



Physical Host Upgrade Guide

for RSA NetWitness® Platform 10.6.6.x to 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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 Dell, 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 Dell.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

April 2019

Contents

Introduction	7
CentOS6 to CentOS7 Upgrade	7
RSA NetWitness® Platform 11.3 Upgrade Path	7
Supported Host Upgrade Path	7
Hardware, Deployments, Services, and Features Not Supported in 11.3	8
Event Stream Analysis (ESA) Upgrade Considerations	9
Upgrade Considerations for ESA Rule Deployments	9
Upgrade Phases	9
Phase 1	9
Phase 2	10
Phase 3 (Optional)	11
Investigate in Mixed Mode	11
Upgrade Workflow	13
Contact Customer Support	13
Upgrade Preparation Tasks	14
General	14
Task 1 - Review Core Ports and Open Firewall Ports	14
Task 2 - Record Your 10.6.6.x admin user Password	15
Task 3 - Create a Backup of the /etc/fstab File	15
Task 4 - Make Sure Password Strength Settings Check Boxes Are Set in 10.6.6.x	15
Task 5 (Conditional) - Extract 10.6.x Public Key Infrastructure (PKI) Certificates	16
Event Stream Analysis (ESA)	19
Task 6 (Conditional) - Record Any String Array Type Meta Keys on the Event Stream Analysis Service	19
Respond	19
Task 7 - Check Aggregation Rules Match Conditions for “Domain” or “Domain for Suspected C&C”	19
Task 8 - Set Data Retention Run Interval to ≥ 24 Hours	20
Reporting Engine	21
(Conditional) Task 9 - Unlink External Storage	21
Warehouse Connector	22
(Conditional) Task 10 - Copy keytab files in root or etc Directory Stored in Other Directory	22
Other Tasks	22
Task 11 - Hardware - Check for BAD-INDEX BIOS Error before Upgrading	22
Backup Instructions	23
Task 1 - Set up an External Host for Backing up Files	24

Task 2 - Create a List of Hosts to Back up	26
Troubleshooting Information	27
Task 3 - Set up Authentication Between Backup and Target Hosts	29
Task 4 - Check for Backup Requirements for Specific Types of Hosts	29
For All Host Types	29
For ESA Hosts with Mongo Databases	30
For Decoder, Concentrator, or Broker Hosts: Stop Data Capture and Aggregation	30
Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh	30
For File Collection Event Sources	32
For Bluecoat Event Sources	32
For Integrations with Web Threat Detection, Archer Cyber Incident & Breach Response or NetWitness Endpoint - List RabbitMQ Usernames and Passwords	32
Task 5 - Check for Adequate Space for the Backup	32
Task 6 - Back up Your Host Systems	33
Post Backup Tasks	36
Task 1 - Save a Copy of the all-systems File and the Backup Tar files	36
Task 2 - Ensure Required Backup Files Were Generated	36
Task 3 - (Conditional) For Multiple ESA Hosts, Copy mongodb tar files to Primary ESA Host	37
Task 4 - Ensure All Required Backup Files are on Each Host	37
Upgrade Tasks	40
Phase 1 - Upgrade SA Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts	40
Task 1 - Upgrade the 10.6.6.x SA Server to 11.3 NW Server	40
Task 2 - Upgrade 10.6.6.x ESA to 11.3	40
Task 3 - Upgrade 10.6.6.x Malware Analysis to 11.3	41
Task 4 - Upgrade 10.6.6.x Broker or 10.6.6.x Concentrator to 11.3	41
Phase 2 - Upgrade All Other Hosts	41
Decoder and Concentrator Hosts	41
Log Decoder Host	41
Virtual Log Collector Host	41
All Other 10.6.6.x Hosts to 11.3	43
Upgrade the 10.6.6.x SA Server Host to the 11.3 NW Server Host	43
Upgrade a 10.6.6.x Component Host to 11.3	51
Phase 3 - (Optional) Install Warm Standby NW Server	59
Update or Install Windows Legacy Collection	60
Post Upgrade Tasks	61
General	61
Task 1 - Remove Backup-Related Files from Host Local Directories	61
Task 2 - Make Sure Port 15671 Is Configured Correctly	62
(Optional) Task 3 - Reissue Certificates for Your Hosts	62

(Conditional) Task 4 - Restore Custom Analysts Roles	62
(Conditional) Task 5 - If NetWitness Platform Has No Web Access, Upload Response .bin File Again (License Server)	62
Task 6 - Migrate Active Directory (AD)	62
Task 7 - Modify Migrated AD Configuration to Upload Certificate	63
Task 8 - Reconfigure Pluggable Authentication Module (PAM) in 11.3	63
Task 9 - Restore NTP Servers	63
Task 10 - Restore Licenses for Environments without FlexNet Operations-On Demand Access	63
(Conditional) Task 11 - If You Disabled Standard Firewall Config - Add Custom IPtables	64
(Conditional) Task 12 - Specify SSL Ports If You Never Set Up Trusted Connections	64
Task 13 (Conditional) Reconfigure Public Key Infrastructure (PKI) Certificates	65
Event Stream Analysis (ESA)	65
Task 14 - Reconfigure Automated Threat Detection for ESA	65
Task 15 (Conditional) Verify String Array Type Meta Keys on the ESA Correlation Service	66
Task 16 (Conditional) Update RSA Live ESA Rules with Meta Type Changes from String to Array	66
Task 17 (Conditional) - Verify ESA Rule Deployment	67
Investigate	67
Task 18 - Make Sure Customized User Roles Have Investigate-server Permissions for Event Analysis Access	67
Log Collection	69
Task 19 - Reset Stable System Values for Log Collector after Upgrade	69
Task 20 - (Conditional) Update SSHD Configuration after Upgrade with Older Windows and UNIX SFTP Agents	69
Task 21 - Enable FIPS Mode	70
Log Decoder and Decoder	70
(Conditional) Task 23 - Enable Metadata for GeoIP2 Parser	70
Malware Analysis	71
Task 24 - Enable Threat - Malware Indicators Dashboard	71
Reporting Engine	71
(Conditional) Task 25 - Restore the CA certificates for External Syslog Servers for Reporting Engine	71
(Conditional) Task 26 - Restore External Storage for Reporting Engine	71
Respond	72
Task 27 - Restore Respond Service Custom Keys	72
Task 28 - Restore Customized Respond Service Normalization Scripts	72
Task 29 - Add Respond Notification Settings for Custom Roles	73
Task 30 - Manually Configure Respond Notification Settings	73
Task 31 - Update Default Incident Rule Group By Values	74
Task 32 - Add Group By Field to Incident Rules	75
Task 33 - Update Incident Rules Identified in the Domain Matching Conditions Upgrade Preparation Task	76

Warehouse	78
Task 34 - Restore keytab Files, Mount NFS, Install Service	78
Task 35 - Refresh Warehouse Connector Lockbox and Start Stream	78
Task 36 - Update Hive Version	78
RSA Archer Cyber Incident & Breach Response	79
Task 37 - Reconfigure RSA Archer Cyber Incident & Breach Response Integration	79
RSA NetWitness® Endpoint	79
Task 38 - Reconfigure Endpoint Alerts Via Message Bus	79
Task 39 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed	79
(Optional) Task 40 - Install Endpoint Log Hybrid and Endpoint Agents	80
RSA NetWitness® UEBA	80
Task 41 - Install NetWitness UEBA	80
NetWitness Platform Integrations	80
(Conditional) Task 42 - For Integrations with Web Threat Detection, RSA Archer® Cyber Incident & Breach Response or NetWitness Endpoint.	80
Other	80
Appendix A. Troubleshooting	81
Section 1 - General Troubleshooting information	81
Command Line Interface (CLI)	81
Backup (nw-backup script)	83
Event Stream Analysis	84
Concentrator Service	84
Log Collector Service (nwlogcollector)	85
NW Server	86
Orchestration	86
Reporting Engine Service	87
NetWitness UEBA	87
Section 2 - Hardware-Related Troubleshooting Information	88
Appendix B. Stopping and Restarting Data Capture and Aggregation	92
Stop Data Capture and Aggregation	92
Start Data Capture and Aggregation	94
Appendix C. Using iDRAC with the DVD ISO Image	95
Configure NFS Server - NFS Server config File	95
Boot iDRAC to NFS Configuration	96
Appendix D. Create External Repository	97
Revision History	100

Introduction

The instructions in this guide apply to the upgrade of physical hosts to RSA NetWitness® Platform 11.3 exclusively. See the *Virtual Host Upgrade Guide for NetWitness Platform 10.6.6.x to 11.3* for instructions on how to upgrade your virtual hosts to 11.3.

NetWitness Platform 11.3 is a major release that affects all products in the NetWitness Platform. The components of the platform are the NetWitness Server (Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, Security sever, and Source server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, UEBA, Warehouse Connector, and Workbench.

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

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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

CentOS6 to CentOS7 Upgrade

NetWitness Platform 11.3 is a major release that involves upgrading to a newer version of the operating system (CentOS6 to CentOS7). In addition, the 11.3 platform environment has been improved greatly to accommodate current and future physical and virtual deployment types. These changes require an upgrade to the new environment and an upgrade of the functionality.

RSA NetWitness® Platform 11.3 Upgrade Path

The earliest supported upgrade path for RSA NetWitness® Platform 11.3 is Security Analytics 10.6.6.x. If you are running a version of NetWitness Platform that is prior to 10.6.6.x, you must update to 10.6.6.x before you can upgrade to 11.3. See the *RSA Security Analytics 10.6.6 Update Guide* (<https://community.rsa.com/docs/DOC-95880>) 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 11.3.
- On-Prem Virtual to On-Prem Virtual

Caution: The 11.3 upgrade does not support mixed-platform upgrades (for example, it does not support physical to virtual).

Hardware, Deployments, Services, and Features Not Supported in 11.3

RSA does not support upgrade of the following hardware, deployments, services, and features to 11.3.

- RSA All-in-One (AIO) Appliance
- Multiple NetWitness Server Deployment
- IPDB service
- Malware Analysis service co-located on the SA Server (upgrade of Malware Analysis Enterprise is supported in 11.3.)
- Standalone Warehouse Connector service (Upgrade of a co-located Warehouse Connector is supported in 11.3.)
- Custom Health & Wellness policy in 10.6.x for the Context Hub Service
After you upgrade to NetWitness 11.3, 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 11.3.
- Defense Information Strategic Agency-Security Technical Information Guide (DISA-STIG) hardened deployments.
- Warehouse Analytics (Data Science)

Event Stream Analysis (ESA) Upgrade Considerations

In RSA NetWitness® Platform 11.3, RSA changed how ESA Correlation Rules store and transmit the alerts the system generates. In 11.3, ESA sends all alerts to a central Alert system. The local MongoDB storage in ESA 10.6.6.x has been removed.

Note: If you did not use Incident Management in 10.6.6.x, you cannot view the 10.6.6.x ESA alerts in the 11.3 Respond component without running a migration script. Use the ESA Alert Migration script to migrate these alerts to the location in 11.3 that will allow Respond to view them. See the *ESA Alert Migration Instructions* knowledge base article (<https://community.rsa.com/docs/DOC-84102>) in RSA Link for instructions on how to run this script.

Upgrade Considerations for ESA Rule Deployments

Caution: In NetWitness Platform 11.3, the ESA Correlation service contains data source changes that require changes to migrated ESA rule deployments. The 11.3 ESA Correlation service replaces the Event Stream Analysis service in earlier versions.

After you upgrade to 11.3, migrated ESA rule deployments have the following changes.

1. If an ESA rule deployment contains two services before you upgrade to 11.3, the deployment splits into two deployments. You can only have one ESA Correlation service in an ESA rule deployment in version 11.3.
2. If an ESA service has multiple ESA rule deployments before you upgrade to 11.3, they are combined into one deployment in version 11.3.

You can still access your old deployments. For a detailed example, see the *ESA Configuration Guide for RSA NetWitness Platform 11.3*.

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 11.3 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. 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 11.3 NetWitness Server (NW Server) cannot communicate with 10.6.6.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2

Upgrade the rest of your hosts.

RSA recommends that you follow the order in Phase 2 to reduce:

- Functionality loss during investigation.
- Downtime that results in the loss of network and log capture.

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

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

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

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

- a. LDs (one LD at a time)
- b. VLCs and LWCs

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

5. All other hosts

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

- Functionality gaps encountered while running in this mode.
- Examples of staggered upgrades.

Phase 3 (Optional)

After you have upgraded all hosts in your deployment to 11.3, you can install a Warm Standby NW Server. Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide for NetWitness Platform for 11.3* for instructions on how to set up a Warm Standby NW Server.

Investigate in Mixed Mode

Mixed mode occurs when the NW Server host and Broker hosts are on the latest version (for example, 11.3) and the other core services such as Concentrators and Decoders are on any older version (for example, 10.6.6.x or 11.1.x.x-11.2.x.x). You must follow the host upgrade sequence as shown in [Upgrade Phases](#) to ensure complete Investigate functionality.

The 11.3 Investigate server is installed when you upgrade the SA Server, but Broker hosts need to be upgraded to 11.3 to access the Event Analysis view. If the Broker is not upgraded, analysts see a warning icon next to the Broker, and no data aggregated to that Broker can be displayed.

Mixed mode (that is, some services are upgraded to 11.3 and some are still at 10.6.6.x) also affects the functionality of Role-Based Access Control (RBAC). In mixed mode, when an analyst conducts an investigation, RBAC is not applied uniformly to viewing and downloads. After you upgrade all services to 11.3, when an analyst conducts an investigation, Role-Based Access Control of downloads works consistently to limit access to restricted data.

In mixed mode, if the `sdk.packets` setting has not been disabled on the 10.6.6.x services, analysts with SDK meta and roles permissions in place to restrict viewing and reconstructing an event's content can download the packet capture (PCAP) file of an event that has content restrictions. Other types of downloads appear to be successful, then generate errors due to insufficient permissions, and the data is still protected.

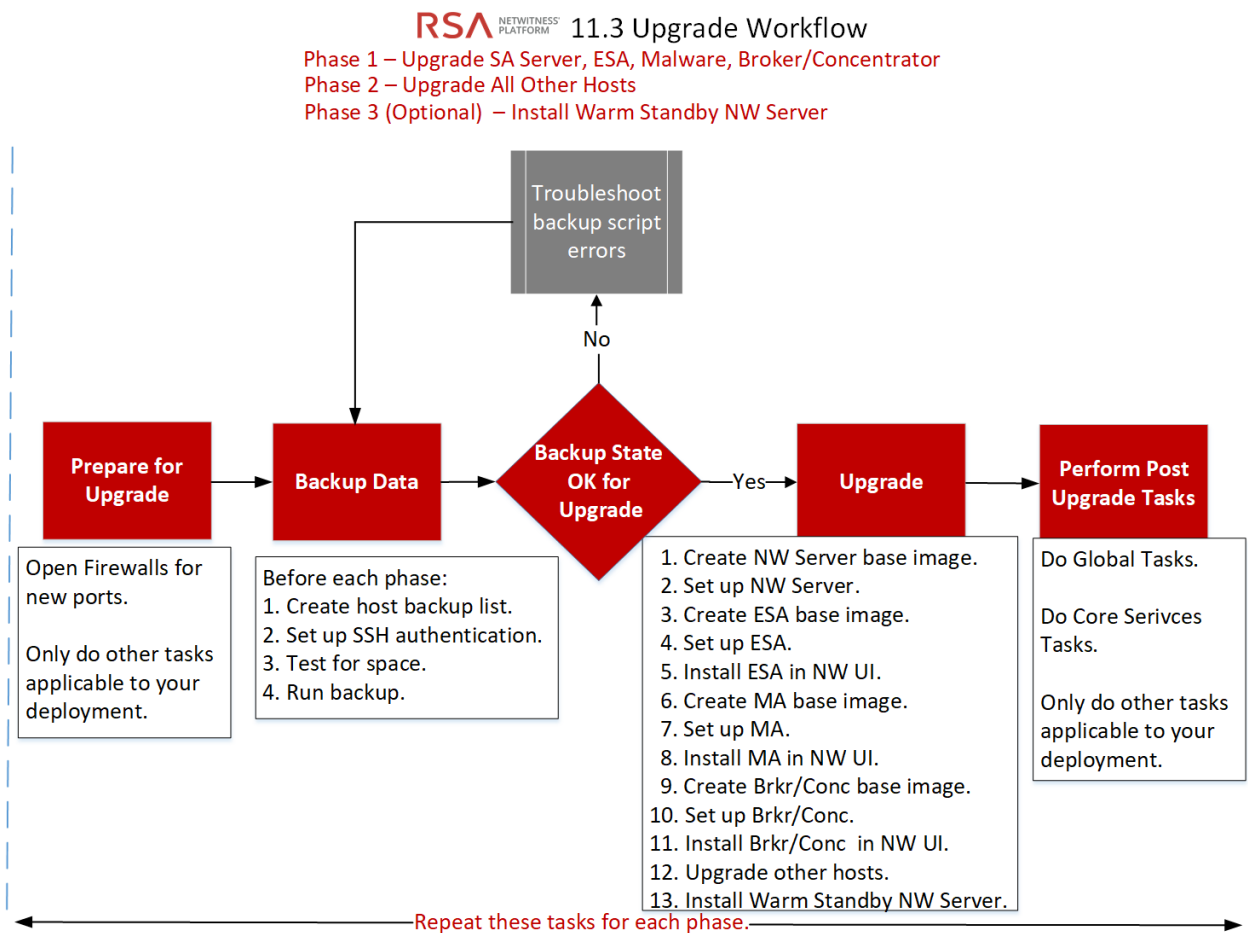
During a phased update, you can disable the `sdk.packets` setting on 10.6.6.x services to prevent analysts from downloading any PCAPs or logs. After you update all services to 11.3 and re-enable `sdk.packets`, RBAC works consistently across all services.

The following table identifies what users with the analysts role can see and download when the NW Server is at version 11.3, and the 11.3 Broker is connected to Concentrators and Decoders at version 10.6.6.x.

Investigate Views Affected	Information Analysts Can See	Restricted Content Analysts Can Download	Restricted Content Analysts Can Download with Errors
Events View	RBAC permitted items	PCAP	File archive (cannot unzip it)
Event Reconstruction View	RBAC permitted items	PCAP	File archive (cannot unzip it)
Event Analysis View	RBAC permitted items	PCAP	Payload (any option: all payloads, request only, response only)

Upgrade Workflow

The following diagram illustrates the RSA NetWitness® Platform 11.3 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 Platform 11.3.

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness Platform 11.3. These tasks are organized by the following categories.

- [General](#)
- [Event Stream Analysis \(ESA\)](#)
- [Reporting Engine](#)
- [Respond](#)
- [Warehouse Connector](#)
- [Other](#)

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

General

Task 1 - Review Core Ports and Open Firewall Ports

The following tables list new ports in 11.3.

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

NW Server Host

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

ESA Host

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

Endpoint Log Hybrid

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

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

Task 2 - Record Your 10.6.6.x admin user Password

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

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

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

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

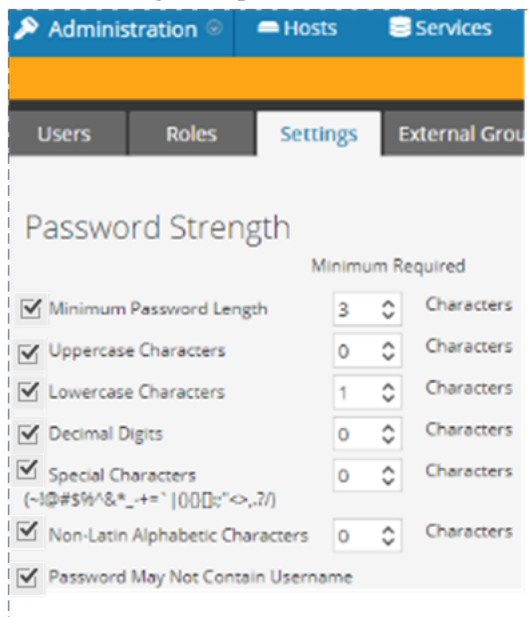
Task 4 - Make Sure Password Strength Settings Check Boxes Are Set in 10.6.6.x

The check box to the left of the **Password Strength Settings** in the **Administration > Security > Settings** tab must be set in 10.6.6.x or these settings will not be migrated to 11.3.

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

1. In Security Analytics 10.6.6.x, go to the **Administration > Security > Settings** tab.
2. Make sure that all of the check boxes to the left of the **Password Strength Settings** are set. If they are not, set them and click **Apply**.

The following example shows all check boxes as set (required in 10.6.6.x before upgrading to 11.3).



Task 5 (Conditional) - Extract 10.6.x Public Key Infrastructure (PKI) Certificates

Before you upgrade to from 10.6.6.x to 11.3, complete the following procedure to extract the existing 10.6.x PKI keystores that contain server certificates with private keys, and the truststores that contain the trusted CA certificates.

1. Download the `rsa-nw-pki-migration-10.6.6.zip` file from **RSA Link > RSA NetWitness Platform > Downloads > RSA NetWitness LOGS & NETWORK > Version 11.3**.
2. Extract the `pki-migration-1.0.jar` file from the `rsa-nw-pki-migration-10.6.6.zip` file.
3. SSH to the 10.6.6.x Security Analytics Server host and log in with the root credentials.
4. Copy the `pki-migration-1.0.jar` file into `/tmp` folder.
5. Run the following command strings to extract the certificates.

```
cd /tmp
java -jar pki-migration-1.0.jar
extract
```

This :

- Creates the `rsa-pki-migration-tool-<yyyy-MM-dd-hh-mm>` directory under the `tmp` directory.
- Extracts output files into the `/tmp/rsa-pki-migration-<yyyy-MM-dd-hh-mm>` directory.
- Creates a keystore (for example, `<keystore-x>.p12`) for each server certificate. The keystore is encrypted with **netwitness** as the password.
- Creates a certificate file (for example, `<certificate-x>.cer`) for each trusted CA certificate in truststore.

Note: Refer to the line in the console output to find the storage location of the

- server certificate (<keystore-x>.p12). For Example:

```
The Entry 1e-056cdfb6-7577-4287-a791-64fbf999ff2d is a Private Key Entry
Storing the entry 1e-056cdfb6-7577-4287-a791-64fbf999ff2d into store at /tmp/rsa-pki-migration-tool-2019-03-04-13-48/keystore-2.p12
```

- trusted CA certificate (<certificate-x>.cer). For example

```
The Entry srv3-server3-ca-29174576837559984330324331352845599851 is a Certificate Key Entry
Writing certificate Entry srv3-server3-ca-29174576837559984330324331352845599851 into file /tmp/rsa-pki-migration-tool-2019-03-04-13-48/certificate-4.cer
```

This process does not modify the original keystores and trusted CA certificates of 10.6.6.x. You can run these steps multiple times, if required.

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

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

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

```
-----BEGIN CERTIFICATE-----
MIIDZTCCAk2gAwIBAgIQZ4o94d5A1LBC4sPXgDYXpTANBgkqhkiG9w0BAQUFADBF
MRUwEwYKCZImiZPyLGBGRYFbG9jYVlwxZARBgoJkiaJk/IsZAEZFgNwa2kxZzAV
BgNVBAMTDnBra51TRVJWRVixLUNBMHB4XDTE1MDgwNzA2MTU1MVoXDTIwMDgwNzA2
MjU1MVoRTEVMBMGCGmSjomT8ixkARKwBwvY2F5MRMwEQYKCZImiZPyLGBGRYD
cGtpMRcwFQYDVOQDEw5wa2ktU0VSVkVSMS1DQTCASwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKNFzsm3rsY70GLb5ZVVVwsfZCu0517Re3eSiHdgWgp86QdT
URTSYDuHwVlnUmMo4CVKNNF0c9nzzJZDG4b0LSL/qkUVmxAhrcw52/0edKCMROa9
auZMPgyYtXeKiA8Ak55qOn2Es3tjJAf90IsAprK1mXOH9cs24Fdtm7ahNCqy1569
cxeB0ykr/xYhU+AkBFd4uv1A8Bf611+70UeUdu3f04XMhYk4VTPF5gI5DNhZgmP
DQi93Bj/nY3MaQ4Woz4r3TFbIVZwe4kRW+FAD5glundA401QfQZQAQI+1cy6pb15
nyi0C9ktEsQ1Ru+mhChOKEjhV9Q5pHaZsdpxfXsCAwEAANRME8wCwYDVR0PBAQD
AgGGA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFNF1TRzf8QR77KIn4I5kjvzG
WUIbMBAGCSsGAQQBgjcVAQQDAgEAMAGCSsGSIb3DQEBBQUAA4IBAQCndbUNKnKp
9FDj3nJRFXPXw8kStBIQWqS4WfyPzHmxCAzmDureN/9YVqNniJhII0KLzesgFj12
FeJ6R1mps4e5IHMKNrOTr+WcNg/ipDOucn2MHol4InLP4FeapVOPXs7E7IiR5iQR
cWw4Iag6LcFAoIwI5gOxnV93Etb2e1VnQHxXlMhtaGnSuHgFudm/WHcZFGWfwX9T
22w4Hf8L4qNmP9w97Cq+Vu/emamd02eIzPgKZJPu4B6oeKxUp6/QwUXCUYHZNrcj
qJ+1a1VnMeDWH+VrZtZf1SeMiAh6q0bwk6sXxQyKAuB8v1vG4svPIFrq1T4KpRXQ
31AXU6iWqYZP
-----END CERTIFICATE-----
```

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

The following is an example of the output.

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

- Exit the keystore.

```
exit
```

You can use:

- One of the .p12 keystore files as a server certificate. Refer to the command output to find .p12 file that corresponds to the server certificate you must use.
- The extracted certificate files (.cer) as trusted CA certificates.


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

Event Stream Analysis (ESA)

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

If you added any string array type meta keys to the Event Stream Analysis service for your ESA correlation rules in 10.6.6.x or earlier, record these meta keys so you can verify that they exist after upgrade to 11.3.

To record your 10.6.6.x string array type meta keys before the 11.3 upgrade:

1. In Security Analytics 10.6.6.x:
 - a. Go to the **Administration** > **Services** view.
 - b. Select the Event Stream Analysis service.
 - c. Click  (actions) > **View** > **Explore**.
2. In the **Explore** view node list, select **Workflow** > **Source** > **netgenAggregationSource**.
3. In the **ArrayFieldNames** list, make a note of any string array type meta keys added to the Event Stream Analysis service so you can verify that they are on the ESA Correlation service after the upgrade.

Respond

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

Make a note of any Incident Management aggregation rules that have match conditions using Domain or Domain for Suspected C&C in the drop-down list in the rule builder. You will need to add back these conditions after you upgrade to 11.3 as described in the "Respond" Post Upgrade Tasks later in this document.

Complete the task for each aggregation rule.

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

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


The screenshot shows the configuration page for a rule named "Verify Domain for Suspected C&C". The "Match Conditions" section is highlighted with a red box, showing two conditions: "Domain is equal to" and "Domain for Suspected C&C is equal to". The "Action" section shows "Group into an Incident" selected. The "Grouping Options" section shows "Group By" set to "Domain" and "Domain for Suspected C&C". The "Incident Options" section shows "Title" set to "\$(ruleName) for \$(groupByValue1)". The "Priority" section shows "Average of Risk Score across all of the Alerts" selected. A risk scale is visible on the right, ranging from 1 (Low) to 90 (Critical).

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

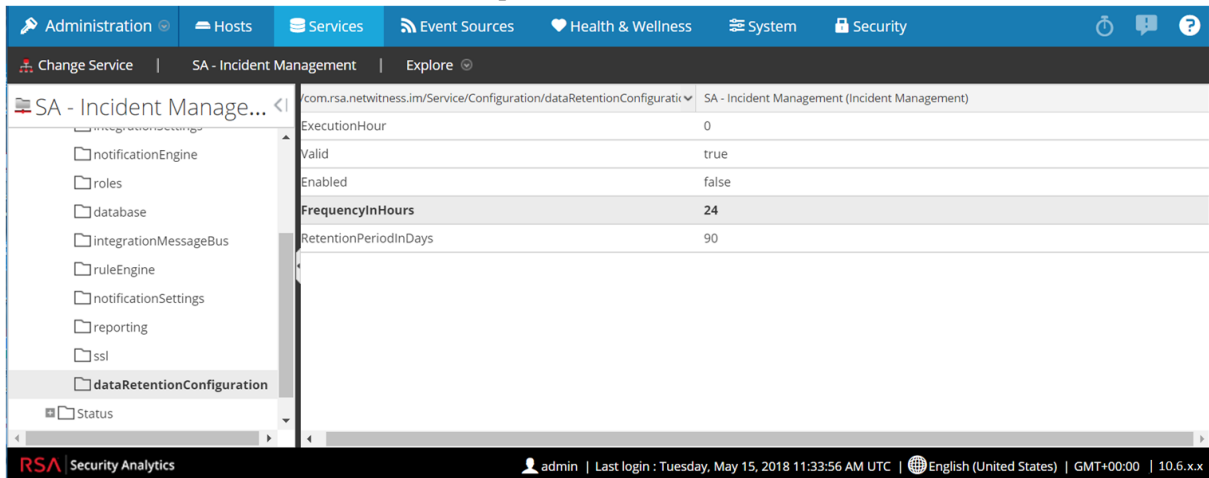
Task 8 - Set Data Retention Run Interval to ≥ 24 Hours

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

Complete the following task to ensure that the Respond service starts after upgrading to 11.3.

1. In Security Analytics 10.6.6.x, go to **ADMIN > Services**.
2. Select the **Incident Management** service, and then select  > **View > Explore**.
3. In the Incident Management **Explore** view, go to **Service > Configuration > dataRetentionConfiguration**.

4. Make sure that the `FrequencyInHours` parameter is ≥ 24 .



Reporting Engine

(Conditional) Task 9 - Unlink External Storage

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

Note: In these steps:

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

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

Warehouse Connector

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

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

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

Other Tasks

Task 11 - Hardware - Check for BAD-INDEX BIOS Error before Upgrading

Complete the following steps to detect a `BAD-INDEX` BIOS error before you upgrade to 11.3.

1. SSH to each host appliance.
2. Run the following command.
`dmidecode`
3. If you receive a `BAD-INDEX` error in the output, contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>).

Backup Instructions

Backing up your configuration data for all your hosts from 10.6.6.x is the first step in upgrading from Security Analytics 10.6.6.x releases to NetWitness Platform 11.3. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Note: 1.) 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 11.3, 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](#). 2.) Disable your Public Key Infrastructure (PKI) settings before starting the backup.

Caution: These services are not supported in the 10.6.6.x backup and upgrade process.

- IPDB
- All in One servers
- Malware Analysis Co-Located on the Security Analytics Server
- Standalone Warehouse Connector
- Warehouse Analytics (Datascience)

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

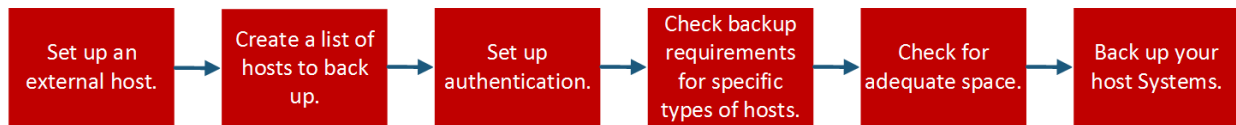
- **Security Analytics Admin Server**
- **Standalone Malware Analysis**
- **Archiver**
- **Broker**
- **Event Stream Analysis** (including Context Hub and Incident Management database)
- **Concentrator**
- **Log Decoder** (including Local Log Collector and Warehouse Connector, if installed)
- **Log Hybrid**
- **Network Decoder** (including Warehouse Connector, if installed)
- **Network 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 Pluggable Authentication Module (PAM) in 11.3.", in the "Global" section of the *Post Upgrade Tasks*.
- `/etc/pfring/mtu.conf` and `/etc/init.d/pf_ring`: To restore these files you must manually retrieve them. The `/etc/pfring/mtu.conf` files will be located in `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`, and the

`/etc/init.d/pf_ring` files will be located in `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. For information about how to restore these files, see "(Conditional) Task 2 - Restore Files for 10G Decoder" in the "Hardware Related Tasks" section of *Post Upgrade Tasks*.

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



The following sections describe each of these tasks:

- [Task 1 - Set up an External Host for Backing up Files](#)
- [Task 2 - Create a List of Hosts to Back up](#)
- [Task 3 - Set up Authentication Between Backup and Target Hosts](#)
- [Task 4 - Check for Backup Requirements for Specific Types of Hosts](#)
- [Task 5 - Check for Adequate Space for the Backup](#)
- [Task 6 - Back up Your Host Systems](#)
- [Post Backup Tasks](#)

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

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

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

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

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

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

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

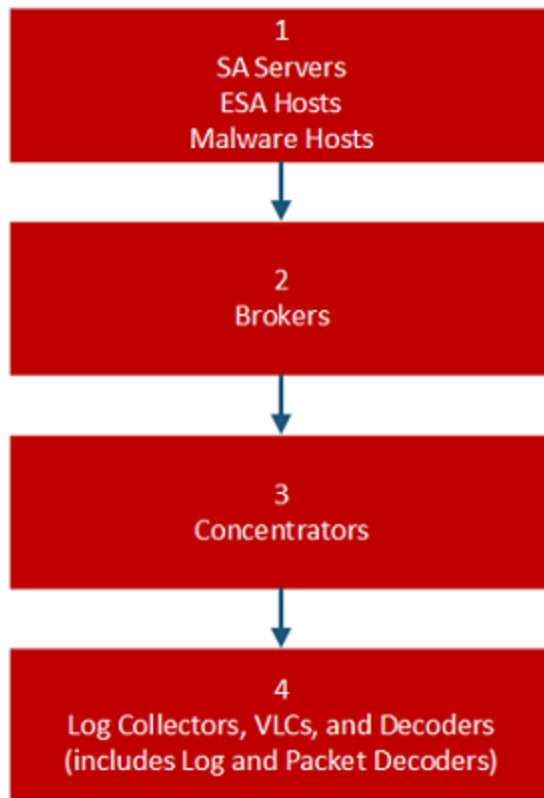
Caution: When performing a mixed-mode upgrade, retain a master copy of the `all-systems` file upgrade until all the hosts in your deployment are upgraded to 11.3. You cannot run the `get-all-systems.sh` a second time because the NW Server, the first host that must be upgraded in mixed mode, will have CentOS7 as an operating system.

- `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 Installation Guide* on for more information.

Note: 1.) If you have used the 10.6.x versions of the backup and restore scripts on your 10.6.6 hosts, you must still run all the scripts listed here. 2.) Do NOT use the scripts in the `nw-backup-v4.3.zip` (on later version of the `nw-backup` script) file for regular backups. These scripts are specifically designed for upgrading from 10.6.6.x to 11.3. 3.) 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 10.6.6 Security Analytics Server:

```
loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fald18d8,10.6.6.0
#nwserver,nwserver106,172.31.255.23,67a9a0eb-1300-4fba-838f-
7be4d8cf5e65,10.6.6.0
```

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

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

Troubleshooting Information

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

- Do not edit the `all-systems-master-copy` file.
- If you create several different versions of the `all-systems` file (for example, for several backup sessions), be sure that each version of the file lists only those hosts that are currently being backed up, and the other hosts are commented out. For more information, see [Post Backup Tasks](#).

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

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

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

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

Task 3 - Set up Authentication Between Backup and Target Hosts

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

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

Complete the following task to set up authentication between backup and target hosts.

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 a password once on every 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 11.3, your custom certificate files will be located in `/etc/pki/nw/trust/import`.
You can convert CA certificates and keys to different formats to make them compatible with specific types of servers or software using OpenSSL. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. To convert the files, SSH to the Security Analytics Server and run the following command strings to perform the conversions listed.

Convert a DER file (.crt .cer .der) to PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM Certificate File and a Private Key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in  
certificate.crt -certfile CACert.crt
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```


Note: Add the following qualifier to the command string to:

- nocerts convert private keys exclusively.
- nokeys convert certificates exclusively.

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

For ESA Hosts with Mongo Databases

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

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

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 the 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.
- Read [For File Collection Event Sources](#) later in this chapter. You may need to restore some SSHD configuration settings from the 10.6.x LC/VLC.
- Read [For Bluecoat Event Sources](#) later in this chapter. You may need to backup VSFTPD key material manually.

Prepare LCs and VLCs for Upgrade

Complete the following task to prepare Log Collectors and Virtual Log Collectors for the 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 upgraded to 11.3.
 - 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 File Collection Event Sources

If you are using older Windows and UNIX SFTP agents to upload log files, they may not be able to connect to the SSHD on the upgraded 11.x LC/VLC if they are using older Ciphers, MACs and Key Exchange Algorithms. If possible, upgrade to the latest Windows and UNIX SFTP agents. If you cannot upgrade to the latest Windows and UNIX SFTP agents, note the Ciphers, MACs and Key Exchange Algorithms, if any, from the `/etc/ssh/sshd_config` file on the 10.6.x LC/VLC on the 10.6.x LC/VLC so that they can be added back to the file after upgrade.

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 on RSA Link contains the steps to configure VSFTPD service on the LC and VLC.

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

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

On the 10.6.6.x Security Analytics Server host, you must get a list of all RabbitMQ usernames and passwords so that after you perform the 11.3. 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*.

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.

Complete the following task to check for adequate disk space.

1. Make the backup script executable by running the following command:

```
chmod u+x nw-backup.sh
```

2. Run the following command at the root directory level:

```
./nw-backup.sh -t
```

The output displays the amount of disk space that is required for the backup.

Note: The `./nw-backup.sh -t` command runs with the `-d` option by default. However, if you are looking for more accurate disk space results, you can override the `-`

d option by using `-D`. Using the `-D` option will show how much space is required on each host for the data that will be backed up, but does not show how much space is available. If there is not enough space available, the `-D` option will throw an error. If you want to know how much space is available on the target host, you must run the `df -h` command on the host.

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

```
***** NW-BACKUP SCRIPT - TEST MODE *****
* * RSA nw-backup script is running in test mode where in it will only verify the disk space required for successful backup.
-----
CONTENT options currently selected:
-----
Backup IPDB? 'no'
Backup Malware Analysis repository? 'no'
Backup Reporting Engine repository? 'no'
Backup ESA DB? 'yes'
Backup SMS RRD? 'yes'
Backup Yum Repo? 'no'
Backup SA Colo MA? 'no'
Backup /var/log? 'no'
Backup Context Hub? 'yes'
-----
Checking that the environment is configured for proper execution of script...
Backup path configured... [ OK ] Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence... [ OK ]
Check for all-systems file... [ OK ]
Dated backup dir... [ OK ] Backup directory: /var/netwitness/database/nw-backup/2017-09-18
Logging to /var/netwitness/database/nw-backup/rsa-nw-backup-2017-09-18.log

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

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

Task 6 - Back up Your Host Systems

Before you run the backup script to do the actual backup, be sure that you have plenty of space. To back up your hosts, you run the `nw-backup.sh` script using the `-u` option. This option is required for upgrading to 11.3.

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 11.3. Enables the upgrade flag to run backup for upgrading to 11.3. 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 11.3, please use the default location! Default: (/var/netwitness/database/nw-backup)

Note: 1.) Do not change the backup path in upgrade (-u) mode. 2.) When you run a backup with the -u option, all services are stopped. If you need to continue to use the 10.6.x machine after running the backup, reboot the 10.6.x system so that services are restarted.

Advanced Content Selection Options

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

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

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

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

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

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

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

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

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

Test Options

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

For example, the command:

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

would run the backup with options as set in the Header of the script itself.

OR, the command:

```
./nw-backup.sh -ue /mnt/external_backup
```

would run a normal backup using the backup path defined in the script, with the following options:

-u : enables the upgrade flag to run backup for upgrading to 11.3. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)

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

For Help: ./nw-backup.sh -h

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

Caution: RSA nw-backup script backs up configuration files, data, and logs on the options provided in the script. It tars the content, with options to store the backup files on the backup server, move or copy them to external storage on a mount point (USB/NFS/SMB), or SCP them back to the target host. This backup script has been qualified on the following versions of Security Analytics:

10.6.6.x

Use of this script on any other versions of the product may not give expected results and may not be supported by RSA Customer Service.

Note: All non-RSA custom files, scripts, Cronjobs and other important files should be placed in /root, /home/'user', OR /etc to be included in the backup.

Complete the following task 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 11.3. Do NOT make any changes to the header of the backup script for the backup path because the path is specific to the upgrade, and that data needs to be in a specific place.

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

A log file, with a name similar to the following example, is created in the backup directory which provides information on the files being backed up:

rsa-nw-backup-2018-03-15.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
<All ESA 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 11.3.

Task 2 - Ensure Required Backup Files Were Generated

After you run the backup scripts, several files are generated. These files are required for the 11.3 upgrade process. Before you begin the upgrade process, you must ensure that the required backup files are on the hosts that you are upgrading, and that you perform the following tasks.

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

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

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

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

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

Note: The backup script copies the following files from all ESA hosts to the Security Analytics Server's backup path.

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

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

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

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

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

Before you upgrade to 11.3, ensure that the appropriate files exist on the hosts that you are upgrading as described in the following lists.

Note: The default paths for backup files are:

- Security Analytics Servers: `/var/netwitness/database/nw-backup`
- ESA hosts: `/opt/rsa/database/nw-backup`
- Malware hosts: `/var/lib/rsamalware/nw-backup`

Required Files for NetWitness Servers

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

Required Files for ESA Hosts

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

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

Required Files for All Other Hosts

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

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

appliance_info
service_info

Note: The paths to the location of the backup and restore files for iptables, NAT configurations, user accounts, and crontab entries are shown in the following list:

Backup paths:

BUPATH=/opt/rsa/database/nw-backup for the ESA Correlation Engine

BUPATH=/var/lib/rsamalware/nw-backup for the Malware Service

BUPATH=/var/netwitness/database/nw-backup for all other services

Restore locations:

BUPATH/restore/etc/sysconfig for Iptable rules

BUPATH/restore/etc/sysconfig for NAT configurations

BUPATH/restore/etc for Crontab entries

BUPATH/restore/etc for User Accounts (users are located in the `passwd` file, and groups are located in the `group` file. These are not restored during the upgrade process but can be restored manually.

BUPATH/restore/etc/ntp.conf for NTP configurations (must be restored using the NetWitness Platform UI)

Upgrade Tasks

This topic contains the tasks you must complete to upgrade Security Analytics 10.6.6.x to NetWitness Platform 11.3. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Caution: 1.) Make sure that you backed up your Security Analytics 10.6.6.x data before attempting to upgrade to NetWitness Platform 11.3.
 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 *Virtual Host Upgrade Guide* for the steps to upgrade virtual hosts.

Complete the major upgrade tasks in the following order.

- [Phase 1 - Upgrade SA Server, Event Stream Analysis, Malware Analysis, and Broker or Concentrator Hosts](#)

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

- [Phase 2 - Upgrade All Other Hosts](#)
- [Phase 3 \(Optional\) Install Warm Standby NW Server](#)

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

Task 1 - Upgrade the 10.6.6.x SA Server to 11.3 NW Server

Follow the instructions under [Upgrade 10.6.6.x SA Server Host to 11.3 NW Server Host](#).

Task 2 - Upgrade 10.6.6.x ESA to 11.3

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

Follow the instructions under [Upgrade a 10.6.6.x Component Host to 11.3](#) to upgrade your ESA hosts to 11.3 plus the following two tasks.

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 10.6.6.x Malware Analysis to 11.3

Follow the instructions under [Upgrade a 10.6.6.x Component Host to 11.3](#).

Task 4 - Upgrade 10.6.6.x Broker or 10.6.6.x Concentrator to 11.3

Follow the instructions under [Upgrade a 10.6.6.x Component Host to 11.3](#).

Note: If you do not have a Broker, upgrade your Concentrator hosts. The 11.3 NW Server cannot communicate with 10.6.6.x core services for the new Investigate functionality. This is why you must upgrade the Broker or Concentrator hosts in Phase 1.

Phase 2 - Upgrade 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 a 10.6.6.x Component Host to 11.3](#).
3. Restart data capture and aggregation.

Log Decoder Host

1. Make sure you have prepared the Log Collector as described in "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the [Backup Instructions](#).
2. Stop data capture on the Log Decoder.
3. Complete the steps in [Upgrade a 10.6.6.x Component Host to 11.3](#).
4. Restart data capture on Log Decoder.

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

Virtual Log Collector Host

1. Make sure you have prepared the Virtual Log Collector as described the "Log Collectors (LC) and Virtual Log Collectors (VLCs): Run prepare-for-migrate.sh" in the [Backup Instructions](#).
2. Back up your 10.6.6.x VLC by editing the `all-systems` file on host where you performed the

backup.

- a. Make sure your `all-systems` file contents has this information before you perform this step.
`vlc,<host-name>,<IP-address>,<UUID>,10.6.6.x`

- b. Run the following command to create backup.

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

See [Backup Instructions](#) for detailed procedures on how to back up the host.

3. Make sure the backup host contains the VLC backup in the following format.

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

4. Power off the 10.6.6.x VLC so that a new 11.3 VM can be created with the same network configuration.
5. Deploy a fresh NetWitness 11.3 Component Host using the 11.3 NetWitness Platform ova.
6. Connect to the VM console of the new VLC.
7. Update the network configuration to be the same as the 10.6.6.x VLC.
 This information is stored in the `<hostname>-<IPaddress>-network.info.txt` 10.6.6.x VLC backup file.

Note: Make sure IPv6 is disabled.

- a. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and update the settings.
 Contents of `ifcfg-eth0` should be as follows.

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

- b. Submit the following command string.

```
systemctl restart network.service
```

8. Create the backup directory.
`# mkdir -p /var/netwitness/database/nw-backup/`
9. Copy the backup from the backup host from `/var/netwitness/database/nw-backup` to the new

VLC in the `/var/netwitness/database/nw-backup` directory.

10. Complete the steps 2 through 12 inclusive in [Upgrade a 10.6.6.x Component Host to 11.3](#) for the rest of the NetWitness Platform components. Make sure that you select **Log Collector** for the service in step 12.

All Other 10.6.6.x Hosts to 11.3

Follow the instructions under [Upgrade a 10.6.6.x Component Host to 11.3](#).

Upgrade the 10.6.6.x SA Server Host to the 11.3 NW Server Host

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

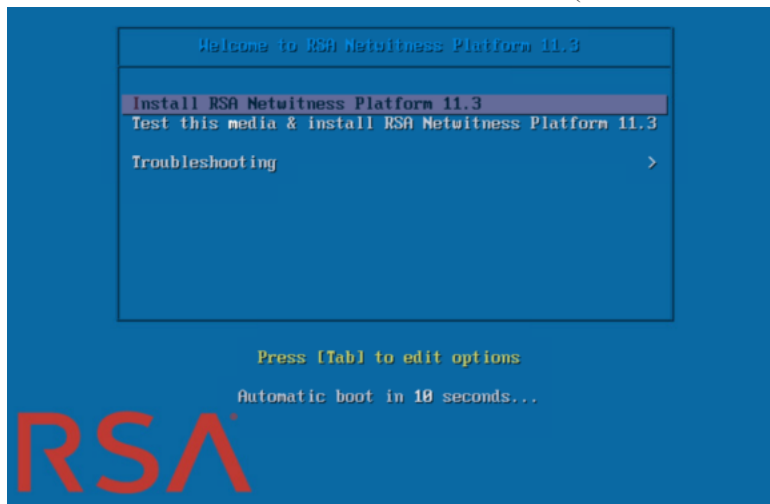
Caution: Run the backup immediately before upgrading the SA Server to 11.3 so that the data is as recent as possible. You must create the **all-systems** file before you upgrade the SA Server because you cannot do this after the SA Server has been upgraded to 11.3.

Complete the following steps to upgrade the 10.6.6.x SA Server host to the 11.3 NW Server host.

1. Create a base image on the host.
 - a. Attach media (media that contains the ISO file, for example, a build stick) to the host. **You must use the build stick labeled “OEMDRV”.**
 - Hypervisor installations - use the ISO image.
 - Physical media - use the ISO to create bootable flash drive media the **Etcher®** or another suitable imaging tool etch an Linux file system on the USB drive. See the *USB Build Stick Instructions and Later* for information on how to create a build stick from the ISO. Etcher is available at: <https://etcher.io>.
 - iDRAC installations - the virtual media type is:
 - **Virtual Floppy** for mapped flash drives.
 - **Virtual CD** for mapped optical media devices or ISO file.
 - 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 system checks during booting, the following **Welcome to RSA NetWitness® Platform 11.3** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

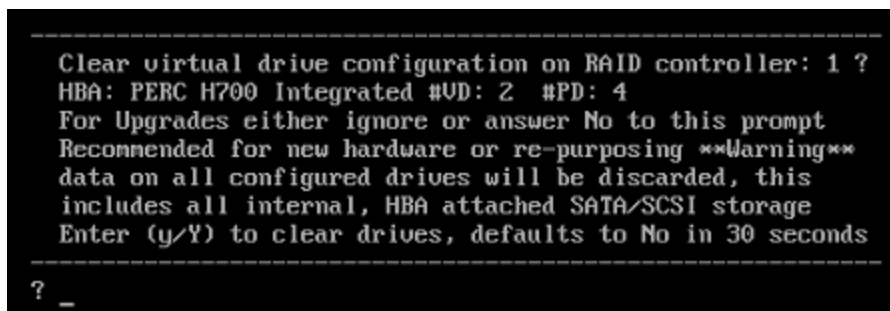
- d. Select **Install RSA Netwitness Platform 11.3** (default selection) and press **Enter**.



The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**.

- e. Enter **n** (No).

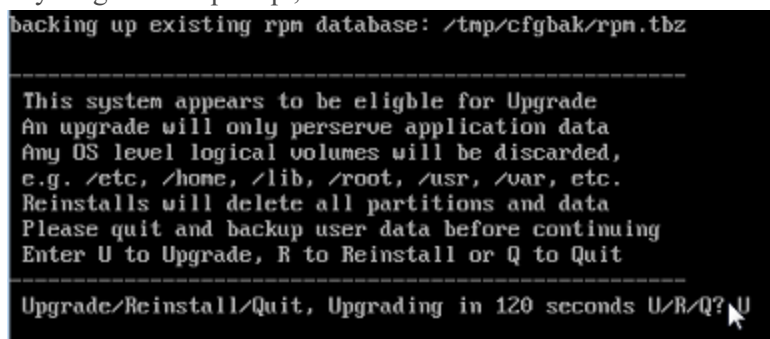
The default action is No, so if you ignore the prompt, it will select No in 30 seconds and will not clear the drives.



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 **Continue (Y/N)?** prompt is displayed.

- g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.

```

=====
Steps to be executed listed below.  Warning:
this is irreversible.
=====
luremove -f /dev/VolGroup00/rabmq
luremove -f /dev/VolGroup00/root
luremove -f /dev/VolGroup00/swap
luremove -f /dev/VolGroup00/tmp
luremove -f /dev/VolGroup00/usrhome
luremove -f /dev/VolGroup00/var
luremove -f /dev/VolGroup00/vartmp
luremove -f /dev/napper/VolGroup01-uax
luremove -f /dev/napper/VolGroup01-rsasoc
ugrename VolGroup00 netwitness_ug00
ugchange -a n VolGroup01
ugmerge netwitness_ug00 VolGroup01
ugchange -a y netwitness_ug00
Continue (Y/N)? Y

```

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.

```
Warning: The old operating system is about to be removed. Continue (Y/N)?
```

When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).

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

```

CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

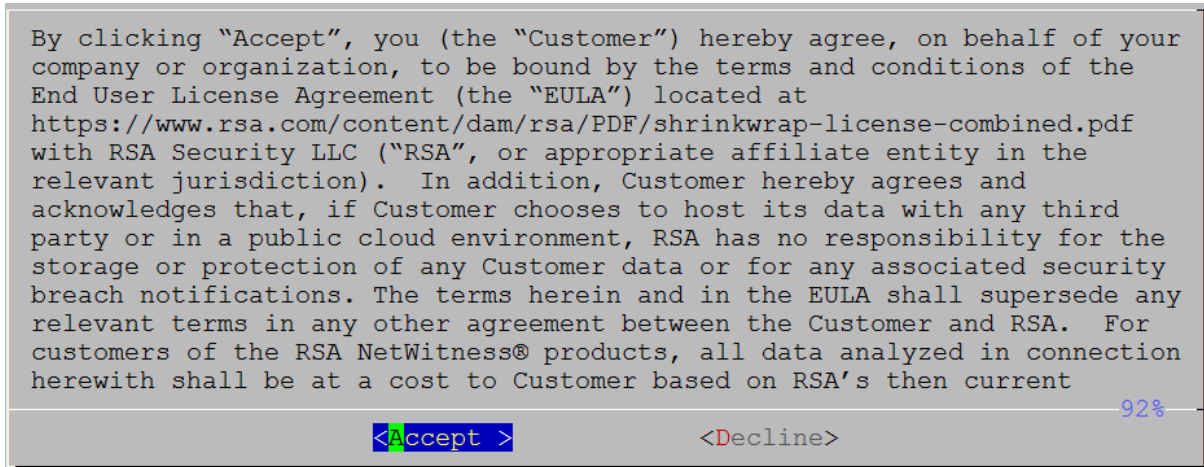
NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#

```

2. Run the `nwsetup-tui` command to set up the host.
This initiates the `nwsetup-tui` (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.

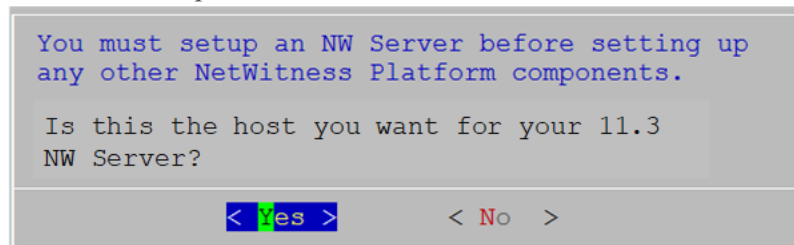
3. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.3 NW Server** prompt is displayed.

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.

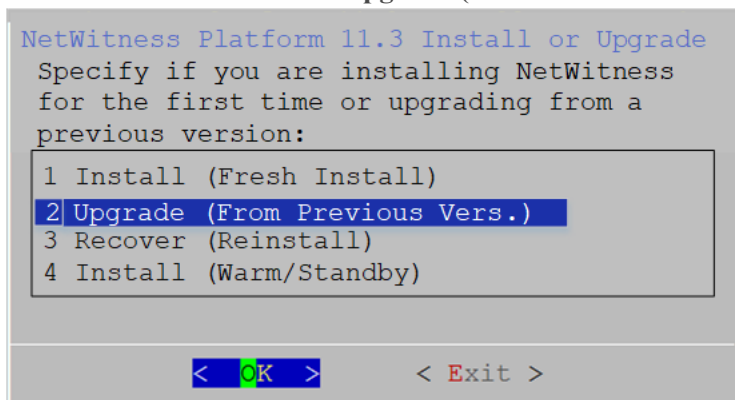
4. Tab to **Yes** and press **Enter**.



Choose **No** if you already upgraded the NW Server to 11.3.

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.

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

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.

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

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

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**.

Master Password

The master password is utilized to set the default password for both the system recovery account and the NetWitness UI "admin" account. The system recovery account password should be safely stored in case account recovery is needed. The NetWitness UI "admin" account password can be updated upon login.

Enter a Master Password.

Password

Verify

< **OK** > <Cancel>

The **Deployment Password** prompt is displayed.

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

Deployment Password

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

Enter a Deploy Password.

Password

Verify

< **OK** > <Cancel>

The **Update Repository** 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**.

NetWitness Platform Update Repository

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

Do you want to set up the NetWitness Platform Update Repository on:

1 The Local Repo (on the NW Server)

2 An External Repo (on an externally-managed server)

< **OK** > <Exit>

- 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 (media that contains the ISO file, for example a build stick) from which upgrade to NetWitness Platform 11.3. If the program cannot find the attached media, you receive the following prompt.

```
NetWitness Platform Update Repository
No media devices detected. Please
insert/attach media and click 'Retry'
to continue.

<Retry > <Ignore>
```

- 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. Refer to [Appendix D. Create External Repository](#) for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

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

< OK > <Cancel>
```

Enter the base URL of the NetWitness Platform external repo and click **OK**.

See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in *Hosts and Services Getting Started Guide* for instructions.

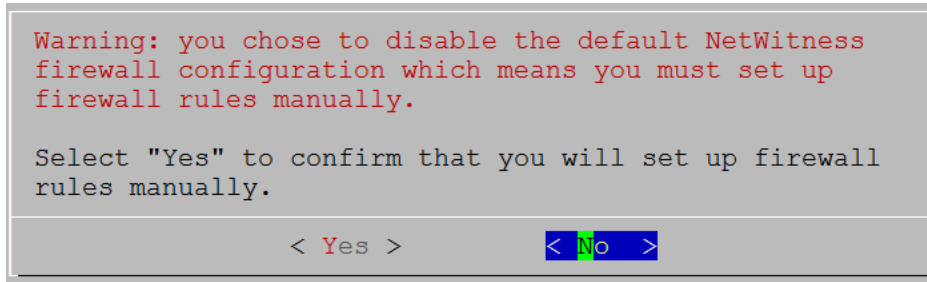
The **Disable** or use standard **Firewall** configuration prompt is displayed.

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.

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

< Yes > < No >
```

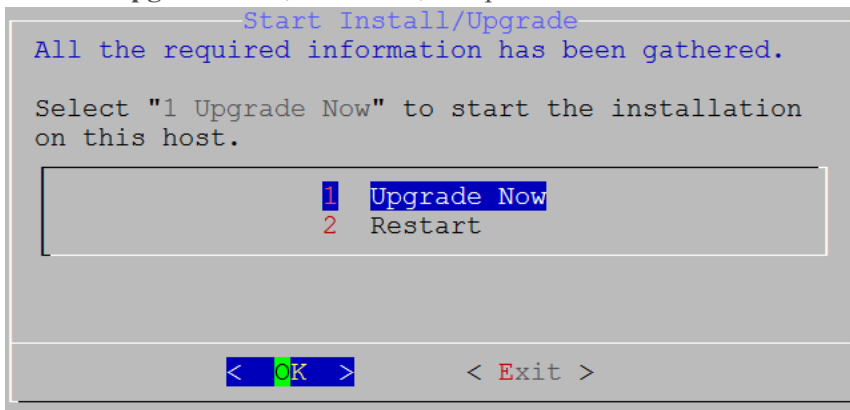

- If you select **Yes** your selection is confirmed.



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

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.3 Disaster Recovery).

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



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

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

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

12. Complete the [Post Upgrade Tasks](#) before you upgrade any of the component hosts to 11.3.

Upgrade a 10.6.6.x Component Host to 11.3

Make sure that you backed up 10.6.6.x data for the host. **You must follow the instructions in [Backup Instructions](#) to back up the host.**

Caution: Run the backup immediately before upgrading the host to 11.3 so that the data is as recent as possible.

Complete the following steps to upgrade a 10.6.6.x component host to 11.3.

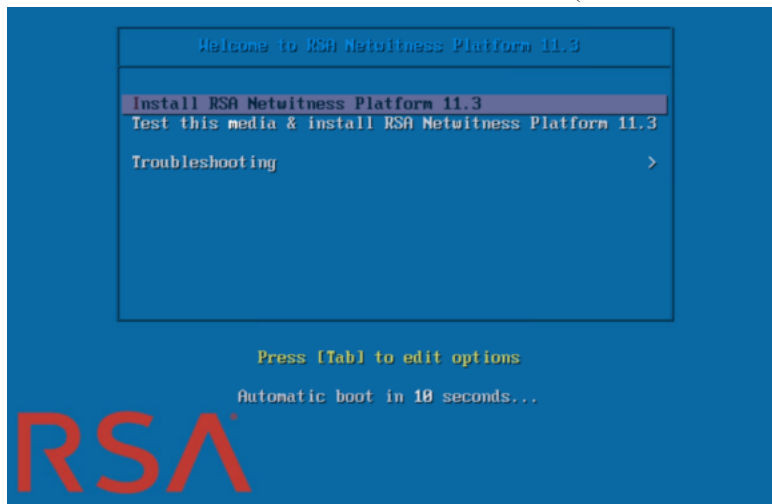
1. Create a base image on the host.
 - a. Attach media (media that contains the ISO file, for example a build stick) to the host. See the *USB Build Stick Instructions and Later* for more information.
 - Hypervisor installations - use the ISO image.
 - Physical media - use the ISO to create bootable flash drive media the **Etcher**® or another suitable imaging tool etch an Linux file system on the USB drive. Etcher is available at: <https://etcher.io>.
 - iDRAC installations - the virtual media type is:
 - **Virtual Floppy** for mapped flash drives.
 - **Virtual CD** for mapped optical media devices or ISO file.

- 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® Platform 11.3** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.

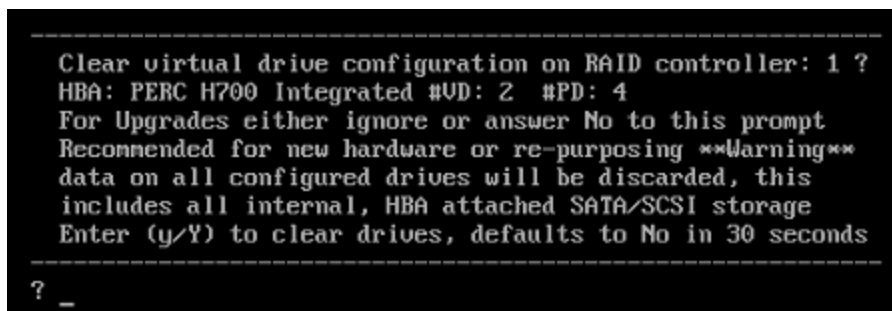
- d. Select **Install RSA Netwitness Platform 11.3** (default selection) and press **Enter**.



The Operating System installation runs and stops at the **Enter (y/Y) to clear drives**.

- e. Enter **n** (No).

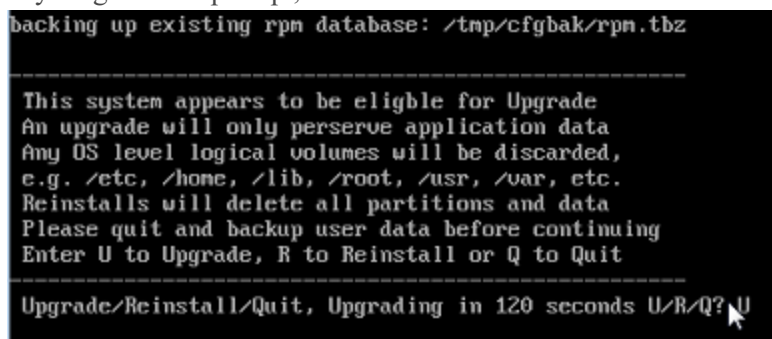
The default action is **No**. If you ignore the prompt, it will select **No** in 30 seconds and will not clear the drives.



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 **Continue (Y/N)?** prompt is displayed.

- g. Type **Y** and press **Enter** to confirm that you want to upgrade this host.

```

=====
Steps to be executed listed below.  Warning:
this is irreversible.
=====
luremove -f /dev/VolGroup00/rabmq
luremove -f /dev/VolGroup00/root
luremove -f /dev/VolGroup00/swap
luremove -f /dev/VolGroup00/tmp
luremove -f /dev/VolGroup00/usrhome
luremove -f /dev/VolGroup00/var
luremove -f /dev/VolGroup00/vartmp
luremove -f /dev/napper/VolGroup01-uax
luremove -f /dev/napper/VolGroup01-rsasoc
vgrename VolGroup00 netwitness_vg00
vgchange -a n VolGroup01
vgmerge netwitness_vg00 VolGroup01
vgchange -a y netwitness_vg00
Continue (Y/N)? Y

```

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.

```
Warning: The old operating system is about to be removed. Continue (Y/N)?
```

When the host is upgraded to CentOS7, the host automatically reboots and prompts you to log in.

Caution: Do not reboot the attached media (media that contains the ISO file, for example a build stick).

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

```

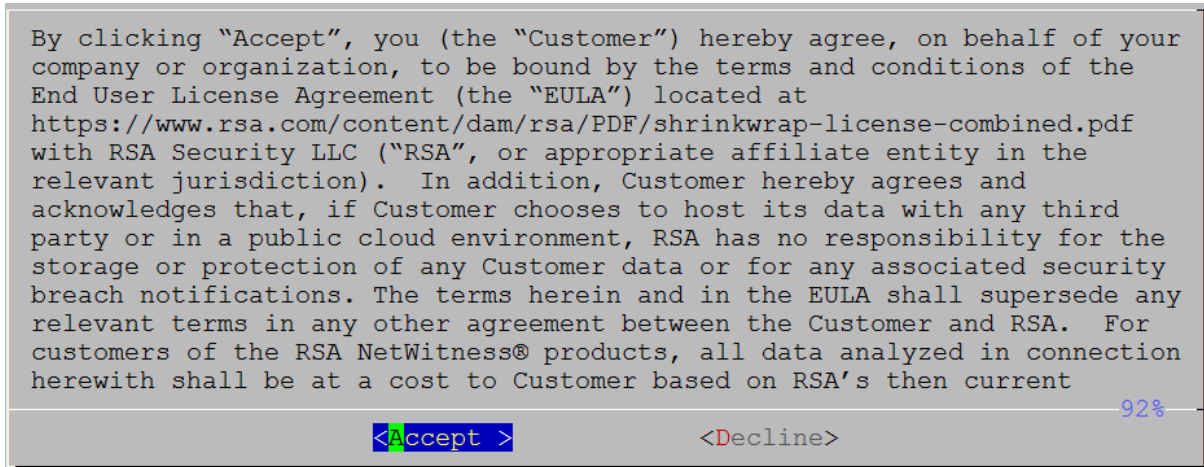
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#

```

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

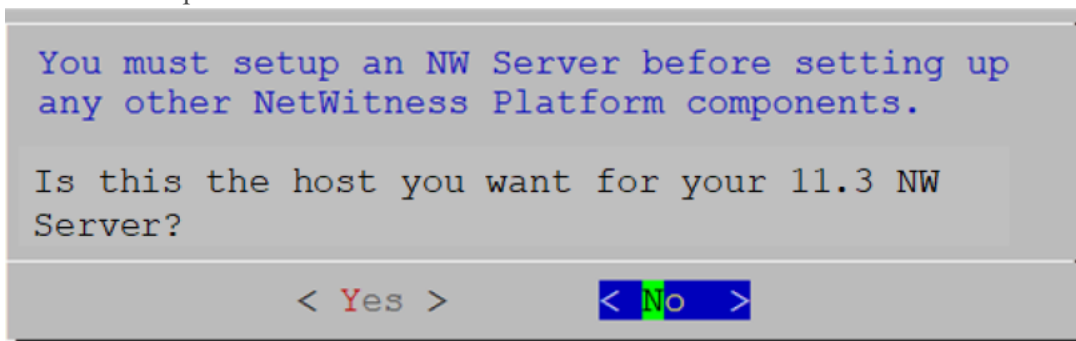
3. Tab to **Accept** and press **Enter**.



The **Is this the host you want for your 11.3 NW Server** prompt is displayed.

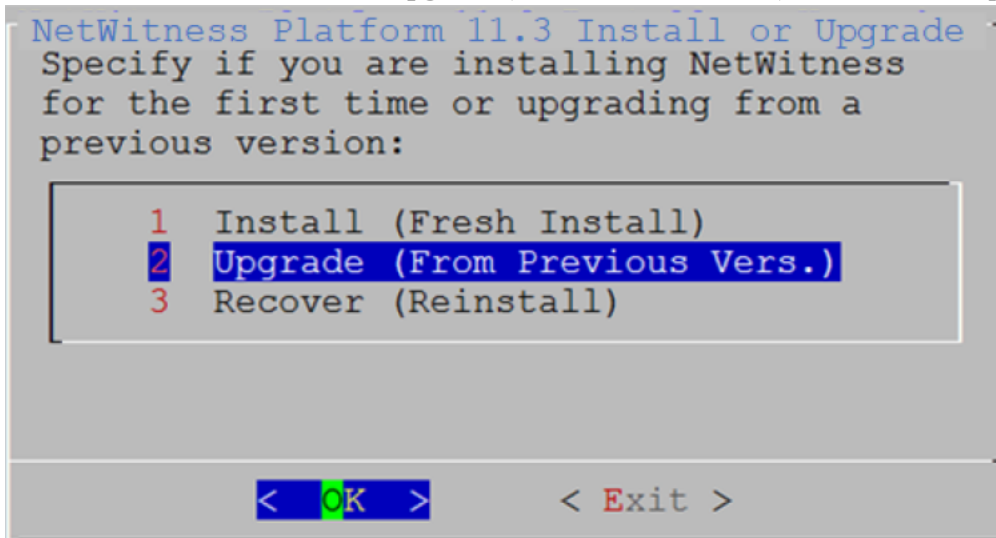
Caution: If you choose the wrong host for the NW Server and complete the upgrade, you must restart the step up program and complete the all the steps (steps 2 through 11) of [Upgrade the 10.6.6.x SA Server Host to the 11.3 NW Server Host](#) to correct this error.

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



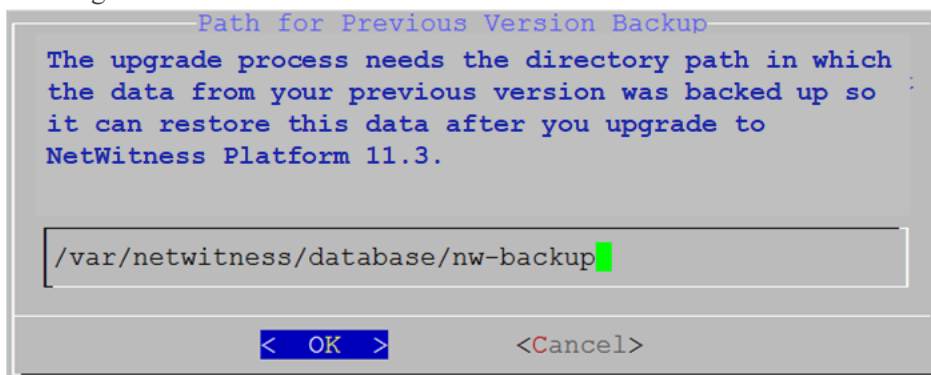
The **Install** or **Upgrade** prompt is displayed.

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



The **Backup** path prompt is displayed.

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.



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

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

The **Deployment Password** prompt is displayed.

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

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

The **Update Repository** prompt is displayed.

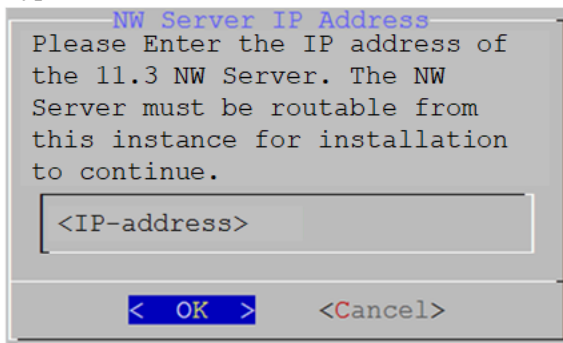
Select the same repo you selected when you upgraded the NW Server Host for all hosts.

8. Use the down and up arrows to select the location from which you want to apply version updates to your hosts (for example, **1 The Local Repo (on the NW Server)**), 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 (media that contains the ISO file, for example a build stick) from which it can upgrade to NetWitness Platform 11.3.
- 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 Platform external repo and click **OK**. The repositories give you access RSA updates and CentOS updates. Refer to [Appendix D. Create External Repository](#) for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.

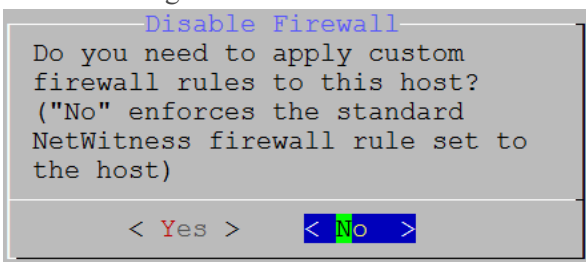
The **NW Server IP Address** prompt is displayed.

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

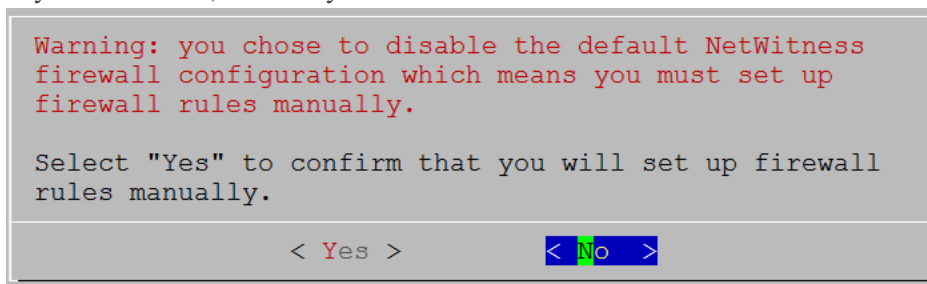


The **Disable** or use standard **Firewall** configuration prompt is displayed.

10. Tab to **No**, and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration. The following example shows **No** with the standard firewall configuration selected.



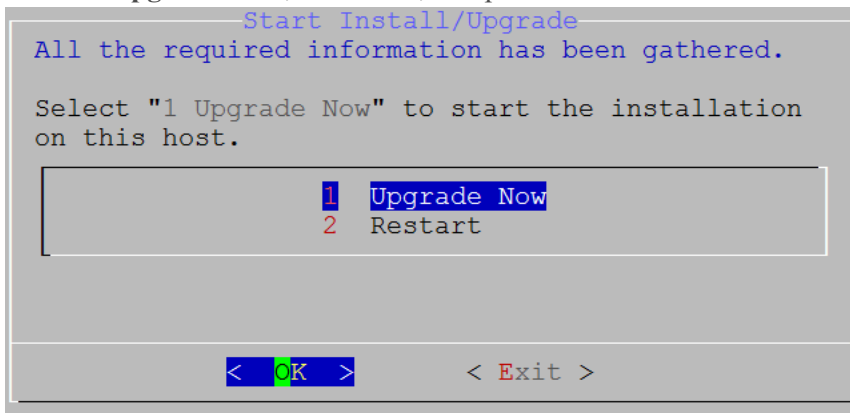
- If you select **Yes**, confirm your selection.



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

The **Install** or **Upgrade** prompt is displayed (**Recover** does not apply to the installation. It is for 11.3 Disaster Recovery).

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




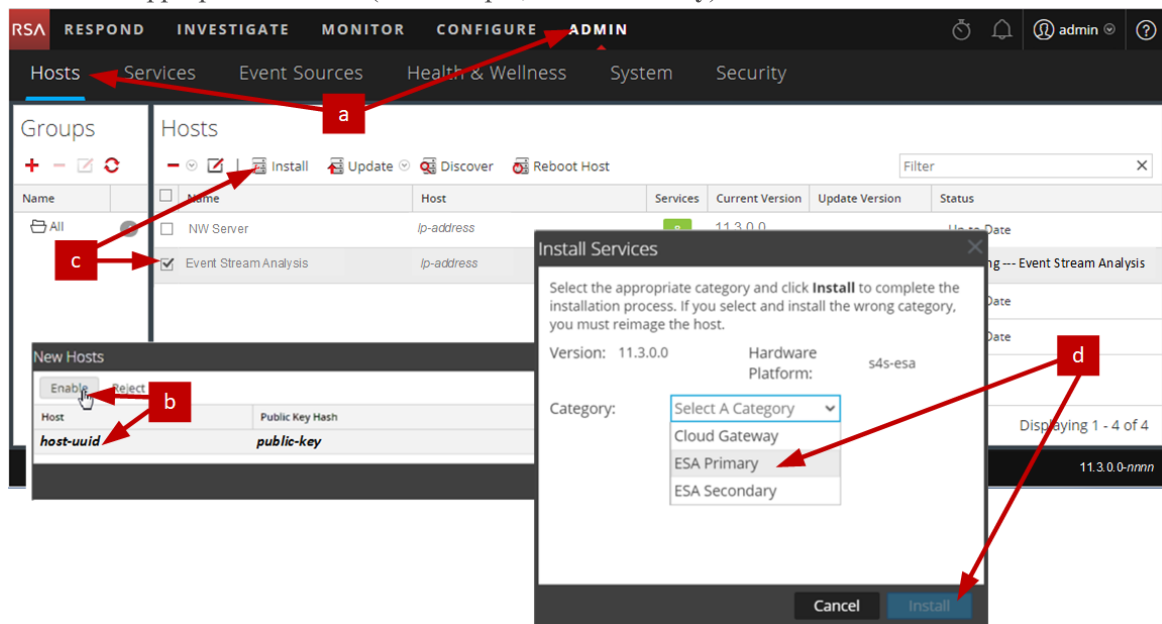
When **Installation complete** is displayed, you have upgraded the host to the 11.3.

12. Install the service on this host:

- a. Log into NetWitness Platform and go to **ADMIN > Hosts**.
The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

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

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



You have completed the upgrade of the Component Host in NetWitness Platform

Phase 3 - (Optional) Install Warm Standby NW Server

Refer to "Warm Standby NW Server Host" under "Deployment Option Setup Procedures" in the *Deployment Guide* for instructions on how to set up a Warm Standby NW Server.

Update or Install Windows Legacy Collection

Refer to the *Windows Legacy Collection Guide for RSA NetWitness 11.x*.

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

Post Upgrade Tasks

You must complete the following tasks after you upgrade your hosts from 10.6.6.x to 11.3. These tasks are organized by the following categories.

- [General](#)
- [Event Stream Analysis](#)
- [Investigate](#)
- [Log Collection](#)
- [Log Decoder and Decoder](#)
- [Malware Analysis](#)
- [Reporting Engine](#)
- [Respond](#)
- [Warehouse](#)
- [RSA Archer® Cyber Incident & Breach Response](#)
- [RSA NetWitness® Endpoint](#)
- [RSA NetWitness® UEBA](#)
- [NetWitness Platform Integrations](#)
- [Other](#)

Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

General

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

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

Caution: 1) You must retain a copy of all backup files on an external host. 2) Validate that you have all your data from your backup restored in 11.3 before you remove the backup-related files from the local directories on your 11.3 hosts.

Backup .tar Files

After all the hosts are upgraded to 11.3, you must remove:

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

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

Task 2 - Make Sure Port 15671 Is Configured Correctly

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

(Optional) Task 3 - Reissue Certificates for Your Hosts

In 11.3.0.0, RSA introduced a `cert-reissue` command line command and its arguments to reissue host certificates. After you update all your hosts to 11.3, you should reissue certificates for all of them as soon as possible to avoid having them expire. If the certificates expire, this places your NetWitness deployment in a bad security state. Refer to the *Security Configuration Guide* for instructions on how to use the `cert-reissue` command.

(Conditional) Task 4 - Restore Custom Analysts Roles

If you had custom analyst roles in 10.6.6.x, you must reinstate them in 11.3. See "Add a Role and Assign Permissions" in the *System Security and User Management Guide*.

(Conditional) Task 5 - If NetWitness Platform Has No Web Access, Upload

Response .bin File Again (License Server)

If your NetWitness Deployment does not have Internet access, after you upgrade to 11.3, you must upload the response .bin file again to view the license information in the **ADMIN > System > Licensing** view in the NetWitness Platform User Interface. See "Upload an Offline Capability Response to NetWitness Platform" in the *Licensing Management Guide* for instructions.

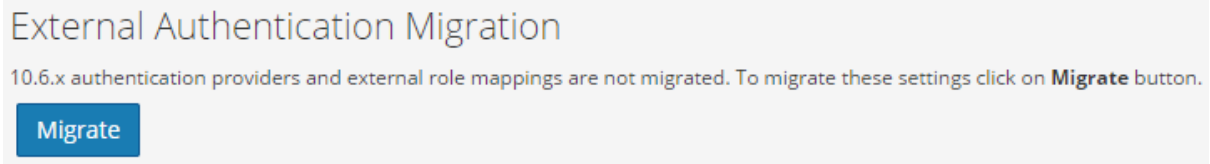
Task 6 - Migrate Active Directory (AD)

The first time you log into the NetWitness Platform 11.3 User Interface, you must click on the Migrate button to complete the migration of AD.

1. Log in to NetWitness Platform 11.3 with your `admin` user credentials.

2. Go to **ADMIN > SECURITY** and click the **Settings** tab.

The following dialog is displayed.




3. Click **Migrate**.

The migration is complete and the dialog closes.

Task 7 - Modify Migrated AD Configuration to Upload Certificate

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

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

1. Log in to **NetWitness Platform 11.3**, go to **ADMIN > Security** and click the **Settings** tab.
2. Under **Active Directory Settings**, select an AD configuration and click .
The Edit Configuration dialog is displayed.
3. Go to the **Certificate File** field, click **Browse**, and select a certificate from your network.
4. Click **Save**.

Task 8 - Reconfigure Pluggable Authentication Module (PAM) in 11.3

You must reconfigure PAM after you upgrade to 11.3. See "Configure PAM Login Capability" in the *System Security and User Management Guide* for instructions.

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

Task 9 - Restore NTP Servers

You must use the NetWitness Platform 11.3 user interface to restore NTP server configurations. NTP server configuration information is located in `$BUPATH/restore/etc/ntp.conf`. Use the NTP server name and hostname from the `/var/netwitness/restore/etc/ntp.conf` file. See "Configure NTP Servers" in the *System Configuration Guide* for detailed instructions on how to add NTP servers.

Task 10 - Restore Licenses for Environments without FlexNet Operations-On Demand Access

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

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

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

Note: You can refer to the `$BUPATH/restore/etc/sysconfig/iptables` and `$BUPATH/restore/etc/sysconfig/ip6tables` in the `restore` folder of the backup to update the `ip6tables` and `iptables` files. The `/etc/netwitness/firewall1.cfg` file contains the standard `iptables` firewall rules.

1. SSH to each host and log in with your root credentials.
2. Update the following `ip6tables` and `iptables` files with the custom firewall rules.

```
/etc/sysconfig/iptables
/etc/sysconfig/ip6tables
```
3. Reload the `iptables` and `ip6tables` services.

```
service iptables reload
service ip6tables reload
```

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


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

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

NetWitness Platform 11.3 cannot communicate with the Core services if you are using a non-SSL port 500XX. You must update the Core service ports to an SSL port in the Edit Service dialog.

1. Log in to **NetWitness Platform** and go to **ADMIN > Services**.
2. Select each core service and change the ports from Non-SSL to SSL ports.

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

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

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

Service	Broker
Host	nwappliance13731
Name	nwappliance13731 - Bro

Connection Details

Port: 56003

SSL: ☒

Test Connection

Cancel Save


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

If you had PKI keystores that contained server certificates with private keys and the truststores that contain the trusted CA certificates, you must reconfigure after you upgrade to 11.3. For instructions on how to configure PKI authentication, see the “*System Security and User Management Guide*”.

Event Stream Analysis (ESA)

Task 14 - Reconfigure Automated Threat Detection for ESA

If you used Automated Threat Detection in 10.6.6.x, you must complete the following steps to reconfigure it using the ESA Analytics service in 11.3.

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

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

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

If you added any string array type meta keys to the Event Stream Analysis service for your ESA correlation rules in 10.6.6.x or earlier, verify that they appear on the ESA Correlation service in 11.3.

1. Follow the “Configure Meta Keys as Arrays in ESA Correlation Rule Values” procedure in the *ESA Configuration Guide* to verify if the string array type meta keys that were added before the upgrade are on the ESA Correlation service. Add any missing string array type meta keys.
2. Do not remove any meta keys from the multi-valued parameter on the ESA Correlation service. In NetWitness Platform 11.3, the ESA rules from Live use meta keys with array syntax and they depend on these meta keys to work correctly. Removing values from the multi-valued list can cause the ESA Rule Deployments to fail.

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

The following table lists the ESA rules from RSA Live that had meta key type changes from String to Array in NetWitness Platform 11.3.

Rule #	Rule Name	Array Type Meta Keys in 11.3
1	RIG Exploit Kit	threat_category
2	AWS Critical VM Modified	alert
3	Multiple Successful Logins from Multiple Diff Src to Same Dest	host.src and host.dst
4	Multiple Successful Logins from Multiple Diff Src to Diff Dest	host.src and host.dst
5	Multiple Failed Logins from Multiple Diff Sources to Same Dest	host.src and host.dst
6	Multiple Failed Logins from Multiple Users to Same Destination	host.src and host.dst
7	User Login Baseline	host.src and host.dst

1. If you:
 - Deployed these rules before version 11.3:
 - a. Note any rule parameters that you have changed so you can adjust the rules for your environment.
 - b. Download the updated rules from RSA Live.

- c. Reapply any changes to the default rule parameters and deploy the rules.
(For instructions, see “Download RSA Live ESA Rules” in the *Alerting with ESA Correlation Rules User Guide*.)
 - Are deploying these rules for the first time in version 11.3, follow the customization directions with the ESA rule descriptions. Rules 3 to 7 in the above table require that the Context Hub lists for `User_Whitelist`, `Host_Whitelist` and `IP_Whitelist` to be added as enrichments to ESA. (See “Configure Context Hub List as an Enrichment Source” in the *Alerting with ESA Correlation Rules User Guide*.)
2. Deploy the ESA rule deployment that contains these rules. (See “ESA Rule Deployment Steps” in the *Alerting with ESA Correlation Rules User Guide*.)

Task 17 (Conditional) - Verify ESA Rule Deployment

After you upgrade to 11.3, verify your ESA rule deployments. For every ESA host, a new deployment is created in the format “<ESA Host name> – ESA Correlation”.


1. Make sure that a new deployment was created.
2. Make sure that the new deployment contains an ESA Correlation service, data sources, and rules for all previous deployments on that ESA host.
3. Make sure that the ESA Correlation service has status of “Deployed”.

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

Investigate

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

After you upgrade to 11.3.0.0, any customized user role does not have `investigate-server.*` permission enabled by default. Complete the following procedure to make sure that the appropriate user roles have permission to access Event Analysis.

1. Log in to NetWitness Platform 11.3.0.0 with your `Admin` user credentials and go to **ADMIN > Security**.
2. Click the **Roles** tab.
3. Select the roles that need `investigate-server.*` permissions and click  (Edit icon).
4. Select the **Investigate-server** tab under **Permissions**.

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

Permissions

< Esa-analytics-server Incidents Integration-server Investigate Investigate-server >	
Assigned	Description ^
<input type="checkbox"/>	Investigate-server
<input checked="" type="checkbox"/>	investigate-server.*

6. Click **Save**.

Log Collection

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


Complete the following tasks to reset stable system values for the Log Collector after you upgrade it to 11.3 to ensure that all collection protocols resume normal operation.

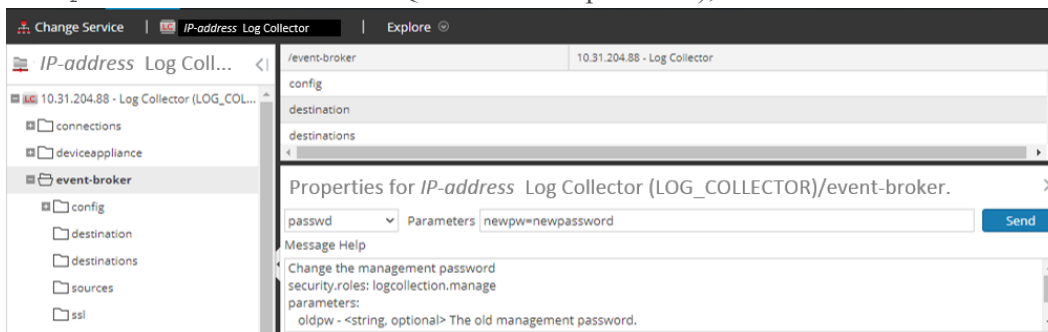
Reset Stable System Values for the Lockbox

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

Update Log Collector Service RabbitMQ User Account Password

If the `logcollector` service RabbitMQ user account password was changed, you must reenter it after the 11.3 upgrade.

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



Task 20 - (Conditional) Update SSHD Configuration after Upgrade with Older Windows and UNIX SFTP Agents

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

If all the event sources:

- Resume collection after upgrade, you do not need to do anything.
- Do not resume collection after the upgrade, you may have to restore Cipher, MACs and Key Exchange Algorithms to the SSHD configuration from the original LC/VLC. Change the `/etc/ssh/sshd_config` file.

1. Make the following changes to `/etc/ssh/sshd_config` file.
 - a. If the `KexAlgorithms` line:
 - Exists, append `diffie-hellman-group1-sha1` to the file.
 - Does not exist, add `KexAlgorithms +diffie-hellman-group1-sha1` line.
 - b. If the `Ciphers` line:
 - Exists, append `aes128-cbc` to the file.
 - Does not exist, add the `Ciphers +aes128-cbc` line to the file.
2. Restart SSHD service.
3. If collection still fails, edit the `/etc/systemd/system/sshd.service.d/sshd-opts-managed.conf` file and change `OWB_ALLOW_NON_FIPS=on` to `OWB_FIPS_MODE=off` in the Environment line and restart SSHD service.
4. If collection still fails, contact RSA Customer Support (<https://community.rsa.com/docs/DOC-1294>).

Task 21 - Enable FIPS Mode

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


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

Log Decoder and Decoder

(Conditional) Task 23 - Enable Metadata for GeoIP2 Parser

By default, the GeoIP2 parser generates less metadata than the GeoIP parser did. After updating to 11.3, if you require any of the additional metadata, you must enable them (once only) for each Decoder. This can also be altered post-upgrade. Note that the `isp` and `org` meta fields usually produce an equivalent value to `domain`.

To enable metadata:

1. Go to **ADMIN > Services**.
2. In the **Administration services** view, select a Log Decoder or a Decoder.
3. Click the settings icon () and select **View > Config**. The Parsers Configuration panel is displayed, from which you can select **GeoIP2** to enable the desired metadata.

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

Malware Analysis

Task 24 - Enable Threat - Malware Indicators Dashboard

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

1. Enable the **Threat - Malware Indicators Dashboard** in 11.3.
2. Set datasource for new dashlets.
See "Dashlets" in RSA Link (<https://community.rsa.com/docs/DOC-81463>) for a description of Dashlets in the context of NetWitness Platform.

Note: After upgrading to 11.3, both the Threat-Indicators and the Threat-Malware Indicators dashboards can be displayed in the User Interface. If this is the case, disable the Threat-Indicators dashboard, and enable the Threat-Malware Indicators report charts and dashboard. For information about disabling dashboards, see the "Managing Dashboards" topic in the *NetWitness Getting Started Guide*.

Reporting Engine

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

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

Complete the following procedure to restore the CA certificates in 11.3.

1. SSH to the NW Server host.
2. Export the CA certificates.
`keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file`
3. Copy the CA PEM file into `/etc/pki/nw/trust/import` directory.

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

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

Respond

Task 27 - Restore Respond Service Custom Keys

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

1. Copy the custom keys from `/opt/rsa/im/fields/alert_rules.json` file in the backup directory.
This directory is where the `alert_rules.json` file is restored from the 10.6.6.x backup.
2. Go to the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.3.
This is the new file for 11.3.
3. Edit the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` to include the custom keys you copied in step one.

Task 28 - Restore Customized Respond Service Normalization Scripts

RSA re-factored the Respond service normalization scripts in 11.3 and moved them to the following new location:

`/var/lib/netwitness/respond-server/scripts`

If you customized these scripts in 10.6.6.x, you must:

1. Go to the `/opt/rsa/im/scripts` directory.
This directory is where the following Respond service normalization scripts are restored from the 10.6.6.x backup.
`data_privacy_map.js`
`normalize_alerts.js`
`normalize_core_alerts.js`
`normalize_ecat_alerts.js`
`normalize_ma_alerts.js`
`normalize_wtd_alerts.js`
`utils.js`
2. Copy any custom logic from the 10.6.6.x scripts.
3. Go to the `/var/lib/netwitness/respond-server/scripts` directory.
This directory is where NetWitness Platform 11.3 stores the re-factored scripts.
4. Edit the new scripts to include the custom logic you copied in step 2 from the 10.6.6.x scripts.
5. Copy any custom logic from `/opt/rsa/im/fields/alert_rules.json` file.
The `alert_rules.json` file contains aggregation rule schema.

Task 29 - Add Respond Notification Settings for Custom Roles

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

To access these settings, you will need to add additional permissions to your existing built-in NetWitness Platform user roles. You will also need to add permissions to your custom roles. See the “Respond Notification Settings Permissions” topic in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*.


Task 30 - Manually Configure Respond Notification Settings

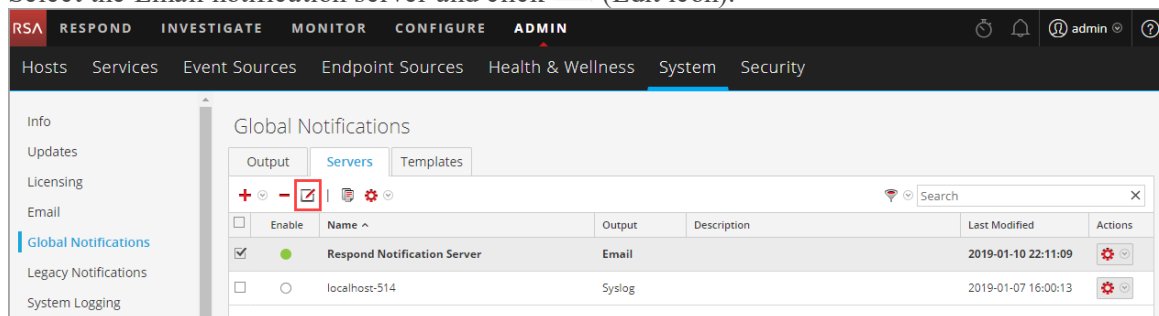
The Incident Management notification settings in NetWitness Platform 10.6.6.x are different from the Respond notification settings available in 11.3, so your existing 10.6.6.x settings will not migrate to 11.3.

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

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

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

1. Log in to **NetWitness Platform** and go to **CONFIGURE > Respond Notifications**.
The Respond Notifications Settings view is displayed. Notice that the email notification servers do not appear in the EMAIL SERVER drop-down list.
2. Click the **Email Server Settings** link.
You will see the Global Notifications panel.
3. Click the **Servers** tab.
4. For each of your email notification servers:
 - a. Select the Email notification server and click  (Edit icon).



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

5. Go back to **CONFIGURE > Respond Notifications**. Your servers will appear in the **EMAIL SERVER** drop-down list.
Custom Incident Management notification templates cannot be migrated to 11.3. No custom templates are supported in 11.3.

Task 31 - Update Default Incident Rule Group By Values

The following default incident rules now use “Source IP Address” as the Group By value.

- **High Risk Alerts: Reporting Engine**
- **High Risk Alerts: Malware Analysis**
- **High Risk Alerts: ESA**

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

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

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

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules** and click on the rule that you want to update in the **Name** column. The **Incident Rule Details** view is displayed.
2. In the **GROUP BY** field, select the new Group By value from the drop-down list.
3. Click **Save** to update the rule.

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

1. In the **NetWitness Platform** menu, select **CONFIGURE > Incident Rules**. The **Incident Rules List** view is displayed.
2. Select the **High Risk Alerts: NetWitness Endpoint** default incident rule and click **Clone**. You will receive a message that you successfully cloned the selected rule.
3. Change the Name of the rule to an appropriate name, such as **High Risk Alerts: NetWitness Endpoint File hash**.
4. In the **GROUP BY** field, remove the previous Group By value and add **File MD5 Hash**. It is important that File MD5 Hash is the only Group By value listed.
5. Click **Save** to create the rule.

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

Task 32 - Add Group By Field to Incident Rules

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

Complete the following steps for each incident rule:

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

> ENDPOINT RISK SCORING SETTINGS

INCIDENT RULES

Create Rule Clone Delete

SELECT	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS
		1		User Behavior	This incident rule captures network user behavior.	0	0
		2		Suspected Command & Control Communication By Domain	This incident rule captures suspected communic...	0	0
		3		High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by t...	0	0
		4		High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by t...	0	0
		5		High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by t...	0	0
		6		High Risk Alerts: ESA	This incident rule captures alerts generated by t...	0	0
		7		IP Watch List: Activity Detected	This incident rule captures alerts generated by l...	0	0
		8		User Watch List: Activity Detected	This incident rule captures alerts generated by n...	0	0
		9		Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicat...	0	0
		10		Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify co...	0	0
		11		Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an al...	0	0
		12		Web Threat Detection	This incident rule captures alerts generated by t...	0	0
		13		User Entity Behavior Analytics	This incident rule captures user entity behavior.	0	0

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

The screenshot shows the RSA NetWitness Platform configuration interface for an incident rule. The interface is divided into several sections:

- BASIC SETTINGS:** Includes a toggle for 'ENABLED', a 'NAME*' field with the value 'User Watch List: Activity Detected', and a 'DESCRIPTION' field with a detailed explanation of the rule's purpose.
- MATCH CONDITIONS*:** Includes a 'QUERY MODE' dropdown set to 'Rule Builder' and an 'Add Group' button. Below this is a table of conditions:

Any of these	FIELD	OPERATOR	VALUE
Add Condition	Source Username	is equal to	jsmith
	Source Username	is equal to	jdoe
- ACTION*:** Includes a section 'CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT' with two radio buttons: 'Group into an Incident' (selected) and 'Suppress the Alert'.
- GROUPING OPTIONS:** Includes a 'GROUP BY*' dropdown menu with the value 'Source Username' selected, and a 'TIME WINDOW' dropdown set to '4 Hours'.

The 'GROUP BY*' dropdown menu is highlighted with a red box. At the bottom right, there are 'Cancel' and 'Save' buttons.

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

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

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

Upgrade Preparation Task

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

For each rule that you previously identified:

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

ENDPOINT RISK SCORING SETTINGS

INCIDENT RULES

Create Rule Clone Delete

	SELECT	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS
	<input type="radio"/>	1		User Behavior	This incident rule captures network user behavior.		0	0
	<input type="radio"/>	2		Suspected Command & Control Communication By Domain	This incident rule captures suspected communic...		0	0
	<input type="radio"/>	3		High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by t...		0	0
	<input type="radio"/>	4		High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by t...		0	0
	<input type="radio"/>	5		High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by t...		0	0
	<input type="radio"/>	6		High Risk Alerts: ESA	This incident rule captures alerts generated by t...		0	0
	<input type="radio"/>	7		IP Watch List: Activity Detected	This incident rule captures alerts generated by l...		0	0
	<input type="radio"/>	8		User Watch List: Activity Detected	This incident rule captures alerts generated by n...		0	0
	<input type="radio"/>	9		Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are Indikat...		0	0
	<input type="radio"/>	10		Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify co...		0	0
	<input type="radio"/>	11		Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an al...		0	0
	<input type="radio"/>	12		Web Threat Detection	This incident rule captures alerts generated by t...		0	0
	<input type="radio"/>	13		User Entity Behavior Analytics	This incident rule captures user entity behavior.		0	0

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

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN

Live Content Incident Rules Respond Notifications ESA Rules Subscriptions Custom Feeds Log Parser Rules

BASIC SETTINGS ☒ ENABLED

NAME*

Verify Domain for Suspected C&C field

DESCRIPTION

This rule had match conditions for Domain & Domain for Suspected C&C in rule builder

MATCH CONDITIONS*

QUERY MODE

Rule Builder

Add Group

All of these Add Condition

FIELD

FIELD

At least one condition is missing a field, operator, or value

ACTION*

CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT

☒ Group into an incident ☐ Suppress the Alert

There is required information missing from the incident rule

Cancel Save

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

Warehouse

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

1. Restore the `keytab` files from `<backup-path>/restore` directory.
2. Restore the Kerberos Realm Configuration from the `<backup-path>/restore/etc/krb5.conf` into `/etc/krb5.conf`.
3. (Conditional) If you perform the upgrade from a Non - FIPS environment and the `isCheckValidationRequired` parameter is not enabled in the destination, to configure the SFTP destination:
 - a. SSH to the Warehouse Connector host and submit the following commands:


```
cd /root/.ssh/
mv id_dsa id_dsa.old
OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_dsa.old -
out id_dsa
```

 You are prompted for the pass phrase.
 - b. Enter the Encryption password.
 - c. Run the following command.


```
chmod 600 id_dsa
```
4. Install the Warehouse Connector.
See the *Warehouse Connector Configuration Guide* for instructions.

Task 35 - Refresh Warehouse Connector Lockbox and Start Stream

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

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


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

Task 36 - Update Hive Version

After you update to 11.3, you must update to the Hive version that is compatible with the 11.3 Warehouse (either Hive version 0.12 or version 1.0).

- Hive Version 0.12
SSH to the NW Server and run the following command.


```
rpm -ivh rsa-nw-hive-jdbc-0.12.0-1.x86_64.rpm
```


- Hive Version 1.0
SSH to the NW Server and run the following command.

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

RSA Archer Cyber Incident & Breach Response

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

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

RSA NetWitness® Endpoint

Task 38 - Reconfigure Endpoint Alerts Via Message Bus

1. On the NetWitness Endpoint Server, modify the virtual host configuration in the `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` file to reflect the following configuration.

```
<add key="IMVirtualHost" value="/rsa/system" />
```

Note: In NetWitness Platform 11.3, the virtual host is `/rsa/system`. For 10.6.6.x and earlier versions, the virtual host is `/rsa/sa`.

2. Restart the API Server and Console Server.
3. SSH to the NW Server and log in with `root` credentials.
4. Submit the following command to add all certificates to the truststore.

```
orchestration-cli-client --update-admin-node
```
5. Submit the following command to restart the RabbitMQ server.

```
systemctl restart rabbitmq-server
```

The NetWitness Endpoint account should automatically be available on RabbitMQ.
6. Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NW Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Task 39 - Reconfigure Recurring Feed Configured from Legacy Endpoint Because Java Version Changed

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

- Import the NetWitness Endpoint CA certificate into the NetWitness Platform Trusted store as described in "Export the NetWitness Endpoint SSL Certificate" under the "Configure Contextual Data from Endpoint via Recurring Feed" topic in the *RSA NetWitness Endpoint Integration Guide* to import the certificate.

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

See:

RSA NetWitness Platform 11.3 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Platform 11.3 Virtual Host Installation Guide for instructions for installation on a virtual host.

RSA NetWitness® UEBA

Task 41 - Install NetWitness UEBA

NetWitness UEBA is new a new feature as of NetWitness Platform 11.3.

See:

RSA NetWitness Platform 11.3 Physical Host Installation Guide for instructions for installation on a physical host.

RSA NetWitness Platform 11.3 Virtual Host Installation Guide for instructions for installation on a virtual host.

RSA NetWitness UEBA User Guide for information about NetWitness UEBA.

NetWitness Platform Integrations

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

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

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

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

```
> rabbitmqctl add_user <username> <password>
```
2. Set permissions for users by running the following command (use the username from step 1).

```
> rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"
```

For example:

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

Other

none

Appendix A. Troubleshooting

There two sections in this appendix.

- [Section 1 - General Troubleshooting Information](#)
- [Section 2 - Hardware-Related Troubleshooting Information](#)

Section 1 - General Troubleshooting information

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

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

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

- [Command Line Interface \(CLI\)](#)
- [Backup Script](#)
- [Event Stream Analysis](#)
- [Concentrator Service](#)
- [Log Collector Service \(nwlogcollector\)](#)
- [Orchestration](#)
- [NW Server](#)
- [Reporting Engine](#)
- [NetWitness UEBA](#)


Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Command Line Interface (CLI)

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

2. Run the `nwsetup-tui` again using correct `deploy_admin` password.

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

Error Message	<p>You receive a message in the User Interface to reboot the host after you update and reboot the host offline.</p> 
Cause	You cannot use CLI to reboot the host. You must use the User Interface.
Solution	Reboot the host in the Host View in the User Interface.

Backup (nw-backup script)

Error Message	WARNING: Incorrect ESA Mongo admin password for host <hostname>.
Cause	ESA Mongo admin password contains special characters (for example, '!@#\$\$%^qwerty').
Solution	Change the ESA Mongo admin password back to the original default of 'netwitness' before running backup.

Error	<p>Backup errors caused by the immutable attribute setting. Here is an example of an error that can be displayed:</p> <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
Cause	If you have any files that have the immutable flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.
Solution	On the host that contains the files with the immutable flag set, run the following command to remove the immutable setting from the files: chattr -i <filename>

Error	<p>Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: <code>/etc/sysconfig/network-scripts/ifcfg-em1</code> Verify contents of <code>/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</code></p>
Cause	<p>There are incorrect or duplicate entries for any one of the following fields: DEVICE, BOOTPROTO, IPADDR, NETMASK or GATEWAY, that were found from reading the primary Ethernet interface configuration file from the host being backed up.</p>
Solution	<p>Manually create a file at the backup location on the external backup server, as well as the backup location local to the host where other backups have been staged. The file name should be of the format <code><hostname>-<hostip>-network.info.txt</code>, and should contain the following entries:</p> <pre> DEVICE=<devicename> ; # from the host's primary ethernet interface config file BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file IPADDR=<value> ; # from the host's primary ethernet interface config file NETMASK=<value> ; # from the host's primary ethernet interface config file GATEWAY=<value> ; # from the host's primary ethernet interface config file search <value> ; # from the host's /etc/resolv.conf file nameserver <value> ; # from the host's /etc/resolv.conf file </pre>

Event Stream Analysis

- For ESA Correlation troubleshooting information, see the *Alerting with ESA Correlation Rules User Guide*.
- For ESA Analytics troubleshooting information, see the *Automated Threat Detection Configuration Guide*.

Concentrator Service

Problem	After you upgrade to 11.3.0.0, pivot to navigate query fails if the Concentrator service version is 10.6.x.
Cause	Pivot to Navigate query fails as it contains meta entities and 10.6.x Concentrator service does not support meta entities.
Solution	You must edit the query and remove meta entities. For example, if query is for user then remove the <code>user.all</code> meta entity and re-run the query.

Log Collector Service (`nwlogcollector`)

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

Error Message	<code><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.</code>
Cause	The Log Collector Lockbox failed to open after the update.
Solution	Log in to NetWitness Platform and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

Error Message	<code><timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
Cause	The Log Collector Lockbox is not configured after the update.
Solution	If you use a Log Collector Lockbox, log in to NetWitness Platform and configure the Lockbox as described in the "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

Error Message	<code><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.</code>
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Solution	Log in to NetWitness Platform and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

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. <pre># /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert</pre>

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 <code>sa.log</code> . Syslog Configuration migration failed. Restart jetty service to fix this issue
Cause	NW Server Global Audit setup migration failed to migrate from 10.6.6.x to 11.3.0.0.
Solution	<ol style="list-style-type: none"> 1. SSH to the NW Server. 2. Submit the following command. <code>orchestration-cli-client --update-admin-node</code>

Orchestration

The orchestration server logs are posted to `/var/log/netwitness/orchestration-server/orchestration-server.log` on the NW Server Host.

Problem	<ol style="list-style-type: none"> 1. Tried to upgrade a non-NW Server host and it failed. 2. Retried the upgrade for this host and it failed again.
Cause	<p>You will see the following message in the <code>orchestration-server.log</code>. <code>"'file' _virtual_ returned False: cannot import name HASHES"</code></p> <p>Salt minion may have been upgraded and never restarted on failed non-NW Server host</p>
Solution	<ol style="list-style-type: none"> 1. SSH to the non-NW Server host that failed to upgrade. 2. Submit the following commands. <code>systemctl unmask salt-minion</code> <code>systemctl restart salt-minion</code> 3. Retry the upgrade of the non-NW Server host.

Reporting Engine Service

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

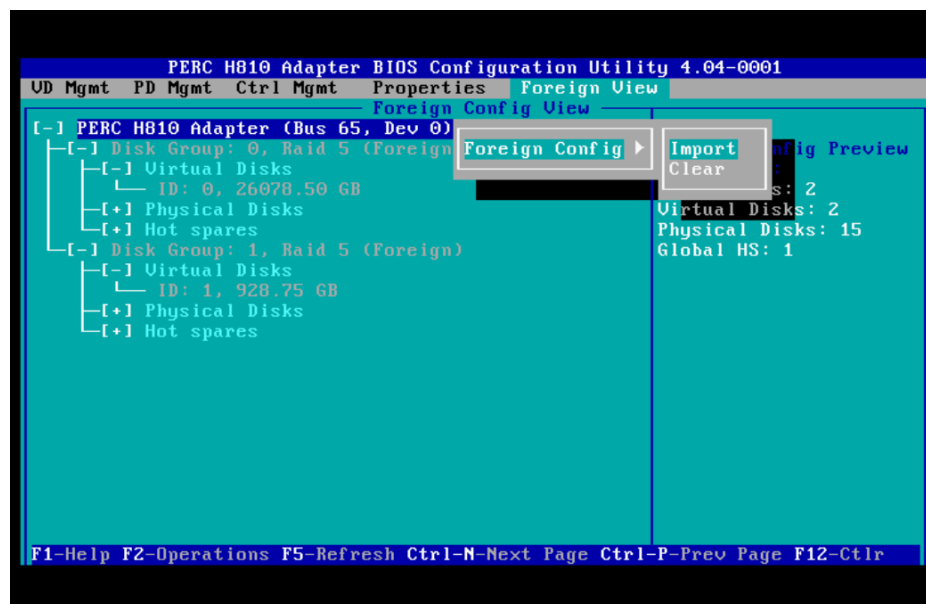
Error Message	<timestamp> : Available free space in <code>/var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB]</code> is less than the required space [<code><required-GB></code>]
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Solution	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the <i>Reporting Engine Configuration Guide</i> for instructions on how to free up disk space.

NetWitness UEBA

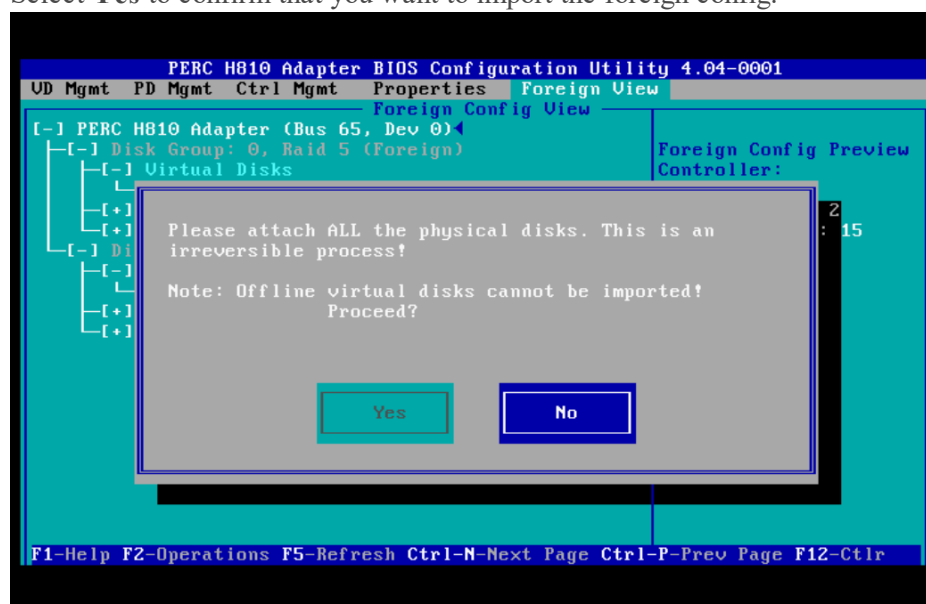
Problem	The User Interface is not accessible.
Cause	You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.
Solution	<p>Complete the following steps to remove the extra NetWitness UEBA service.</p> <ol style="list-style-type: none"> SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services. <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre> From the list of services, determine which instance of the <code>presidio-airflow</code> service should be removed (by looking at the host addresses). Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services): <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> Run the following command to update node 0 to restore NGINX: <pre># orchestration-cli-client --update-admin-node</pre> Log in to NetWitness Platform, go to ADMIN > Hosts, and remove the extra NetWitness UEBA host.

Section 2 - Hardware-Related Troubleshooting Information

Error Message	<p>When you restart a Series 4 Appliance with external storage, the following messages are displayed.</p> <pre> Foreign configuration(s) found on adapter Press any key to continue or 'C' to load the configuration utility, or 'F' to import foreign configuration(s) and continue. All of the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your cables to ensure all disks are present. Press any key to continue, or 'C' to load the configuration utility. Entering the configuration utility in this state will result in drive configuration changes. Press 'Y' to continue loading the configuration utility or please power off your system and check your cables to ensure all disks are present and reboot. </pre>
Cause	<p>If you upgrade a Series 4 Appliance host with an external storage (for example, a DAC) to 11.2 and try to restart the appliance, the system may recognize it as having a foreign configuration.</p>
Solution	<ol style="list-style-type: none"> 1. 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. 2. Press C to start the Configuration utility. <ol style="list-style-type: none"> a. Select the PERC H8x0 Adapter. <div data-bbox="487 953 1421 1549" data-label="Image"> </div> 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.



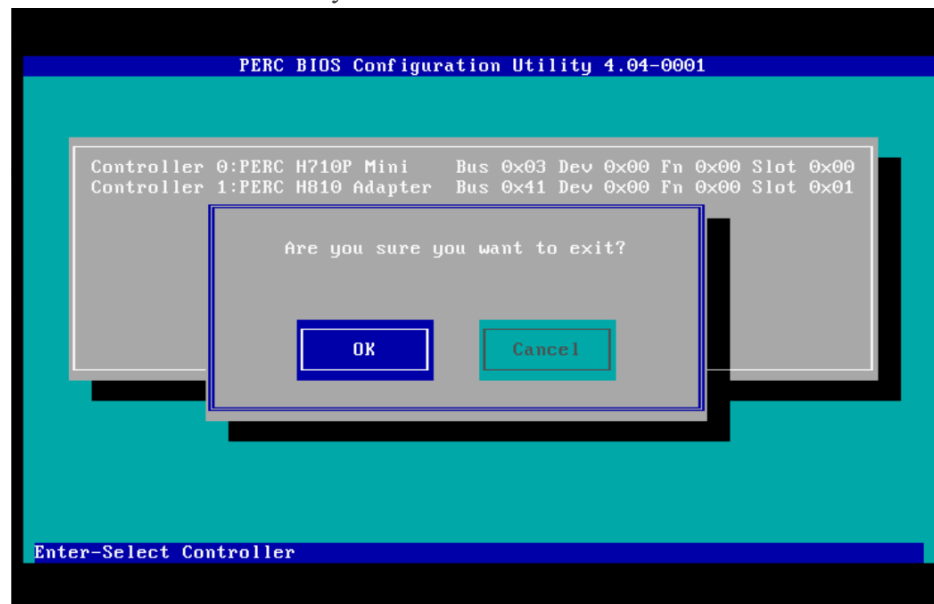
- e. Select **Yes** to confirm that you want to import the foreign config.



- 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.



3. 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>).

Problem	The <code>mtu.conf</code> and <code>pf_ring</code> files for the 10G Decoder were not restored from the <code>./etc/init/pfring_bkup</code> directory after upgrade.
Cause	If you use the 10G Decoder hardware driver and you customized the <code>/etc/init.d/pf_ring</code> script to use MTU from the <code>/etc/pf_ring/mtu.conf</code> file, the <code>mtu.conf</code> and <code>pf_ring</code> files from the <code>./etc/init/pfring_bkup</code> directory are not restored after upgrade.
Solution	<p>Complete the following steps to restore the files.</p> <ol style="list-style-type: none">1. Restore the <code>pf_ring</code> file to <code>/etc/init.d/</code> directory in 11.2. <code>/etc/init.d/pf_ring</code>2. Restore the <code>mtu.conf</code> file to <code>/etc/pf_ring/</code> directory in 11.2. <code>/etc/pf_ring/mtu.conf</code>



Appendix B. Stopping and Restarting Data Capture and Aggregation

RSA recommends that you stop network and log capture and aggregation before upgrading a Decoder, Concentrator, and Broker host to 11.3.0.0. If you do this, you must restart network and log capture and aggregation after updating these hosts.

Stop Data Capture and Aggregation

Stop Network Capture

1. Log in to NetWitness Platform and go to **ADMIN > Services**.
The Services view is displayed.
2. Select each **Decoder** service.

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

Stop Log Capture

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

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

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

4. In the toolbar, click  **Stop Capture**.

Stop Aggregation

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

2. Select the **Broker** service.

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



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

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



Start Data Capture and Aggregation

Restart network and log capture and aggregation after updating to 11.3.0.0.



Start Network Capture

1. Log in to **NetWitness Platform** and go to **ADMIN > Services**.
The Services view is displayed.
2. Select each **Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture**.

Start Log Capture

1. Log in to **NetWitness Platform** and go to **ADMIN > Services**.
The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture**.

Start Aggregation

1. Log in to **NetWitness Platform** and go to **ADMIN > Services**.
The Services view is displayed.
2. For each Concentrator and Broker service.
 - a. Select the service.
 - b. Under  (actions), select **View > Config**.
 - c. In the toolbar, click  **Start Aggregation**.

Appendix C. Using iDRAC with the DVD ISO Image

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

For example:

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

In this situation, you can:

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

Configure NFS Server - NFS Server config File

1. Install NFS and its common utilities using yum.
`yum install nfs-utils`
2. Configure the NFS service to run at boot.
`chkconfig nfs on`
3. Configure the rpcbind service to run at boot.
This service is required by NFS and must be running before NFS can be started.
`chkconfig rpcbind on`
4. Start the rpcbind service.
`service rpcbind start`
5. Start the NFS service.
`service nfs start`
6. Create a directory for our first export.
`mkdir /exports/files`
7. Open the NFS exports file into a text editor.
`vi /etc/exports`

8. To export the directory to everyone with read-only access, add the following line.
`/exports/files *(ro)`
9. Save your changes and exit the editor.
`:wq!`
10. Export the directory defined above.
`exportfs -a`
11. Disable firewall rules while performing upgrades.
`service iptables stop`
12. Copy install media that contains the ISO file to `/exports/files` directory.

Boot iDRAC to NFS Configuration

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

1. Log in to the iDRAC interface.
2. Attach media using Remote File Share.
`<server ip>:/export/files/11.3.0.0.iso`
For example: `10.10.10.10:/exports/files/rsa-11.3.0.0.1948.el7-usb.iso`
3. Click **Connect**.
4. Launch **Console**.
5. From the **next boot** menu, select **Virtual DVD/CD**.
6. Reboot the device.

Appendix D. Create External Repository

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

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

1. Log in to the web server host.
2. Create a directory to host the NW repository (netwitness-11.3.0.0.zip), for example ziprepo under web-root of the web server. For example, if /var/netwitness is the web-root, submit the following command string.
`mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Create the 11.3.0.0 directory under /var/netwitness/<your-zip-file-repo>.
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.0`
4. Create the OS and RSA directories under /var/netwitness/<your-zip-file-repo>/11.3.0.0.
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.0/OS`
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.3.0.0/RSA`
5. Unzip the netwitness-11.3.0.0.zip file into the /var/netwitness/<your-zip-file-repo>/11.3.0.0 directory.
`unzip netwitness-11.3.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.3.0.0`
Unzipping netwitness-11.3.0.0.zip results in two zip files (OS-11.3.0.0.zip and RSA-11.3.0.0.zip) and some other files.
6. Unzip the:
 - a. OS-11.3.0.0.zip into the /var/netwitness/<your-zip-file-repo>/11.3.0.0/OS directory.
`unzip /var/netwitness/<your-zip-file-repo>/11.3.0.0/OS-11.3.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.3.0.0/OS`
The following example illustrates how the Operating System (OS) file structure will appear after




you unzip the file.

 Parent Directory	-
 GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49 1.1M
 HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07 4.6M
 Lib_Uutils-1.00-09.noarch.rpm	03-Oct-2017 10:05 1.5M
 OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 502K
 OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 15K
 PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30 160K
 SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39 204K
 acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04 81K
 adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10 706K
 alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52 421K
 at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56 51K
 atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53 258K
 attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04 66K

- b. RSA-11.3.0.0.zip into the /var/netwitness/<your-zip-file-repo>/11.3.0.0/RSA directory.

```
unzip /var/netwitness/<your-zip-file-repo>/11.3.0.0/RSA-11.3.0.0.zip -d  
/var/netwitness/<your-zip-file-repo>/11.3.0.0/RSA
```

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

Parent Directory			-
 MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M	
 OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K	
 bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K	
 bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K	
 cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K	
 device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K	
 dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K	
 elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M	
 erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K	
 freserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M	
 htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K	
 i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K	
 ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K	
 iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K	
 ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K	

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

7. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 11.3.0.0 Setup program (nwsetup-tui) prompt.

Revision History

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