RSA NETWITNESS® SUITE

Physical Host Upgrade Guide

for Version 10.6.5.x - 11.0

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

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

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

March 2018

Contents

Introduction

The instructions in this guide apply to the upgrade of physical hosts to RSA NetWitness® Suite 11.0 exclusively. See the RSA NetWitness® Suite *Virtual Host Upgrade Guide* for instructions on how to upgrade your virtual hosts to 11.0.

NetWitness Suite 11.0 is a major release that affects all products in the NetWitness Suite suite. The components of the suite are the NetWitness Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Entity Behavior Analytics, Event Stream Analysis, Hybrid, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, Warehouse Connector, and Workbench.

CentOS6 to CentOS7 Upgrade

NetWitness Suite 11.0 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.0 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 11.0 Upgrade Path

The supported Upgrade path for RSA NetWitness® Suite 11.0 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 11.0. See the *RSA Security Analytics 10.6.4 Update Guide* (https://community.rsa.com/docs/DOC-79055) 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 11.0.
- On-Prem Virtual to On-Prem Virtual

Caution: The 11.0 upgrade does not support mixed-platform upgrades (for example, it does not support physical to virtual.

Hardware, Deployments, Services, and Features Not Supported in 11.0

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.0.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- Hosts Deployed in AWS (You can deploy AWS hosts in 11.0, but you cannot upgrade AWS hosts deployed in 10.6.5.x.)
- Hosts Deployed in Azure (You can deploy Azure hosts in 11.0, but you cannot upgrade Azure hosts deployed in 10.6.5.x.)
- IPDB service
- Malware Analysis service co-located on the SA Server (Upgrade of Malware Analysis Enterprise is supported in 11.0.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is

supported in 11.0.)

- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
  After you upgrade to NetWitness 11.0, 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 11.0.
- 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 11.0, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.0, ESA sends all alerts to a central Alert system. The local mongo storage in ESA 10.6.5.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 11.0.

The following guidelines should help you determine whether or not to upgrade your ESA hosts to 11.0.

In your 10.6.5.x deployment, if you have:

- One ESA host, with or without Incident Management configured, upgrade to 11.0.
- Multiple ESA hosts configured to use Incident Management – The system 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 11.0.
- Multiple ESA hosts without configuration to use Incident Management and you are connecting to individual ESA hosts to view alerts, do not upgrade to version 11.0.

Note: If you did not use Incident Management in 10.6.5.x, you cannot view the 10.6.5.x ESA alerts in the 11.0 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.0 that will allow Respond to view them. See the *ESA Alert Migration Instructions for 10.6.5.x to 11.0* knowledge base article (https://community.rsa.com/docs/DOC-81680) in RSA Link for instructions on how to run this script.

User Attribute and Role Changes Affecting Investigate

The following changes affect how NetWitness Suite 11.0 handles user and role attributes in the Investigate component.

- User Attributes
  When you upgrade to 11.0, the user attributes (query prefix, session timeout, and query threshold) available in SA 10.6.5.x no longer exist. The same attributes are available at the role level for use.
  As a workaround, if you used the user attributes to restrict user access, apply the RSA NetWitness® Suite 11.0.0.1 patch immediately after you upgrade to 11.0.0.0.
- User and Role Attributes (Query Prefix) is not applicable to Investigate Event Analysis. The user and role attributes, most importantly the query prefix, do not apply to the new Investigate Event Analysis. Any user can modify the URL in browser to access data that should be restricted from viewing even when query prefix is applied.
  As a workaround, apply the RSA NetWitness® Suite 11.0.0.1 patch immediately after you upgrade to 11.0.0.0.

Caution: If you configured user or role attributes in 10.6.5.x, including query prefix, apply the RSA NetWitness® Suite 11.0.0.1 patch immediately after you upgrade to 11.0.0.0. After applying this patch, complete the patch instructions to apply additional security controls.

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 11.0 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 11.0 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.

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

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

1. 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 11.0 *NetWitness SuiteHosts 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 Version 11.0 to find NetWitness Suite 11.0 documents.

Investigate in Mixed Mode

Mixed mode occurs when some services are upgraded to 11.0 and some are still on 10.6.x. This happens when you upgrade to 11.0 in phases.

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

After you upgrade all services to 11.0, 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 11.0 and some are still on 10.6.x), when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads.

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

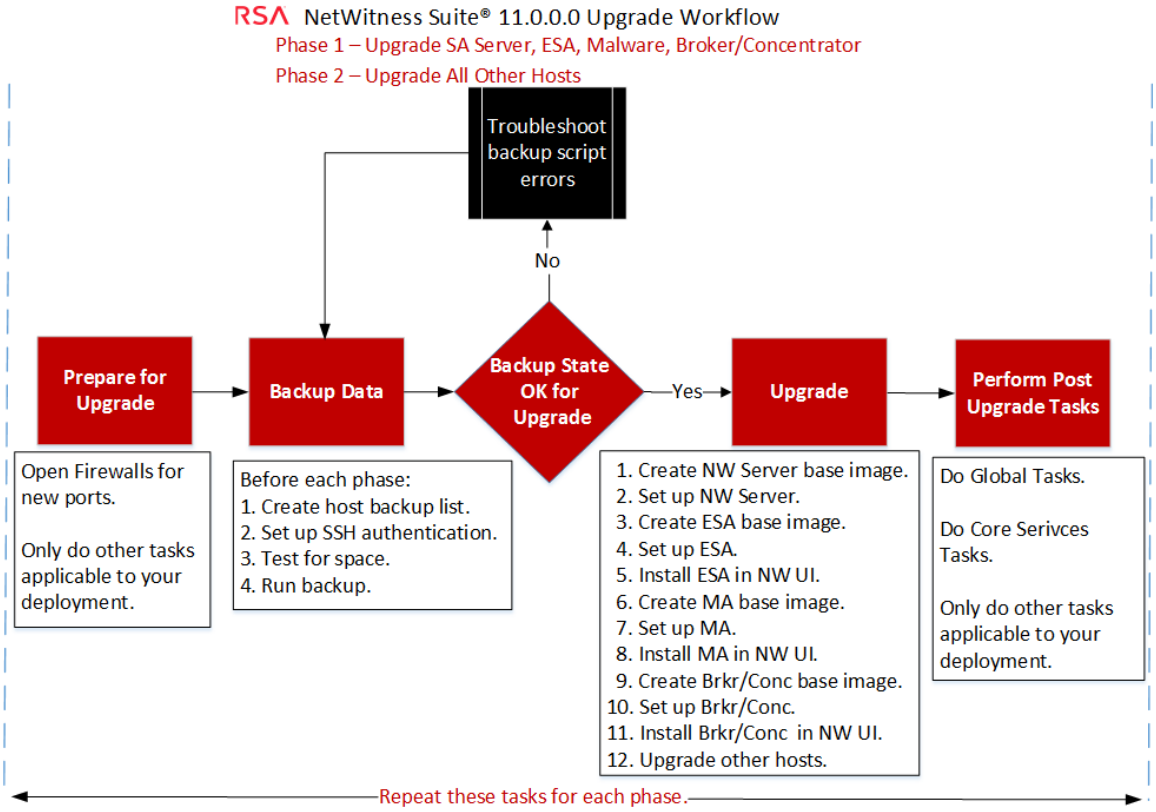
During a phased update, you can disable the `sdk.packets` setting on 10.6.x services to limit the analyst from downloading any PCAPs or logs during mixed mode. After you update all services to 11.0, RBAC works consistently across all services.

This table identifies what you can see and download in Investigate when your NW Server is on version 11.0 connected to services at a lower version.

Connecting Service Version	Affected View	User Role	Can See	Can Download Successfully	Can Download with Errors
11.0 Broker -> 10.x Concentrator -> 10.x Packet Decoder/Log Decoder	Events View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Reconstruction View	Analyst		PCAP	File archive is downloaded but cannot unzip
	Event Analysis View	Analyst		PCAP	Error Retrieving Payload from Service for Payload, Request Payload, Response Payload
	Event Reconstruction View	Admin			Files archive is downloaded but cannot unzip
11.0 Broker -> 11.0 Concentrator ->11.0 Decoder/Log Decoder	Event Reconstruction View	Analyst and Data Privacy Officer	RBAC permitted items		Files archive is downloaded but cannot unzip PCAPs and logs are downloaded as zero bytes
	Event Reconstruction View				

Upgrade Workflow

The following diagram illustrates the RSA NetWitness® Suite 11.0 upgrade workflow.



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 11.0.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Suite 11.0. These tasks are organized by the following categories.

- Global
- Reporting Engine
- Respond and Incident Management
- Warehouse Connector

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 11.0.

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
NW Server	ESA - Context Hub	50022 (SSL/TCP)	Dave - Need verification

ESA Host

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

All NetWitness Suite core ports are listed in the "Network Architecture and Ports" topic in the *RSA NetWitness® Suite Deployment Guide* in case you need to reconfigure NetWitness Suite services and firewalls. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 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 the `/etc/fstab` File

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

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

[ASOC-46625 for ASOC-43895] Task 4 - Delete LIVECONTENT from the Mongo Database

Perform these steps to clean up LIVECONTENT records from the `license_stats` collection of the LES Mongo database.

SSH to the NetWitness Server and run the following commands:

1. `mongo les`
2. `db.getCollection('license_stats').remove({ "category" : "LIVECONTENT" })`
3. `quit()`

Reporting Engine

(Conditional) Task 5 - Unlink External Storage

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

In these steps:

- `/home/rsasoc/rsa/soc/reporting-engine/` is the Reporting Engine home directory.
- `/externalStorage/` is where the external storage is mounted.

1. SSH to the Reporting Engine host and log in with your `root` credentials.
2. Stop the Reporting Engine service.
   `stop rsasoc_re`
3. Switch to `rsasoc` user.
   `su rsasoc`
4. Change to the Reporting Engine the home directory.
   `cd /home/rsasoc/rsa/soc/reporting-engine/`
5. Unlink the `resultstore` directory mounted to external storage.
   `unlink /externalStorage/resultstore`
6. Unlink the `formattedReports` directory mounted to external storage.
   `unlink /externalStorage/formattedReports`

Respond and Incident Management

(Conditional) Task 6 - Disable Incident Management Data Retention

Complete the following procedure to disable Incident Management data retention jobs in 10.6.5.x

1. Log in to RSA Security Analytics 10.6.5.x.
2. Go to **Incident Management** > **Configure** > **Retention Scheduler**.
3. Uncheck the **Enable data retention scheduler** checkbox and click **Apply**.

Warehouse Connector

(Conditional) Task 7 - Copy `keytab` files in `root` or `etc` Directory Stored in Other Directory

Copy the `keytab` files in the `root` or `etc` directory if it is stored in some other directory.

1. Record the absolute path of NFS mount directory and the `keytab` file.
   You need this information to restore the Warehouse Connector after upgrade.
2. Unmount the NFS directory.
   a. SSH to the Warehouse Connector and log in with `root` credentials.
   b. Submit the following commands to unmount the NFS directory.
      `umount <NFS-absolute-path>`

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.5.x is the first step in upgrading from 10.6.5.x releases to 11.0.

Note: It is important that you place Custom Certificate files and any other certificate authority (CA) files in the `/root/customcerts` folder to ensure that these certificate files are backed up. Your custom certificate files that are placed in this directory will be automatically restored during the upgrade process. After upgrading to 11.0, your custom certificate files will be located in `/etc/pki/nw/trust/import`. For more information about backing up these types of files, see step 1 in For All Host Types

Caution:
1) These services are not supported in the 10.6.5.x backup and upgrade process.
- IPDB
- All in One servers
- Malware Analysis Co-Located on the NetWitness Server
- Standalone Warehouse Connector

2) There is a known issue if you have Active Directory users configured in 10.6.5.x. You have two options to address this issue:
• Apply the 10.6.4.2 patch before you back up your data for the 11.0 upgrade.
• If you failed to apply the 10.6.4.2 patch, you can apply the 11.1.0.1 patch immediately after you upgrade to 11.0.

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)

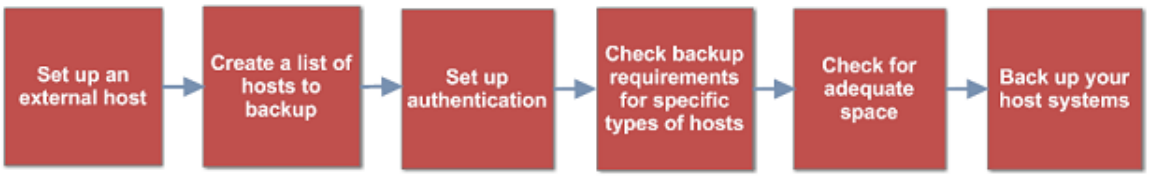
- **Packet Hybrid**
- **Virtual Log Collector**

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 11.0.", in the "Global" section of the Post Upgrade Tasks.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the `/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of Post Upgrade Tasks.

Note: If you have problems during the backup or upgrade processes and you lose data, contact RSA Customer Support (https://community.rsa.com/docs/DOC-1294) for assistance.

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 Version 11.0 to find NetWitness Suite 11.0 documents.

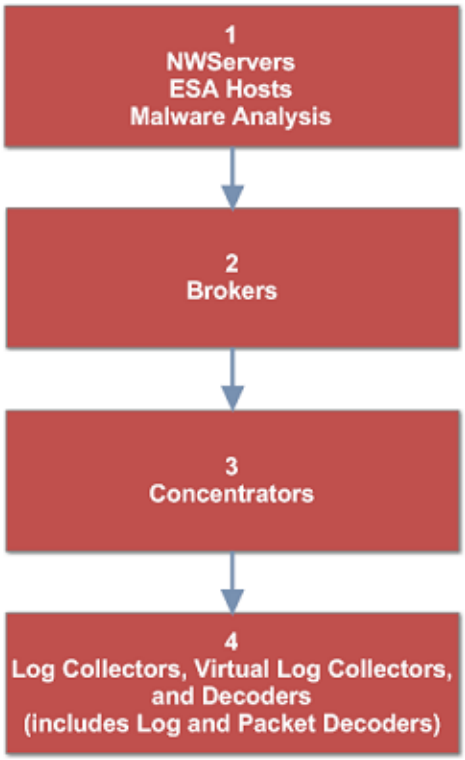
Note: If you have used the 10.6.x versions of the backup and restore scripts on your 10.6.5 hosts, you must still run all the scripts listed here.

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 to 11.0.

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 to remove pre-existing entries from the file so that the file contains only those hosts that are currently being backed up.
    For more information, see Post Backup Tasks.
- If any host systems are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the `all-systems` file is created, you must edit the `all-systems` file manually and add the missing information for these hosts.
- The `get-all-systems.sh` script generates a list of hosts that were defined in the NetWitness Suite user interface. Ensure that all hosts and services are provisioned properly. If any hosts or services are not provisioned properly, they will not be backed up. RSA recommends that when you add hosts and services to NetWitness Suite, you use the NetWitness Suite user interface to ensure that they are provisioned properly. However, if there are any hosts or services that were not defined in the user interface, you must add them to the `all-systems` file manually.

- At the end of the `get-all-systems.sh` script, the script will check for any differences between the systems that the NetWitness Server has listed, and the ones for which the script was able to find all the required information. If any Node ID's or system names are listed as missing, verify the existence of those systems, that their services are all running, and that they are properly communicating with the NetWitness Server. (Any Windows Legacy Collectors or 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 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 11.0.
- Stops all the collection protocols in the Log Collector service.
- Saves the list of Plugin accounts and RabbitMQ accounts.
- Configures the RabbitMQ server so that new events cannot be published to it any longer. Consumers of events in the queues, such as shovels and Log Decoder Event Processors, will continue to run.
- Waits until the Log Collector queues are empty.
- Stops the Log Collector service.
- Creates a marker file indicating that the Log Collector has been successfully prepared for upgrade.

Troubleshooting Information

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

- Sends informational, warning, and error messages to the console.
- Saves a session log in the `/var/log/backup/` directory.

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

- Log Collector queues with events but without consumers are found.
- Unable to stop the Puppet Agent service.
- Unable to stop a collection protocol in the Log Collector service.
- Unable to block event publishers to the RabbitMQ server.
- Unable to or taking too long for queue events to be consumed. The script makes 30 attempts waiting for the events to be consumed. After each attempt, it sleeps for 30 seconds.
- Unable to stop the Log Collector service.

For more information about troubleshooting, see Appendix A. Troubleshooting.

For Integrations with Web Threat Detection, NetWitness SecOps Manager or NetWitness Endpoint: List RabbitMQ Usernames and Passwords

On the 10.6.5.x host, on the NetWitness Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.0. upgrade, you can restore RabbitMQ user accounts.

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

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

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

For Bluecoat Event Sources

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

- If key material exists in `/root/vsftpd/` directory in 10.6.5.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.

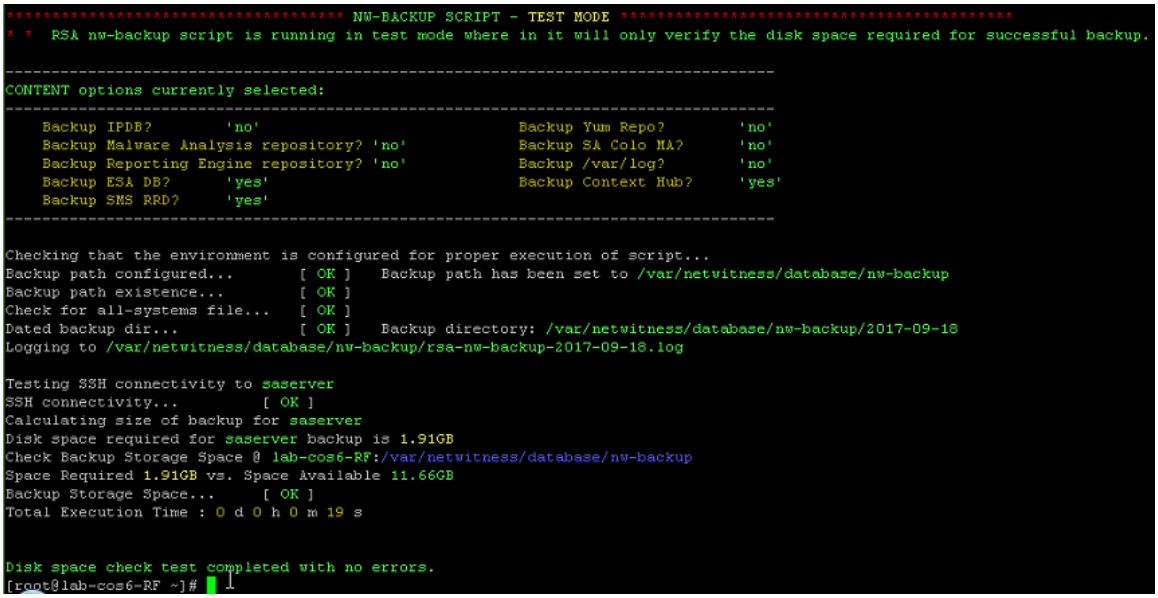
To check for adequate disk space:

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 11.0.

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

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

Usage:

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

General Options

`-u : This option is required for upgrading to 11.0. Enables the upgrade flag to run backup for upgrading to 11.0. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

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

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

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

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

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

-b <path to write backups> : path to the location for storing backup files on a backup server. **For upgrading to 11.0, please use the default location!** Default: (/var/netwitness/database/nw-backup)

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

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 the10.6.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 11.0. 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 11.0.

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

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

4. When the backup has completed, to ensure that the intended files were backed up, you can run the following command to see a list of all the files that were backed up:

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   The following archive files are created:

   For all hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `tar checksum` files

   `<hostname-IPaddress>-network.info.txt`

   For 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 11.0.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.0. upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

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

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

In addition to the files listed above, the following files will be generated on 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 host's backup path .

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

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

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

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

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

Before you upgrade to 11.0., ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

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

Note: The default paths for backup files are:
- Security Analytics server hosts:/var/netwitness/database/nw-backup
- ESA hosts:/opt/rsa/database/nw-backup
- Malware hosts: /var/lib/rsamalware/nw-backup

Required Files for Security Analytics 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)

Upgrade Tasks

This topic contains the tasks you must complete to upgrade Security Analytics 10.6.5.x to NetWitness Suite 11.0 .

Caution: 1.) Make sure that you backed up your Security Analytics 10.6.5.x data before attempting to upgrade to NetWitness Suite 11.0 .
2). Run the backup immediately before upgrading the hosts for each phase so that the data to avoid restoring stale data.
3.) This guide applies to physical host upgrades exclusively. If have physical and virtual hosts in your deployment, see the *RSA NetWitness® Suite 11.0 Virtual Host Upgrade Guide* for the steps to upgrade virtual hosts. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

There two phases that you must complete in the order shown.

- Phase 1 -Upgrade SA Server, Event Stream Analysis (ESA), and Malware Analysis 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 11.0 and they will not be available until the warm up completes.

- Phase 2 -Upgrade All Other Hosts

Phase 1 -Upgrade SA Server, Event Stream Analysis, Malware Analysis Hosts, and Broker or Concentrator

Task 1 - Upgrade the 10.6.5.x SA Server to 11.0 NW Server

Follow the instructions under Upgrade 10.6.5.x SA Server Host to 11.0 NW Server Host.

Task 2 - Upgrade 10.6.5.x ESA to 11.0

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 11.0 and they will not be available until the warm up completes.

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.0 to upgrade your ESA hosts.

1. Create the base image on your primary ESA host, set it up 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, create the base image on your 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 - Upgrade 10.6.5.x Malware Analysis to 11.0

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.0 .

Task 4 - Upgrade 10.6.5.x Broker or 10.6.5.x Concentrator to 11.0

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.0 .

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.0 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 All Other 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 Upgrade Non-NW Server Host to 11.0 .
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in the Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh.
2. Stop data capture on the Log Decoder.

3. Complete the steps in Upgrade Non-NW Server Host to 11.0 .
4. Restart data capture on Log Decoder.

> **Note:** After you upgrade, you will restart log collection after completing the Post Upgrade Tasks in the **Post Upgrade Tasks**.

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described the Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh.
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.0`
   b. Run the following command to create backup.
   `./nw-backup.sh -u`
   See Backup Instructions for detailed procedures on how to back up the host.
3. Make sure the backup host contains the VLC backup in the following format.
   `<hostname>-<IPaddress>-root.tar.gz`
   `<hostname>-<IPaddress>-root.tar.gz.sha256`
   `<hostname>-<IPaddress>-backup.tar.gz`
   `<hostname>-<IPaddress>-backup.tar.gz.sha256`
   `<hostname-IPaddress>-network.info.txt`
   `all-systems-master-copy`
4. Power off the 10.6.5.x VLC so that a new 11.0 VM can be created with the same network configuration.
5. Deploy a fresh NetWitness 11.0 Non-NW Server host using the 11.0 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 Upgrade a 10.6.5.x non-SA Server Host to 11.0 for the rest of the NetWitness Suite components . Make sure that you select **Log Collector** for the service in step 12.

All Other 10.6.5.x Hosts to 11.0

Follow the instructions under Upgrade a 10.6.5.x non-SA Server Host to 11.0 .

Upgrade the 10.6.5.x SA Server Host to the 11.0 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 11.0 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 11.0 .

Complete the following steps to upgrade the 10.6.5.x SA Server host to the 11.0 NW Server host.

1. Create a base image on the host.

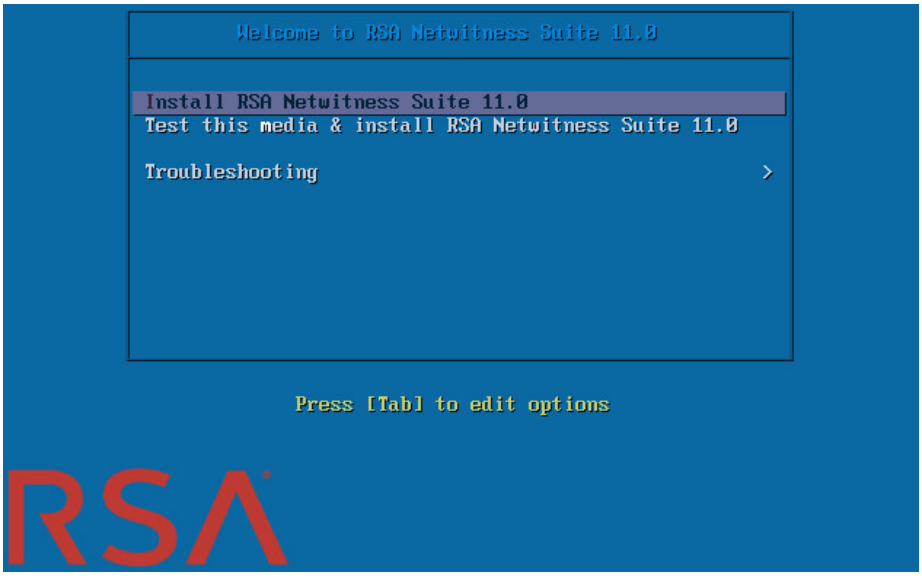
a. Attach media (that is Build Stick or DVD ISO) to the host.
You must use the build stick labeled "OEMDRV".
See the *RSA NetWitness Suite 11.0 Build Stick Instructions* for more information.

- Hypervisor installs - use either the DVD or USB ISO images.
- Physical media - use the DVD ISO to create a bootable optical disk using user provided imaging software or the USB ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the USB ISO. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.
- iDRAC installations - the virtual media type is:
  - **Virtual Floppy** for mapped flash drives.
  - **Virtual CD** for mapped optical media devices or ISO files.

b. Log in to the host with and reboot it.

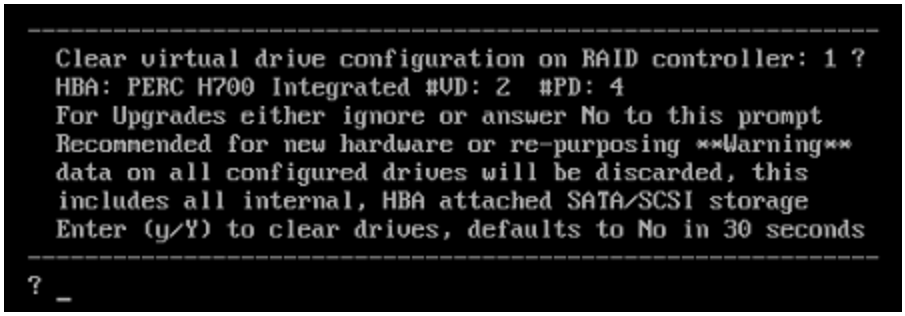
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

c. Select **F11 (boot menu)** during reboot to select a boot device and boot to the connected media.
After some system checks during booting, the following **Welcome to RSA NetWitness® Suite 11.0** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.
DO: Need New Screenshot.

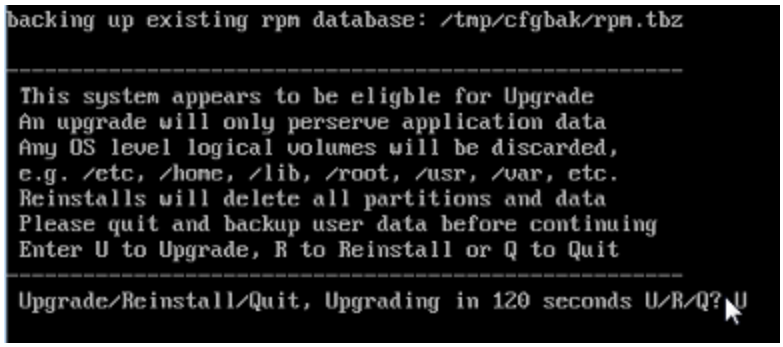


d. Select **Install RSA Netwitness Suite 11.0** (default selection) and press **Enter**.
The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**

prompt that asks you to format the drives.

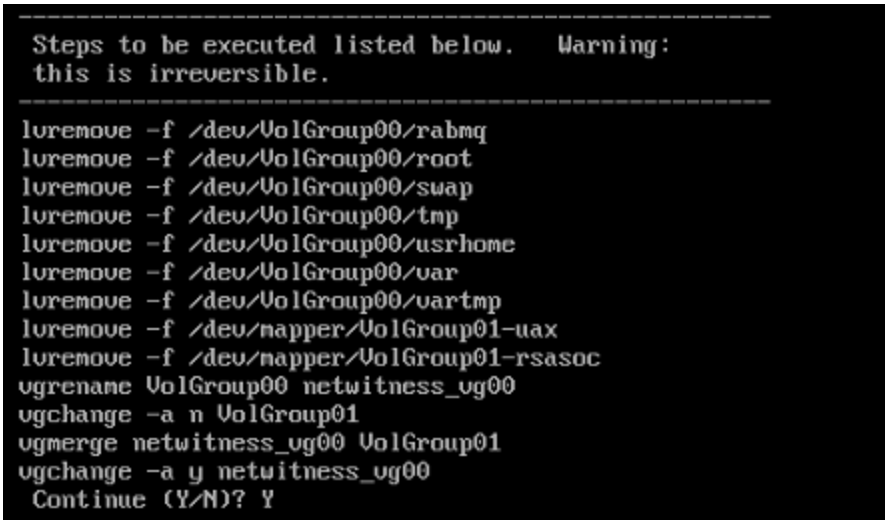


e. Press **Enter** to continue.
The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives. The **Upgrade/Reinstall/Quit(U/Q/R?** prompt is displayed.



f. Type **U** to upgrade the host.
If you ignore the prompt, it will select U in 120 seconds.
It takes a few minutes for CentOS7 components to install. The installation program displays the components as they are installed, which varies depending on the appliance. When CentOS7 installation is complete, the following **Continue (Y/N)?** prompt is

displayed.



g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.
The old operating system is about to be removed. Continue (Y/N)? warning is displayed.

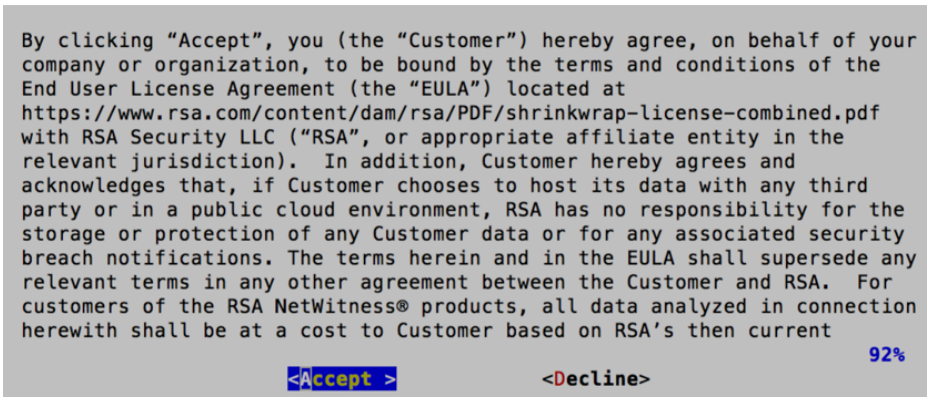
h. Type **Y** and press **Enter** to confirm that you want to replace the operating system.
When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

Caution: Do not reboot the attached media (that is, the Build Stick or DVD ISO).

i. Log in to the host with the root credentials.

2. Run the `nwsetup-tui` command to set up the host.
This initiates the Setup program and the EULA is displayed.

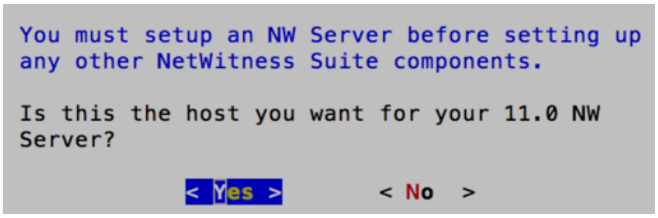
Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use Tab key to move to and from commands (such as **<Yes>**, **<No>**, **<OK>**, and **<Cancel>**. Press **Enter** to register your command response and move to the next prompt.
2.) The Setup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



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

   The "Is this the NW Server" prompt is displayed.

   DO: Need New Screenshot.

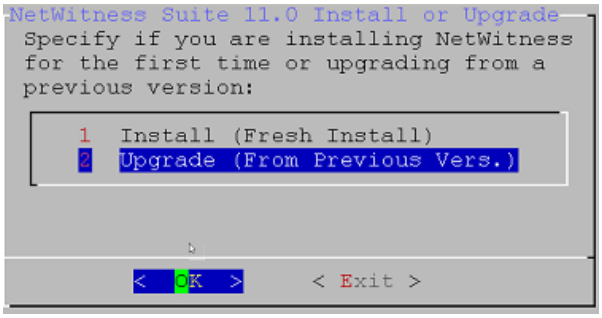


Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must restart the step up program and complete the all the steps (steps 2 through 11) to correct this error.

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

   Choose **No** if you already upgraded the NW Server to 11.0 .

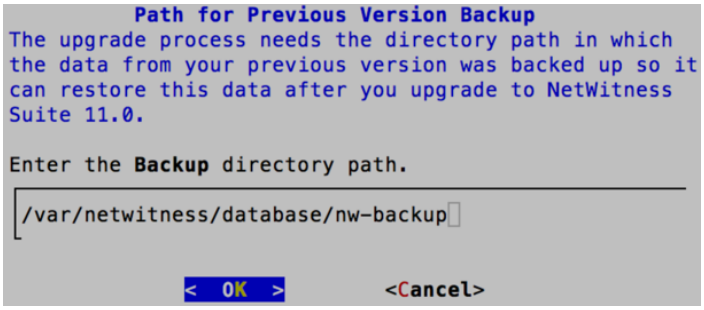
   The Install or Upgrade prompt is displayed.



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

   The backup path prompt is displayed.

DO: Need New Screenshot.



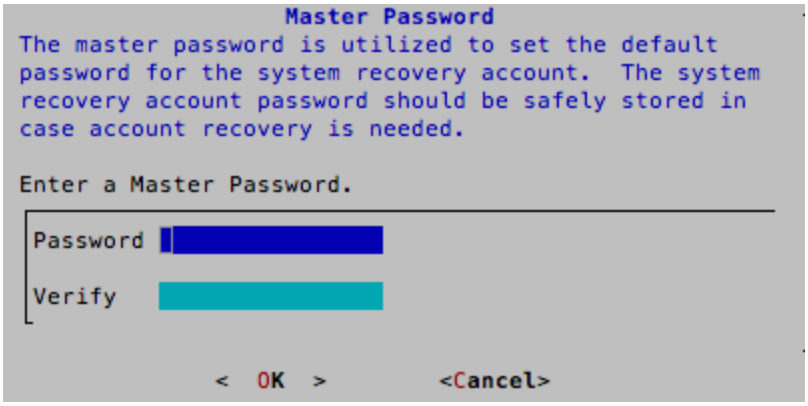
6. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.

   The Master Password prompt is displayed.

   The following list of characters are supported for Master Password and Deployment Password:

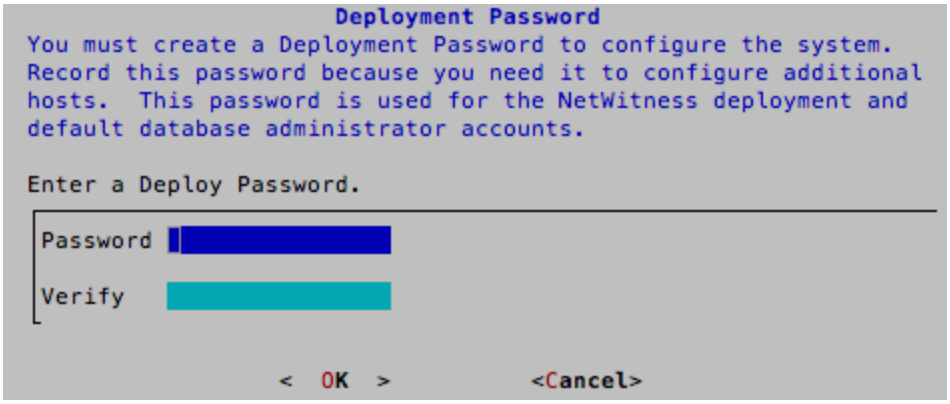
   - Symbols : ! @ # % ^ +
   - Numbers :0-9
   - Lowercase Characters : a-z
   - Uppercase Characters : A-Z

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



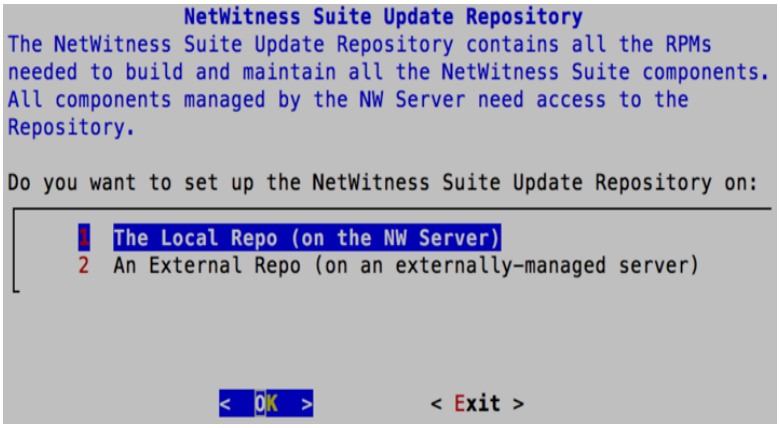
7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

The Deployment Password prompt is displayed.



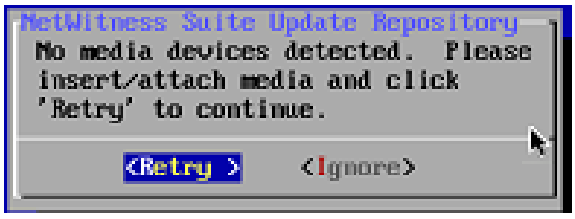
8. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.

   The Update Repo prompt is displayed.

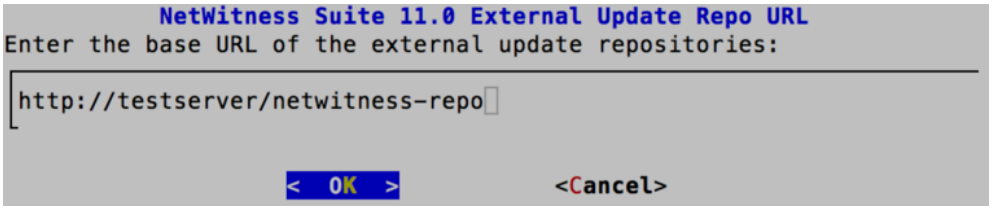


9. Use the down and up arrows to select the location from which you want to apply version updates to your hosts, tab to **OK**, and press **Enter**.

   - If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0 . If the program cannot find the attached media, you receive the following prompt.

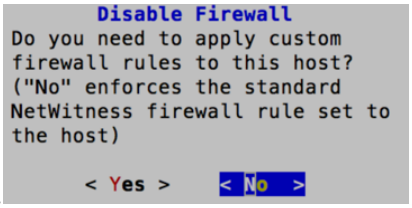


- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates.
  DO: Need New Screenshot.



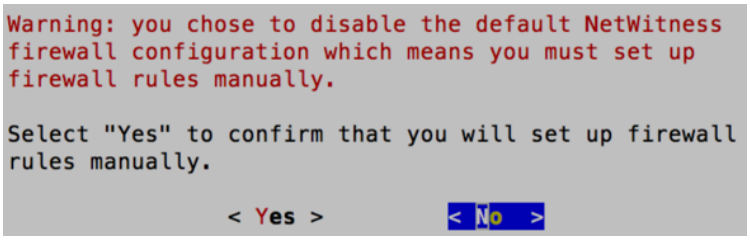
  Enter the base URL of the NetWitness Suite external repo and click **OK**.
  See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Suite 11.0 Hosts and Services Getting Started Guide* for instructions. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

The disable or use standard firewall configuration prompt is displayed.



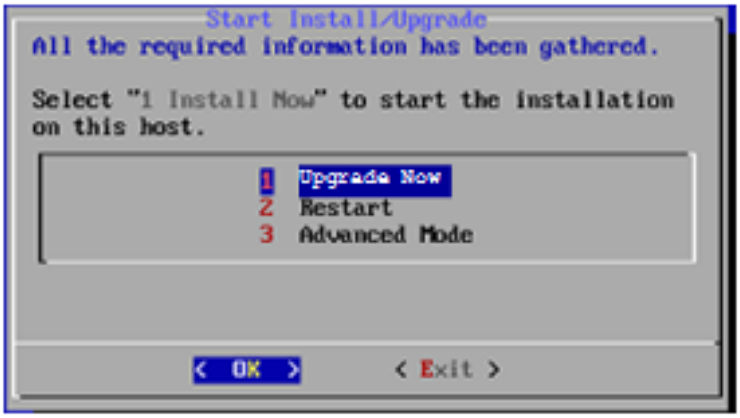
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

- If you select Yes, confirm your selection.



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

The start upgrade prompt is displayed.



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 11.0 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)
```

Upgrade a 10.6.5.x non-SA Server Host to 11.0 .

Make sure that you backed up 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 11.0 so that the data is as recent as possible.

Complete the following steps to upgrade a 10.6.5.x non-SA Server Host to 11.0 .

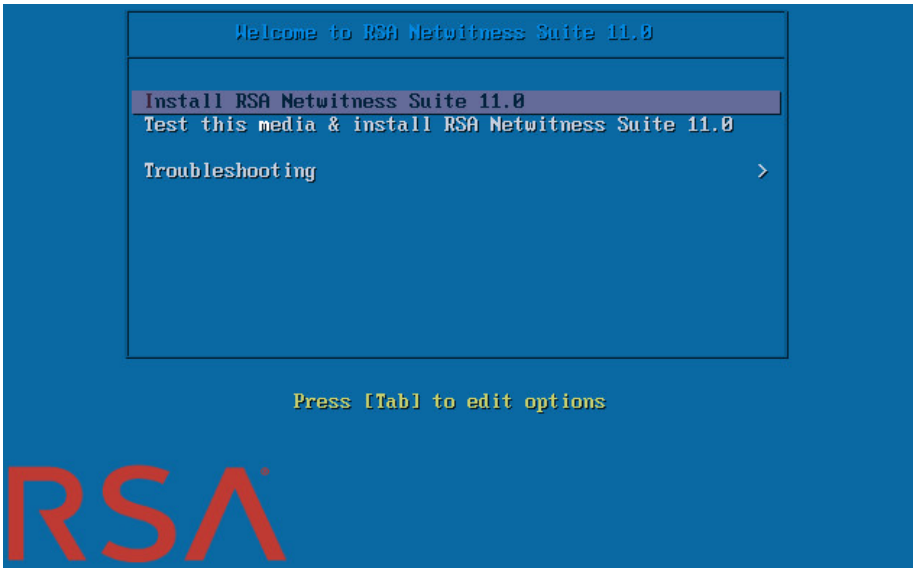
1. Create a base image on the host.
   a. Attach media (that is Build Stick or DVD ISO) to the host.
      See the *RSA NetWitness Suite 11.0 Build Stick Instructions* for more information.

- Hypervisor installs - use either the DVD or USB ISO images.
- Physical media - use the DVD ISO to create a bootable optical disk using user provided imaging software or the USB ISO to create bootable flash drive media using the Universal Netboot Installer (UNetbootin) or another suitable imaging tool. See the *RSA NetWitness® Suite Build Stick Instructions* for information on how to create a build stick from the USB ISO. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.
- iDRAC installations - the virtual media type is:
  - **Virtual Floppy** for mapped flash drives.
  - **Virtual CD** for mapped optical media devices or ISO files.

b. Log in to the host and reboot it.

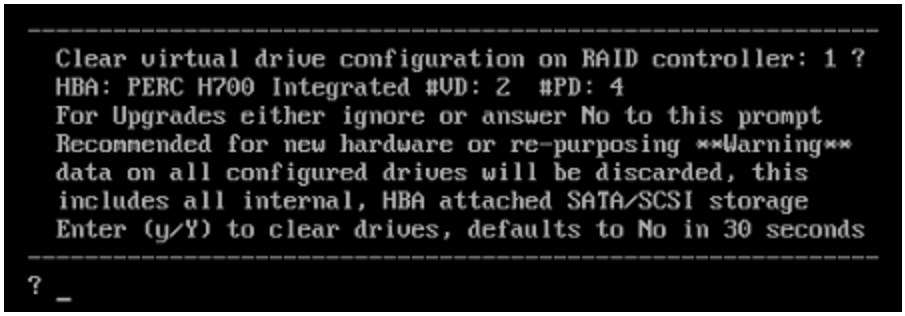
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

c. Select **F11 (boot menu)** during reboot to select a boot device and boot to the connected media.
After some system checks during booting, the following **Welcome to RSA NetWitness® Suite 11.0** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.
DO: Need New Screenshot.

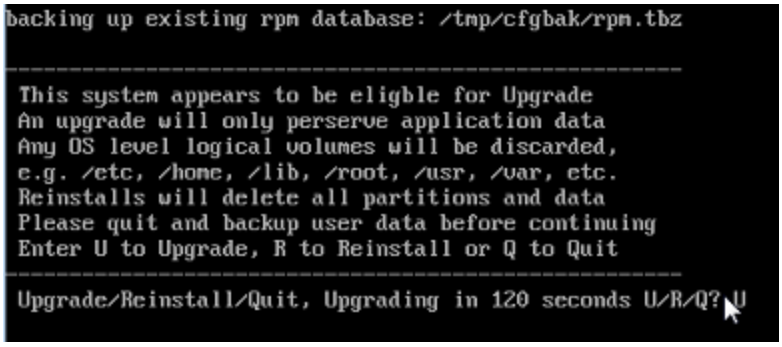


d. Select **Install RSA Netwitness Suite 11.0** (default selection) and press **Enter**.
The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**

prompt that asks you to format the drives.

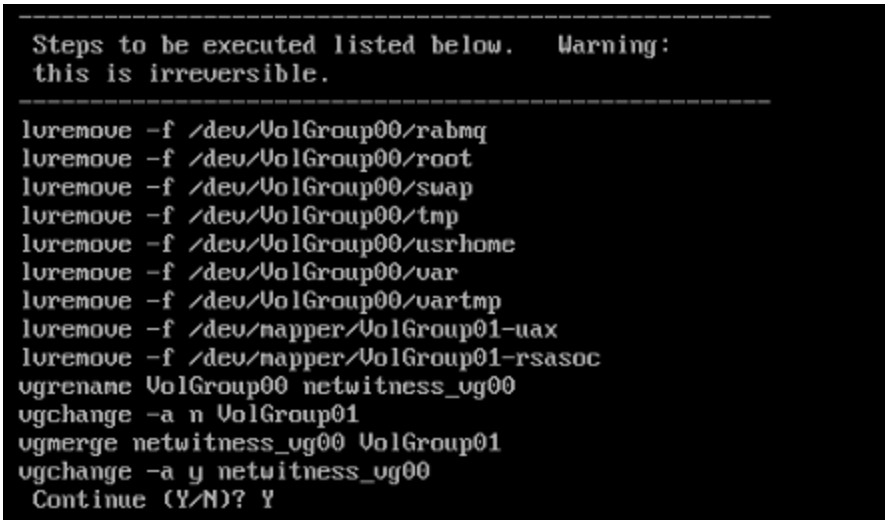


e. Press **Enter** to continue.
   The default action is **No**, so if you ignore the prompt and it will select **No** in 30 seconds and will not clear the drives. The **Upgrade/Reinstall/Quit (U/R/Q?)** prompt is displayed.



f. Type **U** to upgrade the host.
   If you ignore the prompt, it will select **U** in 120 seconds.
   It takes a few minutes for CentOS7 components to install. The installation program displays the components as they are installed which varies depending on the appliance. When CentOS7 installation is complete, the following **Continue (Y/N)?** prompt is

displayed.



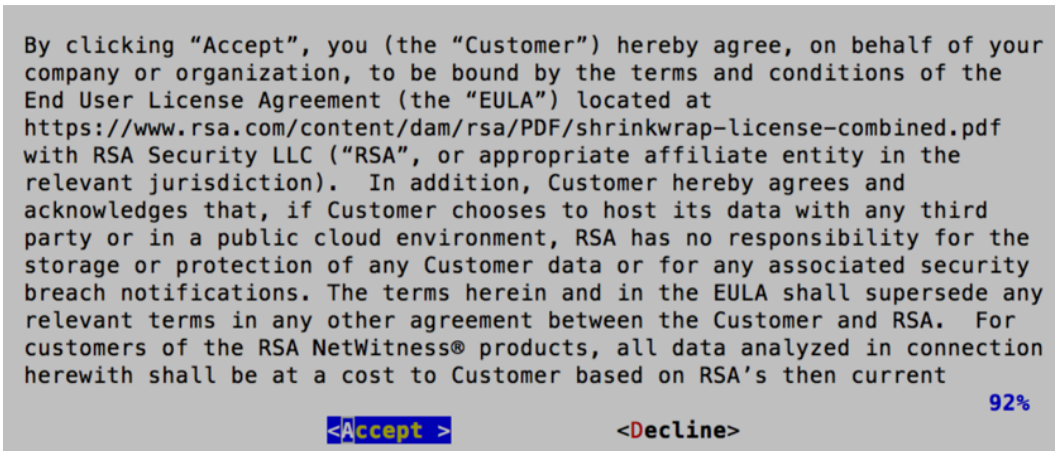
g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.
The old operating system is about to be removed. Continue (Y/N)? warning is displayed.

h. Type **Y** and press **Enter** to confirm that you want to replace the operating system.
When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

Caution: Do not reboot the attached media (that is the Build Stick or DVD ISO).

i. Log in to the host with the root credentials.

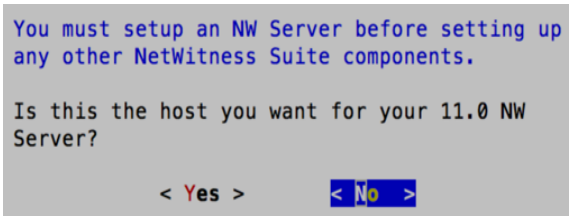
2. Run the `nwsetup-tui` command to set up the host.
This initiates the Setup program and the EULA is displayed.



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

   The "Is this the NW Server" prompt is displayed.

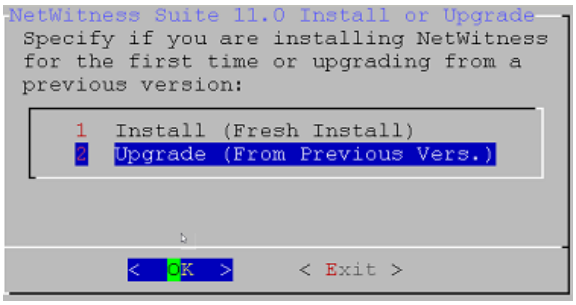
   DO: Need New Screenshot.



Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must restart the step up program and complete the all the steps (steps 2 through 11) of Upgrade the 10.6.5.x SA Server Host to the 11.0 NW Server Host to correct this error.

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

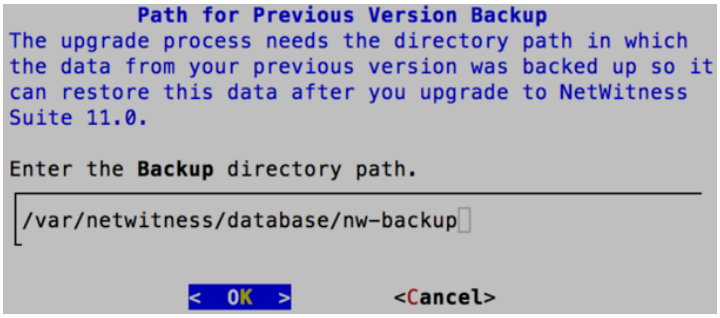
   The Install or Upgrade prompt is displayed.



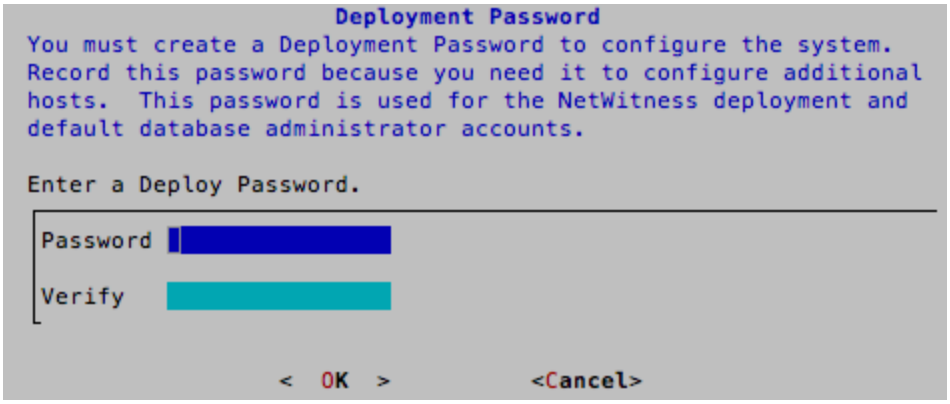
5. Use down arrow to select **2 Upgrade (From Previous Vers.)**, tab to **OK**, and press **Enter**.

   The backup path prompt is displayed.

DO: Need New Screenshot.

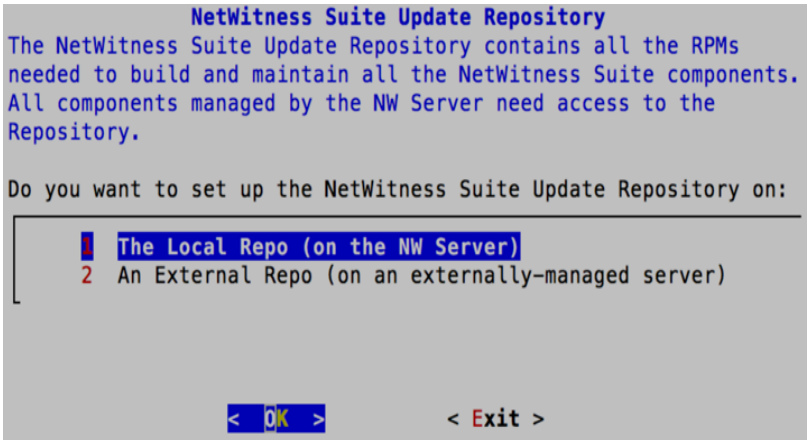


6. Tab to **OK** and press **Enter** if want to keep this path. If not, edit the path, tab to **OK** and press **Enter** to change it.
   The Deployment Password prompt is displayed.



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

7. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**.
   The Update Repo prompt is displayed.
   Select the same repo you selected when you upgraded the NW Server Host for all hosts.



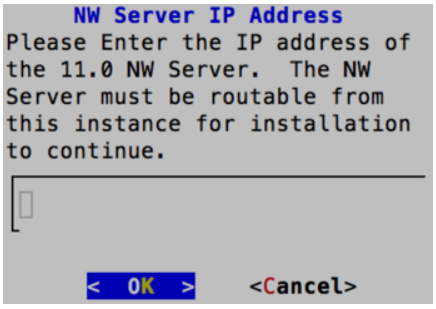
8. Use the down and up arrows to select the location from which you want to apply version updates to your hosts, tab to **OK**, and press **Enter**.

   - If you select **1 The Local Repo (on the NW Server)** the setup program makes sure that you have the appropriate media attached to the host (that is, a build stick or DVD) from which it can retrieve the Install or Update the hosts to NetWitness Suite 11.0 .

   - If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access RSA updates and CentOS updates. Enter the base URL of the NetWitness Suite external repo and click **OK**.

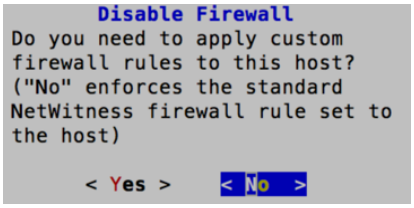
   The NW Server IP Address is displayed.

   DO: Need New Screenshot.



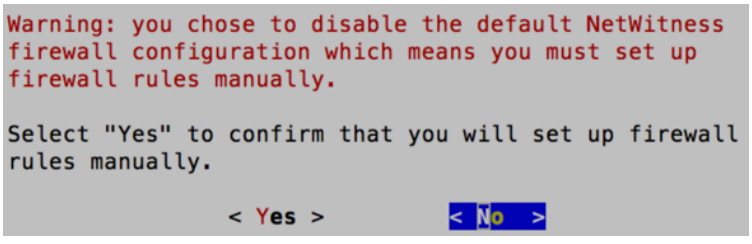
9. Type the IP address of the NW Server, tab to **OK**, and press **Enter**.

   The disable or use standard firewall configuration prompt is displayed.



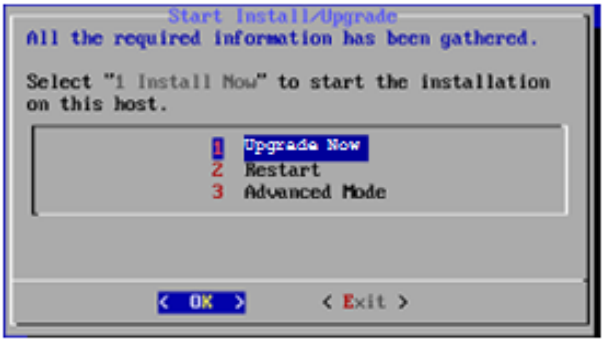
10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

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



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

The start upgrade prompt is displayed.

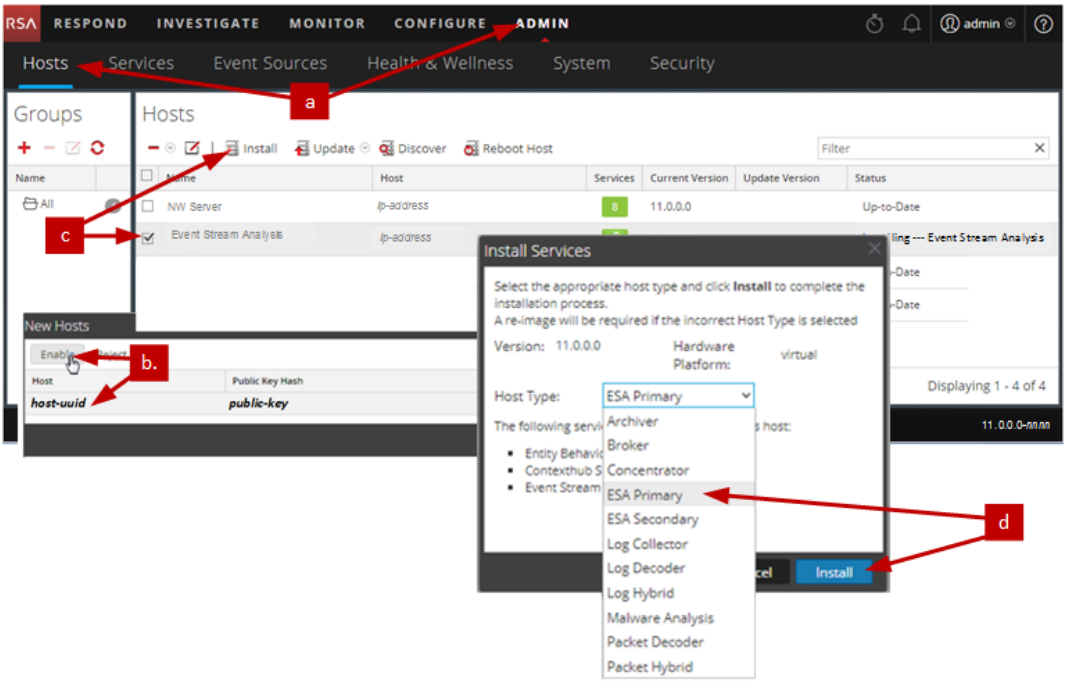


11. Select 1 **Upgrade Now**, tab to **OK**, and press **Enter**.
    When "Installation complete" is displayed, you have upgraded the host to the 11.0 .
12. Install the service on this host:
    a. Log into NetWitness Suite.
       Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Suite Login screen.
    b. Click **ADMIN** > **Hosts**.
       The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

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

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

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



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

Update or Install Legacy Windows Collection

Refer to the *RSA NetWitness 11.0 Legacy Windows Collection Guide* on RSA Link (https://community.rsa.com/docs/DOC-75593) for details about how to install or update Legacy Windows collection.

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

Post Upgrade Tasks

This topic contains the tasks you must complete after you upgrade your hosts from 10.6.5.x to 11.0. These tasks are organized by the following categories.

- Global
- NetWitness Endpoint
  RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, and 4.4 only for NetWitness Suite 11.0.
- Event Stream Analysis
- Log Collection
- Reporting Engine
- Respond
- NetWitness SecOps Manager
- Security
- Warehouse Connector
- Hardware-Related Tasks

Global Tasks

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

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.0. before you remove the backup-related files from the local directories on your 11.0. hosts.

Backup `.tar` Files

After all the hosts are upgraded to 11.0, you must remove:

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

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

Task 2 - Restore NTP Servers

You must use the NetWitness Suite 11.0 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 11.0 System Configuration Guide* for detailed instructions on how to add NTP servers. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Task 3 - 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 Version 11.0 to find NetWitness Suite 11.0 documents.

(Conditional) Task 4 - 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 5 - 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.x.

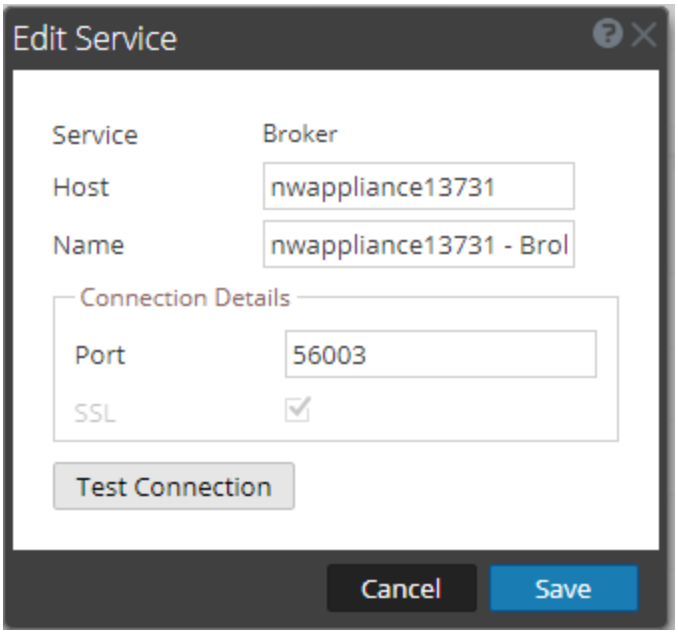
NetWitness Suite 11.0 cannot communicate with the core services for these customers because they are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. Log in to NetWitness Suite
2. Go to **ADMIN** > **Services**.
3. Select each core service and change there ports from Non-SSL to SSL ports.

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

4. Click (Edit) from the SERVICES view toolbar.
   The Edit Srvice dialog is displayed.

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



NetWitness Endpoint

Task 6 - 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 11.0, 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 7 - 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 11.0.

1. Log in to NetWitness Suite 11.0.
2. Click **ADMIN** > **System** > **ESA Analytics**.
   The Suspicious Domains modules, Command and Control (C2) for Packets and C2 for Logs, require a whitelist named "**domains_whitelist**".
3. Conditional - If your previous Automated Threat Detection whitelist appears on the **Lists** tab of the Context Hub service:
   a. Click **ADMIN**> **Services**, select the Context Hub service, in the action commands () drop-down menu, click **View** > **Config** > **Lists** tab).
   b. Rename your old Automated Threat Detection whitelist to "`domains_whitelist`" for the Suspicious Domains module.

For more information, see the *NetWitness Suite Automated Threat Detection Guide* and the "Configure ESA Analytics" section of the *NetWitness Suite ESA Configuration Guide*. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Task 8 - 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 9 - Enable Threat - Malware Indicators Dashboard

In 11.0, 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 11.0.
2. Set datasource for new dashlets.
   See "Dashlets" in the RSA Link (https://community.rsa.com/docs/DOC-81463).

Task 10 - (Conditional) For Automated Threat Detection - Change the "Group By" from “Domain” back to “Domain for Suspected C&C".

If you used Automated Threat Detection in 10.6.5.x, you must complete the following steps to change the **Group By** from **Domain** back to **Domain for Suspected C&C**.

1. Log in to NetWitness Suite 11.0.
2. Click **CONFIGURE** > **Incident Rules** > **Aggregation Rule**.
3. Select the **Suspected Command & Control Communication by Domain** Rule, and double-click to open it.
4. Change the **Group By** condition to **Domain**.

For more information, see the *NetWitness Suite Automated Threat Detection Guide*. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Log Collection

Task 11 - Reset Stable System Values for Log Collector after Upgrade

Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.0 to ensure that all collection protocols resume normal operation.

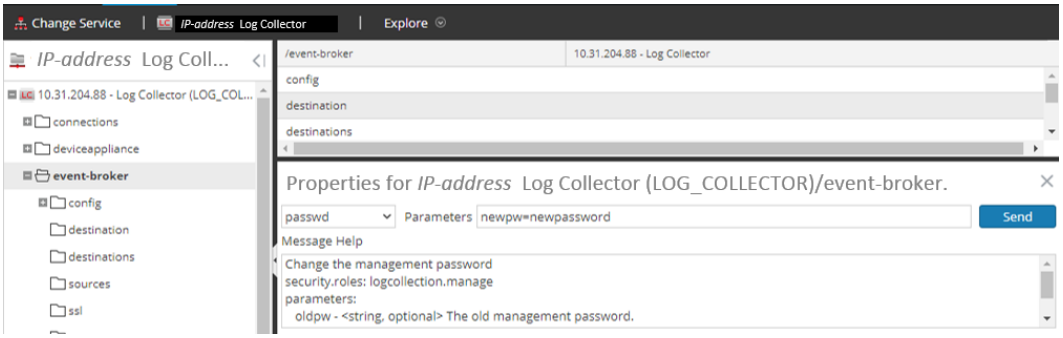
Reset Stable System Values for the Lockbox

The Lockbox stores the key for encrypting event source and other passwords for the Log Collector. The Log Collector service cannot open the Lockbox because of the stable system value changes. As a result, you must Reset Stable System Values for the Lockbox . See "Log Collection: Step 3. Set Up a Lockbox" in the *RSA NetWitness® SuiteLog Collection Configuration Guide* for instructions. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Update Log Collector Service RabbitMQ User Account Password

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

1. Log in to NetWitness Suite.
2. Click **ADMIN** > **Services**.
3. Select the Log Collector service.
4. Click  (Actions) > **View** > **Explore**.
5. Right click `event-broker` > **Properties** .
6. Select `passwd` from the drop-down list, enter `newpw=><newpassword>` in Parameters (where `<newpassword>` is the RabbitMQ user account password), and click **Send**.



(Optional for Upgrades from 10.6.5.x with FIPS enabled for Log Collectors, Log Decoders and Packet Decoders) Task 12 - 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 Version 11.0 to find NetWitness Suite 11.0 documents.

Reporting Engine

Task 13 - 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 11.0.

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 14 - 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 Version 11.0 to find NetWitness Suite 11.0 documents.

Respond

Task 15 - 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 11.0.
   This is the new file for 11.0.

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

Task 16 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.0 and moved them to the following new location:
`/var/lib/netwitness/respond-server/scripts`
If you customized these scripts in 10.6.5.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 11.0 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.5.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.

(Conditional) Task 17 - Enable Disabled 10.6.5.x Incident Management Data Retention

Complete the following procedure to enable the Incident Management data retention jobs you disabled prior to upgrade.

1. Log in to RSA NetWitness® Suite.
2. Go to **ADMIN** > **Services** and select the **Respond server**.
3. Click the  (Actions), **View** > **Explore**.
4. Go to the `respond/dataretention` node.
5. Set the `enable` parameter to `true`.

(Conditional) Task 18 - Restore Custom Analysts Roles

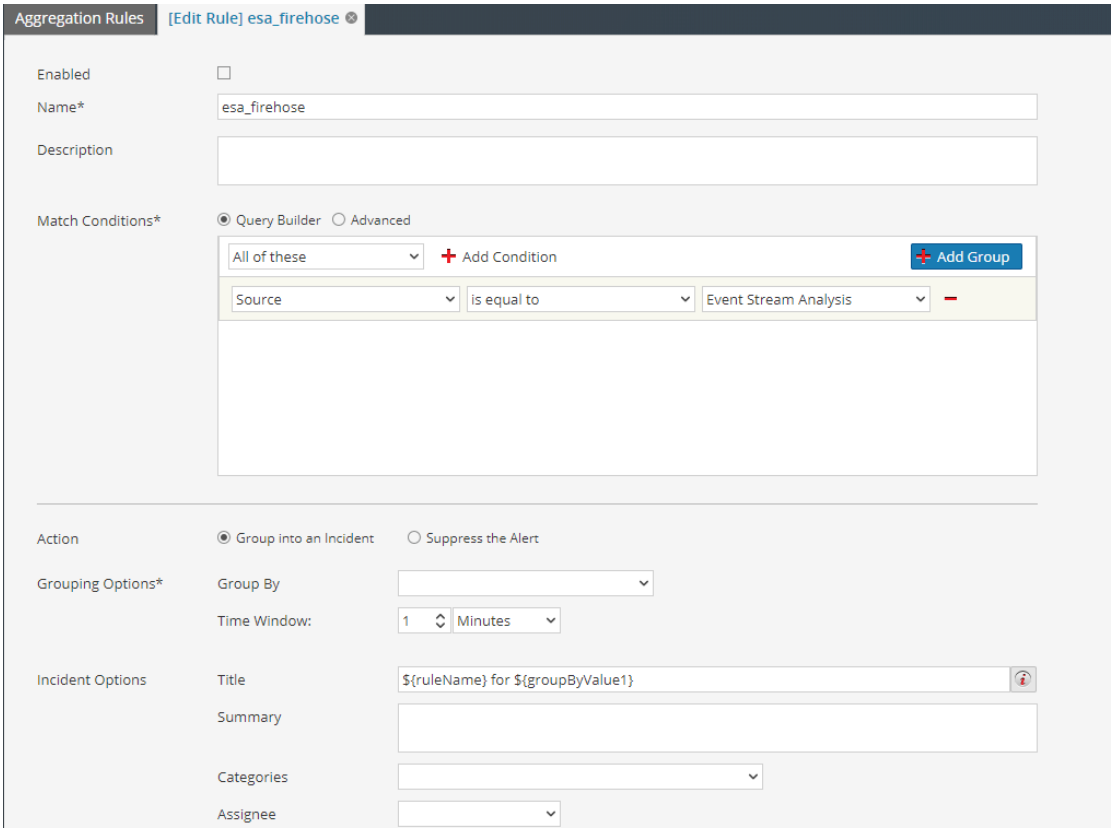
If you had custom analyst roles in 10.6.5.x, you must reinstate them in 11.0. See *Adding Roles and Assigning Permissions for the Roles* in the *RSA NetWitness Suite Warehouse Analytics Guide*. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Task 19 - Add Group By Field to Incident Rules

The **Group By** field is not required in 10.6.5, but it is required in 11.0. After you upgrade to 11.0, incident rules will not have a **Group By** field so you must add them to the rules or the rules will not fire.

Complete the following steps for each incident rule.

1. Log in to RSA NetWitness® Suite.
2. Go to **CONFIGURE** > **Incident Rules** and select a rule.
   The Rule Editor is displayed.



3. In **Grouping Options** field, select the a method in the **Group By** field and click Save. 

NetWitness SecOps Manager

Task 20 - 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 Version 11.0 to find NetWitness Suite 11.0 documents.

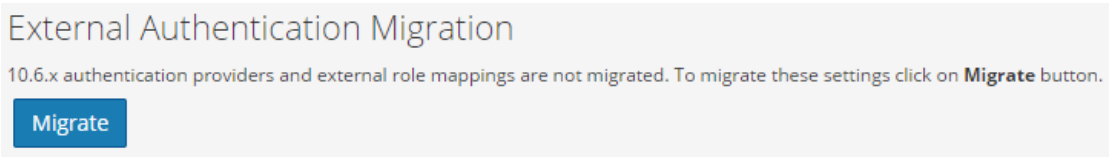
Security

Task 21 - Migrate Active Directory (AD)

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

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

1. Log in to NetWitness Suite with your `admin user` credentials.
2. Click **ADMIN** > **SECURITY** and click the **Settings** tab.
   The following dialog is displayed.



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

Task 22 - 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, you must modify the migrated AD configuration to upload the Active Directory server certificate.

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

1. Log in to NetWitness Suite.
2. Click **ADMIN** > **Security** and click the **Settings** tab.
3. Under **Active Directory Settings**, select an AD configuration and click .
   The Edit Configuration dialog is displayed.

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

Task 23. Address Authentication Failure in 11.0

Users cannot log in to NetWitness Suite User Interface after you upgrade to 11.0 because the Interface cannot retrieve user account information from MongoDB.

- Apply the 11.0.0.1 patch to fix this issue immediately after you upgrade to 11.0.

Task 24 - Reconfigure Pluggable Authentication Module (PAM) in 11.0

You must reconfigure PAM after you upgrade to 11.0. 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 Version 11.0 to find NetWitness Suite 11.0 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.

Warehouse Connector

Task 25 - Restore `keytab` Files, Mount NFS, Install Service

1. Restore the `keytab` files from `<backup-path>/restore` directory.
2. Restore the Kerberos Realm Configuration from the `<backup-path>/restore/etc/krb5.conf` into `/etc/krb5.conf`.
3. (Conditional) If you perform the upgrade from a Non - FIPS environment and the `isCheckValidationRequired` parameter is not enabled in the destination, to configure the SFTP destination:
   a. SSH to the Warehouse Connector host and submit the following commands:
   ```
   cd /root/.ssh/
    mv id_dsa id_dsa.old
   OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_
   dsa.old -out id_dsa
   ```
   You are prompted for the pass phrase.
   b. Enter the Encryption password.
   c. Run the following command.
   ```
   chmod 600 id_dsa
   ```
4. Install the Warehouse Connector.

See the *NetWitness Suite Warehouse Connector Configuration Guide* for instructions. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Task 26 - Refresh Warehouse Connector Lockbox and Start Stream

Note: If the streams have auto start turned on in 10.6.5.x, there will be a small delay before you will see the Warehouse Connector service in the NetWitness Suite User Interface.

1. Refresh the Lockbox of Warehouse Connector.
2. SSH to the Warehouse Connector and log in with root credentials.
3. Restart the service.

   ```
   service nwwarehouseconnector restart
   ```

4. (Conditional) If the auto start was not enabled in 10.6.5.x, you must start the stream manually after the service restarts.

(Conditional) Task 27 - For Warehouse Connector with Log Collector Service, Edit the sshd_config File

If you have a Warehouse Connector service installed with a Log Collector, perform the following steps ensure that both services function correctly:

1. In the `/etc/ssh/sshd_config` file, comment the following line:
   ```
   #Subsystem sftp /usr/libexec/openssh/sftp-server
   ```
2. Add the following sections to the file:

   ```
   # SFTP server settings added for NwLogCollector
   StrictModes no

   Subsystem sftp internal-sftp

   Match User sftp
        AllowTCPForwarding no
        PasswordAuthentication no
        X11Forwarding no
        ForceCommand internal-sftp
        ChrootDirectory /var/lib/logcollector

   Match Group uploads
        ChrootDirectory /var/lib/logcollector/upload_chroot
        X11Forwarding no
        AllowTcpForwarding no
        PasswordAuthentication no
   ```

3. Make sure that the `sshd` file contents are similar to the following example:

   ```
   # Accept locale-related environment variables
   AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_
   MESSAGES
   AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
   AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
   AcceptEnv XMODIFIERS

   # override default of no subsystems
   #Subsystem sftp /usr/libexec/openssh/sftp-server

   # Example of overriding settings on a per-user basis
   #Match User anoncvs
   #      X11Forwarding no
   #      AllowTcpForwarding no
   #      PermitTTY no
   #      ForceCommand cvs server
   ```

```
#disabled CBC mode cipher encryption and MD5 or 96-bit MAC algorithms

Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512

# SFTP server settings added for NwLogCollector
StrictModes no

Subsystem sftp internal-sftp

Match User sftp
     AllowTCPForwarding no
     PasswordAuthentication no
     X11Forwarding no
     ForceCommand internal-sftp
     ChrootDirectory /var/lib/logcollector

Match Group uploads
     ChrootDirectory /var/lib/logcollector/upload_chroot
     X11Forwarding no
     AllowTcpForwarding no
     PasswordAuthentication no
```

4. Save the file, and restart the sshd service by running the following command:

   ```
   systemctl restart sshd
   ```

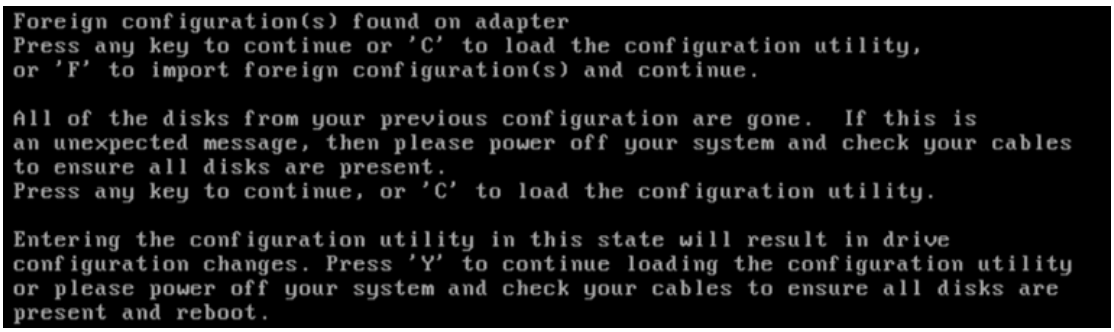
Hardware Related Tasks

(Conditional) Task 28 - Import Foreign Config for Series 4 Appliance with External Storage

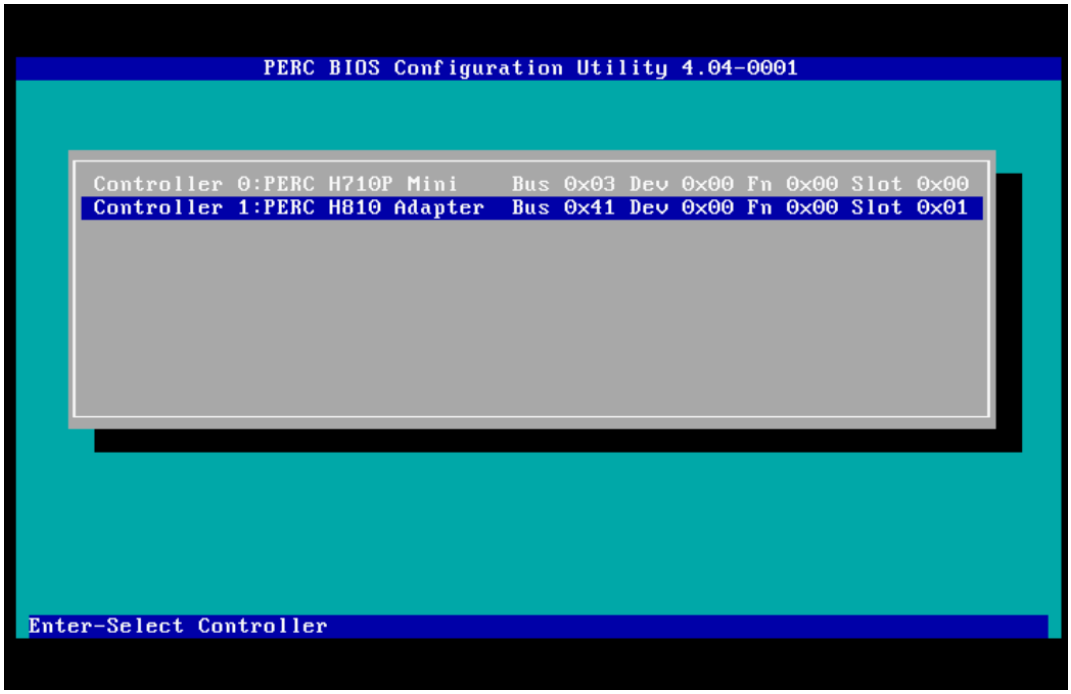
If you upgrade a host with a external storage (for example, a DAC) to 11.0 and try to restart the appliance, the system may recognize it as having a foreign configuration. If you receive this error, complete the following steps.

1. Restart the appliance with external storage.

   The following messages are displayed.

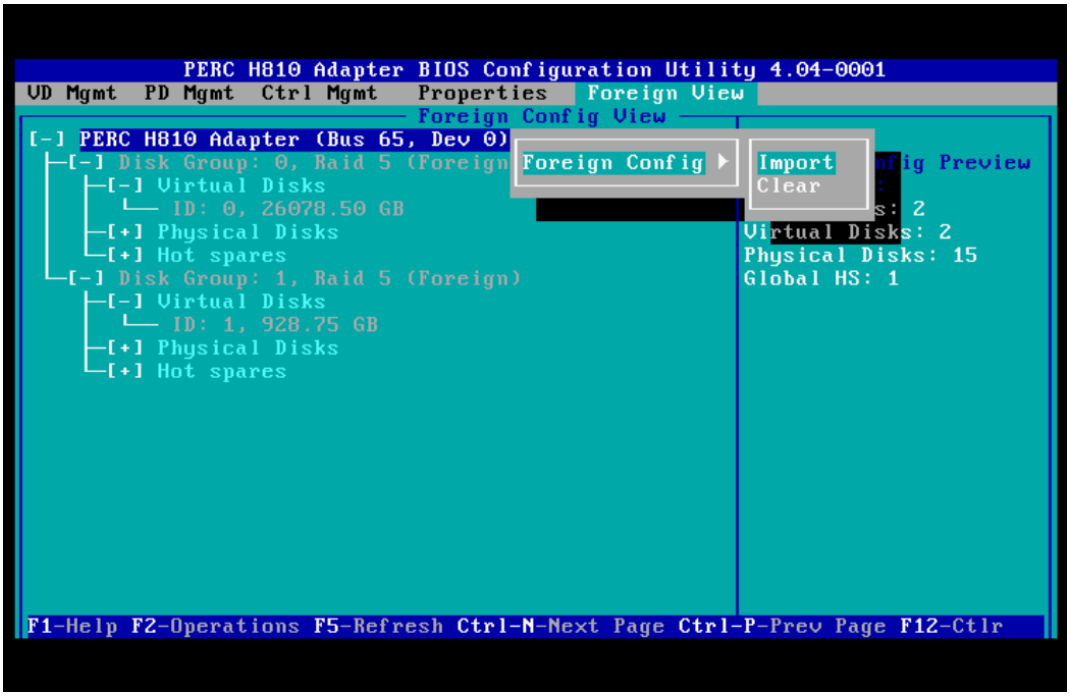


2. Press the **F** key and restart the appliance.
   If this successfully imports the configuration and restarts the appliance, you are finished. If it does not work, go to step 3.
3. Press **C** to start the Configuration utility.
   a. Select the **PERC H8x0 Adapter**.

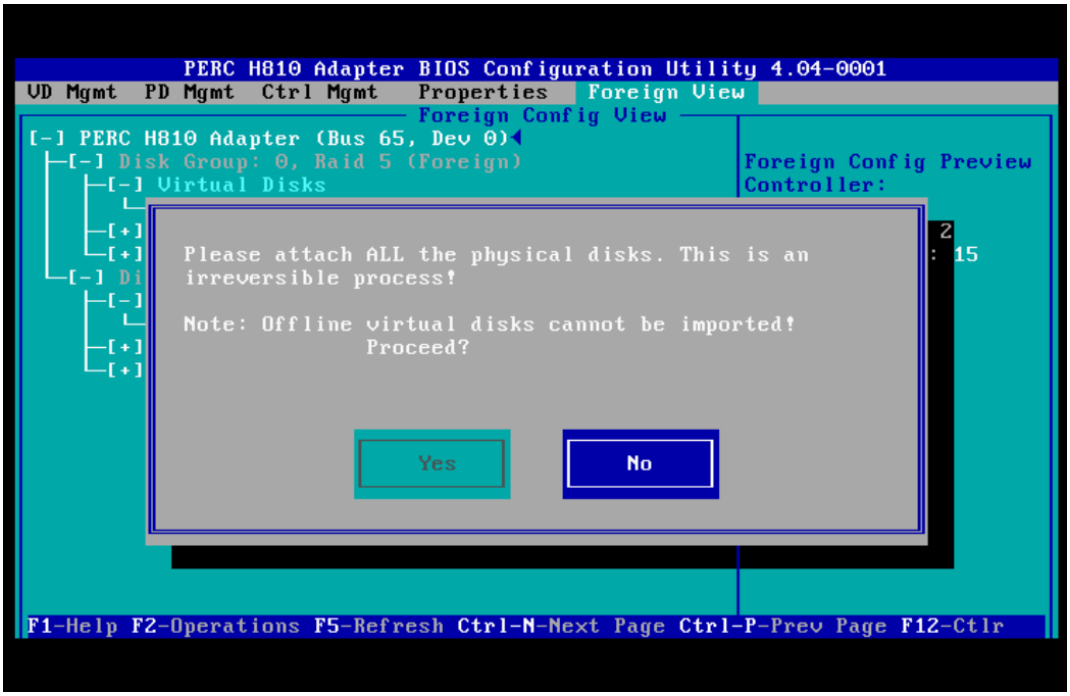


   b. Highlight the top row [for example, **PERC H810 Adapter (Bus 65, Dev 0)**].
   c. Select **Foreign View** from the menu bar.

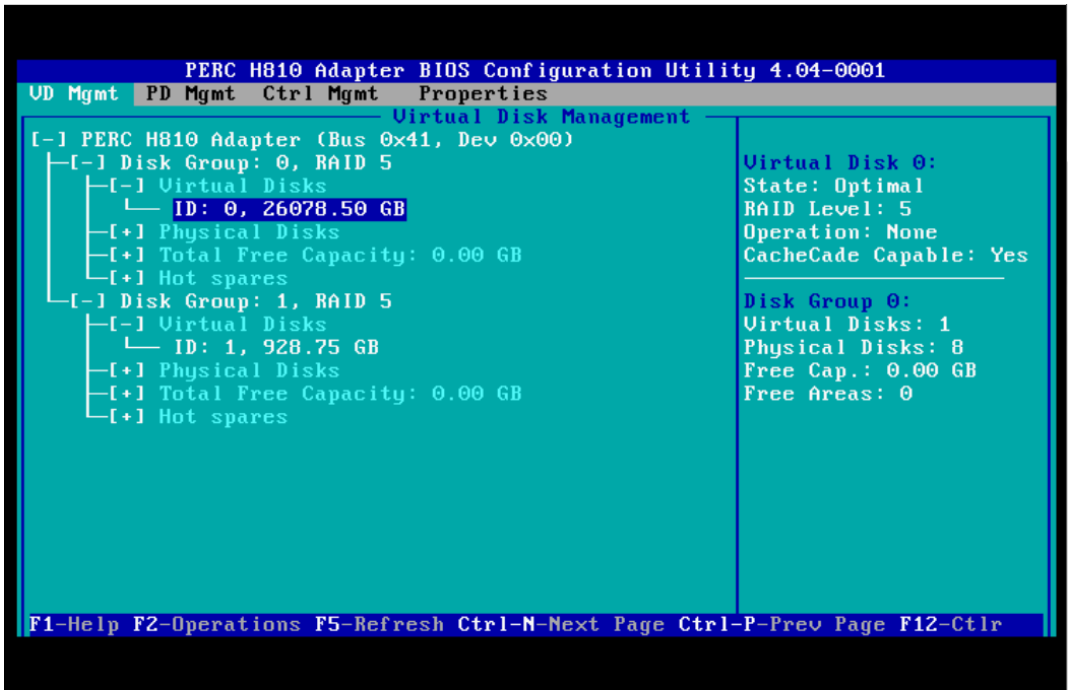
d. Press **F2** to display the **Foreign Config** drop down menu and select **Import**.



e. Select **Yes** to confirm that you want to import the foreign config.

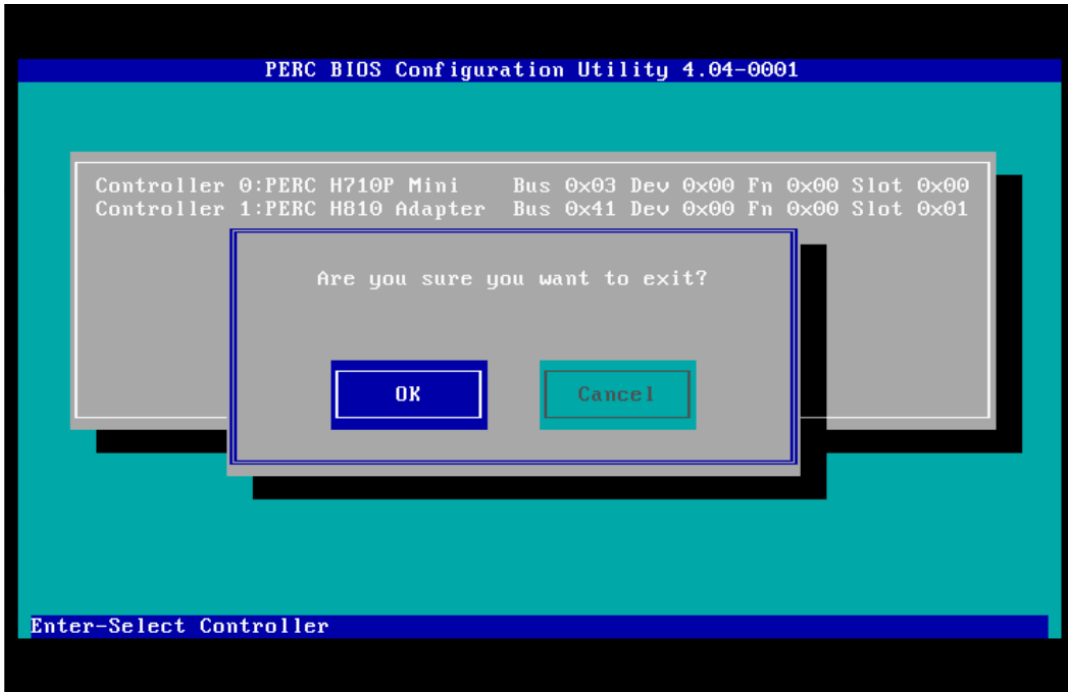


f. Verify that there are no more foreign configs present on the system.



g. Press the **Esc** key to exit.

h. Select **Yes** to confirm that you want to exit.



4. Press **Ctrl-Alt-Delete** to restart (reboot) the appliance.

Caution: If the foreign config fails, Contact Customer Support (https://community.rsa.com/docs/DOC-1294).

(Conditional) Task 29 - Restore Files for 10G Decoder

If you use the 10G Decoder hardware driver and you customized the `/etc/init.d/pf_ring` script to use MTU from the `/etc/pf_ring/mtu.conf` file, you must restore `mtu.conf` and `pf_ring` files from the `./etc/init/pfring_bkup` directory.

1. Restore the `pf_ring` file to /etc/init.d/ directory in 11.0.
   `/etc/init.d/pf_ring`
2. Restore the `mtu.conf` file to `/etc/pf_ring/` directory in 11.0.
   `/etc/pf_ring/mtu.conf`

Appendix A. Troubleshooting

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

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

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

- Backup
- Event Stream Analysis
- General
- Log Collector Service (`nwlogcollector`)
- NW Server
- Reporting Engine

Backup (`nw-backup` script)

Message	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	ESA Mongo admin password contains special characters (for example, '!@#$%^qwerty').
Solution	Change the ESA mongo admin password back to the original default of 'netwitness' before running backup. See "ESA Config: Change MongoDB Password for admin Account" the the *RSA NetWitness® Suite Event Stream Analysis Configuration Guide. Go to the* Master Table of Contents *for Version 11.0 to find NetWitness Suite 11.0 documents.*

Event Stream Analysis

Problem	ESA service crashes after you upgrade to 11.0 from a FIPS enabled setup.
Cause	ESA service is pointing to an invalid keystore.

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

General

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

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

Message	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt is nGB` `<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.`
Cause	Low or insufficient disk space allocated for the SMS service.
Solution	RSA recommends that you provide a minimum of 10 GB of disk space for the SMS service to run optimally.

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

Log Collector Service (`nwlogcollector`)

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

Message	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness 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 Version 11.0 to find NetWitness Suite 11.0 documents.

Message	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Solution	(Conditional) If you use a Log Collector Lockbox, log in to NetWitness 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 Version 11.0 to find NetWitness Suite 11.0 documents..

Message	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness 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 Version 11.0 to find NetWitness Suite 11.0 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 10.6.4 to 11.0.
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.

Message	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. Go to the Master Table of Contents for Version 11.0 to find NetWitness Suite 11.0 documents.

Appendix B. Stopping and Restarting Data Capture and Aggregation

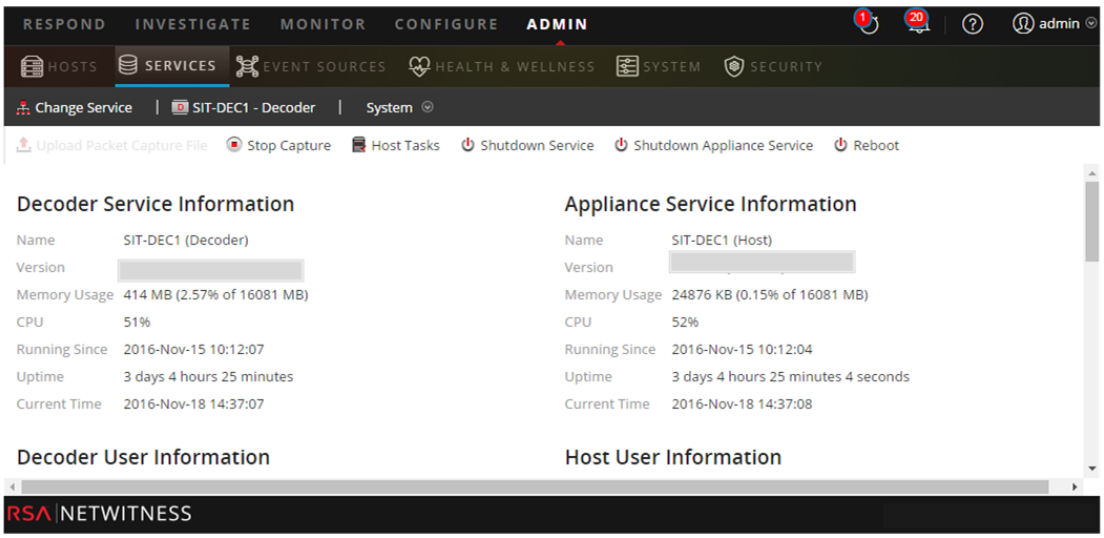
RSA recommends that you stop packet and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.0. If you do this, you must restart packet and log capture and aggregation after updating these hosts.

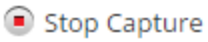
Stop Data Capture and Aggregation

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.



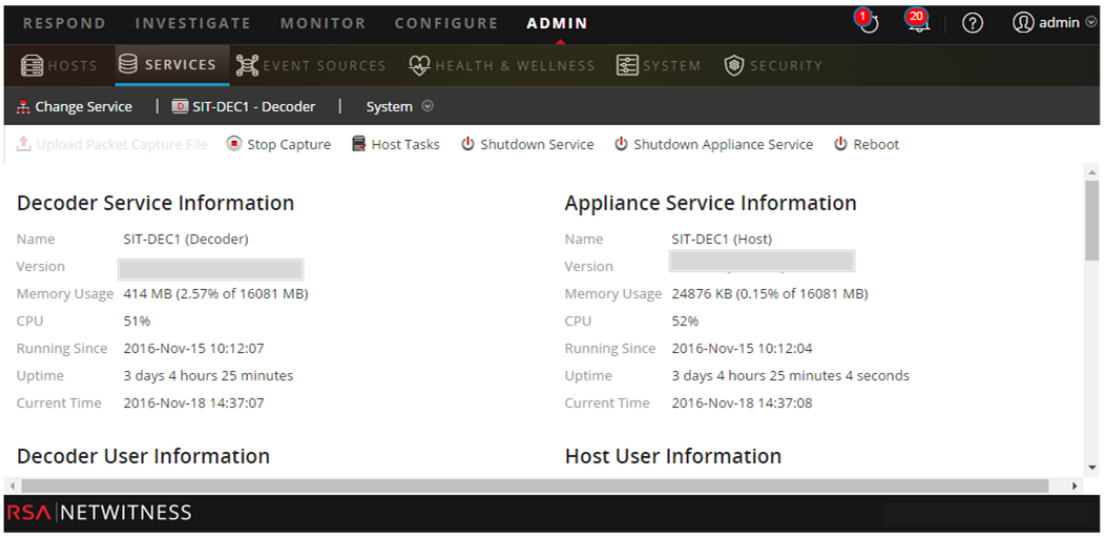
3. Under  (actions), select **View** > **System**.
4. In the toolbar, click  .

Stop Log Capture

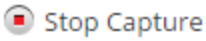
To stop log capture:

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 

.

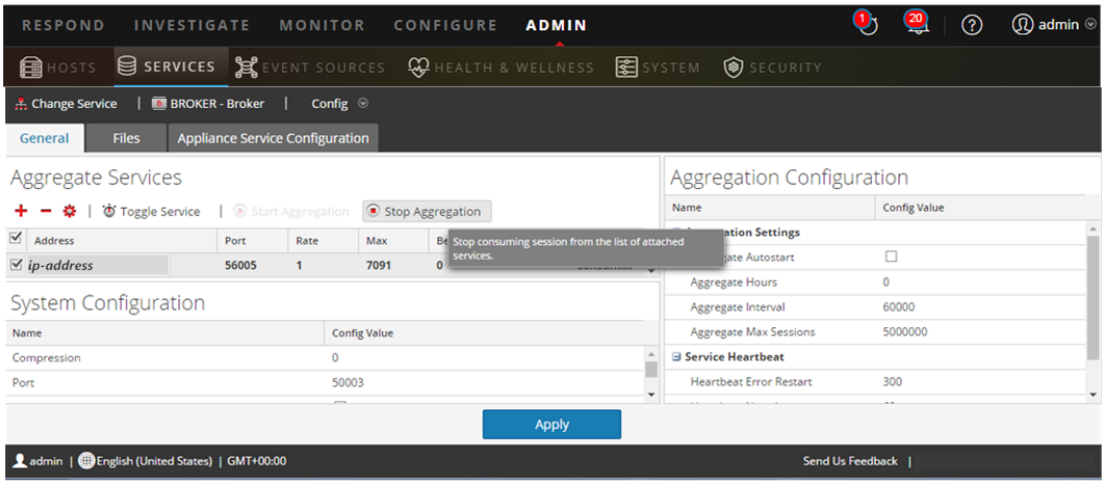
Stop Aggregation

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 11.0.

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

During the upgrade from 10.6.5.x to 11.0, the Broker Service is restarted and this automatically starts aggregation.

Revision History

Revision	Date	Description	Author
0.1	10-Jan-18	Internal Review Draft	IDD
0.2	23-Jan-18	Changes for Active Directory	IDD
0.3	24-Jan-18	Changes to backup instructions for ASOC-48707 and to upgrade preparation tasks for ASOC-46625.	IDD
0.4	7-Feb-18	ASOC-49820	IDD