**
- **Log Decoder** (including Local Log Collector and Warehouse Connector, if installed)
- **Log Hybrid**
- **Packet Decoder** (including Warehouse Connector, if installed)
- **Packet Hybrid**
- **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 11.1.", 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**.

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



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 Security Analytics stack of hosts.

Note: If you are not able to use an external host for backing up files, contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

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-v4.0.sh`) from RSA Link at this location: https://community.rsa.com/docs/DOC-81514 and copy it over to your CentOS 6 backup system. Extract the zip file to access the scripts. The scripts are:

- `get-all-systems.sh`: Creates the `all-systems` file, which contains a list of all your Security Analytics 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.
- `azure-mac-retention.ps1`: Applies only if you are using AZURE. See the *AZURE Deployment Guide* on for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

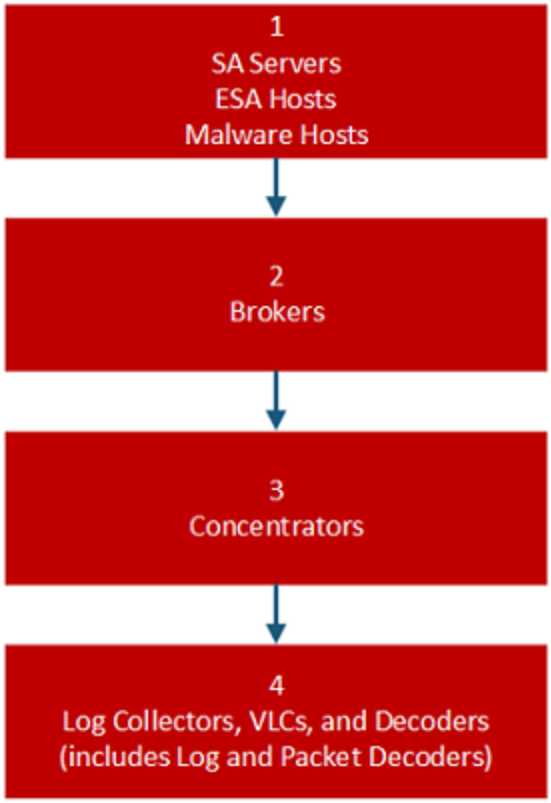
Note: If you have used the 10.6.x versions of the backup and restore scripts on your 10.6.5 hosts, you must still run all the scripts listed here.

Note: Do NOT use the scripts in the `nw-backup-v4.0.zip` file for regular backups. These scripts are specifically designed for upgrading from 10.6.5.x to 11.1.

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:



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-SA-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. RSA recommends that you comment out the hosts that you do not want to back up (add the number sign (#) to the beginning of the line that contains the host that will not be backed up).
   The following examples shows how to comment out the 10.6.5 Security Analytics Server:
   `loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.5.0`
   `#nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.5.0`

   > **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,10.6.5.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.5.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.5.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.5.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.5.0
```

And here is an example of an `all-systems` file that could be used in the first backup session, where only the Security Analytics Server, ESA host, and Malware Analysis host are backed up:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

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 that each version of the file lists only those hosts that are currently being backed up, and the other hosts are commented out.
    For more information, see Post Backup Tasks.
- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.
- The `get-all-systems.sh` script generates a list of hosts that were defined in the Security Analytics 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 Security Analytics, you use the Security Analytics 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 Security Analytics 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 Security Analytics Server. (Any Windows Legacy Collectors or AWS Cloud Collectors will not be added to the `all-systems` file, and may account for discrepancies. **DO NOT add these items to the `all-systems` file manually**.)
- If the syntax in the `all-systems` file is incorrect, the script will fail. For example, if there is an extra space at the beginning or the end of a host entry, the script will fail.

Task 3 - Set up Authentication Between Backup and Target Hosts

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

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

1. On the external backup host system, make the `ssh-propagate.sh` script executable by running the following command:
   `chmod u+x ssh-propagate.sh`
2. At the root directory, run the following command, where `<path-to-all-systems-file>` is the path to the directory where the `all-systems` file is stored:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. You are prompted for the password once per host, but you will not need to enter it repeatedly later during the backup process.

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

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

For All Host Types

Perform the following steps for all host types:

1. On the Security Analytics 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 11.1., 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 Security Analytics 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 ESA Hosts with Mongo Databases

The default 10.6.x Mongo database password is `netwitness`. If you have customized this password, you could encounter an error while running the backup script. You can either use your custom Mongo database password during the backup, or you could change that password back to `netwitness` before running the `nw-backup.sh` script.

1. Find out if the Mongo database password is `netwitness` or if it has been modified.
2. If it has been modified, either change it back to `netwitness`, or be sure you know what the customized password is so that you can enter it during the backup.

See "ESA Config: Change MongoDB Password for admin Account" in the *NetWitness Suite Event Stream Analysis Configuration Guide* for more information. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

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

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

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

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

Prerequisites

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

- If Lockbox was initialized on the LC and VLC, you must know the Lockbox password. It is required to reconfigure the Lockbox after upgrade.
- If you set the password for `logcollector` user for RabbitMQ, you must know the password so you can set it again after the upgrade.

Prepare LCs and VLCs for Upgrade

1. SSH to the Log Collector.
2. Submit the following command string.

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

   This command:

   - Stops the Puppet Agent service.
   - Disables the file collection accounts ("sftp" and all users in the group "upload") used for uploading log files to the Log Collector. The log files accumulate on the event sources until the Log Collector has been upgrade to 11.1.
   - 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, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the Security Analytics Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.1. 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 10.6.5.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 10.6.5.x, it is backed up and restored.

Task 5 - Check for Adequate Space for the Backup

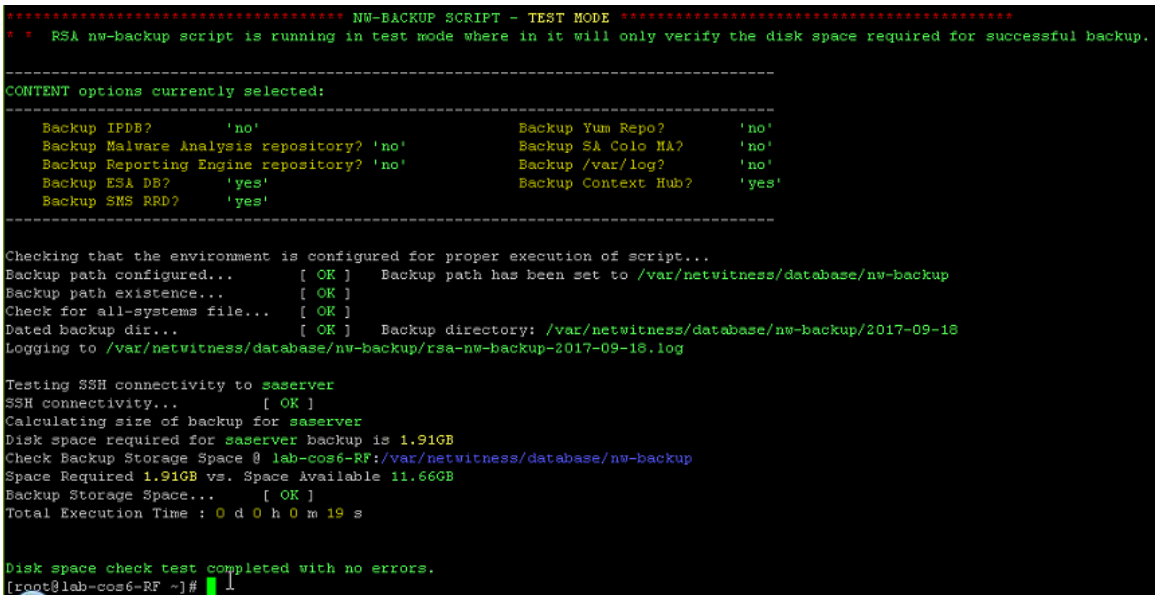
You can run the backup test script to check the amount of disk space that is required for the backup using the `-t` option described in Test Options. You run the script without actually backing up files or stopping any services. RSA recommends that you perform this step to ensure that you provide adequate 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 11.1.

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

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

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

General Options

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. 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 11.1, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

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

Note: When you run a backup with the `-u` option, all services are stopped. If you need to continue to use the 10.6.x machine after running the backup, reboot the 10.6.x system so that services are restarted.

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 11.1. 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:
10.6.5.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. For information, see Task 2 - Create a List of Hosts to Back up.
2. Make the backup script executable by running the following command:
   `chmod u+x nw-backup.sh`
3. Begin the backup process by running the following command at the root directory level:

```
./nw-backup.sh -u
```

Note: You must use the `-u` option so that your files will be restored correctly during the upgrade to 11.1. Do NOT make any changes to the header of the backup script for the backup path because the path is specific to the upgrade, and that data needs to be in a specific place.

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 Security Analytics 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 Security Analytics Server (specifically the Admin service) to 11.1.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.1. 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 the Security Analytics 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 Security Analytics Server'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 11.1., 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:
- Security Analytics Servers:`/var/netwitness/database/nw-backup`
- ESA hosts:`/opt/rsa/database/nw-backup`
- Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

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

Required Files for ESA Hosts

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

Required Files for All Other Hosts

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

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

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

Migrate Disk Drives from 10.6.5.x to 11.1

These instructions tell you how to upgrade virtual hosts from 10.6.5.x to 11.1.

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 out-dated.
3.) This guide applies to virtual host upgrades exclusively. If have both physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite 11.1 Physical Host Upgrade Instructions* for the steps you must complete to upgrade physical hosts. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Note: The machines must be in VMware ESX.

There are five tasks you must complete to migrate your Virtual Machine (VM) deployment disk drives from 10.6.5.x to 11.1:

Task 1 - Back up data in your 10.6.5.x VMs.

Task 2 - Deploy the same VM Stack in 11.1 as you have in 10.6.5.x.

Task 3 - Copy the VMDK Files and add them as a hard disk to the new VMs.

Task 4 - Retain MAC address of upgraded SA Server VM.

Task 5 - Restore backup data in 10.6.5.x to 11.1 VMs.

Task 1 - Back Up Data in 10.6.5.x VMs

1. Prepare Log Collector for the migration:
   a. Log in to the Log Collector using root credentials.
   b. Go to the `/opt/rsa/nwlogcollector/nwtools/` directory and run the following command.
      `sh prepare-for-migrate.sh --prepare`
      See Virtual Log Collector Host (VLC) for detailed instructions on how to upgrade the VLC.
2. Download the `.zip` file that contains the 10.6.5.x backup scripts from RSA Link https://community.rsa.com/docs/DOC-81514)) to the external backup host.

   Note: 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 Suite stack of hosts.
3. Run the following commands from the `nw-backup/scripts` directory (see Backup Instructions for a detailed descriptions of the backup scripts).
   `./get-all-systems.sh <SA-IP>`
   `./ssh-propagate.sh <path-to-backup-directory/all-systems>`
   `./nw-backup.sh -u`
   (if you have a Malware VM, substitute `-m -u` for `-u` in this command string (for example, `./nw-backup.sh -m -u`).

Task 2 - Deploy Same 10.6.5.x VM Stack in 11.1

You must set up the same virtual host stack in 11.1 that you had in 10.6.5.x. See the *RSA NetWitness® Suite 11.1 Virtual Host Installation Guide* for instructions.Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

The following steps are the high-level steps on how to deploy an OVA host in the ESXi environment.

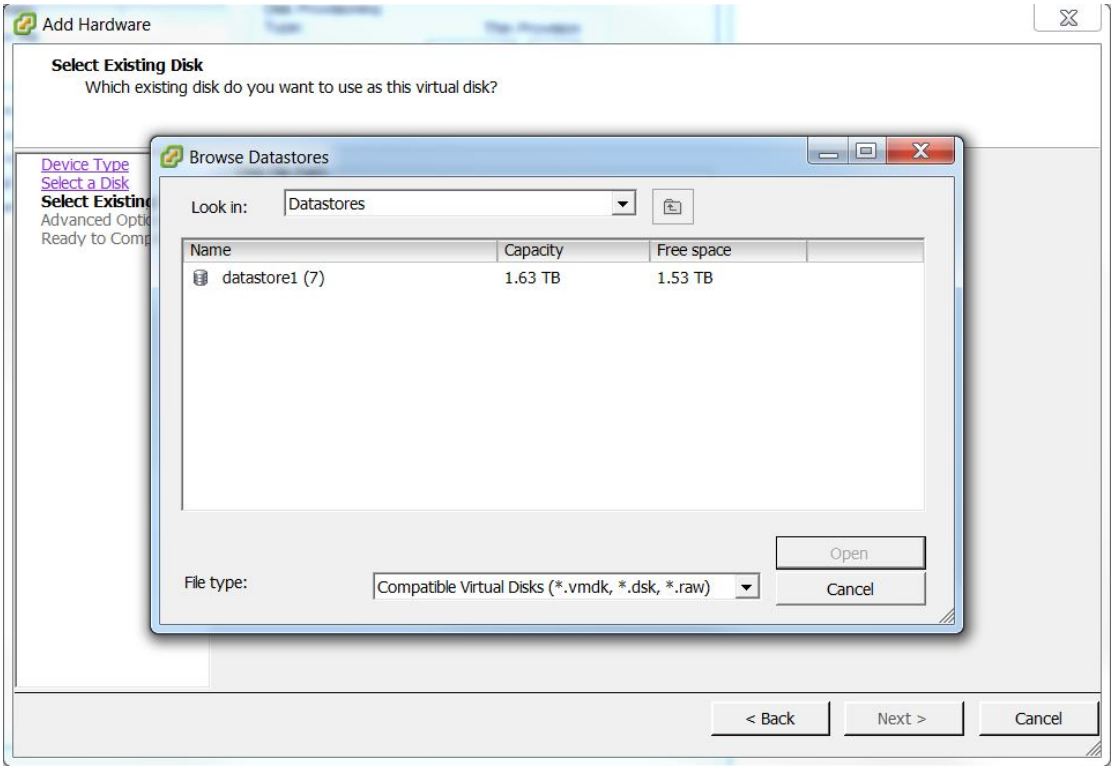
Download the 11.1 OVA, from RSA Link Download Central to a local directory.

1. Log on to the ESXi environment.
2. In the **File** drop-down, select **Deploy OVF Template**.
   The Deploy OVA Template dialog is displayed.
3. Browse your local directory for the 11.1 OVAs you downloaded.
4. Select the to deploy in the virtual environment , and click **Next**.

5. Select the appropriate Configuration for the VM and click **Next**.
6. Power on the VM, go to Console, and log in to the machine.
   The VM now has the 11.1 base image required to run the Setup Program (that is, `nwsetup-tui`).

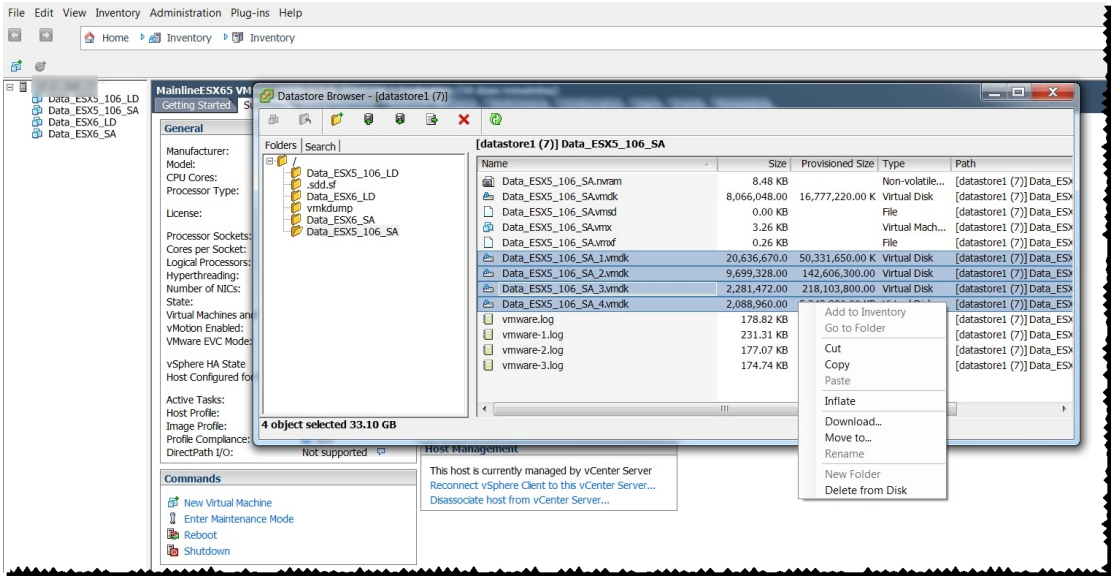
Task 3 - Copy VMDK Files and Add Them as Hard Disk to New VMs

1. Power off both the 10.6.5.x and 11.1 VMs.
2. Go to the desired ESX server, click the **Configuration** tab > **Storage**.
3. Right-click the required datastore and click **Browse Datastore**.



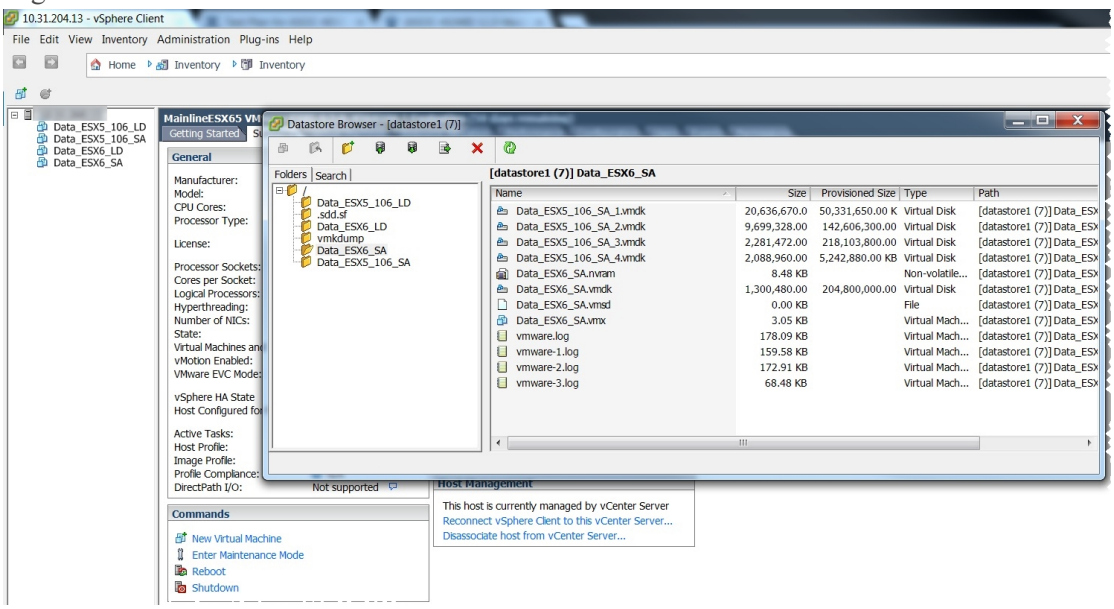
4. Navigate to the existing 10.6.5.x VM in the datastore.
5. Select all the VMDK files in the datastore, right-click, and click **Copy**.

> **Caution:** Do not copy the base VMDK file (for example, `Data_106_SA`) because it contains CentOS6.
>
> You must copy all the numbered VMDK files. For example, if the 10.6.5.x VM name is `Data_106_SA`, you would copy all the `Data_106_SA_1`, `Data_106_SA_2`, `Data_106_SA_3`, etc files.



6. Navigate to the new 11.1 VM in the datastore.

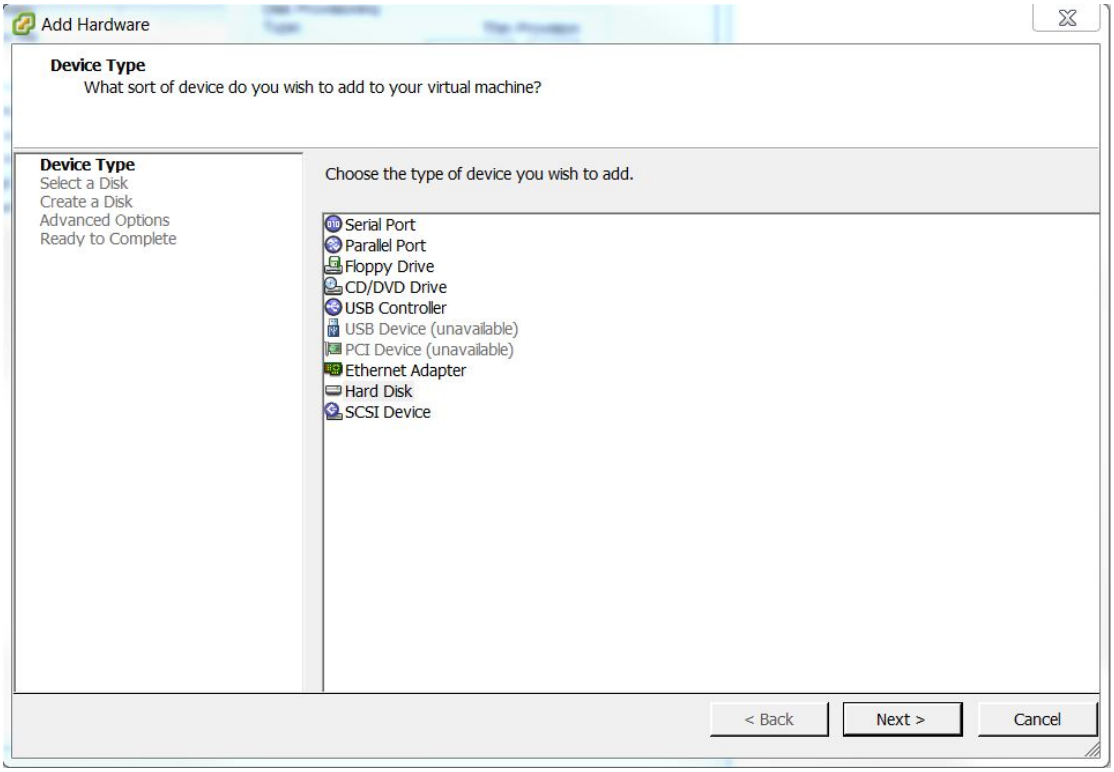
7. Right-click and click **Paste**.



Note: You must wait until all the VMDK files from the previous VM are completely copied into the datastore of the new VM.

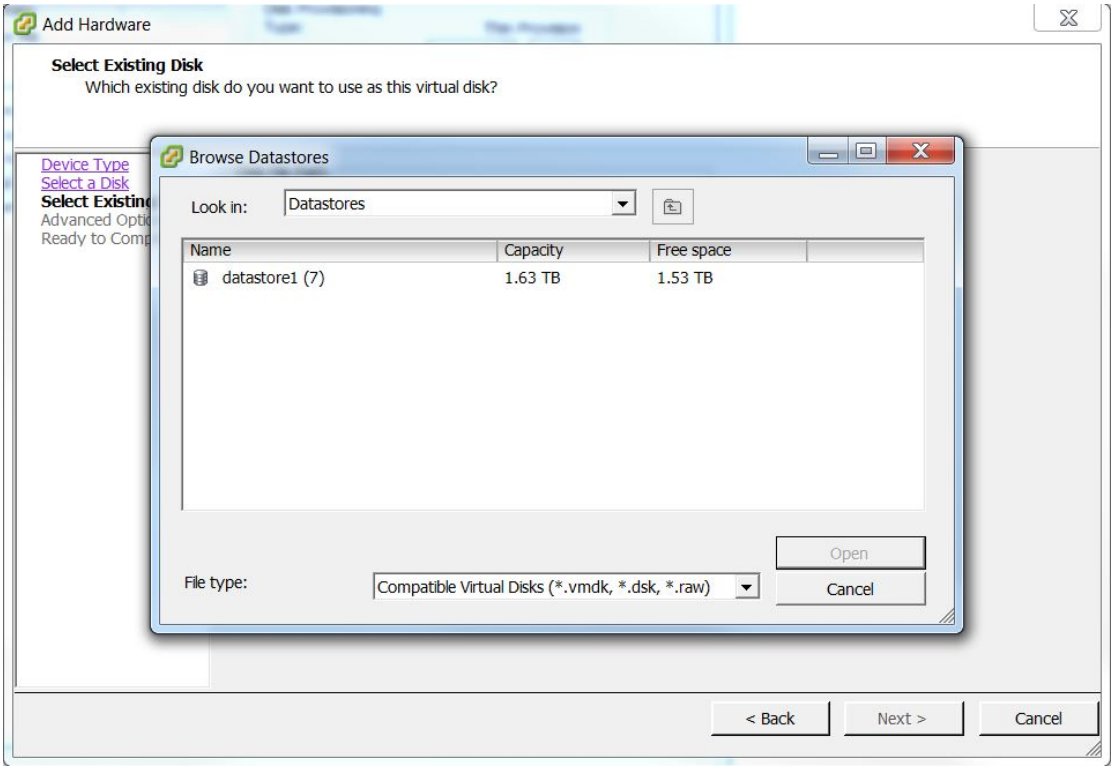
8. Select the 11.1 VM, click **Edit Settings** > **Add**.

9. In the dialog box, click **HardDisk** > **Next**.

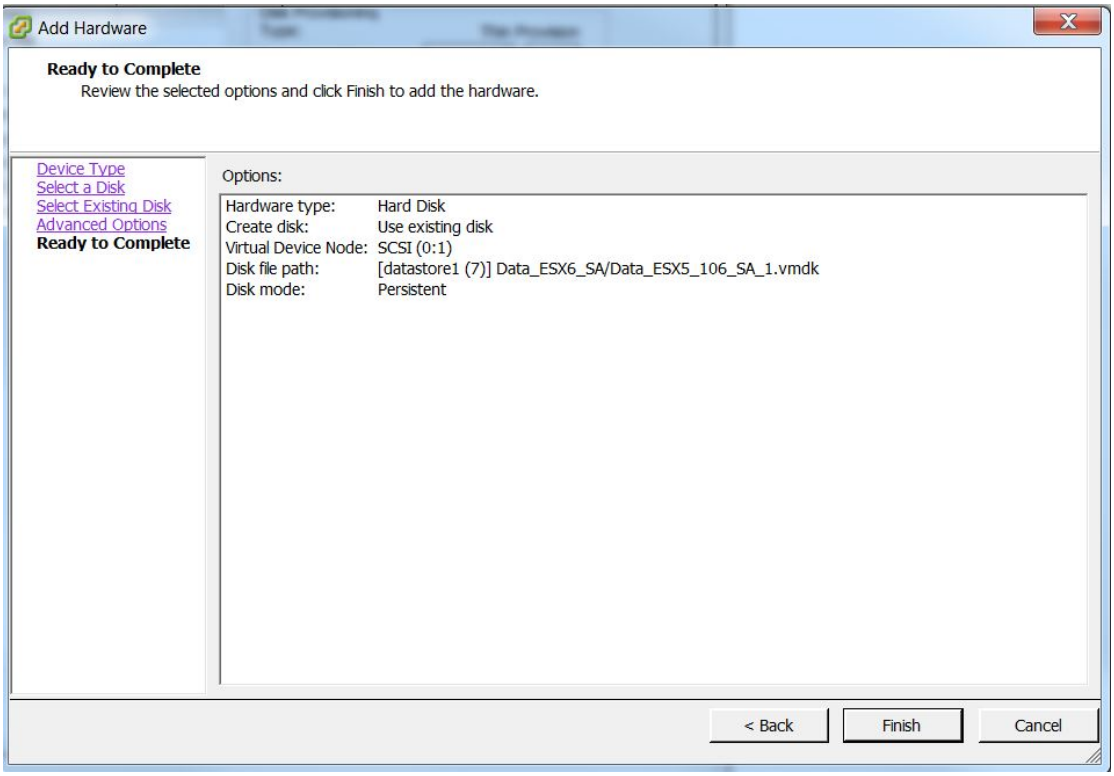


10. Click **Already existing hard disk** > **Next**.

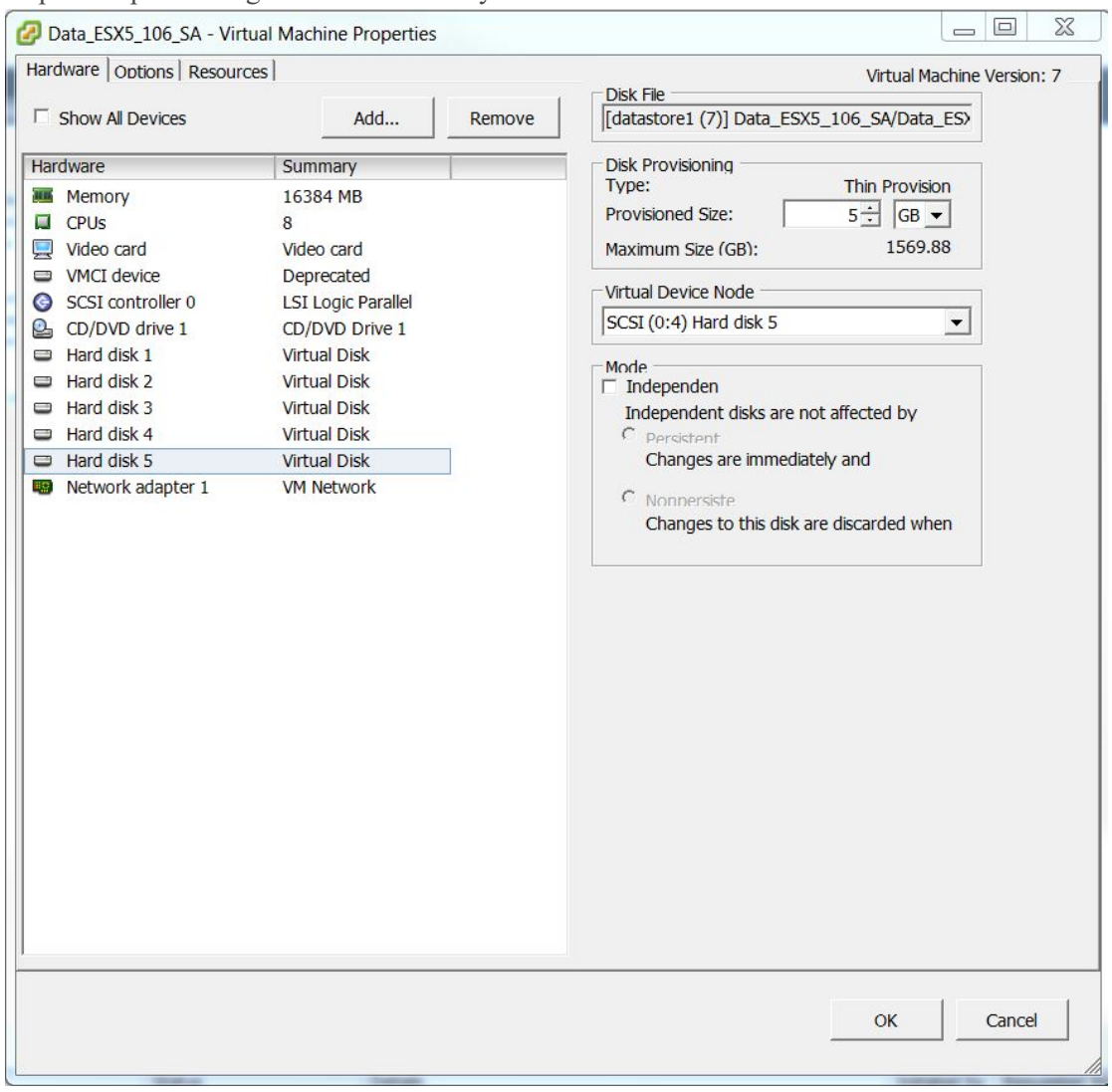
11. Click **Browse** and browse to the datastore location to which you copied the vmdk files.



12. Select the VMDK file from the 11.1 VM that you want to add as a disk.



13. Repeat steps 8 through 12 for each disk you want to add.



14. Click **OK**.

Task 4 - Retain MAC Address of Upgraded SA Server VM

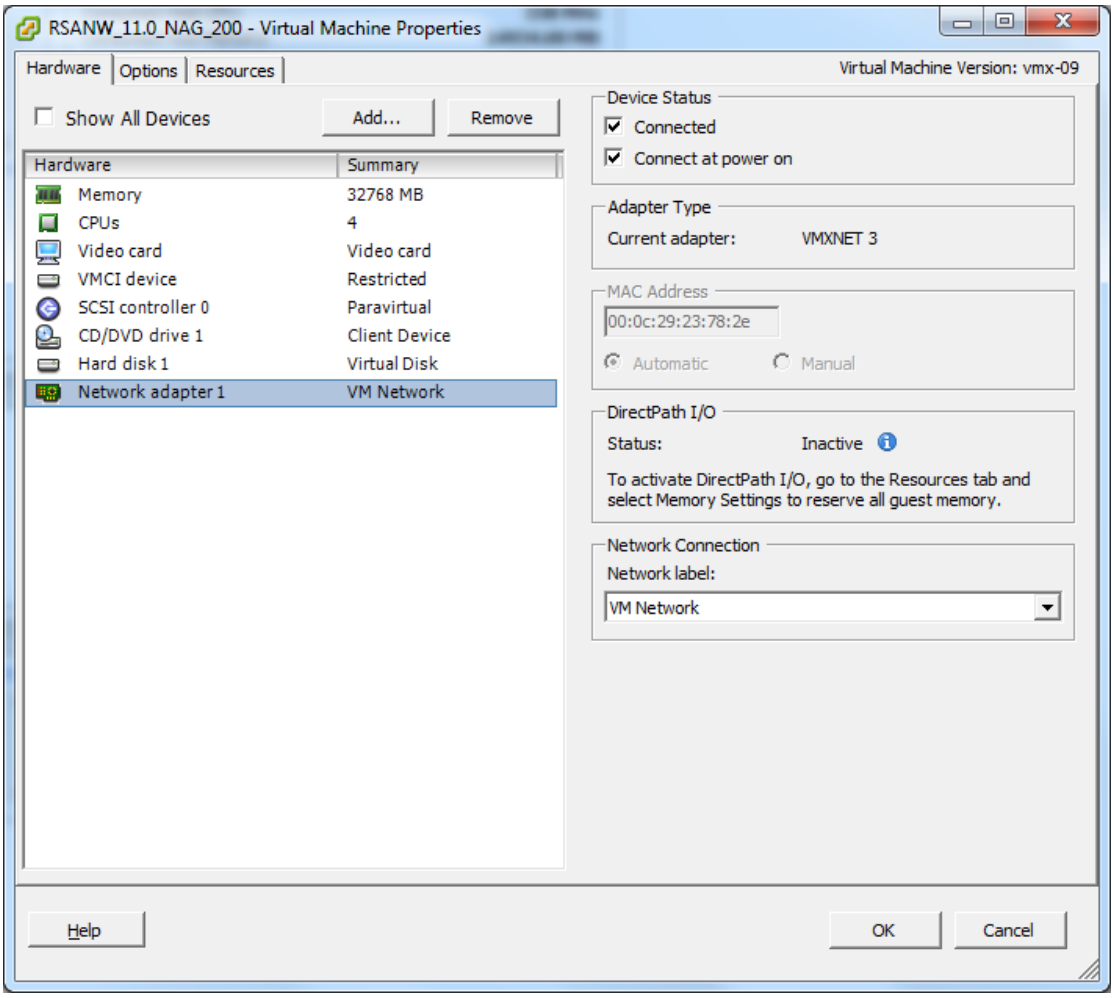
To retain the MAC address of migrated Security Analytics (SA) Server Virtual Machine (VM):

Note: These steps apply to the SA Server VM (created with "Automatic" MAC address assignment selected) to the 11.1 NetWitness Server. For VMs with a Static MAC address, you can change the MAC address by going to Edit Settings for a VM and typing in the MAC address.

1. Log in to vCenter server.

   Note: The supported versions of vCenter is 5.5 through 6.5 inclusive.

2. (Conditional) If they are powered on, **Power Off** both VMs (NetWitness 10.6.5.x and 11.1).
3. Click **Summary** tab, right-click **Datastore** and browse for the datastore location.
4. Go to the VM folder and download the `.vmx` file of 10.6.5.x and 11.1 to the local repository. By default, the VM generated with the MAC address is created in the format (as shown in the below figure).



Note: 00:0c:29:XX:YY:ZZ – 00:0c:29 is the unique identifier for an automatically generated MAC address. **00:50:56:XX:YY:ZZ – 00:50:56** is the unique identifier for a static or manually generated MAC address. This is valid only if the vCenter is not deployed. If vCenter is deployed, this MAC address denotes the unique identifier for an automatically generated MAC address.

5. Using a text editor, copy the `uuid.location` and `ethernet0.generatedAddress` values from 10.6.5.x **.vmx** file into the 11.1 **.vmx** file.

Note: If you deployed the 10.6.5.x stack on the ESX server directly (not through VCenter), you must copy the value for `uuid.bios` in addition to `uuid.location` and `ethernet0.generatedAddress` from 10.6.5.x **.vmx** file into the 11.1 **.vmx** file.

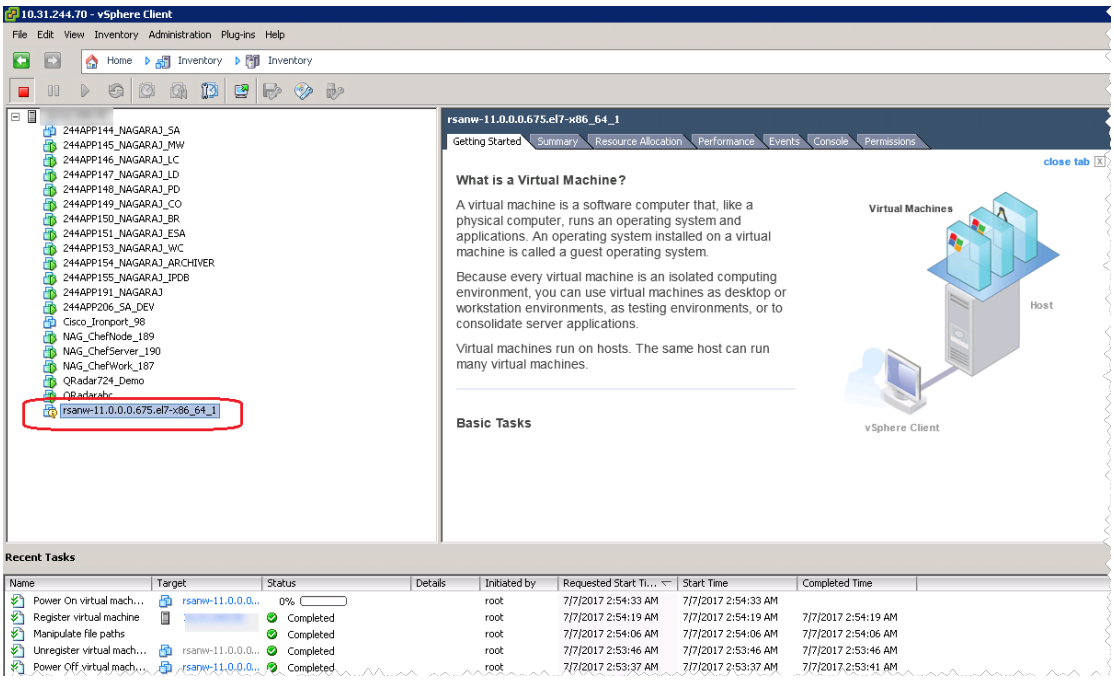
6. Remove both the 10.6.5.x and the 11.1 VMs from inventory.
   a. Navigate to the vCenter server.
   b. Right-click both the 10.6.5.x and the 11.1 VMs.

c. Select Remove from Inventory.

7. Upload the modified 11.1 **.vmx** file to the datastore location by replacing it with the existing **.vmx** file.

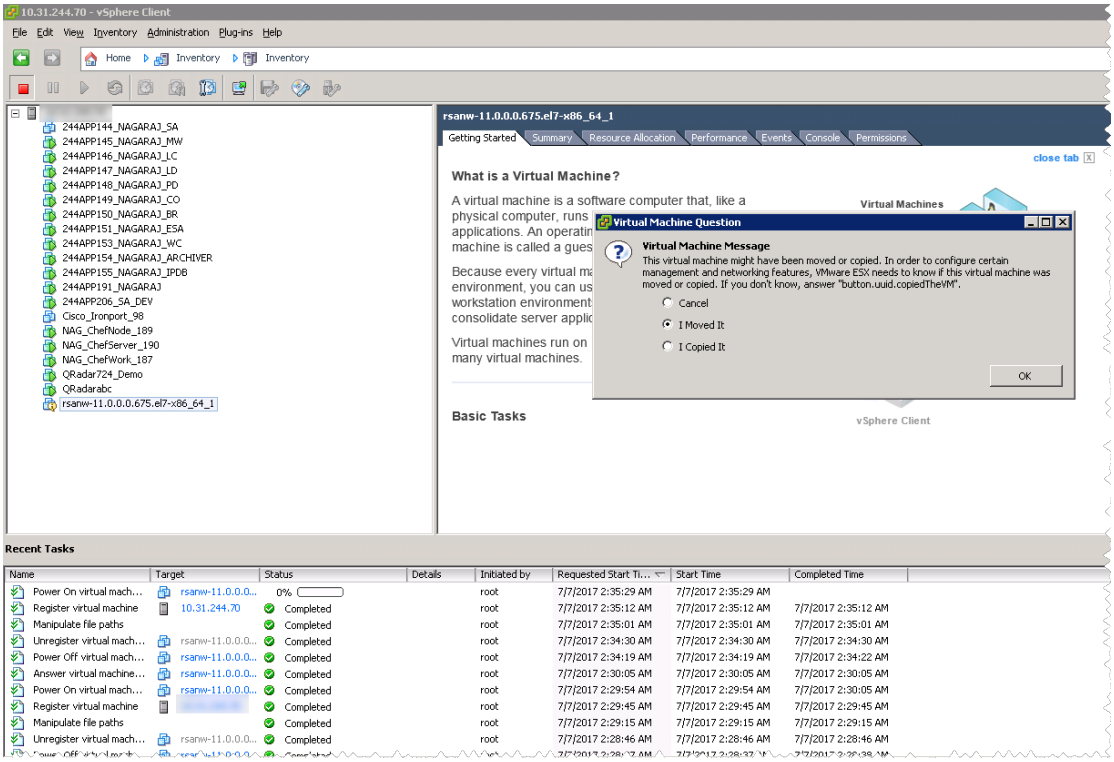
8. From the datastore, right- click the 11.1 **.vmx** file and select Add to Inventory.

9. Navigate to the vCenter server and **Power On** the 11.1 VM.
The following message is displayed.
The virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "I Copied it."



10. Right-click the VM and select **Guest** > **Answer Question**.

    The following figure is displayed.



11. Select **I Moved It**.

12. Click **OK**.

    The MAC address is retained to the MAC address from 10.6.5.x to 11.1.

Task 5 - Restore Backup Data in 10.6.5.x to 11.1 VMs

Complete the following steps to **Power On** the 11.1 VM.

1. Copy backed-up data from the `nw-backup` directory to the 11.1 VMs.

   - For the NW Server (SA Server in 10.6.5.x):

     Note: See Virtual Log Collector Host (VLC) for detailed instructions on how to upgrade the VLC.

     a. Create the `nwhome` directory under `/tmp`.

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

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

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

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

d. Mount `VolGroup02-redb` on `/var/netwitness/database`.
```
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

> **Note:** Make sure that the `/var/netwitness/database/nw-backup` directory exists with backup tarballs of the appliance.

e. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- For the Archiver, Broker, Concentrator, Log Decoder/Log Collector, and Packet Decoder:

> **Note:** If your 10.6.5.x Decoder or Log Decoder had multiple network interfaces:
> 1. **Power Off** the 11.1 VM 11.1 Decoder or Log Decoder VM.
> 2. Go to **Edit Settings** for the VM and add the required number of Ethernet Adapters.
> 3. **Power On** the VM.
> 4. Add the ethernet adapters before restoring the backup data.

a. Create the `nwhome` directory under `/tmp`.

b. Create a temporary mount `VolGroup00-nwhome` on `/tmp/nwhome/`.
```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

c. Copy the contents of `/tmp/nwhome/` directory to `/var/netwitness/`.
```
cp -r /tmp/nwhome/* /var/netwitness/
```

d. Unmount `VolGroup00-nwhome` from `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- For Malware Analysis (Co-located Malware Not Supported in 11.1 Upgrade):

a. Create the `apps` directory under `/tmp/`.

b. Create a temporary mount `VolGroup01-apps` on `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copy the `nw-backup` directory to `/var/netwitness/`.
```
cp -r /tmp/apps/database/nw-backup /var/netwitness/database
```

d. Unmount `VolGroup01-apps` from `/tmp/apps/`.
```
umount /tmp/apps
```

- For Event Stream Analysis:

a. Create the `apps` directory under `/tmp/`

b. Create a temporary mount `VolGroup01-apps` on `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copy the `nw-backup` directory to `/var/netwitness`.
```
cp -r /tmp/apps/database/nw-backup /var/netwitness/database
```

d. Unmount `VolGroup01-apps` from `/tmp/apps/`.
```
umount /tmp/apps
```

2. Mount the disks.

Note: If you have configured any external mount points on the VMs in the stack for any of the following directories, re-mount the external mount points in place of the following mounts.

- For the NW Server:

```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Note: Make sure that the `/var/netwitness/database/nw-backup` directory exists with backup tarballs of the appliance.

- For the Log Decoder/Log Collector:

Note: The following mounts are not required for the Virtual Log Collector.

```
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
```

- For the Packet Decoder:

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/decoder/packetdb
```

- For the 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
```

- For the Archiver:
  ```
  mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
  mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
  ```
- For the Broker:
  ```
  mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
  ```

8. Add the following mount entries to `/etc/fstab`.
   - For the NW Server:
     ```
     /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 the Log Decoder/Log Collector:

     Note: The following mounts are not required for the Virtual Log Collector.

     ```
     /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 the Packet Decoder:
     ```
     /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
     xfs defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
     defaults,noatime,nosuid 1 2
     ```

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

- For the Concentrator:
  ```
  /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
  defaults,noatime,nosuid 1 2
  /dev/mapper/VolGroup01-sessiondb
  /var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime
  1 2
  /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
  defaults,noatime,nosuid 1 2
  /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
  xfs defaults,noatime,nosuid 1 2
  ```
- For the Archiver:
  ```
  /dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
  defaults,nosuid,noatime 1 2
  /dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
  defaults,nosuid,noatime 1 2
  ```
- For the Broker:
  ```
  /dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
  defaults,nosuid,noatime 1 2
  ```

Set Up Virtual Hosts in 11.1

There two phases to set up your 11.1 virtual stack that you must complete in the order shown.

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

  Note: For Event Stream Analysis, if you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 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, Malware Analysis, and Broker or Concentrator Hosts

Task 1 - Set Up 11.1 NetWitness Server

Follow the instructions under Set Up 11.1 NW Server Host.

Task 2 - Set Up 11.1 ESA

Caution: If you had C2 modules enabled in 10.6.5.x, the modules will enter a warm-up after you upgrade the Event Stream Analysis service to 11.1 and they will not be available until the warm up completes.

Follow the instructions under Set Up 11.1 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 11.1 Malware Analysis

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Task 4 - Set Up 11.1 Broker or Concentrator

Follow the instructions under Set Up 11.1 Non-NW Server Host.

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.1 NW Server cannot communicate with 10.6.5.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Set Up The Rest of the Component Hosts

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

Decoder and Concentrator Hosts

1. Stop data capture and aggregation.
2. Complete the steps in Set Up 11.1 Non-NW Server Host.
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the **Backup Instructions**.
2. Stop data capture on the Log Decoder.
3. Complete the steps in Set Up 11.1 Non-NW Server Host.
4. Restart data capture on Log Decoder.

Note: After you upgrade, you will restart log collection after completing the Task 29 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task in the **Post Upgrade Tasks**

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described in the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the **Backup Instructions**.
2. Back up your 10.6.5.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>,10.6.5.x
```

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 10.6.5.x VLC so that a new 11.1 VM can be created with the same network configuration.
5. Deploy a fresh Non-NW Server host using the 11.1 NetWitness Suite ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.5.x VLC.
This information is stored in the `<hostname-IPaddress>-network.info.txt` 10.6.5.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 11.1 Non-SA Server Host for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

Set Up 11.1 NW Server Host

Make sure that you have backed up 10.6.5.x data for the SA Server host. **You must follow the instructions in Backup Instructions to back up the host**.

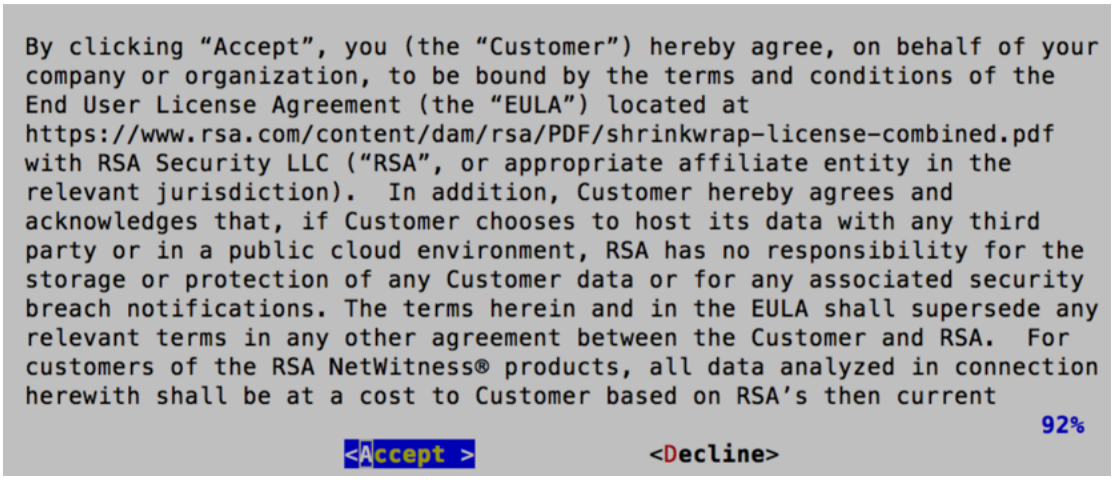
Caution: Run the backup immediately before upgrading the SA Server to 11.1 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.1.

Complete the following steps to set up the 11.1 NW Server host.

1. Log in to 11.1 NW Server VM's console 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.

2. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

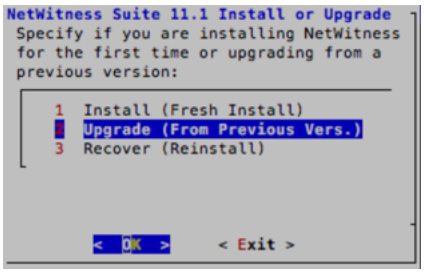
Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

3. Tab to **Yes** and press **Enter**.

Choose **No** if you already upgraded the NW Server to 11.1.

The **Install or Upgrade** prompt is displayed.

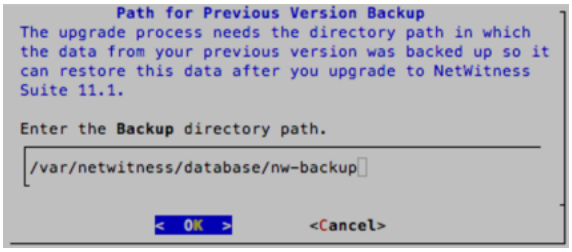
4. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.



The **Backup** path prompt 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.

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.



This table lists the backup and restore paths by host/service.

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

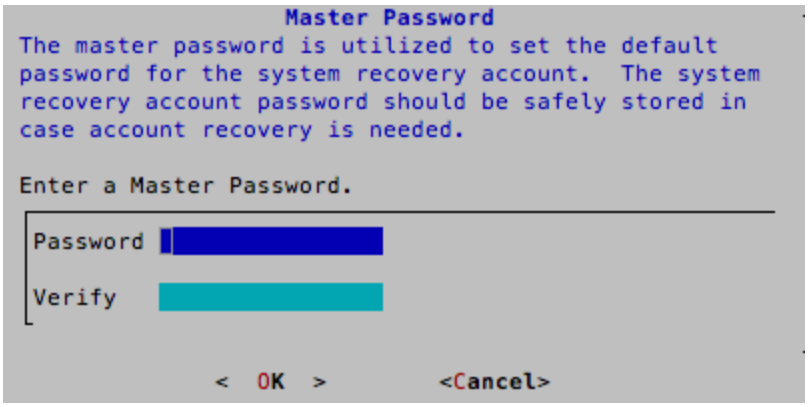
The **Master Password** prompt is displayed.

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

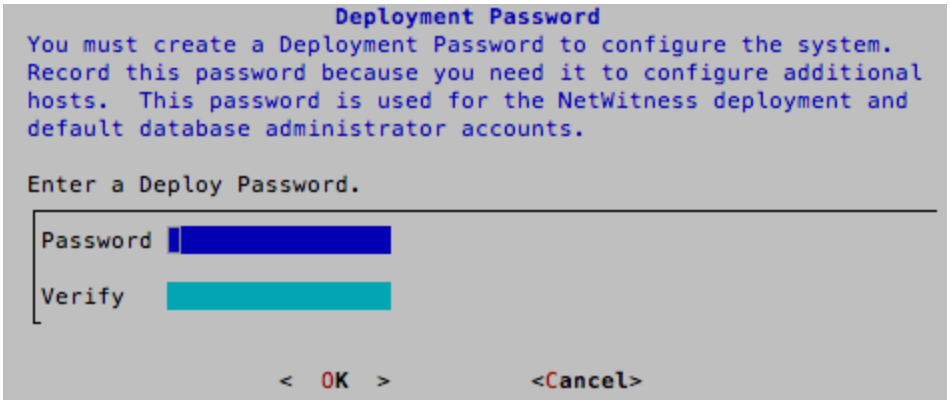
No ambiguous characters are supported for Master Password and Deployment Password. For example:
space { } [ ] ( ) / \ ' " ` ~ ; : . < > -

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



The **Deployment Password** prompt is displayed.

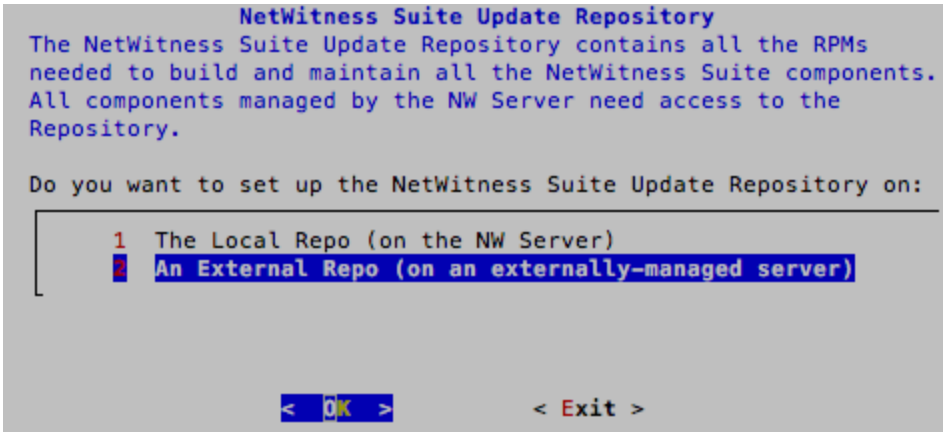
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



The **Update Repository** prompt is displayed.

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

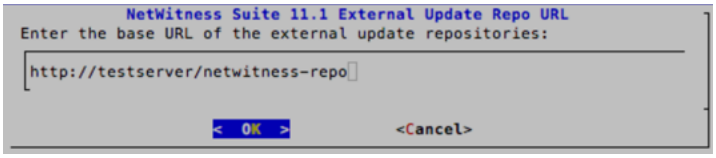
8. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**.



The **External Update Repo URl** prompt is displayed.

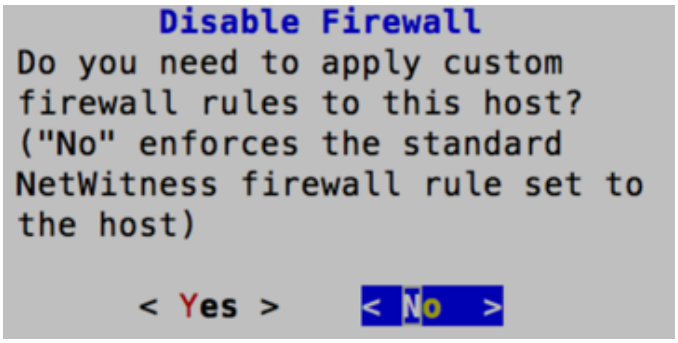
Refer to Appendix D. Create External Repository for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

9. Enter the base URL of the NetWitness Suite external repo (for example, **http:/testserver/netwitness-repo**)and click **OK**.

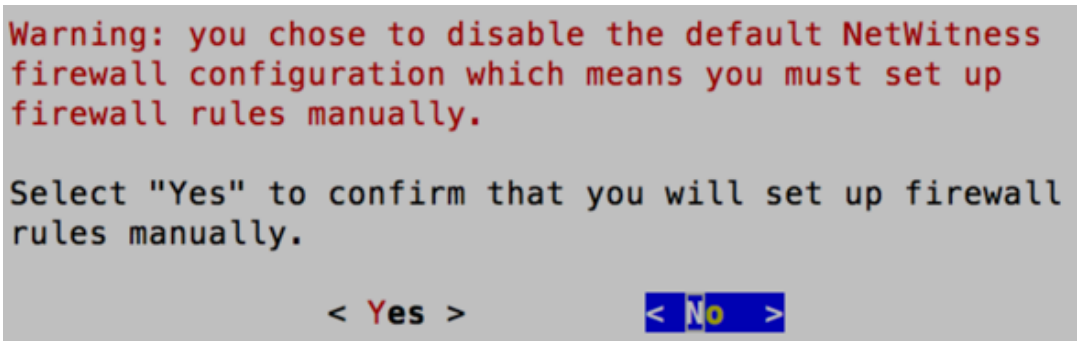


The **Disable** or use standard **Firewall** configuration prompt is displayed.

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

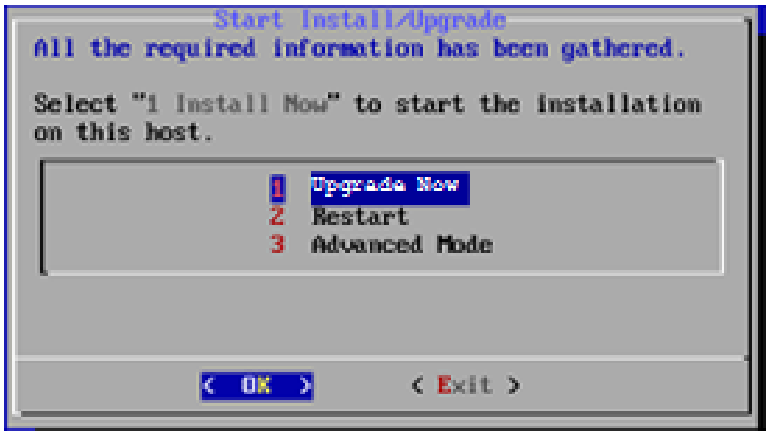


- If you select **Yes**, confirm your selection or **No** to use the standard firewall configuration.



The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press Enter.



When **Installation complete** is displayed, you have upgraded the 10.6.5.x SA Server to the 11.1 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)
```

12. Complete the NW Server before you upgrade any of the non-SA Server hosts to 11.1.

Set Up 11.1 Non-NW Server Host

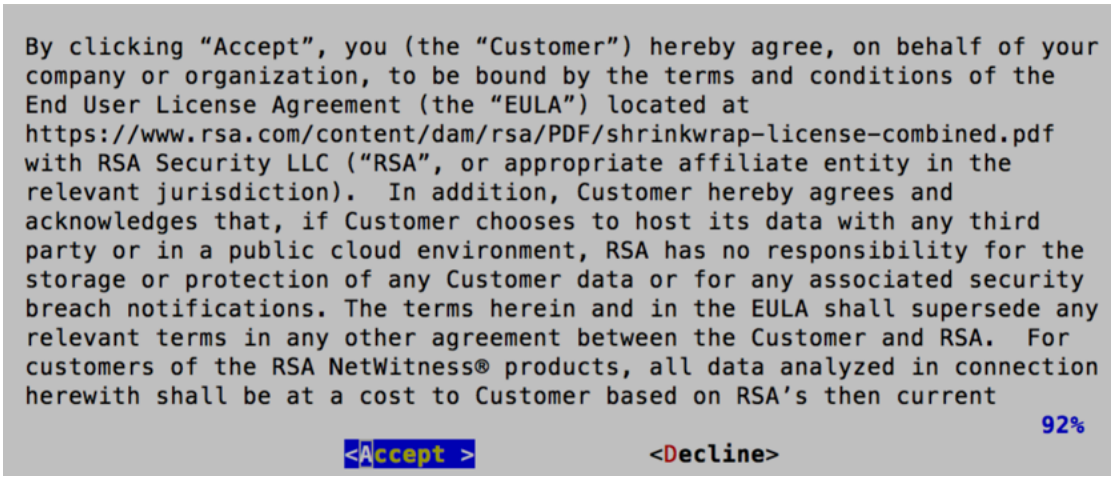
Make sure that you Back up your 10.6.5.x data for the host. **You must follow the instructions in Backup Instructions to back up the host.**

Caution: Run the backup immediately before upgrading the host to 11.1 so that the data is as recent as possible.

Complete the following steps to set up an 11.1 Non-NW Server host.

1. Log in to 11.1 non-NW Server VM console and run the `nwsetup-tui` command.
   This initiates the Setup program and the EULA is displayed.

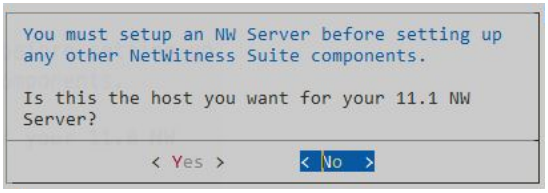
2. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.1 NW Server** prompt is displayed.

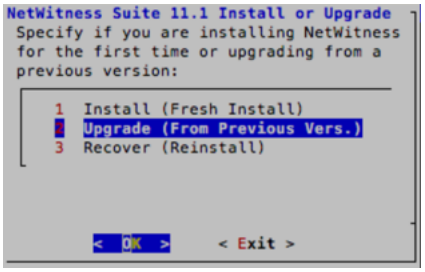
Caution: If you choose the wrong the host for the NW Server and complete the upgrade, you must repeat steps 1 through 11 of Set Up 11.1 NW Server Host to correct this error.

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



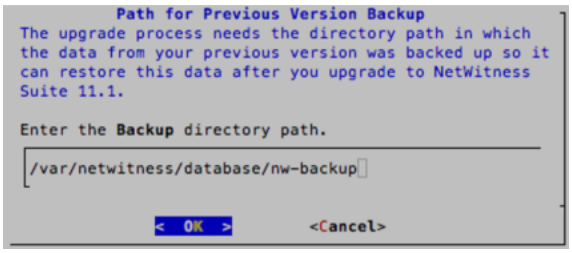
The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

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



The **Backup** path prompt is displayed.

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.



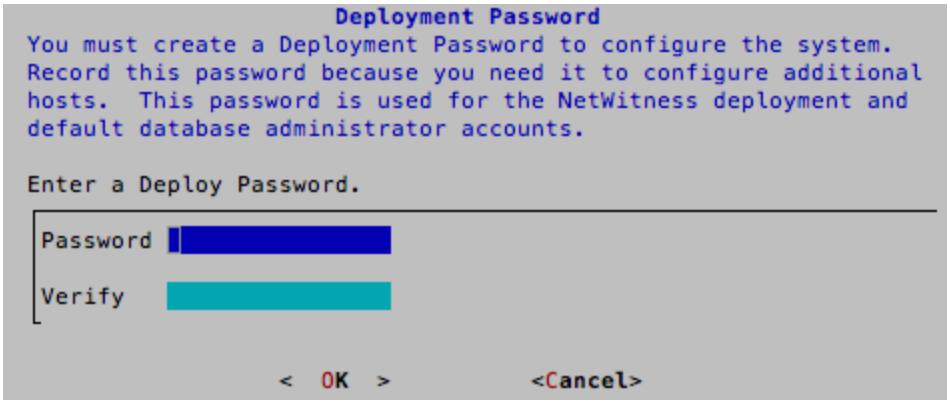
This table lists the backup and restore paths by host/service.

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

The **Deployment Password** prompt is displayed.

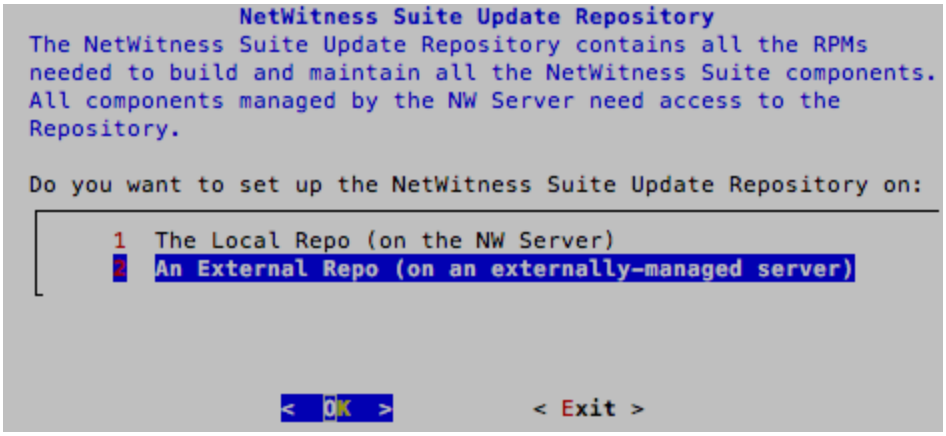
Note: You must use the same deployment password that you used when you upgraded the NW Server.

6. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.



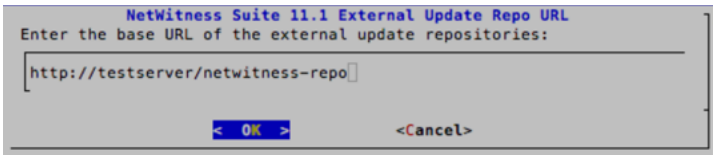
The **Update Repository** prompt is displayed.

7. Use the down and up arrows to select **2 An External Repo (on an externally-managed server)**, tab to **OK**, and press **Enter**.



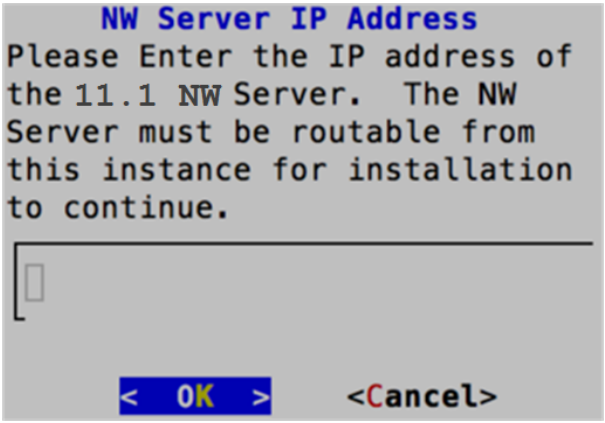
The **External Update Repo URL** prompt is displayed.
The repositories give you access RSA updates and CentOS updates.

8. Enter the base URL of the NetWitness Suite external repo (for example, **http://testserver/netwitness-repo**)and click **OK**. Refer to Appendix D. Create External Repository for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



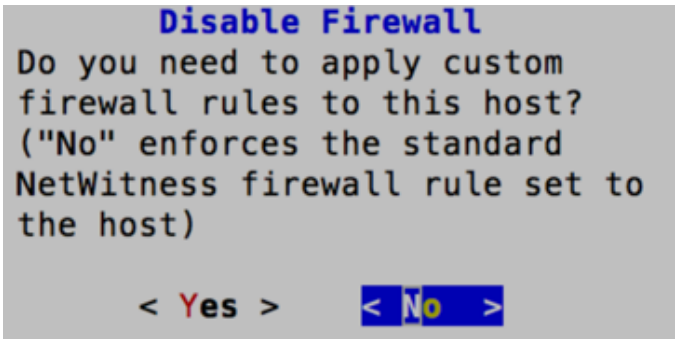
The **NW Server IP Address** is displayed.

9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

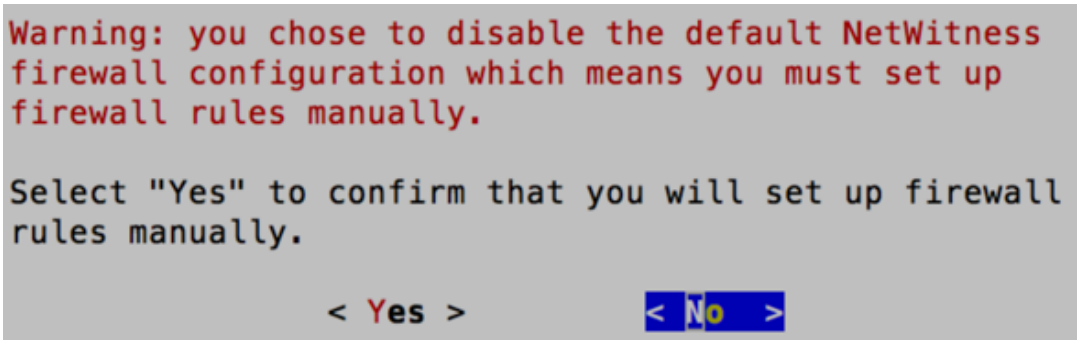


The **Disable** or use standard **Firewall** configuration prompt is displayed.

10. Tab to **No** (default), 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 **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.1 Disaster Recovery).

11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.

When **Installation complete** is displayed, you have upgraded the host to the 11.1.

12. Install the service on this host:

    a. Log into NetWitness Suite and click **ADMIN** > **Hosts**.

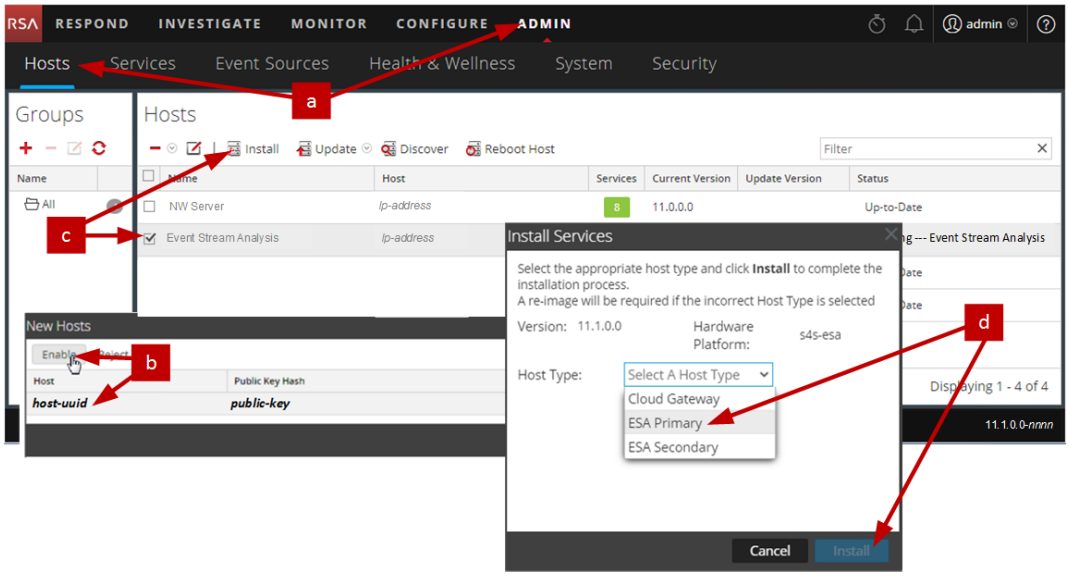
    The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

b. 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.

c. Select that host in the **Hosts** view (for example, **Event Stream Analysis**) and click Install.
The **Install Services** dialog is displayed.

d. Select the appropriate service (for example, **ESA Primary**) and click **Install**.



You have completed the upgrade of the non-NW Server host in NetWitness Suite

Note: When you upgrade a Respond host from 10.6.5.x to 11.1, it takes a period of time for Respond to come back online. This is caused by Respond indexing data while it is restored. The size of the data in the Mongo database will determine the time.

Update or Install Legacy Windows Collection

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

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

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.1. These tasks are organized by the following categories.

- General
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Investigate
- Log Collection
- Reporting Engine
- Respond
- RSA NetWitness® SecOps Manager
  (RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)
- Backup

General

Task 1 - Make Sure New 15796 Port Is Configured Correctly

Port 15796 is new in 11.x. Make sure that you configure port 15976 and all the other ports as shown in the "Network Architecture and Ports" topic in the *RSA NetWitness® SuiteDeployment Guide* . Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

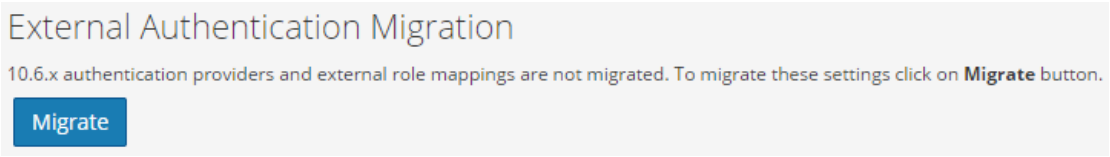
NW Server

Task 2 - Migrate Active Directory (AD)

The first time you log into the NetWitness Suite 11.1 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Suite 11.1 with your `admin user` credentials.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **SECURITY** and click the **Settings** tab.

   The following dialog is displayed.



3. Click **Migrate**.

   The migration is complete and the dialog closes.

Task 3 - Modify Migrated AD Configuration to Upload Certificate

If you authenticated through Active Directory (AD) server, and enabled SSL for the AD connection in 10.6.5.x, you must modify the migrated AD configuration to upload the Active Directory server certificate.

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

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** and click the **Settings** tab.
2. Under **Active Directory Settings**, select an AD configuration and click .

   The Edit Configuration dialog is displayed.
3. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
4. Click **Save**.

Task 4 - Reconfigure Pluggable Authentication Module (PAM) in 11.1

You must reconfigure PAM after you upgrade to 11.1. See "Configure PAM Login Capability" in the *RSA NetWitness® Suite System Security and User Management Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

You can refer to your 10.6.5.x PAM configuration files in the **/etc** directory in the your 10.6.5.x backup data for guidance.

Task 5 - Restore NTP Servers

You must use the NetWitness Suite 11.1 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® Suite System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 6 - 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 Suite 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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 7 - Remap Virtual NW Server License to 10.6.5.x MAC Address

If you are upgrading a Security Analytics server running on a virtual machine, change the 11.1 NW Server virtual host to the 10.6.5.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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

(Conditional) Task 8 - 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 9 - 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 10.6.5.

NetWitness Suite 11.1 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.

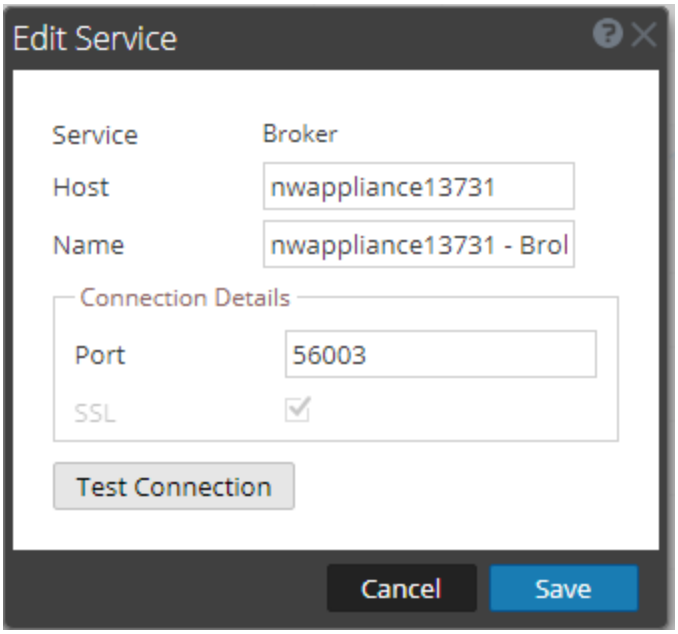
1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Services**.
2. Select each core service and change there ports from Non-SSL to SSL ports.

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

3. Click (Edit) from the **Services** view toolbar.

   The Edit Service dialog is displayed.

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



Task 10 - (Conditional) Correct Audit Log Templates That Are Not Updated in Logstash Output Conf File

Problem: When a user updates from 10.6.5 to 11.1 and 11.0.0.0 to 11.1, if they have a global auditing set up, audit log templates are not getting updated in Logstash output conf file.

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

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

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications**. The **Global Notifications** view is displayed.
2. Click the **Servers** tab, select any syslog server.
3. Click (edit icon) and click **Save**.

RSA NetWitness® Endpoint

Task 11 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

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

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

RSA NetWitness® Endpoint Insights

(Optional) Task 12 - Install Endpoint Hybrid or Endpoint Log Hybrid

See:

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

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

Task 13 - 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 Suite 11.1, the virtual host is `/rsa/system`. For 10.6.5.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 14 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.1.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
2. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. 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 Suite ESA Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 15 - For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint Configure Mutually Authenticated SSL

If you integrate with Web Threat Detection, NetWitness SecOps Manager 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 10.6.5.x data (see Backup Instructions).

1. Create a user on the host system that is integrating with NetWitness Suite 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 16 - Enable Threat - Malware Indicators Dashboard

In 11.1.0, the 10.6.5.x **Threat -Indicators Dashboard** was renamed to **Threat - Malware Indicators Dashboard**. If you used this dashboard in 10.6.5.x, you must:

1. Enable the **Threat - Malware Indicators Dashboard** in 11.1.
2. Set datasource for new dashlets.

   See "Dashlets" in RSA Link (https://community.rsa.com/docs/DOC-81463) for a description of Dashlets in the context of NetWitness Suite.

Investigate

Task 17 - Make Sure User Roles Have Customized User Roles Have `Investigate-server` Permissions for Event Analysis Access

After you upgrade to 11.1.0.0, any customized user role does not have `investigate-server.*` permission enabled by default. Complete the following procedure to make sure that the appropriate user roles have permission to access Event Analysis.

1. Log in to NetWitness Suite 11.1.0.0 as an `Admin` user.
2. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **Security** .
3. Click the **Roles** tab.
4. Select the roles that need `investigate-server.*` permissions and click (edit icon).
5. Select the **Investigate-server** tab under under **Permissions**.

6. If investigate-server checkbox is not checked, check it for the users that require Event Analysis access.

7. Click **Save**.

Log Collection

Task 18 - 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 11.1 to ensure that all collection protocols resume normal operation.

Reset Stable System Values for the Lockbox

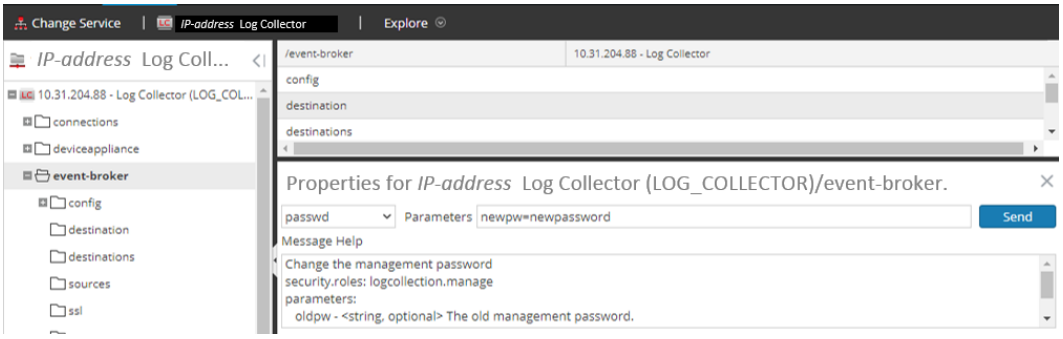
The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 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 11.1 upgrade.

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN > Services**.
2. Select the Log Collector service.
3. Click  (Actions) > **View** > **Explore**.
4. Right click `event-broker` > **Properties**.

5. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders)

Task 19 - 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® SuiteSystem Maintenance Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Reporting Engine

Task 20 - 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 10.6.5.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 11.1.

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 21 - 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® Suite Reporting Engine Configuration Guide* for instructions. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Respond

(Conditional) Task 22 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.1. See "Add a Role and Assign Permissions" in the *RSA NetWitness Suite System Security and User Management Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 23 - Restore Respond Service Custom Keys

In 10.6.5.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 10.6.5.x backup.

2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.1.

   This is the new file for 11.1.

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

Task 24 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.1 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.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 10.6.5.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 10.6.5.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
   This directory is where NetWitness Suite 11.1 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
   The `alert_rules.json` file contains aggregation rule schema.

Task 25 - Add Respond Notification Settings for Custom Roles

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

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

Task 26 - Manually Configure Respond Notification Settings

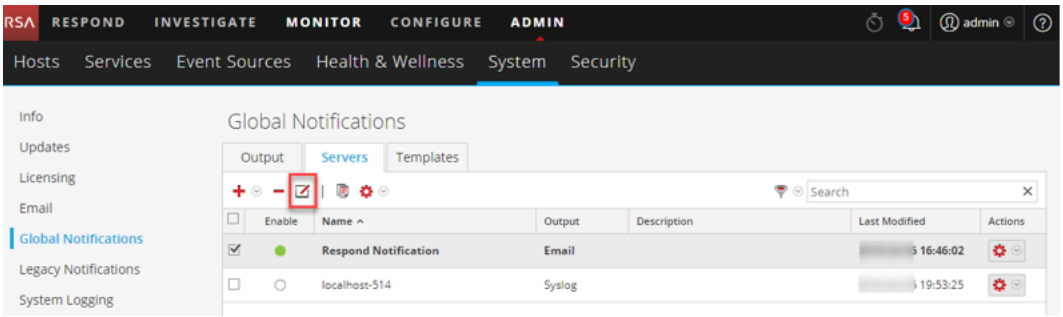
The Incident Management notification settings in NetWitness Suite 10.6.5.x to 11.1 are different from the Respond notification settings available in 11.1, so your existing 10.6.5.x to 11.1 settings will not migrate to 11.1.

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

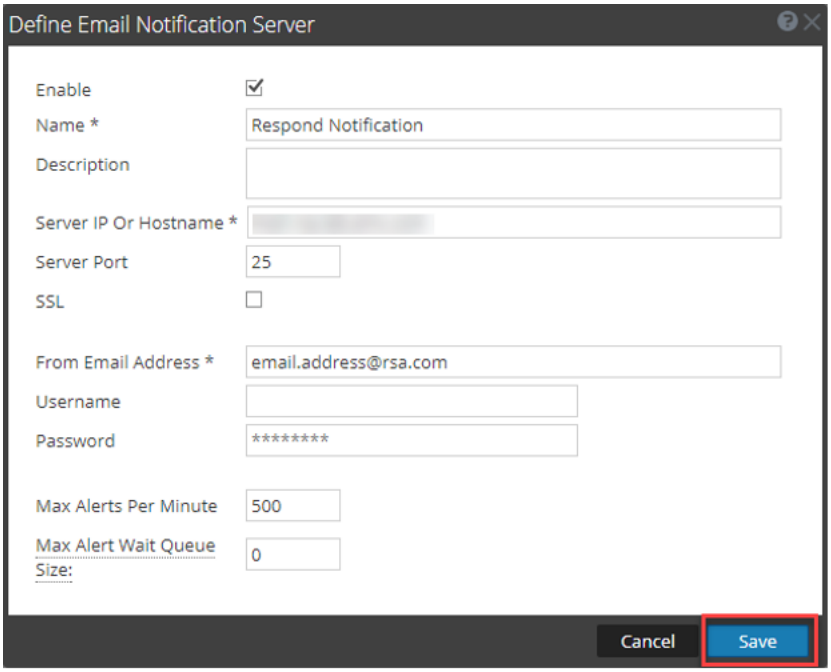
To manually configure the Respond Notification Settings, go to **CONFIGURE** > **Respond Notifications.** See the "Configure Respond Email Notification Settings" procedure in the *NetWitness Respond Configuration Guide*.

Notification Servers from 10.6.5.x to 11.1 will not display in the Email Server drop-down list. The email servers must be edited and saved in the Global Notification Servers panel (**ADMIN** > **System** > **Global Notifications** > **Server** tab).

1. In the **NetWitness Suite** 11.1 menu, select **ADMIN** > **System** > **Global Notifications** > **Server** tab.
2. Go to **CONFIGURE** > **Respond Notifications**. The Respond Notifications Settings view is displayed.
3. Notice that the email notification servers do not appear in the EMAIL SERVER drop-down list.
4. Click the **Email Server Settings** link. You will see the Global Notifications panel.
5. Click the **Servers** tab.
6. For each of your email notification servers:
   a. Select the Email notification server and click .



b. In the Define Email Notification Server dialog, click **Save**.



7. Go back to **CONFIGURE** > **Respond Notifications**. Your servers will appear in the **EMAIL SERVER** drop-down list.
   Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

Task 27 - Update Default Incident Rule Group By Values

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

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

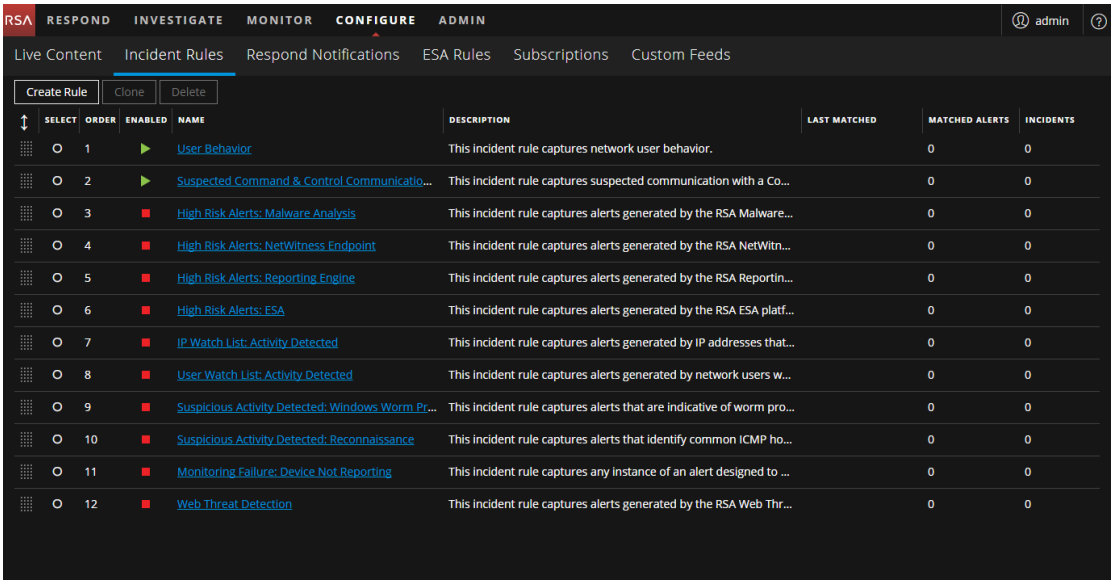
1. Go to **CONFIGURE** > **Incident Rules** and click the link in the **Name** column for the rule that you want to update. The Incident Rule Details view is displayed.
2. In the **Group By** field, select the new Group By value.
3. Click **Save** to update the rule.

Task 28 - Add Group By Field to Incident Rules

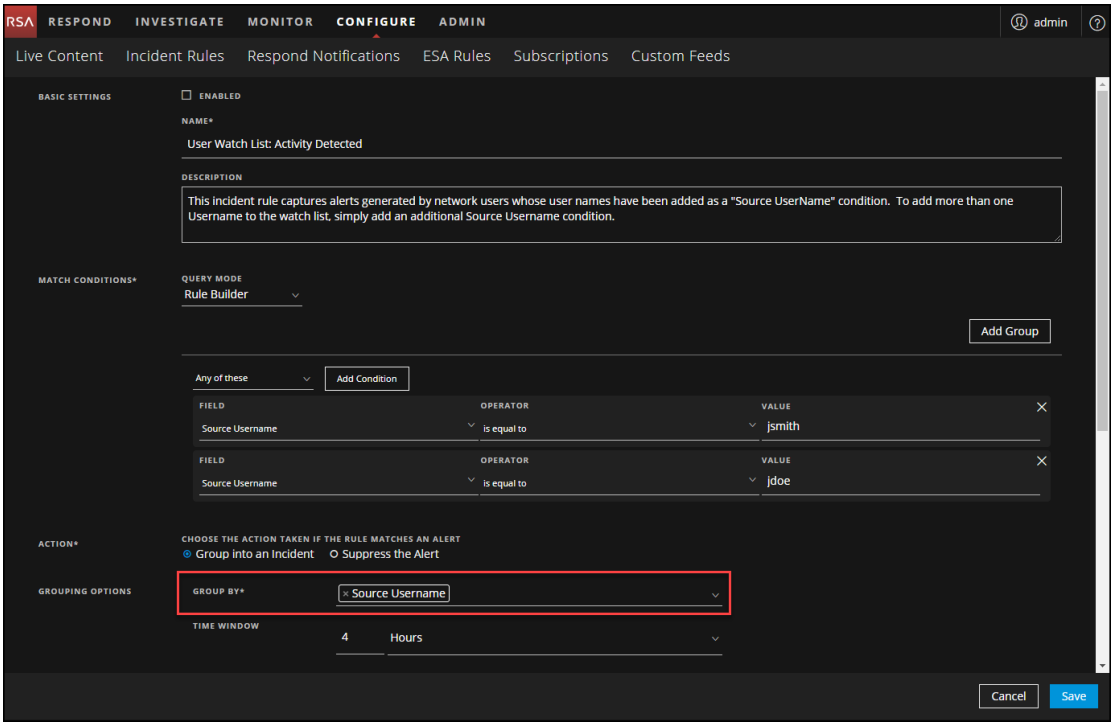
The **Group By** field is not required in 10.6.5, but it is required in 11.1. After you upgrade to 11.1, some incident rules will not have a **Group By** field, so you must add them to the rules or the rules will not work and they will not create incidents.

Complete the following steps for each incident rule:

1. In the **NetWitness Suite** 11.1 menu, select Go to **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



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



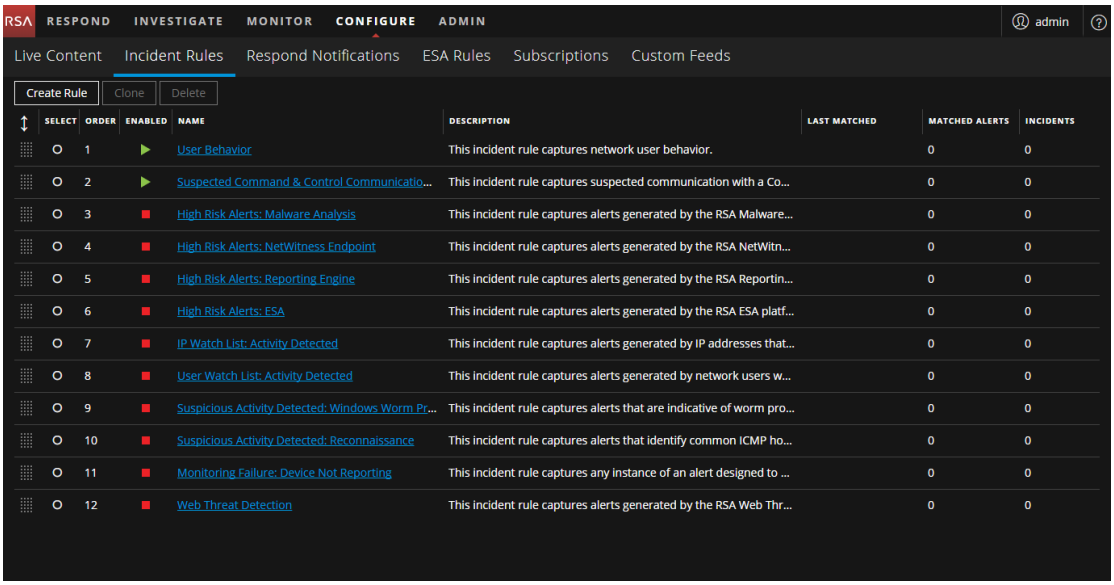
3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Task 29 - Update Incident Rules Identified in the Domain in the Matching Conditions Upgrade Preparation Task

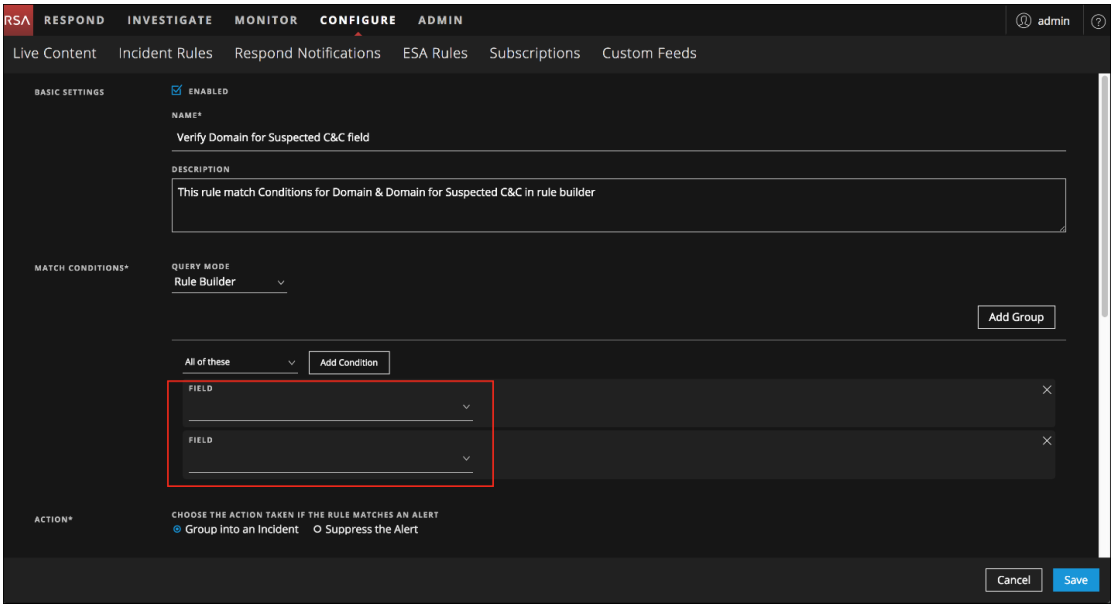
Modify the incident rules that you identified in the Task 4 - Check Aggregation Rules Match Conditions for "Domain" or "Domain for Suspected C&C" upgrade preparation task, which contained Domain or Domain for Suspected C&C in the matching conditions in rule builder, to use only Domain.

For each rule that you previously identified:

1. In the **NetWitness Suite** 11.1 menu, select **CONFIGURE** > **Incident Rules** and click the link in the Name column for the rule that you want to update.



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



3. Click **Save** to update the rule.
   For information about incident rules, see the *NetWitness Respond Configuration Guide*. Go to the Master Table of Contents for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

RSA NetWitness® SecOps Manager

(RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management and RSA Archer Issues Management)

Task 30 - 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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Backup

Task 31 - 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 11.1 before you remove the backup-related files from the local directories on your 11.1 hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.1, you must remove:

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

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

Appendix A. Troubleshooting

This section describes solutions to problems that you may encounter during installations and upgrades. In most cases, NetWitness Suite creates log messages when it encounters these problems.

Note: If you cannot resolve an 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.

- Command Line Interface (CLI)
- Backup Script
- Event Stream Analysis
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

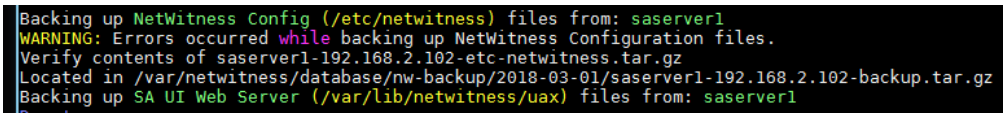
Command Line Interface (CLI)

Error Message	Command Line Interface (CLI) displays: "Orchestration failed." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Entered the wrong `deploy_admin` password in `nwsetup-tui`.
Solution	Retrieve your `deploy_admin` password password. 1. SSH to the NW Server host. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` SSH to the host that failed. 2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

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

Backup (`nw-backup` script)

Error 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 *Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.*

Error	Backup errors caused by the `immutable` attribute setting. Here is an example of an error that can be displayed: 
Cause	If you have any files that have the immutable flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.
Solution	On the host that contains the files with the immutable flag set, run the following command to remove the immutable setting from the files: `chattr -i <filename>`

Error	Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: `/etc/sysconfig/network-scripts/ifcfg-em1` Verify contents of `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Cause	There are incorrect or duplicate entries for any one of the following fields: DEVICE, BOOTPROTO, IPADDR, NETMASK or GATEWAY, that were found from reading the primary Ethernet interface configuration file from the host being backed up.

Solution	Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format `<hostname>-<hostip>-network.info.txt`, and should contain the following entries:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.1.0.0 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

Solution	1. SSH to the ESA Primary 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.

Log Collector Service (`nwlogcollector`)

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

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

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

Error 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 Suite 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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 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 10.6.5.x to 11.1.0.0.
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.

Error Message	`<timestamp> : Available free space in /var/netwitness/re-server/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 for NetWitness Logs & Packets 11.x to find all NetWitness Suite 11.x documents.

Appendix B. Stopping and Restarting Data Capture and Aggregation

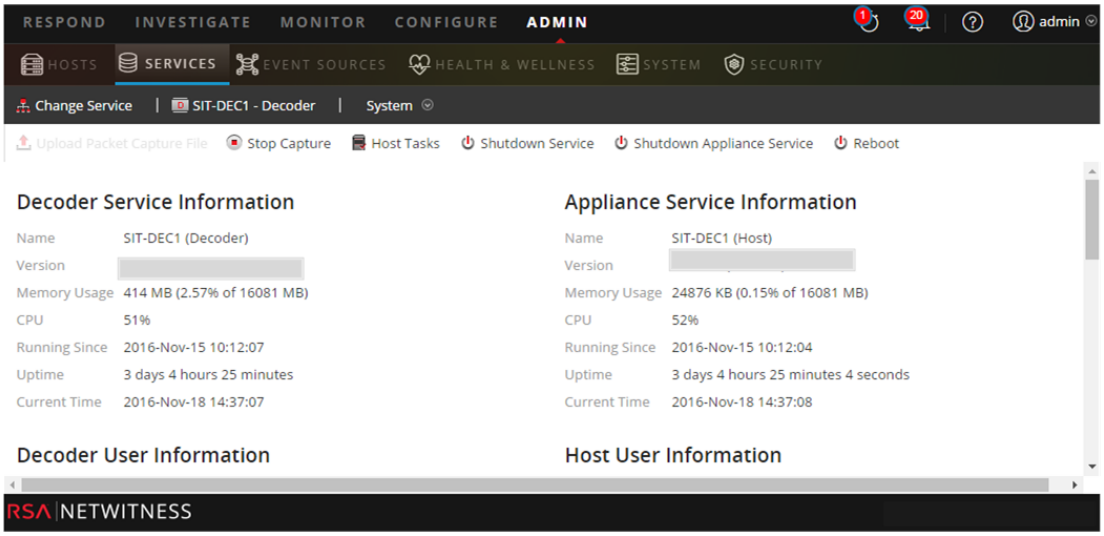
RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.1.0.0. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Packet Capture

To stop packet capture:

1. Log in to NetWitness Suite 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 

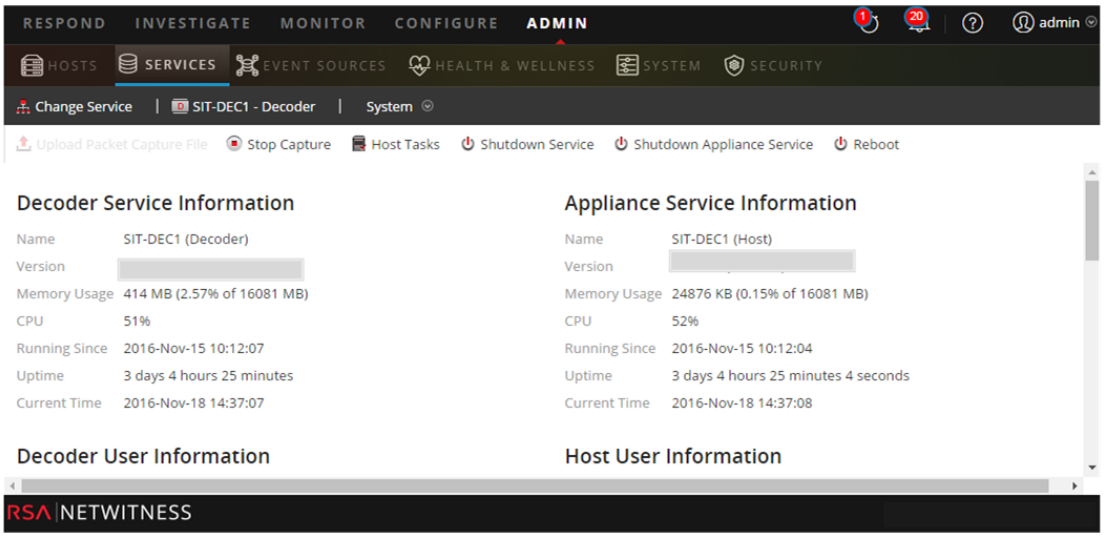
.

Stop Log Capture

To stop log capture:

1. Log in to NetWitness Suite 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 

.

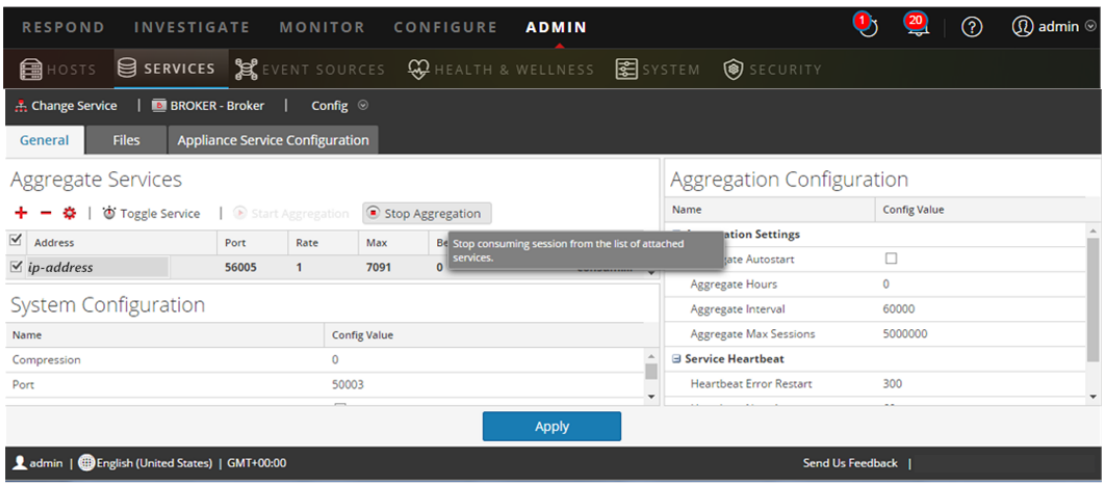
Stop Aggregation

1. Log in to NetWitness Suite 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 

.

Start Data Capture and Aggregation

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

Start Packet Capture

To start packet capture:

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

.

Start Log Capture

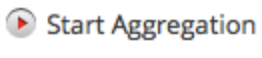
To start log capture:

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

.

Start Aggregation

To start aggregation:

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

.

Appendix C. Using iDRAC

Many customers have remote sites with limited physical access and limited bandwidth from the administrator's desktop. If this the case, you may want to use iDRAC with the ISO Image shared out from an NFS share that is local to the devices being upgraded or installed. This also gives you the ability to use an existing NetWitness device as the sharing host.

For example, you have:

- a Concentrator and Decoder at a site in a remote geographic location.
- the bandwidth is relatively low to that site from the administrator's site.
- shipping a USB stick and arranging to have person to go plug it into the boxes while you upgrade is not practical.

In this situation, you can:

1. Install the nfs-utils rpm.
2. Configure the NFS share.
3. Configure iDRAC to connect to that share.
   Make sure that you update your iDRAC firmware Supported Windows and Linux Operating Systems. You do this by downloading and running the Dell Update Packages for supported Windows and Linux operating systems from Dell Support website at http://www.support.dell.com. For more information, see the Dell Update Package User's Guide available on the Dell Support website at http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.
4. Boot to the virtual media that contains the ISO file and continue with the upgrade.

Configure NFS Server - NFS Server config File

1. Install NFS and it’s common utilities using yum.
   ```
   yum install nfs-utils
   ```
2. Configure the NFS service to run at boot.
   ```
   chkconfig nfs on
   ```
3. Configure the rpcbind service to run at boot.
   This service is required by NFS and must be running before NFS can be started.
   ```
   chkconfig rpcbind on
   ```

4. Start the rpcbind service.
   `service rpcbind start`
5. Start the NFS service.
   `service nfs start`
6. Create a directory for our first export.
   `mkdir /exports/files`
7. Open the NFS exports file into a text editor.
   `vi /etc/exports`
8. To export the directory to everyone with read-only access, add the following line.
   `/exports/files *(ro)`
9. Save your changes and exit the editor.
   `:wq!`
10. Export the directory defined above.
    `exportfs -a`
11. Disable firewall rules while performing upgrades.
    `service iptables stop`
12. Copy install media that contains the ISO file to `/exports/files` directory.

Boot iDRAC to NFS Configuration

Note: You must verify idrac firmware is at least 1.57.57 for Series 4 (R620).

1. Log into iDRAC interface.
2. Attach media via Remote File Share.
   `<server ip>:/export/files/11.1.0.0.iso`
   For example: `10.10.10.10:/exports/files/rsa-11.1.0.0.1948.el7-usb.iso`
3. Click **Connect**.
4. Launch **Console**.
5. From **next boot** menu select **Virtual DVD/CD**.
6. Reboot device.

Appendix D. Create External Repository

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

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

1. Log in to the web server host.
2. Create directory to host the NW repository (`netwitness-11.1.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, `/var/netwitness` is the `web-root`, submit the following command string.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Create the 11.1.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Unzip the `netwitness-11.1.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0` directory.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Unzipping `netwitness-11.1.0.0.zip` results in two zip files (`OS-11.1.0.0.zip` and `RSA-11.1.0.0.zip`) and some other files.
6. Unzip the:
   a. `OS-11.1.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS` directory.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      The following example illustrates how the Operating System (OS) file structure will appear after you unzip the file.

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

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

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

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

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

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

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.1.0.0 Setup program (`nwsetup-tui`) prompt.

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD
1.1	31-May-18	Added Respond Pre-Upgrade task for Data Retention.	IDD
1.2	7-Jun-18	Added "Task 1 - Make Sure New 15796 Port Is Configured Correctly" to the Post Upgrade Tasks.	IDD
1.3	8-Jun-18	Added Caution in Upgrade Tasks about making sure that backup path in the nw-setuptui is the same as the path in which your backup is stored.	IDD
1.4	26-Nov-18	Fixed broken link to ESA Knowledge Base Article (SADOCS-1624).	IDD