



Deployment Guide

for RSA NetWitness® Platform 11.4



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base 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 <https://www.rsa.com/en-us/company/rsa-trademarks>.

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. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

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.

July 2020

Contents

- The Basics 6**
 - Basic Deployment 7
 - Process 7
 - NetWitness Platform High-Level Deployment Diagram 8
 - RSA NetWitness Platform Detailed Host Deployment Diagram 9
 - Deployment Options 10
- Deployment Optional Setup Procedures 11**
 - Analyst User Interface 11
 - Features and Limitations 11
 - Use Case 12
 - Deployment 12
 - Group Aggregation 14
 - RSA Group Aggregation Deployment Recommendations 14
 - Advantages of Using Group Aggregation 14
 - Configure Group Aggregation 16
 - Prerequisites 16
 - Set up Group Aggregation 17
 - Health and Wellness (BETA for Standalone Virtual Host Only) 20
 - Hybrid Categories on Series 6 (R640) Hardware 21
 - NW Server Deployment on ESA Hardware 22
 - Second Endpoint Server 23
 - Warm Standby NW Server Host 24
 - Procedures 24
 - Planned Fail-Over Scenario 25
 - Required Fail-Over Scenario without Hardware Replacement 25
 - Required Fail-Over Scenario with Hardware Replacement 25
 - Set Up Secondary NW Server in Standby Role 26
 - Fail Over Primary NW Server to Secondary NW Server with Same IP Address 38
 - Fail Over Primary NW Server to Secondary NW Server with Different IP Address 39
 - VLC Using NAT IP address to connect to NW Server 40
 - SSO 40
 - Reporting Engine 41
 - Analyst User Interface 42
 - UCF 42
 - PAM 42
 - ECAT 42

Component Host Types to Reboot	45
Fail Back Secondary NW Server to Primary NW Server	45
Network Architecture and Ports	46
NetWitness Platform Network Architecture Diagram	46
NetWitness Network (Packets) Architecture Diagram with Ports	47
NetWitness Logs Architecture Diagram with Ports	48
Event Stream Analysis Network (Packets) Architecture Diagram with Ports	49
Event Stream Analysis (Logs) Architecture Diagram with Ports	50
NetWitness Platform Firewall Requirements Summary	51
Comprehensive List of NetWitness Platform Host, Service, and iDRAC Ports	55
NW Server Host (Primary and Warm Standby NW Server Host)	56
Analyst UI Host	57
Archiver Host	58
Broker Host	59
Concentrator Host	60
Endpoint Log Hybrid	61
Endpoint Relay Server	62
Event Stream Analysis (ESA) Host	63
Health & Wellness (Beta Version)	64
iDRAC Ports	65
Log Collector Host	66
Log Decoder Host	67
Log Hybrid Host	68
Log Hybrid - Retention Host	70
Malware Host	71
Network Decoder Host	72
Network Hybrid Host	73
UEBA Host	74
NetWitness Endpoint Architecture	75
NetWitness Endpoint 4.4 Integration with NetWitness Platform	75
NetWitness Endpoint 11.3.1 Architecture with Ports	76
How to Change UDP Port for Endpoint Log Hybrid	76
Task 1 - Tell All Agents to Use a New UDP Port	76
Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment	77
Site Requirements and Safety	79
Intended Application Uses	79
Service	79
Safety Information	79
Site Selection	79
Equipment Handling Practices	79

Power and Electrical Warnings	80
Rack Mount Warnings	80
Cooling and Air Flow	80

The Basics

This guide describes the basic requirements of a NetWitness Platform deployment and outlines optional scenarios to address needs of your enterprise. Even in small networks, planning can ensure that all goes smoothly when you are ready to bring the hosts online.

Note: This document refers to several additional documents available on RSA Link. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

There are many factors you must consider before you deploy NetWitness Platform. The following items are just some of these factors. You need to estimate growth and storage requirements when you consider these factors

- The size of your enterprise (that is, the number of locations and people that will use NetWitness Platform)
- The volume of network data and logs you need to process
- The performance each NetWitness Platform user role needs to do their jobs effectively.
- The prevention of downtime (that is, how to avoid a single point of failure).
- The environment in which you plan to run NetWitness Platform
 - RSA Physical Hosts (software running on hardware supplied by RSA)
See the *RSA NetWitness® Platform Physical Host Installation Guide* for detailed instructions on how to deploy RSA Physical Hosts.
 - Software Only provided by RSA:
 - On-Premises (On-Prem) Virtual Hosts
See the *RSA NetWitness® Platform Virtual Host Installation Guide* for detailed instructions on how to deploy on-prem virtual hosts.
 - VCloud:
 - Amazon Web Services (AWS)
See the *RSA NetWitness® Platform AWS Installation Guide* for detailed instructions on how to deploy virtual hosts in AWS.
 - Azure
See the *RSA NetWitness® Platform Azure Installation Guide* for detailed instructions on how to deploy virtual hosts in Azure.

Basic Deployment

Before you can deploy NetWitness Platform you need to:

- Consider the requirements of your enterprise and understand the deployment process.
- Have a high-level picture of the complexity and scope of a NetWitness Platform deployment.

Process

The components and topology of a NetWitness Platform network can vary greatly between installations, and should be carefully planned before the process begins. Initial planning includes:

- Consideration of site requirements and safety requirements.
- Review of the network architecture and port usage.
- Support of group aggregation on Archivers and Concentrators, and virtual hosts.

When ready to begin deployment, the general sequence is:

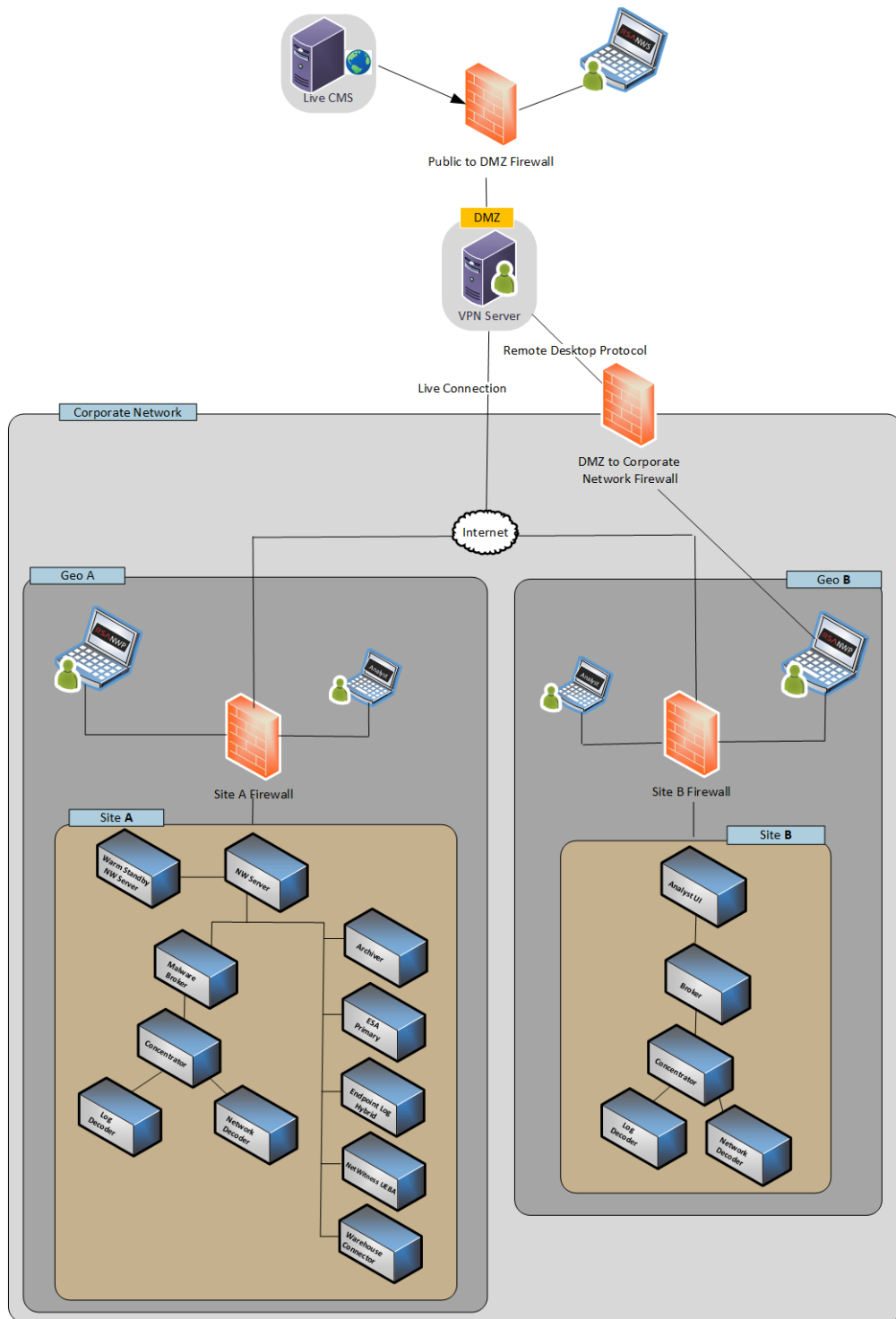
- For RSA Physical Hosts:
 1. Install physical hosts and connect to the network as described in the RSA NetWitness® Platform Hardware Setup Guides and the *RSA NetWitness® Platform Physical Host Installation Guide*.
 2. Set up licensing for NetWitness Platform as described in the *RSA NetWitness® Platform Licensing Guide*.
 3. Configure individual physical hosts and services as described in *RSA NetWitness® Platform Host and Services Getting Started Guide*. This guide also describes the procedures for applying updates and preparing for version upgrades.
- For On-Prem virtual hosts, follow the instructions in the *RSA NetWitness® Platform Virtual Host Setup Guide*.
- For AWS, follow the instructions in the *RSA NetWitness® Platform AWS Installation Guide*.
- For Azure, follow the instructions in the *RSA NetWitness® Platform Azure Installation Guide*.

When updating hosts and services, follow recommended guidelines under the "Running in Mixed Mode" topic in the *RSA NetWitness Platform Host and Services Getting Started Guide*.

You should also become familiar with Hosts, Host Types, and Services as they are used in the context of NetWitness Platform also described in the *RSA NetWitness Platform Host and Services Getting Started Guide*.

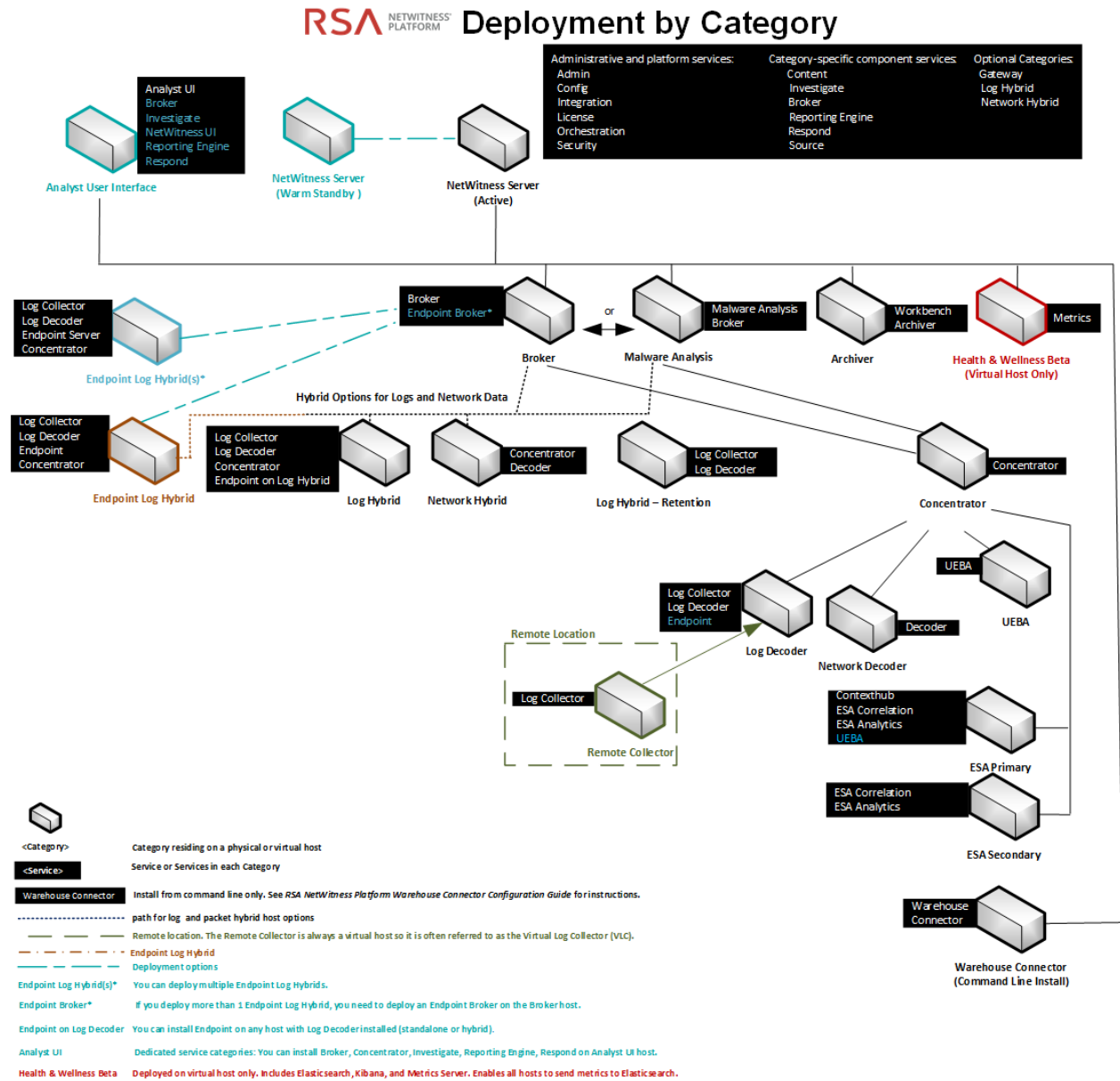
NetWitness Platform High-Level Deployment Diagram

The following diagram illustrates a basic, multi-site NetWitness Platform Deployment.



RSA NetWitness Platform Detailed Host Deployment Diagram

The following diagram is an example of a NetWitness Platform deployment hosted on physical or virtual machines. For instructions on how to install NetWitness Platform see the *Physical Host Installation Guide*, *Virtual Host Installation Guide*, *AWS Installation Guide*, or *Azure Installation Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.



Deployment Options

You deploy RSA NetWitness Platform with the following options.

- Analyst User Interface
- Group Aggregation
- Health & Wellness Search (Beta Version for Virtual Host Only)
- Hybrid Categories on the NW Server
- Second Endpoint Server
- Warm Standby NW Server
- NW Server Deployment on ESA Hardware

See [Deployment Optional Setup Procedures](#) for instructions.

Deployment Optional Setup Procedures

[Analyst User Interface](#)

[Group Aggregation](#)

[Health and Wellness Search \(Beta Version for Standalone Virtual Host Only\)](#)

[Hybrid Categories on Series 6 \(R640\) Hardware](#)

[NW Server Deployment on ESA Hardware](#)

[Second Endpoint Server](#)

[Warm Standby NW Server](#)

Analyst User Interface

The Analyst User Interface (UI) gives you access to a subset of features in the NetWitness Platform UI that you can set up in individual locations when you deploy NetWitness Platform in multiple locations. It is designed to reduce latency and improve the performance that can occur when accessing all functionality from the Primary User Interface on the NW Server Host (Primary UI).

You can have multiple Analyst UI instances provisioned in the same manner as the other NW component hosts

Features and Limitations

Each Analyst UI host:

- Can be deployed to specific organizational groups. For example: the Americas, EMEA, APAC, Tier 1 Analysts, Tier 3 Analysts.
- If Analyst UI hosts are deployed regionally, you have the capability of querying those regional brokers directly (less latency), instead of than having to route through the Primary UI.
- Helps distribute load off the Primary UI.
- Has its own Reporting Engine (RE).
- If it becomes unavailable for any planned or unplanned reason, it will not affect the Primary UI or any other Analyst UI instances.
- Provides the same pre-query filter verification, Data Privacy protection, and RBAC functionality as the Primary UI.
- Points back to the primary NW Server for authentication and configuration.
- Does not have access to any administrative functions. All administration functions take place on the Primary UI.
- Does not allow you to create or manage Content (that is, ESA rules, app rules, feeds). All Content creation and management takes place on the Primary UI.

Use Case

Large environments that include Geo distribution with a single data center and multiple NW Servers require Analyst UI instances in all their NetWitness locations or managed entities.

For example, if an Analyst UI is deployed for the EMEA SOC team, analysts can query their EMEA NetWitness Platform hosts directly. If the EMEA team has Broker hosts and Concentrator hosts within the region, the Analyst UI can connect and query them instead of connecting back to Primary user Interface (Primary UI).

Deployment

You must install the **Analyst UI** service category on a dedicated host and you install it in the same manner as any component service category on a host.

See the "Task 2 - Install 11.4 on Other Component Hosts" in the RSA NetWitness Platform Installation Guides for instructions on how to install any component service. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

After you provision the Analyst UI host (that is after you run the nwsetup-tui for the component host designated for the Analyst UI), complete the following steps to install the Analyst UI service category on the provisioned host.

1. 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.

2. Select the host in the **New Hosts** dialog and click **Enable**.

The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

3. Select that host in the **Hosts** view (for example, **Analyst UI**) and click  **Install** .

The **Install Services** dialog is displayed.

4. Select **Analyst UI** in **Category** and click **Install**.

The screenshot displays the RSA NetWitness Platform Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'Hosts' tab is active, showing a table of hosts with columns for Name, Host, Version, and Status. A red arrow labeled '1' points to the 'Install' button in the Hosts table. A second red arrow labeled '2' points to the 'Enable' button in the 'New Hosts' section. A third red arrow labeled '3' points to the 'Analyst UI' checkbox in the Hosts table. A fourth red arrow labeled '4' points to the 'Install' button in the 'Install Services' dialog box. The dialog box shows the 'Analyst UI' category selected in a dropdown menu, and a list of services to be installed: Investigate Server, Broker, NetWitness UI, Reporting Engine, and Respond Server.

5. Configure NetWitness Platform for each Analyst UI instance. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

- a. Make sure that each Analyst UI instance is connected to the correct local Reporting Engine and has the appropriate Investigation parameters set. The *Getting Started Guide for RSA NetWitness Platform 11.4* describes the default Analyst UI Dashboard and how you manage dashboards.

Note: You must add data sources to each Reporting Engine instance to execute Reports and Charts on an Analyst UI. See "Configure the Data Sources" in the *Reporting Engine Configuration Guide for RSA NetWitness Platform 11.4* for instructions.

- b. Configure whether to normalize alerts for any Respond Server (NW Server or Analyst UI) by

enabling or disabling alert normalization. "Configure Analyst UI for Respond Server Alert Normalization" in the *NetWitness Respond Configuration Guide for RSA NetWitness Platform 11.4* tells you how to configure Respond Server alert normalization for the Analyst UI.

Group Aggregation

You use Group Aggregation to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them. You can configure multiple Archiver services or Concentrator services to efficiently aggregate from multiple Log Decoder services to improve query performance on the data:

- Stored in the Archiver.
- Processed through the Concentrator.

RSA Group Aggregation Deployment Recommendations

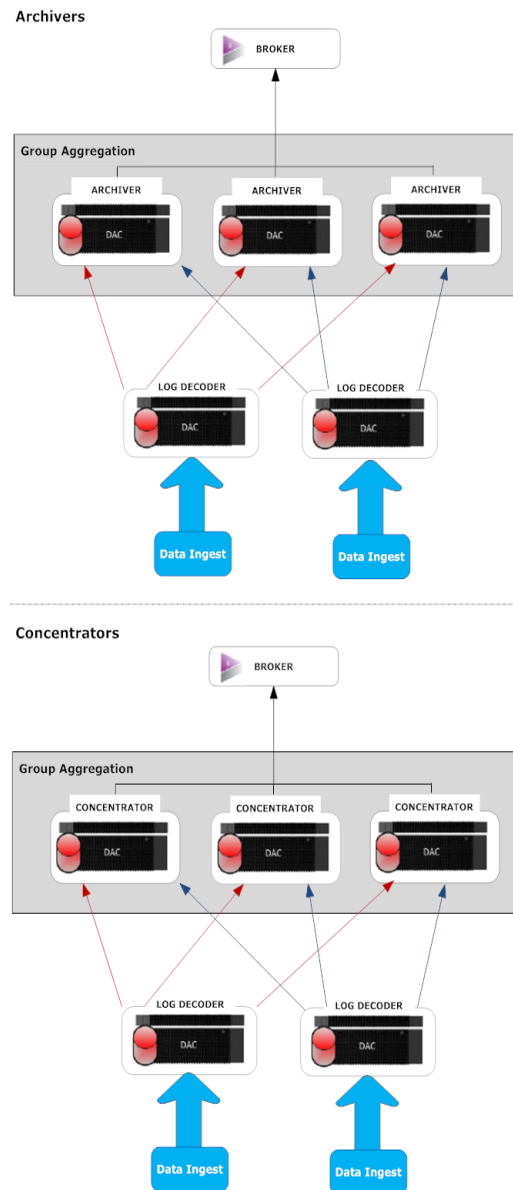
RSA recommends the following deployment for Group Aggregation:

- 1 - 2 Log Decoders
- 3 - 5 Archivers or Concentrators

Advantages of Using Group Aggregation

- Increases the speed of RSA NetWitness® Platform queries.
- Improves the performance of aggregate queries (Count and Sum) on the environment.
- Enhances investigation service performance.
- Gives you the option of storing data for a longer duration for investigation purposes.

The following diagram illustrates Group Aggregation.



You can have any number of Archivers or Concentrators grouped together and form an aggregation group. The Archiver or Concentrator services in the group divide all the aggregated session between them based on the number of sessions defined in the Aggregate Max Sessions parameter.

For example, in an aggregation group containing two Archiver services or two Concentrator services with the Aggregate Max Sessions parameter, set to 10000 the services would divide the session between themselves as illustrated in the following table.

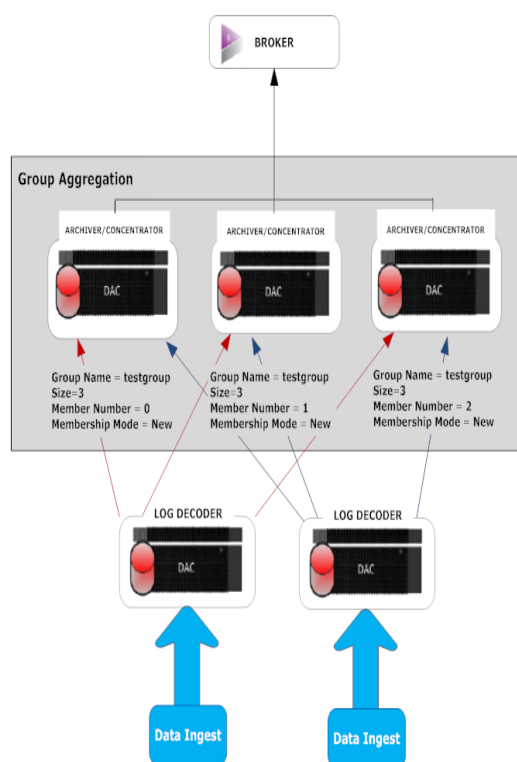
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

Configure Group Aggregation

Complete this procedure to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.

Prerequisites

Plan the network design for group aggregation. The following figure is an example of a group aggregation setup.



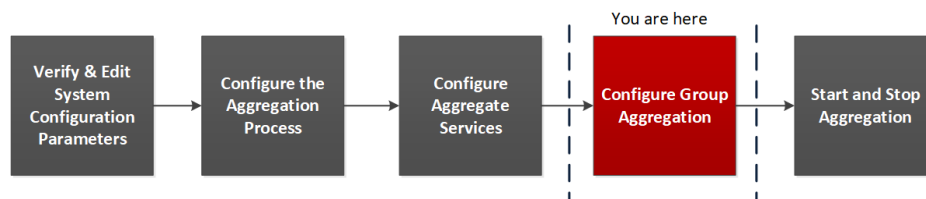
Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

Parameter	Description
Group Name	It determines the group to which the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All Archiver or Concentrator services in the group should have the same group name.
Size	It determines the number of Archiver or Concentrator services in the aggregation group.
Member Number	It determines the position of the Archiver or Concentrator in the aggregation group. For a group of size N, member number from 0 to N-1 must be set on each of the Archiver or Concentrators services in the aggregation group. For example: If the size of the aggregation group is 2, the member number of one of the Archiver or Concentrator service should be set to 0 and the member number of the other Archiver or Concentrator should be set to 1.
Membership Mode	There are two membership modes: <ul style="list-style-type: none"> • New: Adding a new Archiver or Concentrator service as a member to the existing aggregation group or creating an aggregation group. The Archiver or Concentrator service does not aggregate any existing sessions from the service as other members of the group would have already aggregated all the sessions on the service. This Archiver or Concentrator service will only aggregate new sessions as they appear on the service. • Replace: Replacing an existing aggregation group member. The Archiver or Concentrator will begin aggregation from the oldest session available on the service it is aggregating from.

Note: Membership mode parameter has an effect only when no sessions have been aggregated from the service. After some sessions are aggregated, this parameter has no effect.



Set up Group Aggregation

This workflow shows the procedures you complete to configure group aggregation.

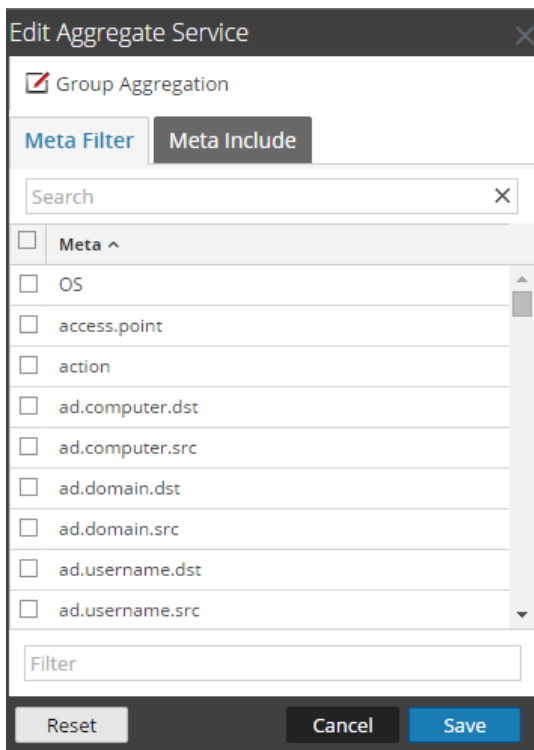


Complete the following steps to set up group aggregation.

1. Configure multiple Archiver or Concentrator services in your environment. Make sure that you add the same Log Decoder as data source to all the services.
2. Perform the following on all the Archiver or Concentrator services that you want to be part of aggregation group:

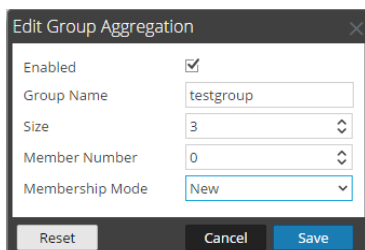
- a. Go to **Admin > Services**.
- b. Select the Archiver or Concentrator service, and in the **Actions** column, select **View > Config**.
The Service Config view of the Archiver or Concentrator is displayed.
- c. In the **Aggregate Services** section, select **Log Decoder**.
- d. Click  **Toggle Service** to change the status of the Log Decoder to offline if it is online.
- e. Click .

The **Edit Aggregate Service** dialog is displayed.



- f. Click .

The **Edit Group Aggregation** dialog is displayed.



- g. Select the **Enabled** checkbox and set the following parameters:

- In the **Group Name** field, type the group name.
 - In the **Size** field, select the number of Archiver or Concentrator services in the aggregation group.
 - In the **Member Number** field, select the position of the Archiver or Concentrator in the aggregation group.
 - In the **Membership Mode** drop-down menu, select the mode.
- h. Click **Save**.
- i. In the Service Config View page, click **Apply**.
- j. Perform **Step b** to **Step i** on all other Archiver or Concentrator services that need to be part of group aggregation.
3. In the **Aggregation Configuration** section, set the **Aggregate Max Sessions** parameter set to **10000**.

The screenshot displays the RSA NetWitness Suite Admin interface. The top navigation bar includes 'Respond', 'Investigate', 'Monitor', 'Configure', and 'Admin'. The main content area is divided into several sections:

- Aggregate Services:** A table with columns: Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, Status. The selected service is at 10.31.125.246, Port 50002, Rate 0, Max 0, Behind 0, Meta Fields empty, Filter empty, Meta Include 'no', Grouped 'yes', and Status 'offline'.
- Aggregation Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	
Aggregate Max Sessions	10000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180
- System Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input checked="" type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20

An 'Apply' button is located at the bottom center of the configuration panels.

Health and Wellness (BETA for Standalone Virtual Host Only)

You deploy the Health & Wellness (BETA) on a dedicated, virtual host. It includes Elasticsearch, Kibana, and Metrics Server and enables all hosts in your deployment to start sending metrics to Elasticsearch. After you deploy Health & Wellness (BETA), see the "NetWitness Health and Wellness (BETA)" topic in the *System Maintenance Guide* for instructions how to configure and use this feature.

This is a BETA of this feature and it is not completely implemented in 11.4 (for example, Health & Wellness BETA does not have integrated authentication to Kibana and it cannot post alerts to output actions). Please direct any Health and Wellness Beta feedback to nw.health.wellness.feedback@rsa.com.

Note: You can only deploy Health & Wellness Search (BETA) on a dedicated, virtual host.

After you provision the Health & Wellness host (that is after you run the `nwsetup-tui` for the component host designated for the Health & Wellness), complete the following steps to install the **Health and Wellness Beta** service category on the provisioned host.

1. Log into NetWitness Platform and go to **ADMIN > Hosts**.

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

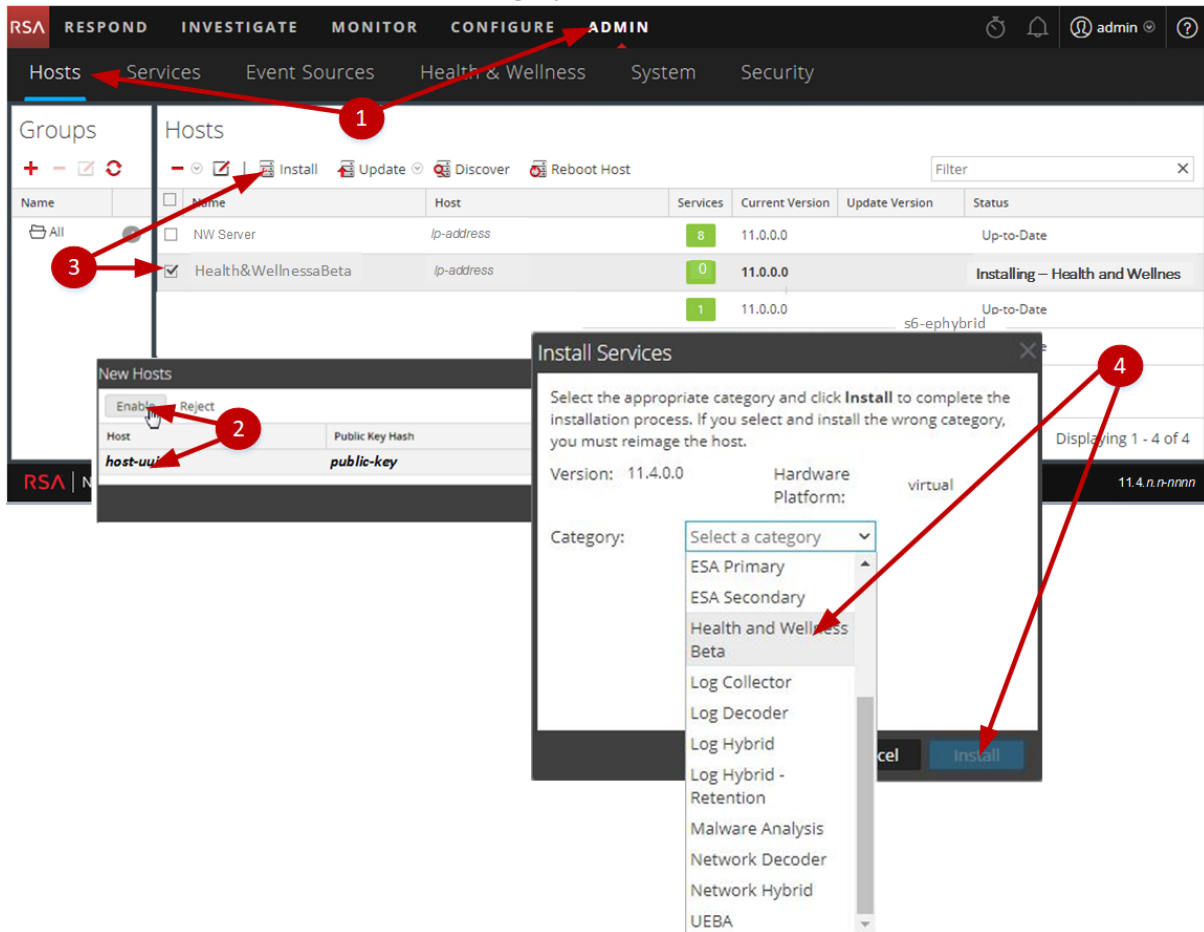
Note: If the **New Hosts** dialog is not displayed, click **Discover** in the Hosts view toolbar.

2. Select the host in the **New Hosts** dialog and click **Enable**.

The **New Hosts** dialog closes and the host is displayed in the **Hosts** view.

3. Select that host in the **Hosts** view (for example, **Health and Wellness Beta**) and click  **Install** .
The **Install Services** dialog is displayed.

4. Select **Health and Wellness Beta** in **Category** and click **Install**.



5. Refresh all hosts to write to elastic search.

a. SSH to the NW Server host.

b. Run the following commands.

```
nw-manage --refresh-host --host-all
```

This may take 30-45 minutes for the changes to take effect based on the number of hosts in your deployment.

Note: After you review your initial datastore configuration, you may determine that you need to add a new volume. For information on adding a new volume see “Add New Volume and Extend Existing File Systems” topic in the *Virtual Host Installation Guide*.

Hybrid Categories on Series 6 (R640) Hardware

You can install Hybrid Categories such as Log Hybrid and Network (Packet) Hybrid service categories on a Series 6 (R640) Physical host. This gives you the ability to attach multiple PowerVault external storage devices to the Series 6 (R640) Physical host.

NW Server Deployment on ESA Hardware

You now have the option to deploy the NW Server host on Series 6 Analytics hardware. The Series 6 Analytics Hardware has more memory and storage capacity than the standard Core appliance on which NW Server has typically been deployed. This results in better overall responsiveness and larger retention capacity for Report Engine.

Note: You can install the NW Server on ESA Hardware, but you cannot co-locate any ESA services (categories) with the NW Server on this hardware.

Second Endpoint Server

Complete the following procedure to deploy a second Endpoint Server.

1. Set up a new host in NetWitness Platform.
 - For a physical host, complete steps 1 to 14 inclusive in the in "Task 2 - Install 11.4 on Other Component Hosts" under "Installation Tasks" of the *Physical Host Installation Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.
 - For a virtual host, follow the instructions in the *Virtual Host Installation Guide* in "Task 2 - Install 11.4 on Other Component Hosts" under "Step 4. Install RSA NetWitness Platform."

2. SSH to the host that you set up in step 1.

3. Submit the following command string.

```
mkdir -p /etc/pki/nw/nwe-ca
```

Note: You do not need to modify permissions.

4. Copy the following two files from the previously deployed endpoint server to the new/second endpoint server:

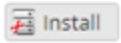
```
/etc/pki/nw/nwe-ca/nwerootca-cert.pem
```

```
/etc/pki/nw/nwe-ca/nwerootca-key.pem
```

5. Install Endpoint on the 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. Select the new 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, Endpoint Server II) and click  **Install**.
The **Install Services** dialog is displayed.
- d. Select **Endpoint** in **Host Type** and click **Install**.

Warm Standby NW Server Host

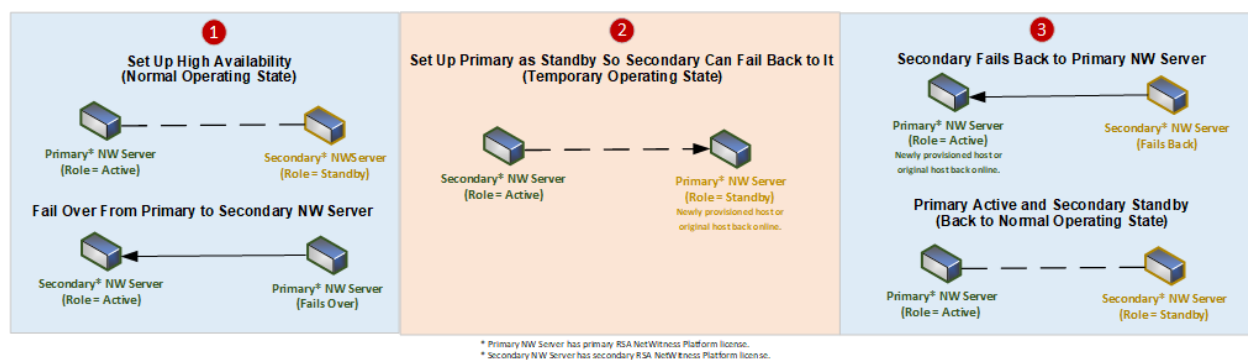
The Warm Standby NW Server duplicates the critical components and configurations of your active (primary) NW Server Host to increase reliability.

A secondary NW Server remains in the standby role and, when configured, receives backups of the primary NW Server in the active role at regular intervals. If the primary NW Server fails (goes offline), the fail-over procedure must be executed to allow the secondary NW Server to assume the active role.

When you set up a secondary NW Server as a Warm Standby, a failure or scheduled switch from the primary NW Server to the secondary NW Server is referred to as a fail-over. You fail back to return to the normal operating state (that is, the primary NW Server in the active role and the secondary NW Server in the standby role).

The following diagram illustrates the fail-over and fail-back process.

1. Set up secondary NW Server as standby (initial setup). This is the normal operating state.
2. The primary NW Server fails over to the secondary NW Server. After the fail-over, get the primary NW Server back online and set it up in the standby role. This is a temporary operating state.
3. Fail the secondary NW Server back to the primary. The primary NW Server is back to the active role and secondary is back to the standby role. This is the normal operating state.



IMPORTANT: During a fail-over, if possible, assign the same IP address as the primary NW Server to the secondary NW Server so it can assume the active role. If you cannot use the same IP address for the secondary NW Server, you will need to follow the steps in [Fail Over Primary NW Server to Secondary NW Server with Different IP Address](#).

Procedures

Complete the following task to set up a secondary NW Server in the standby role for fail-over:

- [Set up a secondary NW Server in the standby role.](#)

Complete the following tasks when required to maintain high availability.

- [Fail over the primary NW Server to secondary NW Server.](#)
- [Fail back the secondary NW Server to primary NW Server.](#)

Planned Fail-Over Scenario

This scenario occurs when you schedule a fail over (see **Planned Fail-Over** under step 3 in the [Fail Over primary NW Server to Secondary NW Server](#) procedure). You should not need do anything after the fail-over completes.

Required Fail-Over Scenario without Hardware Replacement

This scenario occurs when the primary NW Server fails (see *Required Fail-Over* under step 3 in the [Fail Over Primary NW Server to Secondary NW Server](#) topic), but you are able to recover it easily without re-imaging (for example, the active NW Server has corrupt or insufficient RAM). You do not need to run the `nwsetup-tui` and you do not need to contact Customer Support to reestablish correct licensing when:

1. The active (primary NW Server) fails over to the Standby (secondary NW Server) and that secondary host temporarily assumes the role of the active NW Server.
2. You fix the problem with the primary NW Server (for example, install new RAM) and fail back to it from the secondary host.

Required Fail-Over Scenario with Hardware Replacement

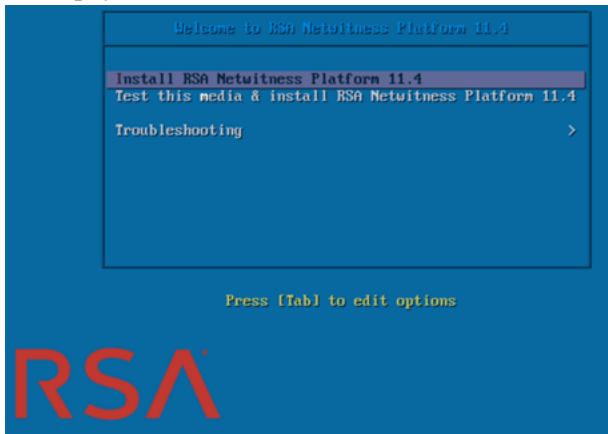
This scenario occurs when the active NW Server completely fails and the hardware requires replacement, for example, you receive a Return Merchandise Authorization (RMA). You need to reconfigure the host with the `nwsetup-tui` script and contact Customer Support (<https://community.rsa.com/docs/DOC-1294>) to reestablish licensing. If you choose to rebuild the replacement host as a temporary standby (for example, until your scheduled fail-back occurs), you must answer "Yes" to the **Standby Host Recovery Mode** `nw-setup-tui` prompt when configuring this temporary standby for failing back (see step 4 in the [Set Up Secondary NW Server in Standby Role](#) procedure for the context of this prompt).

Set Up Secondary NW Server in Standby Role

1. Before you install a secondary NW Server host for the standby role, make sure that:
 - a. The primary NW Server is running 11.4.
 - b. All component hosts are running 11.4
If you are:
 - Installing NetWitness Platform 11.4, follow the instructions in the *RSA NetWitness Platform Physical Host Installation Guide for Version 11.4*.
 - Updating from 11.x to 11.4, follow the instructions in *RSA NetWitness Platform Update Guide for Version 11.x to 11.4*.
Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.
2. Create a base image on the secondary NW Server:
 - a. Attach media (ISO) to the host.
See the *RSA NetWitness Platform Build Stick Instructions* for more information.
 - Physical media - use the ISO to create bootable flash drive media (the **Etcher**®) or another suitable imaging tool to etch a Linux file system on the USB drive. See the *RSA NetWitness® Platform Build Stick Instructions* 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 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 11.4** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



- d. Select **Install RSA NetWitness Platform 11.4** (default selection) and press **Enter**. The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.

```

-----
Clear virtual drive configuration on RAID controller: 0?
HBA: PERC H710P Mini #UD: 0 #PD: 4
For Upgrades either ignore or answer No to this prompt
Recommended for new hardware or re-purposing **Warning**
data on all configured drives will be discarded, this
includes all internal, HBA attached SATA/SCSI storage
encrypted, unencrypted or foreign and is irreversible
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----
?

-----
No root level logical volumes found for Upgrade
Assuming this system is new or being reinstalled
Upgrade cannot proceed, system will be reimaged
If you had intended to upgrade please quit and
contact support for assistance.
-----
Enter Q to Quit or R to Reinstall, Reinstalling in 120 seconds? r
-----
The current drive configuration is invalid
for the selected appliance: bootstrap
The system will auto restart in 30 seconds
If upgrading please wait for restart

Enter (y/Y) to continue the installation
NOTE: this will clear the existing disks
*Discarding All Data* and is Irreversible
-----
Enter Y to Continue, Restart in 30 seconds? y

Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting

```

Caution: You must respond y or Y to this prompt even if the host does not have an internal RAID configuration or the installation will fail.

- e. Type **Y** to continue.

The default action is No, so if you ignore the prompt and it will select No in 30 seconds and will not clear the drives. The **Press enter to reboot** prompt is displayed.

```
? y
Clearing drive configuration in 30 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
-
```

The system displays the all installation tasks it is performing. This can take a minute or so. After it completes the tasks, the installation program reboots the host.

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64
NWAPPLIANCE5070 login:
```

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

2. Run the `nwsetup-tui` command.

Note: 1.) When you navigate through the Setup program prompts, use the down and up arrows to move among fields, use the 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.) During the Setup program, when you are prompted for the network configuration of the host, be sure to specify the same network configuration that was used for the original installation of 11.x on this host (it must be exactly the same).

This initiates the `nwsetup-tui` (Setup program) and the EULA is displayed.

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

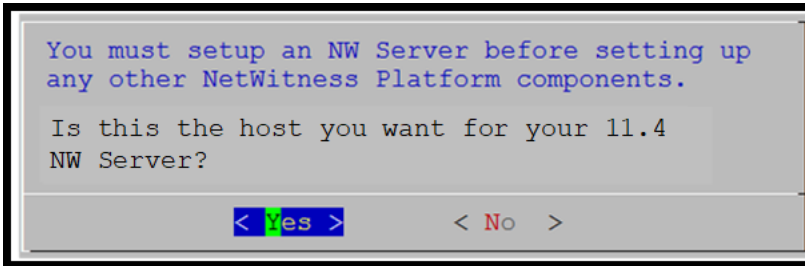
92%

`<Accept >`

`<Decline>`

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

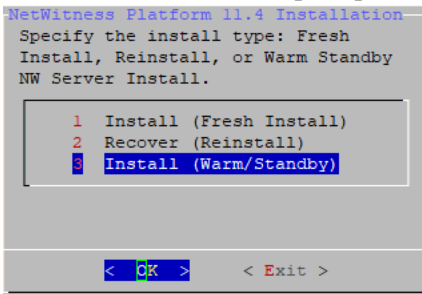
The **Is this the host you want for your 11.4 NW Server** prompt is displayed.



Your response to this prompt identifies a host as either the primary or secondary during a fresh install (and the selected response stays constant regardless of the current or future role, that is active or standby of the host).

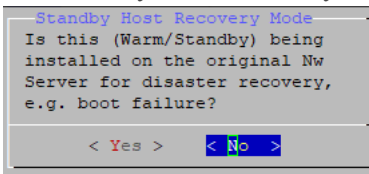
4. Tab to **Yes** and press **Enter**.

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



5. Tab to **3 Install (Warm Standby)** and press **Enter**.

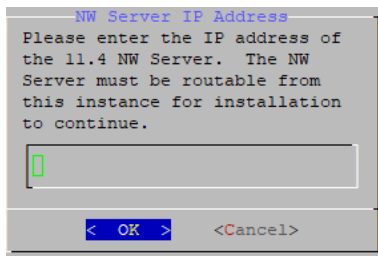
The **Standby Host Recovery Mode** prompt is displayed.



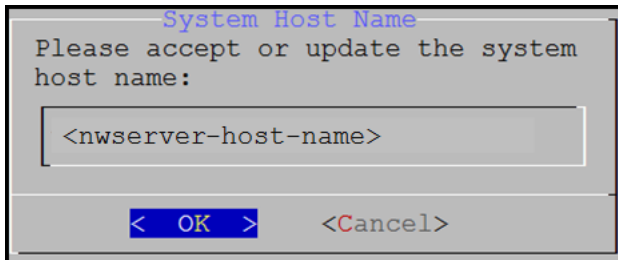
6. Tab to:

- **No** and press **Enter** to set up a secondary NW Server with the standby role (most common scenario).
- **Yes** and press **Enter** to set up a host that was previously used as a primary NW Server with the standby role so you can execute a fail-over and fail-back (less common scenario).

The NW Active Server IP Address prompt is displayed.



7. Type the IP Address of the NW Server in the active role, tab to **OK**, and press **Enter**. The **Host Name** prompt is displayed



Caution: If you include "." in a host name, the host name must also include a valid domain name.

8. Press **Enter** if want to keep this name. If not edit the host name, tab to **OK**, and press **Enter** to change it.

The **Master Password** prompt is displayed.

Note: You must use the same Master and Deploy Admin credentials for the Warm Standby NW Server Host that you used for the Active NW Server Host.

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

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

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

Master Password

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

Enter a Master Password.

Password

Verify

< OK > <Cancel>

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

Deployment Password

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

Enter a Deploy Password.

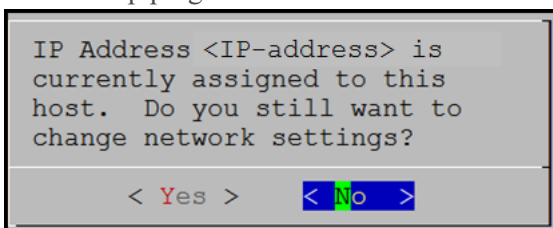
Password

Verify

< OK > <Cancel>

10. Type in the **Password**, down arrow to **Verify**, retype the password, tab to **OK**, and press **Enter**. One of the following conditional prompts is displayed.

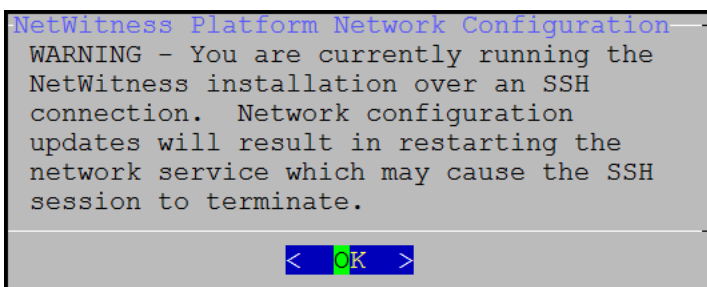
- If the Setup program finds a valid IP Address for this host, the following prompt is displayed.



Press **Enter** if you want to use this IP and avoid changing your network settings. Tab to **Yes** and press **Enter** if you want to change the IP configuration found on the host.

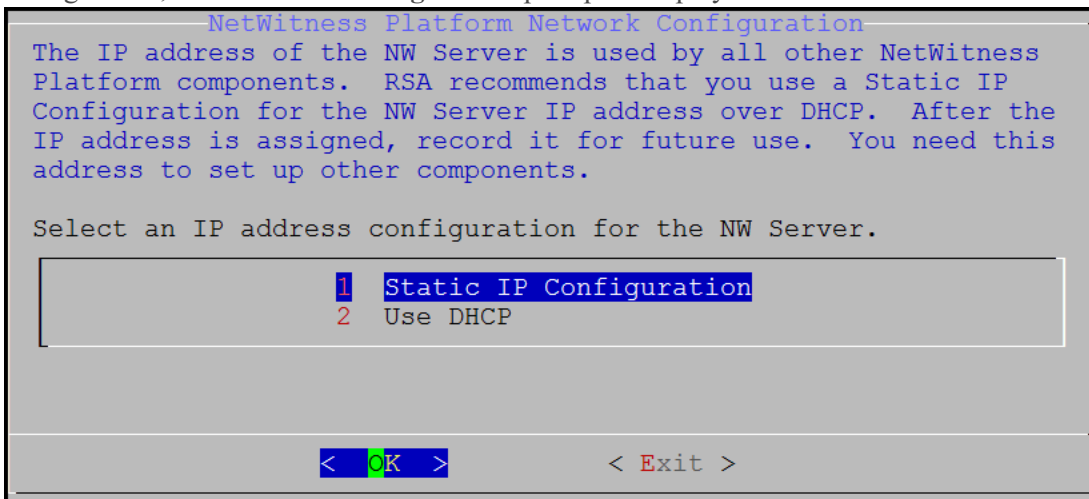
- If you are using an SSH connection, the following warning is displayed.

Note: If you connect directly from the host console, the following warning will not be displayed.

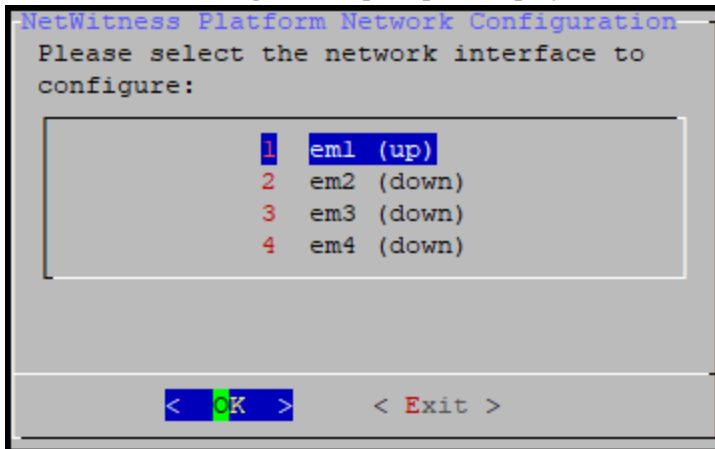


Press **Enter** to close warning prompt.

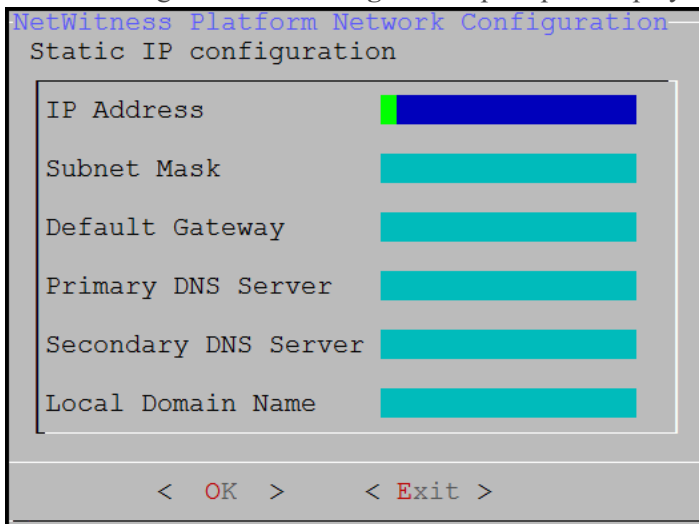
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration** prompt is displayed.



11. Tab to **OK** and press **Enter** to use **Static IP**.
If you want to use DHCP, down arrow to **2 Use DHCP** and press **Enter**.
The **Network Configuration** prompt is displayed.



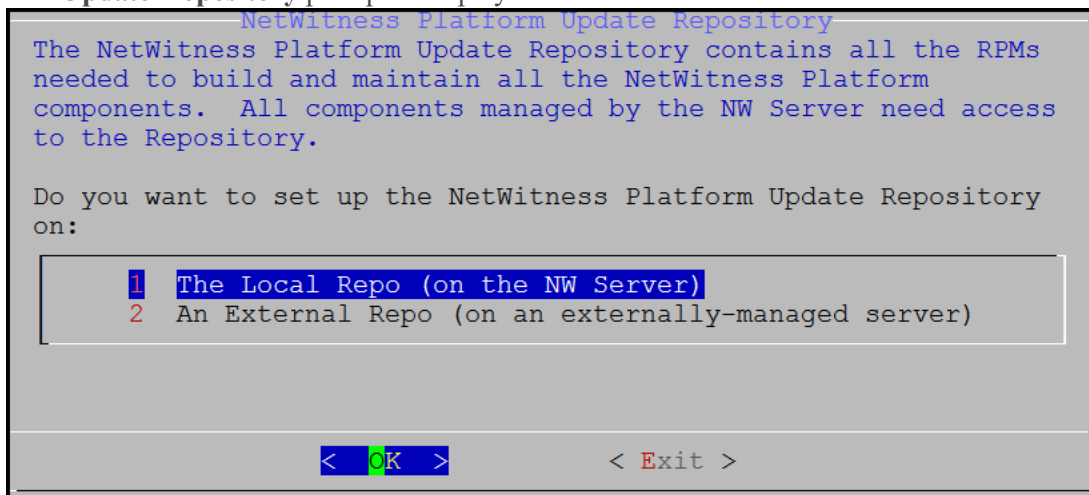
12. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.
The following **Static IP Configuration** prompt is displayed.



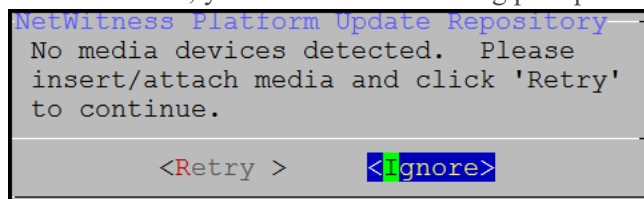
13. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an All fields are required error message is displayed (**secondary DNS Server** and **Local Domain Name** fields are not required). If you use the wrong syntax or character length for any of the fields, an Invalid <field-name> error message is displayed.

Caution: If you select **DNS Server**, make sure that the DNS Server is correct and the host can access it before proceeding with the installation.

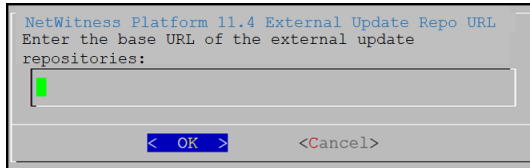
The **Update Repository** prompt is displayed.



14. Press **Enter** to choose the **Local Repo** on the NW Server. If you want to use an external repo, down arrow to **External Repo**, tab to **OK**, and press **Enter**.
 - If you select **1 The Local Repo (on the NW Server)** in the Setup program, make 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 install NetWitness Platform 11.4.0.0. If the program cannot find the attached media, you receive the following prompt.



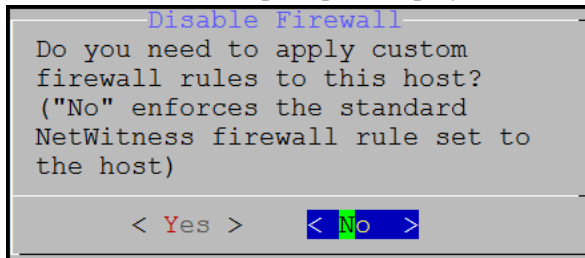
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to "Appendix B. Create an External Repo" in the *Physical Host Installation Guide* for instructions on how to create this repo and its external repo URL so you can enter it in the following prompt.



Enter the base URL of the NetWitness Platform external repo and click **OK**. The **Start Install** prompt is displayed.

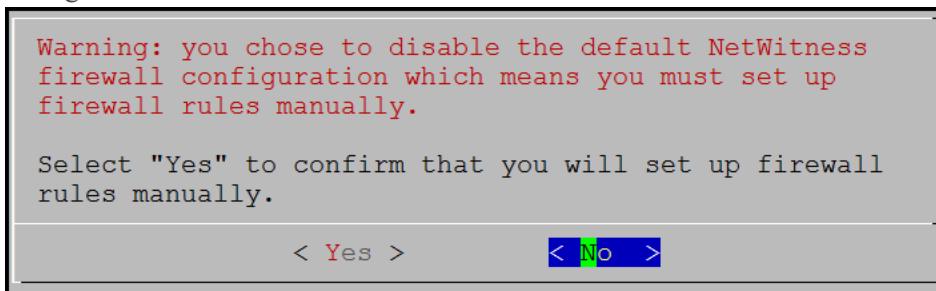
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for instructions. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

The Disable firewall prompt is displayed.

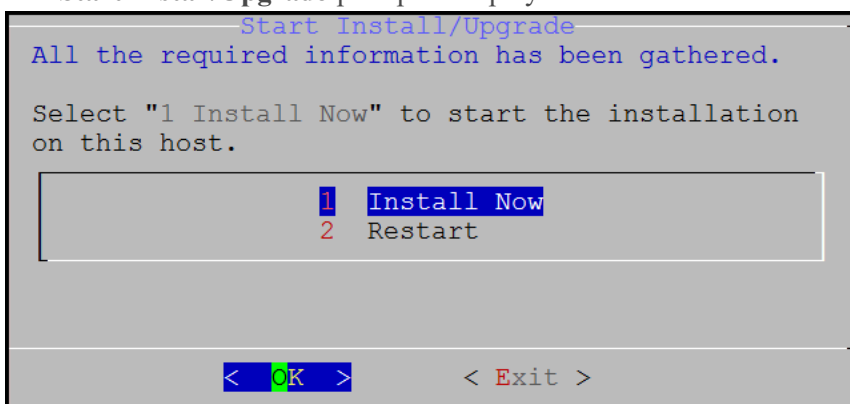


15. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

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



The **Start Install/Upgrade** prompt is displayed.



16. Press **Enter** to install 11.4 on the NW Server.

When **Installation complete** is displayed, you have installed the 11.4 NW Server on this host.

Note: Ignore the hash code errors similar to the errors shown in the following figure 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)

```

17. License the secondary NW Server.

- a. Log in to the secondary NW Server User Interface, click **ADMIN > System > Info**, and note the **License Server ID** under **Version Information**.

- b. SSH to the primary NW Server.

- c. Edit the `/opt/netwitness/flexnetls/local-configuration.yaml` file and add the backup up `hostid` (that is, the **License Server ID**).

This is an example of the section of the `local-configuration.yaml` file before you add the **License Server ID**.

```
# Hostid of the backup server, if in fail over configuration.
#backup-hostid:
```

This is an example of the section of the `local-configuration.yaml` file after you add the MAC address (for example, `000c2918c80d`) of the Warm Standby NW Server Host.

```
# Hostid of the backup server, if in fail over configuration.
backup-hostid: "000c2918c80d"
```

- d. Restart the `fneserver` service.

```
systemctl restart flexnetls-RSALM
```

- e. (Conditional) If your NetWitness Platform deployment is prohibited from accessing the Internet (Air Gap), you must:
 - i. Download the capability request from NetWitness Platform User Interface.
 - ii. Upload the request to FNO.
 - iii. Upload the response from FNO to the NetWitness Platform User Interface.
18. Schedule the backup of the primary NW Server and the copying of this backed-up data to the secondary NW Server.
- a. SSH to the primary NW Server.
 - b. Submit the following commands.


```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync -di <warm-standby-admin-server-ip>
```

This backs up the primary NW Server data and copies the backup archive file to the secondary NW Server daily for future fail-over use. It also schedules the backup and copy to execute on a daily basis. You can display help for the `schedule-standby-admin-data-sync` script with the following command string.

```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync --help
```

This returns the following help to which you can refer to customize the host data backup (such as backup frequency).

```
Schedule Data Synch between AdminServer and Standby AdminServer
Script also executes a synchronization each time.
```

Usage:

```
schedule-standby-admin-data-sync command [options]
```

Commands:

<code>-h, --help</code>	Display Help
<code>-d, --daily</code>	Schedule daily data synchronization
<code>-w, --weekly</code>	Schedule weekly data synchronization
<code>-c, --custom <crontab formatted></code>	Schedule custom data synchronization
	i.e. to schedule for midnight on 1st and 10th of the month: <code>'0 0 1,10 * *'</code>
<code>-i, --standby-ip <ip address></code>	IP address of standby Admin Server
<code>-v, --verbose</code>	Enable verbose output

Fail Over Primary NW Server to Secondary NW Server with Same IP Address

Initially, the primary NW Server fails over to the secondary NW Server. When the primary NW Server is back up, the secondary NW Server fails over to the primary NW Server, and that is referred to as a fail-back. When it is possible for the secondary NW Server to have the same IP address as the primary NW Server after failover, complete the following procedure to fail over from the primary NW Server to the secondary NW Server.

1. SSH to the secondary NW Server.
2. Run the `nw-failover` script with the appropriate arguments. For example:

```
nw-failover --make-active --ip-address <active-nw-server-host-ip> --name <primary-nw-server-hostname>
```

After the script completes, the following message is displayed.

```
*** Please update network ip and reboot host to complete the fail over process ***
```

3. Update the CentOS network configuration to swap IP Addresses.
 - **Planned Fail-Over** - primary NW Server did not fail:
 - a. SSH to the primary NW Server.
 - b. Assign an unused IP Address to the primary NW Server.
 - c. Run the `fail-over` script with the appropriate arguments to assign the standby role to the primary NW Server. For example:

```
nw-failover --make-standby --ip-address <unused-ip-or-previous-standby-ip> --name <previous-standby-nw-server-hostname>
```
 - d. Shut down the primary NW Server.
 - e. SSH to the secondary NW Server.
 - f. Assign the IP Address of the primary NW Server that you recorded to the secondary NW Server.
 - **Required Fail-Over** - primary NW Server failed:
 - a. SSH to the secondary NW Server.
 - b. Assign the IP address of the primary NW Server to the secondary NW Server.

Note: If you have a catastrophic failure, you may need to provision a new host or re-image the primary NW Server and complete the [Set Up secondary NW Server in Standby Role](#) procedure for this host to create a new primary NW Server so you can fail back to it.

4. Reboot the host.

5. Make sure that the fail-over is set up correctly.
 - a. SSH to the Standby NW Server.
 - b. Make sure that the Active NW Server:
 - i. Can resolve its uuid (Universal Unique Identifier).


```
source /usr/lib/netwitness/bootstrap/resources/nwcommon 2>/dev/null >
/dev/null
nslookup $(getNodeID)
nslookup should return the current Active NW Server IP address.
```
 - ii. Matches the same IP address that was resolved in the previous step

Fail Over Primary NW Server to Secondary NW Server with Different IP Address

If your secondary NW Server must have a different IP address from your primary NW Server, for example, if the secondary NW Server is located in a different datacenter from the primary NW Server, follow these steps to fail over from the primary NW Server to the secondary NW Server.

1. SSH to the secondary NW Server.
2. Run the failover script, providing the current IP address and host name of the secondary NW server:


```
nw-failover --make-active --ip-address <this-secondary-nw-server-ip> --name
<this-secondary-nw-server-hostname>
```

After the script completes, **ignore** the following message.

```
*** Please update network ip and reboot host to complete the fail over
process ***
```
3. (Optional) If you want to swap the primary host with the secondary host, perform this step.

Note: If you are keeping the primary server up and running, you must complete this step.

- a. SSH to the primary NW Server.
- b. Run the fail-over script on the primary NW Server, using the appropriate arguments to assign the standby role to the primary NW Server. For example:


```
nw-failover --make-standby --ip-address <primary-nw-server-IP address> -
-name <primary-nw-server-hostname>
```
4. You have two options for configuring your NW Servers. Start by running the commands in step 4a. If anything fails to run for these two commands on any NW Server systems, run the commands in step 4b.
 - a. Run the following commands on the primary (formerly active) server (where <secondary-nw-server-ip> is the former standby, now active, secondary NW Server):
 - ```
salt -C 'not G@master:127.0.0.1' cmd.run "netconfig --update-dns --dns
<secondary-nw-server-ip> && sed -Ei 's/^master:./master: <secondary-
nw-server-ip>/g' /etc/salt/minion"
```

- `salt -C 'not G@master:127.0.0.1' cmd.run_bg 'salt-call service.restart salt-minion'`
- b. If the commands in step 4a fail on any NW Server system, run the following commands on each component host:
- `netconfig --update-dns --dns <secondary-nw-server-ip>`
  - `sed -Ei 's/^master:./master: <secondary-nw-server-ip>/g' /etc/salt/minion`
  - `systemctl restart salt-minion`

Follow the steps in the sections that apply to your environment, and then proceed to [Component Host Types to Reboot](#). If none of these sections apply to your environment, proceed directly to [Component Host Types to Reboot](#).

- [VLC Using NAT IP address to connect to NW Server](#)
- [SSO](#)
- [Reporting Engine](#)
- [Analyst User Interface](#)
- [UCF](#)
- [PAM](#)
- [ECAT](#)

### VLC Using NAT IP address to connect to NW Server

If you are running a VLC that uses a NAT IP address to reach the NW Server, run the following commands on the VLC component host:

- `netconfig --update-dns --dns <NAT-ip-address>`
- `sed -Ei 's/^master:./master: <NAT-ip-address>/g' /etc/salt/minion`
- `systemctl restart salt-minion`

### SSO

If you are using SSO, run the following commands:

1. SSH to admin server node.
2. Connect to `nw-shell`.
3. Connect to admin server service using the `connect --service admin-server` command.
4. Log in to the NW Server using the `login` command.
5. Enter the admin username and password.



## 6. Run the following commands:

- `cd /rsa/security/authentication/web/saml/sso-enabled`
- `set false`
- `logout`
- `exit`
- `systemctl restart rsa-nw-admin-servernew`

```

[root@SA ~]# nw-shell
RSA
RSA NetWitness Shell. Version: 5.9.0-SNAPSHOT

offline » connect --service admin-server
INFO: Connected to admin-server (b6877f16-a3c1-4938-88a4-c7d4d9a36795)
admin-server:Folder:/rsa » login
user: admin
password: *****
admin@admin-server:Folder:/rsa » cd /rsa/security/authentication/web/saml/sso-enabled
admin@admin-server:Configuration:/rsa/security/authentication/web/saml/sso-enabled » show

```

| Configuration | /rsa/security/authentication/web/saml/sso-enabled       |
|---------------|---------------------------------------------------------|
| value         | true                                                    |
| valueType     | boolean                                                 |
| defaultValue  | false                                                   |
| description   | Flag to enable or disable SAML based SSO authentication |

```

admin@admin-server:Configuration:/rsa/security/authentication/web/saml/sso-enabled » set false
admin@admin-server:Configuration:/rsa/security/authentication/web/saml/sso-enabled » show

```

| Configuration | /rsa/security/authentication/web/saml/sso-enabled       |
|---------------|---------------------------------------------------------|
| value         | false                                                   |
| valueType     | boolean                                                 |
| defaultValue  | false                                                   |
| description   | Flag to enable or disable SAML based SSO authentication |

```

admin@admin-server:Configuration:/rsa/security/authentication/web/saml/sso-enabled » logout
admin-server:Configuration:/rsa/security/authentication/web/saml/sso-enabled » exit

```

7. Generate the new metadata and reupload it in ADFS. For more information, see the *Configure SAML 2.0 provider settings for portals* topic in the Microsoft documentation (<https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/configure-saml2-settings>).

## Reporting Engine

If you are using the Reporting Engine, you must manually configure the new IP address.

1. Log in to NetWitness Platform.
2. Go to **Admin > Services > Reporting Engine > View > Config**.
3. Click the **Output Actions** tab.
4. Add the new IP address in the **Hostname** field.

5. Click **Apply**.
6. Click the **Sources** tab and add the data sources again.

## Analyst User Interface

If you are running any Analyst UIs, for each Analyst UI host, run the following command on the failed-over (active) NW Server:

```
nw-manage --refresh-host --host-addr <analyst-ui-host-address>
```

## UCF

To enable UCF to communicate with NetWitness Platform:

1. On the UCF server, execute the `runConnectionManager.bat` file (the same file that is used for adding connection details).
2. Select **Option #2, Edit endpoints**.
3. Select the NW Server connection from the options that are displayed.
4. When you are prompted for Host Address (the old IP address is shown in parentheses) enter the new IP address.

**Note:** Do not change any other setting.

## PAM

If you have PAM configured, after the failover, you must configure the system again using the instructions in the "Configure PAM Login Capability" topic in the *System Security and User Management Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

## ECAT

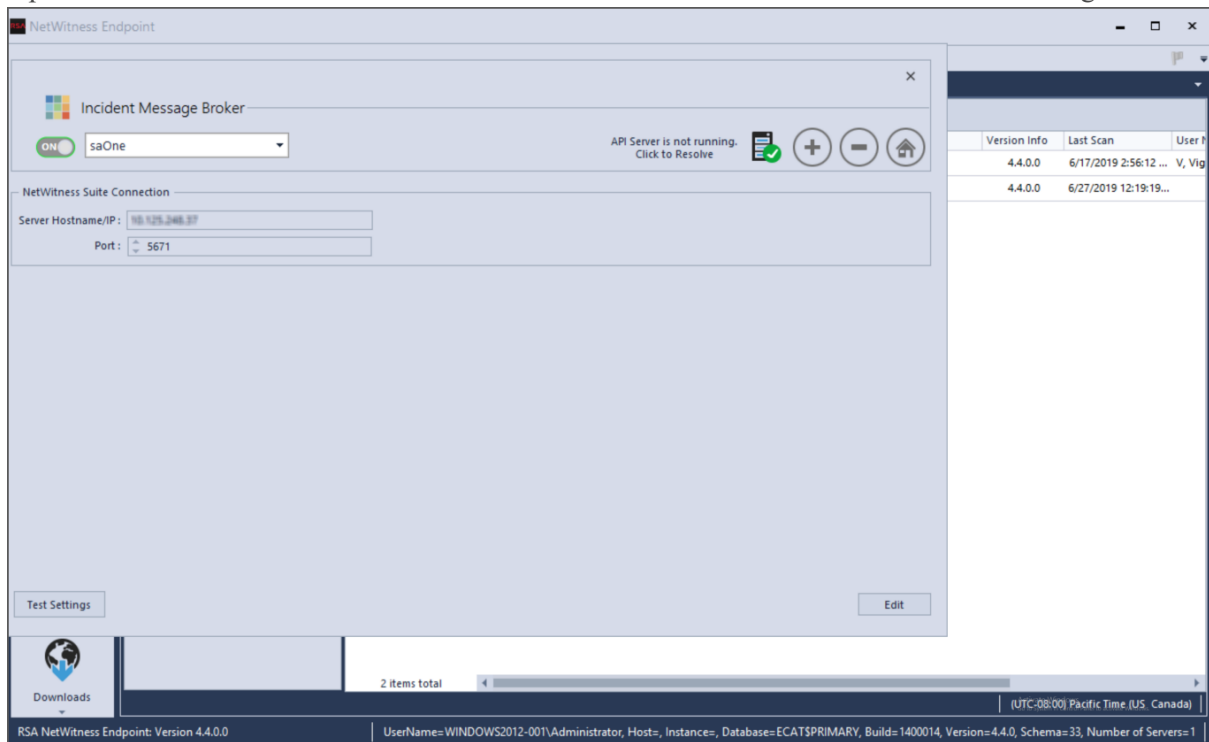
Update the following services:

- [Incident Message Broker](#)
- [NetWitness Suite](#)
- [Orchestrator](#)

### Incident Message Broker

1. Log in to the NetWitness Endpoint user interface and go to **Configure > Monitoring and External Components Configuration > Incident Message Broker**.

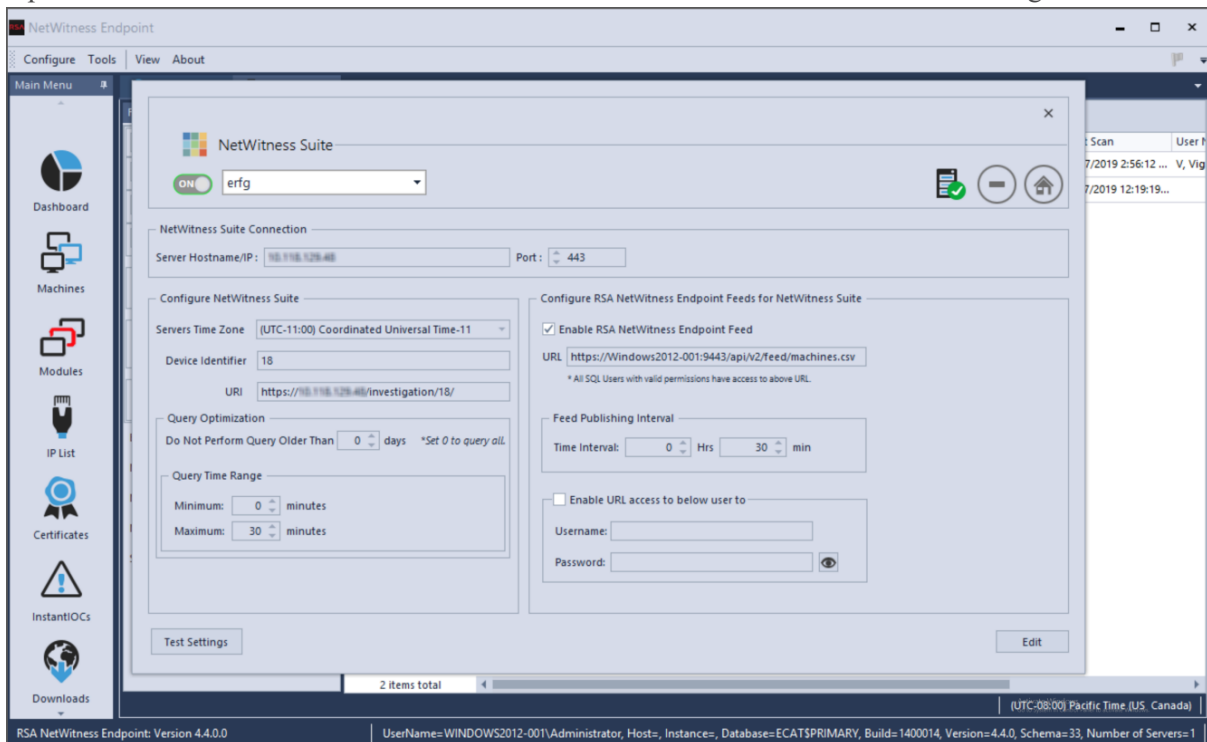
2. Update the server Hostname and IP Address to the current active server and test the settings.



## NetWitness Suite

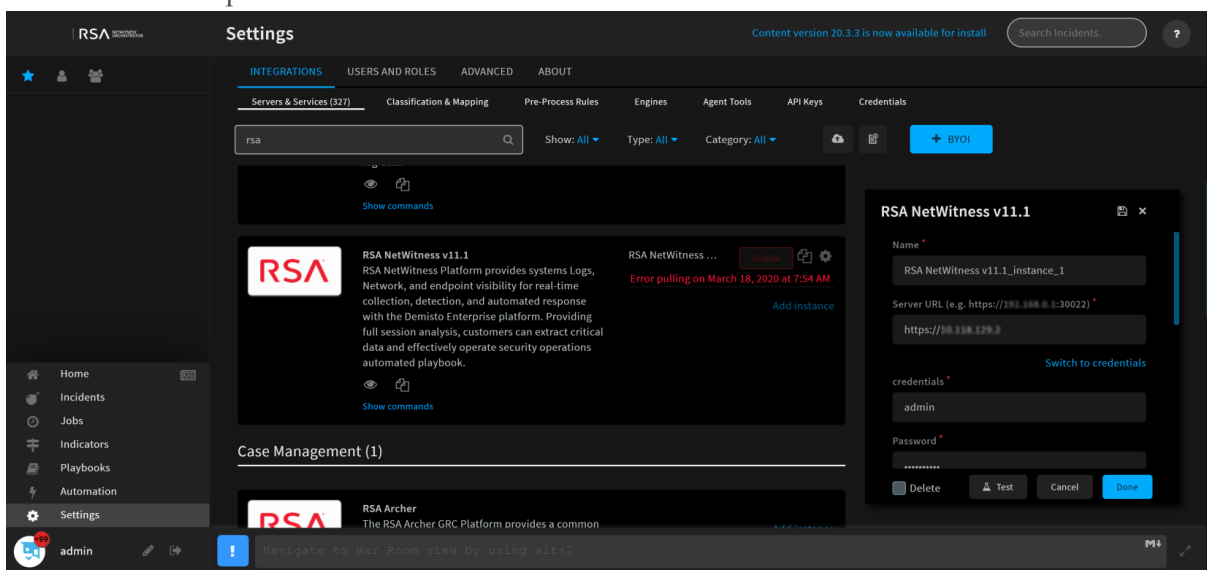
1. Log in to the NetWitness Endpoint user interface and go to **Configure > Monitoring and External Components Configuration > Netwitness Suite**.

- Update the server Hostname and IP address to the current active server and test settings.



## Orchestrator

- Log in to Orchestrator and go to **Settings > server&services**.
- Edit the RSA NetWitness V11.1 instance by updating the server URL to the current active NW Server to fetch respond incidents and alerts.



## Component Host Types to Reboot

If you have the following types of hosts, reboot them:

- ESA
- UEBA
- Endpoint Log Hybrid
- Analyst UI
- Malware
- Endpoint Broker
- Endpoint service installed on Log Decoders

**Caution:** If you have any Broker hosts (other than NW Server) that are aggregating from the Broker service on the NW Server, remove and re-add the Broker service on those hosts.

**Note:** If you added any content to the `/etc/hosts` file on the primary server, the contents of that file are available under `/var/netwitness/standby-data/unmanaged/etc` on the failover server. You can manually copy those files to the `/etc/hosts` file on the failover server after the failover is complete.

## Fail Back Secondary NW Server to Primary NW Server

After a fail-over from the primary NW Server to the secondary NW Server, you need to fail back to your original setup of the primary NW Server in the active role and the secondary NW Server in the standby role.

Essentially, you follow the same steps described under [Fail Over Primary NW Server to Secondary NW Server](#) to fail back to your original setup (that is primary NW Server-active and secondary NW Server-standby). The difference is that you now need to fail over from the secondary NW Server to the primary NW Server.

# Network Architecture and Ports

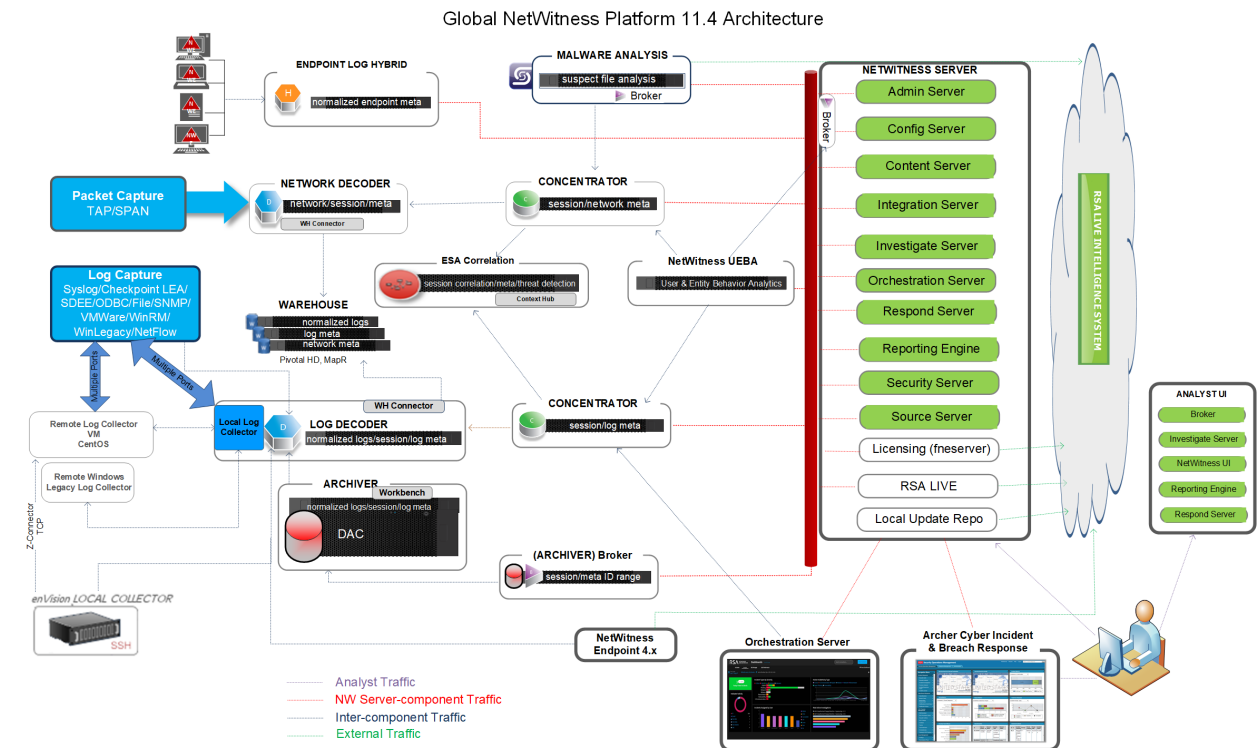
Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness Platform deployment to communicate with each other.

See [NetWitness Endpoint Architecture](#) at the end of this topic for individual Endpoint Architectural diagrams.

## NetWitness Platform Network Architecture Diagram

The following diagram illustrates the NetWitness Platform network architecture including all of its component products.

**Note:** NetWitness Platform core hosts must be able to communicate with the NetWitness Server (Primary Server in a multiple server deployment) through UDP port 123 for Network Time Protocol (NTP) time synchronization.

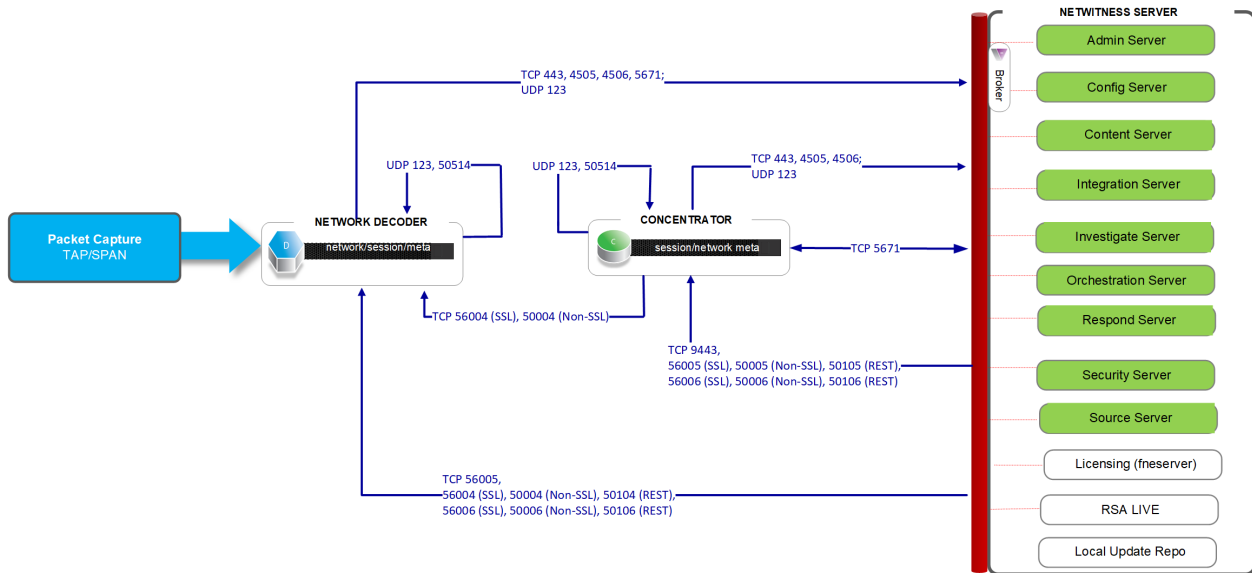


**Note:**  
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server.  
 The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).  
 NW Endpoint needs to access <https://cms.netwitness.com> to download Live Feeds.  
 RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.  
 See [RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide](#) for information on the Cloud Gateway service.



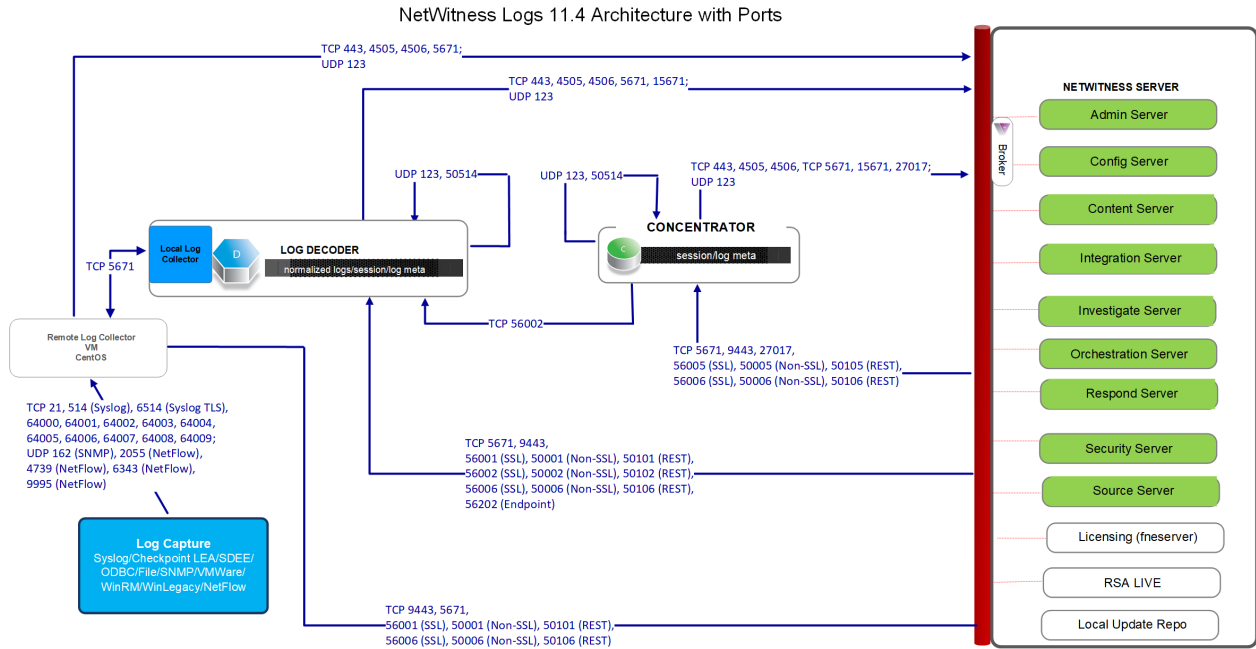
# NetWitness Network (Packets) Architecture Diagram with Ports

NetWitness Network 11.4 Architecture with Ports



**Notes:**  
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

# NetWitness Logs Architecture Diagram with Ports



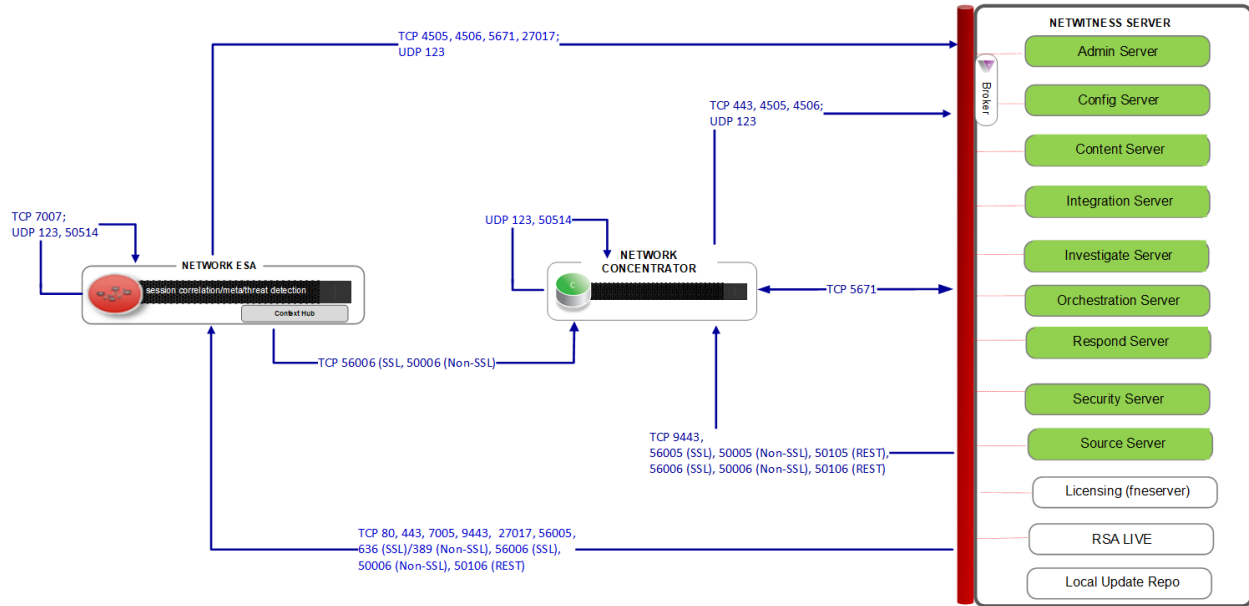
**Note:** Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).



# Event Stream Analysis Network (Packets) Architecture Diagram with Ports

The following diagram illustrates the Event Stream Analysis network architecture with packet capture.

Event Source Analysis (ESA) Network 11.5 Architecture with Ports

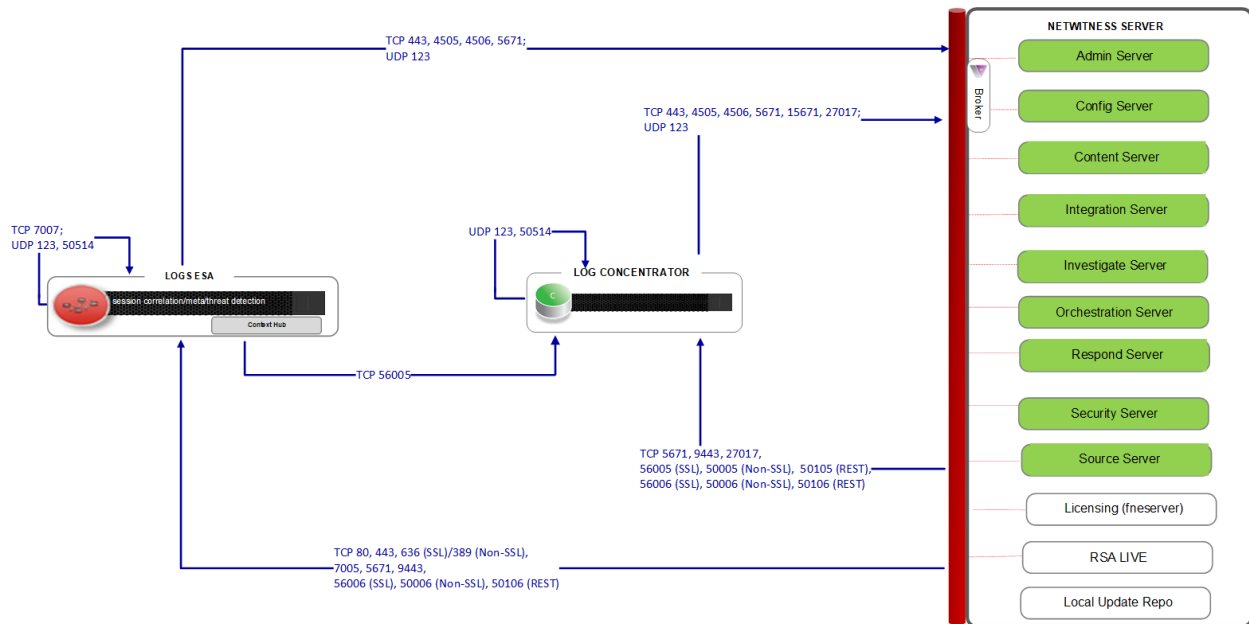


**Notes:**  
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates). Port 7005 is used by Context Hub as its HTTP port for REST calls, and is only installed on ESA Primary hosts.

## Event Stream Analysis (Logs) Architecture Diagram with Ports

The following diagram illustrates the Event Stream Analysis network architecture with log collection.

Event Stream Analysis (ESA) Logs 11.5 Architecture with Ports



**Note:**  
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates). Port 7005 is used by Context Hub as its HTTP port for REST calls, and is only installed on ESA Primary hosts.

## NetWitness Platform Firewall Requirements Summary

The following table lists all the ports that need to be open in your firewall by host.

**Note:** The "NW Server" host ports apply to both the Primary and Warm Standby NW Server. Synchronization between the Primary and Warm Standby is done through TCP Port 22.

| Source Host | Destination Host              | Ports                                                                                                                                                                                                                   |
|-------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NW Server   | ESA Primary                   | <b>TCP:</b> 22, 80, 443, 5671, 7005<br><b>UDP:</b> 123                                                                                                                                                                  |
| NW Server   | ESA                           | <b>TCP:</b> 22, 80, 443, 5671<br><b>UDP:</b> 123                                                                                                                                                                        |
| NW Server   | Network Decoder               | <b>TCP:</b> 22, 5671, 50004 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50106 (REST), 56004 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                                                                         |
| NW Server   | Broker                        | <b>TCP:</b> 5671, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST) 56003 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                                                                              |
| NW Server   | Concentrator (Network & Logs) | <b>TCP:</b> 22, 5671, 50005 (Non-SSL), 50006 (Non-SSL), 50105 (REST), 50106 (REST), 56005 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                                                                         |
| NW Server   | Network Hybrid                | <b>TCP:</b> 22, 5671, 50004 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50105 (REST), 50106 (REST), 56004 (SSL), 56005 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                             |
| NW Server   | Log Decoder                   | <b>TCP:</b> 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                             |
| NW Server   | Log Hybrid                    | <b>TCP:</b> 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL)<br><b>UDP:</b> 123 |

| Source Host              | Destination Host       | Ports                                                                                                                                                                                                                                                 |
|--------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NW Server                | Log Hybrid - Retention | <b>TCP:</b> 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                                             |
| NW Server                | Endpoint Log Hybrid    | <b>TCP:</b> 22, 5671, 7050, 7054, 50001 (Non-SSL), 50002 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL), 56202 (Endpoint)<br><b>UDP:</b> 123 |
| NW Server                | VLC                    | <b>TCP:</b> 22, 5671, 50001 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50106 (REST), 56001 (SSL), 56006 (SSL)<br><b>UDP:</b> 123                                                                                                                       |
| NW Server                | Archiver               | <b>TCP:</b> 22, 514, 5671, 6514, 50006(Non-SSL), 50007 (Non-SSL), 50008 (Non-SSL), 50106 (REST), 50107 (REST), 50108 (REST), 56006 (SSL), 56007 (SSL), 56008 (SSL)<br><b>UDP:</b> 123, 514                                                            |
| NW Server                | Malware                | <b>TCP:</b> 22, 5671, 5432, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST), 56003 (SSL), 56006 (SSL), 60007<br><b>UDP:</b> 123                                                                                                          |
| NW Server                | UEBA                   | <b>TCP:</b> 22, 15671, 5671, 443<br><b>UDP:</b> 123                                                                                                                                                                                                   |
| ESA                      | NW Server              | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017<br><b>UDP:</b> 123, 53                                                                                                                                                                        |
| ESA                      | Active Directory       | <b>TCP:</b> 389 (Non-SSL), 636 (SSL)                                                                                                                                                                                                                  |
| ESA                      | Archer                 | <b>TCP:</b> 80 (Non-SSL), 443 (SSL),                                                                                                                                                                                                                  |
| ESA Secondary            | ESA Primary            | <b>TCP:</b> 27017                                                                                                                                                                                                                                     |
| ESA Primary or Secondary | Concentrator           | <b>TCP:</b> 50005 (Non-SSL), 56005 (SSL)                                                                                                                                                                                                              |
| Network Decoder          | NW Server              | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017,<br><b>UDP:</b> 53, 123                                                                                                                                                                       |

| Source Host                   | Destination Host    | Ports                                                                                                                                           |
|-------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Concentrator (Network & Logs) | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017<br><b>UDP:</b> 53, 123                                                                  |
| Network Hybrid                | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017)<br><b>UDP:</b> 53, 123                                                                 |
| Log Decoder                   | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017<br><b>UDP:</b> 53, 123                                                                  |
| Log Hybrid                    | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671,15671, 27017<br><b>UDP:</b> 53, 123                                                                   |
| Log Hybrid - Retention        | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671,15671, 27017<br><b>UDP:</b> 53, 123                                                                   |
| VLC                           | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671,15671, 27017<br><b>UDP:</b> 53, 123                                                                   |
| VLC                           | Log Collector       | <b>TCP:</b> 5671                                                                                                                                |
| Log Collector                 | VLC                 | <b>TCP:</b> 5671                                                                                                                                |
| Endpoint Log Hybrid           | NW Server           | <b>TCP:</b> 53, 80, 443, 5671, 4505, 4506, 15671, 27017<br><b>UDP:</b> 53, 123                                                                  |
| Endpoint Log Hybrid           | Log Decoder         | <b>TCP:</b> 50202 (Non-SSL), 50102 (REST), 56202 (SSL)<br><b>UDP:</b> 514                                                                       |
| Endpoint Agent                | Log Decoder         | <b>TCP:</b> 514, 6514<br><b>UDP:</b> 514                                                                                                        |
| Endpoint Agent                | Endpoint Log Hybrid | <b>TCP:</b> 443<br><b>UDP:</b> 444                                                                                                              |
| UEBA                          | NW Server           | <b>TCP:</b> 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 50003 (Broker-Non-SSL), 50103 (Broker/REST), 56003 (Broker/SSL)<br><b>UDP:</b> 53, 123 |
| UEBA                          | Concentrator        | <b>TCP:</b> 50005 (Non-SSL), 50105 (REST), 56005 (SSL)                                                                                          |

www connections

| Source Host                     | Destination Host                                                                                                                                                                  | Ports               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NW Server                       | cloud.netwitness.com<br>cms.netwitness.com<br>download.rsasecurity.com<br>panacea.threatgrid.com<br>quantum.subscribenet.com<br>rsasecurity.subscribenet.com<br>smcupdate.emc.com | <b>TCP:</b> 80, 443 |
| ESA<br>(Primary &<br>Secondary) | cloud.netwitness.com<br>cms.netwitness.com<br>download.rsasecurity.com<br>panacea.threatgrid.com<br>quantum.subscribenet.com<br>rsasecurity.subscribenet.com<br>smcupdate.emc.com | <b>TCP:</b> 80, 443 |
| Malware                         | panacea.threatgrid.com<br>cloud.netwitness.com                                                                                                                                    | <b>TCP:</b> 443     |

## Comprehensive List of NetWitness Platform Host, Service, and iDRAC Ports

**Note:** For ports used in event collection through the NetWitness Logs, see the "The Basics" in the *RSA NetWitness Suite Log Collection Deployment Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

This section contains the port specifications for the following hosts.

| NW Server Host             | iDRAC Ports            |
|----------------------------|------------------------|
| Analyst UI Host            | Log Collector Host     |
| Archiver Host              | Log Decoder Host       |
| Broker Host                | Log Hybrid Host        |
| Concentrator Host          | Log Hybrid - Retention |
| Endpoint Log Hybrid Host   | Malware Host           |
| Endpoint Relay Server      | Network Decoder Host   |
| Event Stream Analysis Host | Network Hybrid Host    |
| Health & Wellness Beta     | UEBA Host              |

## NW Server Host (Primary and Warm Standby NW Server Host)

| Source Host       | Destination Host     | Destination Ports               | Comments                                                  |
|-------------------|----------------------|---------------------------------|-----------------------------------------------------------|
| Admin Workstation | NW Server            | TCP 443, 80                     | nginx - NetWitness UI                                     |
| Admin Workstation | NW Server            | TCP 15671                       | RabbitMQ Management UI                                    |
| Admin Workstation | NW Server            | TCP 22                          | SSH<br>Primary to Standby NW Server synchronization port. |
| NW Hosts          | NW Server            | TCP 53<br>UDP 53                | DNS                                                       |
| NW Hosts          | NW Server            | TCP 15671                       | RabbitMQ Management UI                                    |
| NW Hosts          | NW Server            | TCP 4505, 4506                  | Salt Master Ports                                         |
| NW Hosts          | NW Server            | TCP 443                         | RSA Update Repository                                     |
| NW Hosts          | NW Server            | TCP 5671                        | RabbitMQ-amqp                                             |
| NW Hosts          | NW Server            | UDP 123                         | NTP                                                       |
| NW Hosts          | NW Server            | TCP 27017                       | MongoDB                                                   |
| NW Server         | cloud.netwitness.com | TCP 443                         | Live                                                      |
| NW Server         | cms.netwitness.com   | TCP 443                         | Live                                                      |
| NW Server         | smcupdate.emc.com    | TCP 443                         | Live                                                      |
| NW Server         | NFS Server           | TCP 111, 2049,<br>UDP 111, 2049 | iDRAC Installations                                       |
| NW Server         | NW Hosts             | UDP 123                         | NTP                                                       |
| NW Server         | NW Endpoint          | TCP 443, 9443                   | For NW Endpoint 4.x integrations                          |



## Analyst UI Host

| Source Host | Destination Host | Destination Ports | Comments                                          |
|-------------|------------------|-------------------|---------------------------------------------------|
| Analyst UI  | NW Server        | TCP 7006          | The Content Server is listening on this port.     |
| Analyst UI  | NW Server        | TCP 7009          | The Admin Server is listening on this port.       |
| Analyst UI  | NW Server        | TCP 7012          | The Integration Server is listening on this port. |
| Analyst UI  | NW Server        | TCP 7015          | The Source Server is listening on this port.      |
| Analyst UI  | NW Server        | TCP 7016          | The License Server is listening on this port.     |
| NW Hosts    | Analyst UI       | TCP 5671          | RabbitMQ-amqp                                     |
| Analyst UI  | NW Server        | UDP 123           | NTP                                               |

## Archiver Host

| Source Host       | Destination Host | Destination Ports                              | Comments                                       |
|-------------------|------------------|------------------------------------------------|------------------------------------------------|
| Admin Workstation | Archiver         | TCP 15671                                      | RabbitMQ Management UI                         |
| Archiver          | NW Server        | TCP 15671                                      | RabbitMQ Management UI                         |
| Archiver          | NW Server        | TCP 443                                        | RSA Update Repository                          |
| Admin Workstation | Archiver         | TCP 22                                         | SSH                                            |
| NW Server         | Archiver         | TCP 50008 (Non-SSL), 56008 (SSL), 50108 (REST) | Archiver Application Ports                     |
| NW Server         | Archiver         | TCP 56006 (SSL), 50106 (REST)                  | NetWitness Appliance Ports                     |
| NW Server         | Archiver         | TCP 5671                                       | RabbitMQ (AMQPS) message bus for all NW hosts. |
| NW Server         | Archiver         | TCP 50007 (Non-SSL), 56007 (SSL), 50107 (REST) | Workbench Application Ports                    |
| Archiver          | NFS Server       | TCP 111 2049<br>UDP 111 2049                   | iDRAC Installations                            |

## Broker Host

| Source Host       | Destination Host | Destination Ports                              | Comments                                       |
|-------------------|------------------|------------------------------------------------|------------------------------------------------|
| Admin Workstation | Broker           | TCP 15671                                      | RabbitMQ Management UI                         |
| Broker            | Concentrator     | TCP 50005 (Non-SSL), 56005                     | Concentrator Application Port                  |
| Broker            | NW Server        | TCP 15671                                      | RabbitMQ Management UI                         |
| Broker            | NW Server        | TCP 443                                        | RSA Update Repository                          |
| Admin Workstation | Broker           | TCP 22                                         | SSH                                            |
| NW Server         | Broker           | TCP 50003 (Non-SSL), 56003 (SSL), 50103 (REST) | Broker Application Ports                       |
| NW Server         | Broker           | TCP 56006 (SSL), 50106 (REST)                  | NetWitness Appliance Ports                     |
| NW Server         | Broker           | TCP 5671                                       | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Broker            | NW Server        | TCP 111 2049<br>UDP 111 2049                   | iDRAC Installations                            |
| Endpoint Broker   | NW Server        | TCP 443                                        | RSA Update Repository                          |

## Concentrator Host

| Source Host       | Destination Host | Destination Ports                              | Comments                                       |
|-------------------|------------------|------------------------------------------------|------------------------------------------------|
| Admin Workstation | Concentrator     | TCP 15671                                      | RabbitMQ Management UI                         |
| Concentrator      | Log Decoder      | TCP 50002 (Non-SSL), 56002 (SSL)               | Log Decoder Application Port                   |
| Concentrator      | Network Decoder  | TCP 56004, 50004 (Non-SSL)                     | Network Application Port                       |
| Concentrator      | NW Server        | TCP 15671                                      | RabbitMQ Management UI                         |
| Concentrator      | NW Server        | TCP 443                                        | RSA Update Repository                          |
| Admin Workstation | Concentrator     | TCP 22                                         | SSH                                            |
| NW Server         | Concentrator     | TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST) | Concentrator Application Ports                 |
| Malware           | Concentrator     | TCP TCP 50005 (Non-SSL), 56005 (SSL)           | Malware                                        |
| NW Server         | Concentrator     | TCP 56006 (SSL), 50106 (REST)                  | NetWitness Appliance Ports                     |
| NW Server         | Concentrator     | TCP 5671                                       | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Concentrator      | NFS Server       | TCP 111 2049<br>UDP 111 2049                   | iDRAC Installations                            |

## Endpoint Log Hybrid

| Source Host         | Destination Host                     | Destination Ports                                                         | Comments                                                                                                                                              |
|---------------------|--------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Endpoint Agent      | Endpoint Log Hybrid                  | TCP 443<br>UDP 444                                                        | NGINX HTTPS<br>NGINX UDP. If UDP port 444 is not acceptable in your environment, see <a href="#">How to Change UDP Port for Endpoint Log Hybrid</a> . |
| Endpoint Agent      | Log Decoder or Virtual Log Collector | TCP 514 (Syslog)<br>UDP 514 (Syslog)<br>TLS 6514                          | Windows Log Collection                                                                                                                                |
| Endpoint Log Hybrid | Log Decoder (External)               | TCP 50102 (REST)<br>56202 (Protobuf SSL)<br>50202 (Protobuf)              | To forward meta to an external Log Decoder                                                                                                            |
| Endpoint Log Hybrid | NW Server                            | TCP 443                                                                   | RSA Update Repository                                                                                                                                 |
| NW Server           | Endpoint Log Hybrid                  | TCP 7050                                                                  | UI web traffic                                                                                                                                        |
| Endpoint Log Hybrid | NW Server                            | TCP 5671                                                                  | Message Bus                                                                                                                                           |
| Endpoint Log Hybrid | NW Server                            | TCP 27017                                                                 | MongoDB                                                                                                                                               |
| NW Server           | Endpoint Log Hybrid                  | TCP 7054                                                                  | UI web traffic                                                                                                                                        |
| NW Server           | NFS Server                           | TCP 111, 2049<br>UDP 111, 2049                                            | iDRAC Installations                                                                                                                                   |
| NW Server           | Endpoint Log Hybrid                  | TCP 50001 (Non-SSL),<br>56001 (SSL), 50101<br>(REST)                      | Log Collector application ports                                                                                                                       |
| NW Server           | Endpoint Log Hybrid                  | TCP 50002 (Non-SSL),<br>56002 (SSL), 56202<br>(Endpoint), 50102<br>(REST) | Log Decoder application ports                                                                                                                         |
| Admin Workstation   | Endpoint Log Hybrid                  | TCP 15671                                                                 | RabbitMQ Management UI                                                                                                                                |
| Endpoint Log Hybrid | NW Server                            | TCP 15671                                                                 | RabbitMQ Management UI                                                                                                                                |

## Endpoint Relay Server

| Source Host         | Destination Host | Destination Ports | Comments                                 |
|---------------------|------------------|-------------------|------------------------------------------|
| Endpoint Agent      | Relay Server     | TCP 443           | To forward host data to the Relay Server |
| Endpoint Log Hybrid | Relay Server     | TCP 443           | Pull host data from the Relay Server     |

## Event Stream Analysis (ESA) Host

**Note:** The ports in this table are for the ESA Primary and ESA Secondary hosts. The Content Hub, Correlation and ESA Analytics services are co-located on the ESA Primary host. The Correlation and ESA Analytics services are co-located on the ESA Secondary host.

| Source Host               | Destination Host   | Destination Ports            | Comments                                       |
|---------------------------|--------------------|------------------------------|------------------------------------------------|
| Admin Workstation         | ESA                | TCP 15671                    | RabbitMQ Management UI                         |
| ESA Primary and Secondary | NW Server          | TCP 15671                    | RabbitMQ Management UI                         |
| ESA Primary and Secondary | NW Server          | TCP 443                      | RSA Update Repository                          |
| Admin Workstation         | ESA                | TCP 22                       | SSH                                            |
| NW Server, ESA Secondary  | ESA Primary        | TCP 27017                    | MongoDB                                        |
| NW Server                 | ESA Primary        | TCP 7005                     | Context Hub Launch Port - (ESA Primary)        |
| NW Server                 | ESA                | TCP 5671                     | RabbitMQ (AMQPS) message bus for all NW hosts. |
| ESA Primary and Secondary | cms.netwitness.com | TCP 443                      | Live                                           |
| ESA Primary and Secondary | NFS Server         | TCP 111 2049<br>UDP 111 2049 | iDRAC Installations                            |
| ESA Primary and Secondary | Active Directory   | 636 (SSL)/389 (Non-SSL)      |                                                |
| NW Server                 | ESA                | 80 (HTTP)/ 443 (HTTPS)(REST) |                                                |
| ESA Primary               | Archer             | 443 (SSL)/80 (Non-SSL)       |                                                |
| ESA Primary               | ESA Primary        | TCP 7007                     | Launch Port                                    |

## Health & Wellness (Beta Version)

| Source Host       | Destination Host                  | Destination Ports | Comments                                       |
|-------------------|-----------------------------------|-------------------|------------------------------------------------|
| Admin Workstation | Standalone Health & Wellness Host | TCP 22            | SSH                                            |
| Admin Workstation | Standalone Health & Wellness Host | TCP 5601          | Kibana UI                                      |
| NW Hosts          | Standalone Health & Wellness Host | TCP 9200          | Elasticsearch REST API Port                    |
| NW Server         | Standalone Health & Wellness Host | TCP 5671          | RabbitMQ (AMQPS) message bus for all NW hosts. |
| NW Server         | Standalone Health & Wellness Host | TCP 15671         | RabbitMQ Management UI                         |
| NW Server         | Standalone Health & Wellness Host | TCP 7018          | Metrics Server Launch Port                     |
| NW Server         | Standalone Health & Wellness Host | TCP 7020          | Node Infra Server Launch Port                  |



## iDRAC Ports

| Port      | Function                                                                                               | Comments                                                               |
|-----------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 22*       | SSH                                                                                                    | Default, configurable port through which iDRAC listens for connections |
| 443*      | HTTP                                                                                                   | Default, configurable port through which iDRAC listens for connections |
| 5900*     | Virtual Console keyboard and mouse redirection, Virtual Media, Virtual Folders, and Remote File Share. | Default, configurable port through which iDRAC listens for connections |
| 111, 2049 | TCP                                                                                                    | NetWitness Platform hosts to NFS Server                                |
| 111, 2049 | UDP                                                                                                    | NetWitness Platform hosts to NFS Server                                |

## Log Collector Host

| Source Host           | Destination Host      | Destination Ports                                                                                                                                      | Comments                                       |
|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Admin Workstation     | Log Collector         | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |
| Log Collector         | NW Server             | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |
| Log Collector         | NW Server             | TCP 443                                                                                                                                                | RSA Update Repository                          |
| Admin Workstation     | Log Collector         | TCP 22                                                                                                                                                 | SSH                                            |
| Log Collector         | Log Event Sources     | See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all RSA NetWitness Platform 11.x documents. |                                                |
| Log Event Sources     | Log Collector         | TCP 514 (Syslog)<br>UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"                                      | Log Collection Ports                           |
| Log Event Sources     | Log Collector         | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009                                                                            | Log Collection FTP/S Ports                     |
| NW Server             | Log Collector         | TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)                                                                                                         | Log Collector Application Ports                |
| NW Server             | Log Collector         | TCP 56006 (SSL), 50106 (REST)                                                                                                                          | NetWitness Appliance Ports                     |
| NW Server             | Log Collector         | TCP 5671                                                                                                                                               | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Log Collector         | NFS Server            | TCP 111 2049<br>UDP 111 2049                                                                                                                           | iDRAC installations                            |
| Log Collector         | Virtual Log Collector | TCP 5671                                                                                                                                               | In Pull Mode                                   |
| Virtual Log Collector | Log Collector         | TCP 5671                                                                                                                                               | In Push Mode                                   |

## Log Decoder Host

| Source Host       | Destination Host  | Destination Ports                                                                                                                                      | Comments                                       |
|-------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Admin Workstation | Log Decoder       | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |
| Log Decoder       | NW Server         | TCP 443                                                                                                                                                | RSA Update Repository                          |
| Admin Workstation | Log Decoder       | TCP 22                                                                                                                                                 | SSH                                            |
| Log Decoder       | Log Event Sources | See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all RSA NetWitness Platform 11.x documents. |                                                |
| Log Event Sources | Log Decoder       | TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)                                         | Log Collection Ports                           |
| Log Event Sources | Log Decoder       | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009                                                                           | Log Collection FTP/S Ports                     |
| NW Server         | Log Decoder       | TCP 50001 (Non-SSL),56001 (SSL), 50101 (REST)                                                                                                          | Log Collector Application Ports                |
| NW Server         | Log Decoder       | TCP 50002 (Non-SSL), 56002 (SSL),56202 (Endpoint), 50102 (REST)                                                                                        | Log Decoder Application Ports                  |
| NW Server         | Log Decoder       | TCP 56006 (SSL), 50106 (REST)                                                                                                                          | NetWitness Appliance Ports                     |
| NW Server         | Log Decoder       | TCP 5671                                                                                                                                               | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Log Decoder       | Log Collector     | TCP 6514                                                                                                                                               |                                                |
| Log Decoder       | NFS Server        | TCP 111 2049<br>UDP 111 2049                                                                                                                           | iDRAC Installations                            |
| Log Decoder       | NW Server         | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |

## Log Hybrid Host

| Source Host       | Destination Host  | Destination Ports                                                                                                                                      | Comments                        |
|-------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Admin Workstation | Log Hybrid        | TCP 15671                                                                                                                                              | RabbitMQ Management UI          |
| Log Hybrid        | NW Server         | TCP 15671                                                                                                                                              | RabbitMQ Management UI          |
| Log Hybrid        | NW Server         | TCP 443                                                                                                                                                | RSA Update Repository           |
| Admin Workstation | Log Hybrid        | TCP 22                                                                                                                                                 | SSH                             |
| Log Collector     | Log Event Sources | See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all RSA NetWitness Platform 11.x documents. |                                 |
| Log Event Sources | Log Hybrid        | TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)                                         | Log Collection Ports            |
| Log Event Sources | Log Hybrid        | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009                                                                           | Log Collection FTP/S Ports      |
| NW Server         | Log Hybrid        | TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)                                                                                                         | Log Collector Application Ports |
| NW Server         | Log Hybrid        | TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)                                                                                       | Log Decoder Application Ports   |
| NW Server         | Log Hybrid        | TCP TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)                                                                                                     | Concentrator Application Ports  |

| Source Host | Destination Host | Destination Ports                | Comments                                                   |
|-------------|------------------|----------------------------------|------------------------------------------------------------|
| NW Server   | Log Hybrid       | TCP 56006 (SSL),<br>50106 (REST) | NetWitness<br>Appliance<br>Ports                           |
| NW Server   | Log Hybrid       | TCP 5671                         | RabbitMQ<br>(AMQPS)<br>message bus<br>for all NW<br>hosts. |
| Log Hybrid  | NFS Server       | TCP 111 2049<br>UDP 111 2049     | iDRAC<br>Installations                                     |

## Log Hybrid - Retention Host

| Source Host            | Destination Host       | Destination Ports                                                                                                                                      | Comments                                       |
|------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Admin Workstation      | Log Hybrid - Retention | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |
| Log Hybrid - Retention | NW Server              | TCP 15671                                                                                                                                              | RabbitMQ Management UI                         |
| Log Hybrid - Retention | NW Server              | TCP 443                                                                                                                                                | RSA Update Repository                          |
| Admin Workstation      | Log Hybrid - Retention | TCP 22                                                                                                                                                 | SSH                                            |
| Log Collector          | Log Event Sources      | See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all RSA NetWitness Platform 11.x documents. |                                                |
| Log Event Sources      | Log Hybrid - Retention | TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)                                         | Log Collection Ports                           |
| Log Event Sources      | Log Hybrid - Retention | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009                                                                           | Log Collection FTP/S Ports                     |
| NW Server              | Log Hybrid - Retention | TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)                                                                                                         | Log Collector Application Ports                |
| NW Server              | Log Hybrid - Retention | TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)                                                                                       | Log Decoder Application Ports                  |
| NW Server              | Log Hybrid - Retention | TCP 56006 (SSL), 50106 (REST)                                                                                                                          | NetWitness Appliance Ports                     |
| NW Server              | Log Hybrid - Retention | TCP 5671                                                                                                                                               | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Log Hybrid - Retention | NFS Server             | TCP 111 2049<br>UDP 111 2049                                                                                                                           | iDRAC Installations                            |

## Malware Host

| Source Host       | Destination Host       | Destination Ports                | Comments                                       |
|-------------------|------------------------|----------------------------------|------------------------------------------------|
| Admin Workstation | Malware                | TCP 15671                        | RabbitMQ Management UI                         |
| Malware           | NW Server              | TCP 15671                        | RabbitMQ Management UI                         |
| Malware           | NW Server              | TCP 443                          | RSA Update Repository                          |
| Admin Workstation | Malware                | TCP 22                           | SSH                                            |
| NW Server         | Malware                | TCP 60007                        | Malware Application Ports                      |
| NW Server         | Malware                | TCP 56006 (SSL),<br>50106 (REST) | NetWitness Appliance Ports                     |
| NW Server         | Malware                | TCP 5671                         | RabbitMQ (AMQPS) message bus for all NW hosts. |
| NW Server         | Malware                | TCP 5432                         | Postgresql                                     |
| NW Server         | Malware                | TCP 56003 (SSL),<br>50103 (REST) | Broker Application Ports                       |
| Malware           | panacea.threatgrid.com | TCP 443                          | Threatgrid                                     |
| Malware           | cloud.netwitness.com   | TCP 443                          | Community evaluation / Opswat                  |
| Malware           | NFS Server             | TCP 111 2049<br>UDP 111 2049     | iDRAC Installations                            |

## Network Decoder Host

| Source Host       | Destination Host | Destination Ports                              | Comments                                       |
|-------------------|------------------|------------------------------------------------|------------------------------------------------|
| Admin Workstation | Network Decoder  | TCP 15671                                      | RabbitMQ Management UI                         |
| Network Decoder   | NW Server        | TCP 15671                                      | RabbitMQ Management UI                         |
| Network Decoder   | NW Server        | TCP 443                                        | RSA Update Repository                          |
| Admin Workstation | Network Decoder  | TCP 22                                         | SSH                                            |
| NW Server         | Network Decoder  | TCP 56004 (SSL), 50104 (REST), 50004 (Non-SSL) | Network Decoder Application Ports              |
| NW Server         | Network Decoder  | TCP 56006 (SSL), 50106 (REST)                  | NetWitness Appliance Ports                     |
| NW Server         | Network Decoder  | TCP 5671                                       | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Network Decoder   | NFS Server       | TCP 111 2049<br>UDP 111 2049                   | iDRAC Installations                            |



## Network Hybrid Host

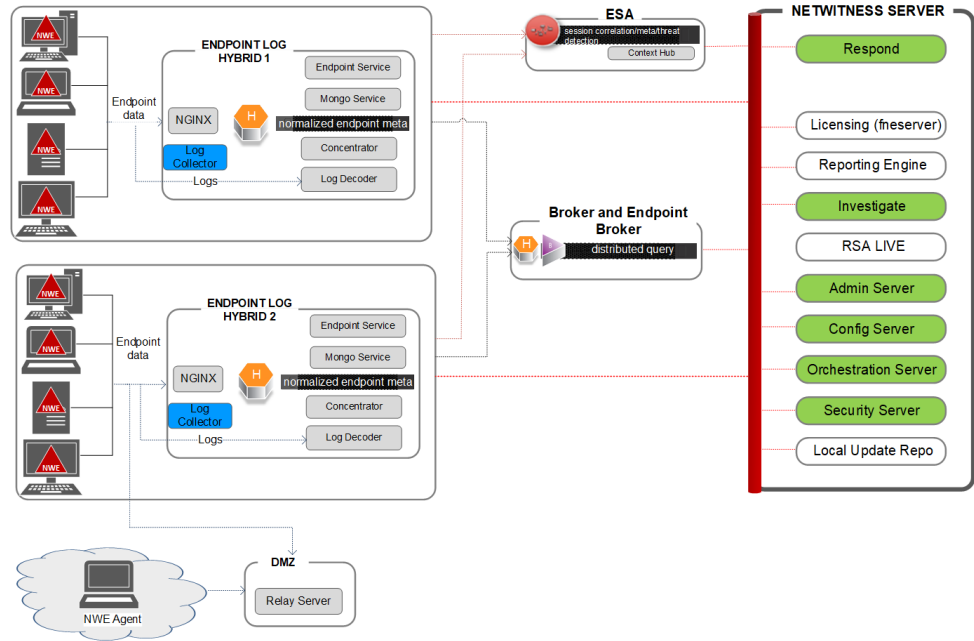
| Source Host       | Destination Host | Destination Ports                              | Comments                                       |
|-------------------|------------------|------------------------------------------------|------------------------------------------------|
| Admin Workstation | Network Hybrid   | TCP 15671                                      | RabbitMQ Management UI                         |
| Network Hybrid    | NW Server        | TCP 15671                                      | RabbitMQ Management UI                         |
| Network Hybrid    | NW Server        | TCP 443                                        | RSA Update Repository                          |
| Admin Workstation | Network Hybrid   | TCP 22                                         | SSH                                            |
| NW Server         | Network Hybrid   | TCP 56004 (SSL), 50104 (REST), 50004 (Non-SSL) | Network Decoder Application Ports              |
| NW Server         | Network Hybrid   | TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST) | Concentrator Application Ports                 |
| NW Server         | Network Hybrid   | TCP 56006 (SSL), 50106 (REST)                  | NetWitness Appliance Ports                     |
| NW Server         | Network Hybrid   | TCP 5671                                       | RabbitMQ (AMQPS) message bus for all NW hosts. |
| Network Hybrid    | NFS Server       | TCP 111 2049<br>UDP 111 2049                   | iDRAC Installations                            |

## UEBA Host

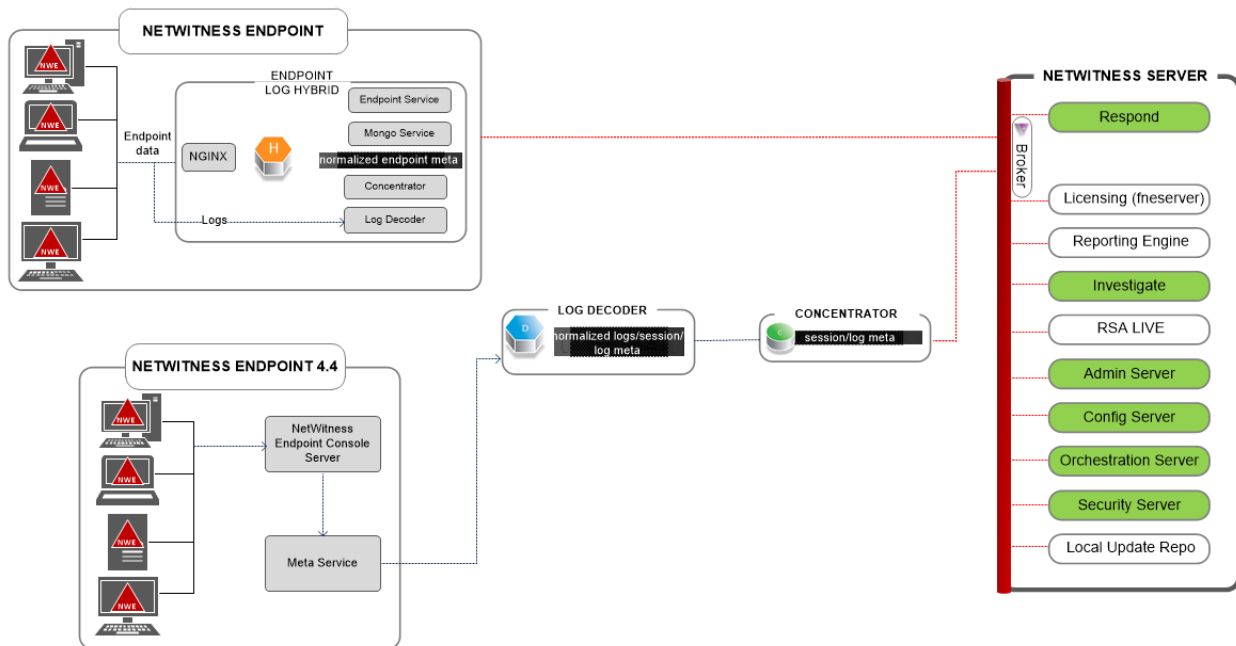
| Source Host       | Destination Host | Destination Ports                                  | Comments                                      |
|-------------------|------------------|----------------------------------------------------|-----------------------------------------------|
| UEBA Server       | NW Server        | TCP 443                                            | RSA Update Repository                         |
| UEBA Server       | Broker           | TCP 56003 (SSL), 50103 (REST)                      | Broker Application Ports                      |
| UEBA Server       | Concentrator     | TCP TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST) | Concentrator Application Ports                |
| Admin Workstation | UEBA Server      | 443                                                | UEBA Monitoring                               |
| Admin Workstation | UEBA Server      | 22                                                 | SSH                                           |
| Admin Workstation | UEBA Server      | TCP 15671                                          | RabbitMQ Management UI                        |
| UEBA Server       | NW Server        | TCP15671                                           | UEBA Alerts forwarding to Respond             |
| NW Server         | NFS Server       | TCP 111, 2049<br>UDP 111, 2049                     | iDRAC Installations                           |
| NW Server         | UEBA Server      | TCP 5671                                           | RabbitMQ (AMQPS) message bus for all NW hosts |

# NetWitness Endpoint Architecture

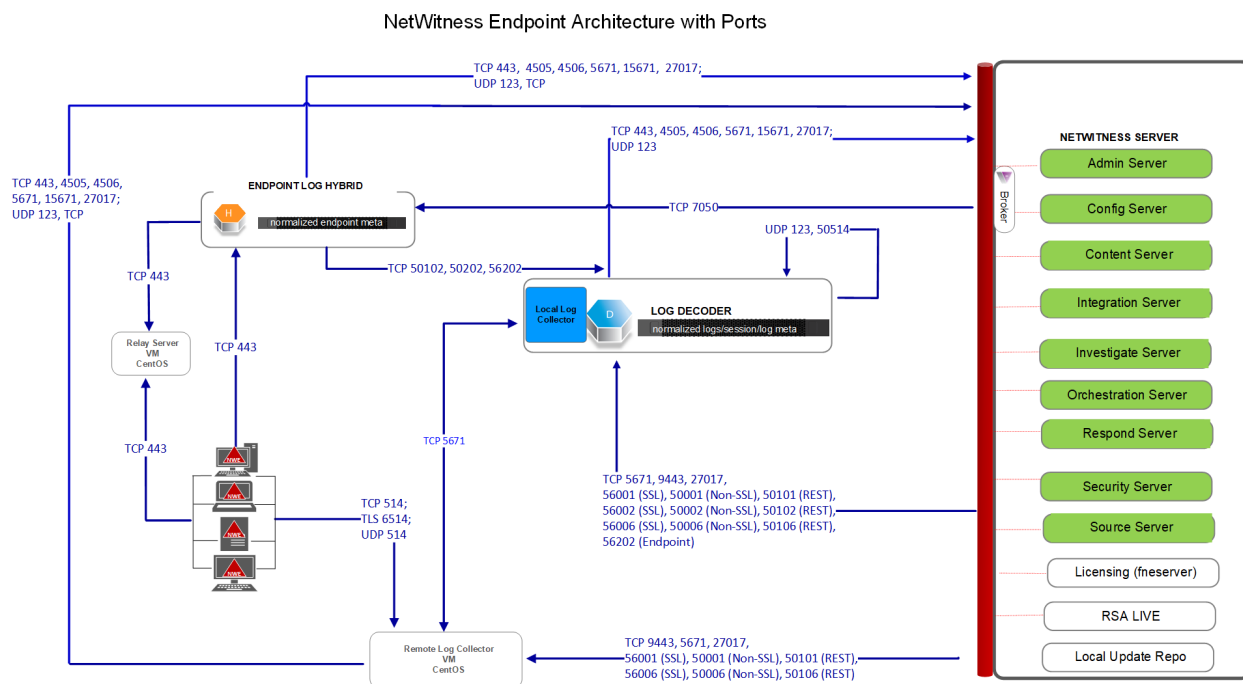
NetWitness Endpoint Architecture



# NetWitness Endpoint 4.4 Integration with NetWitness Platform



## NetWitness Endpoint 11.3.1 Architecture with Ports



For more information on the services running on Endpoint Log Hybrid, see *RSA NetWitness Endpoint Configuration Guide*.

## How to Change UDP Port for Endpoint Log Hybrid

The following steps tell you how to change the Endpoint Log Hybrid default UDP port 444 if it is not acceptable in your environment. 555 is the example this procedure uses as a replacement for 444 UDP port.

There are two tasks you need to do to change the Endpoint Log Hybrid default UDP port 444:

[Task 1 - Tell All Agents to Use a New UDP Port](#)

[Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment](#)

**Note:** If you did not select the custom firewall rules option when you ran the `nwsetup-tui`, NetWitness platform overwrites the firewall rules after a period of time. Please refer to the following Knowledge Base Article 00036446 (<https://community.rsa.com/docs/DOC-93651>) if this is the case.

### Task 1 - Tell All Agents to Use a New UDP Port

Complete the following steps to update the UDP port in the default Enterprise Data Replication (EDR) policy, and all other policies you have, to tell all agents to use a new UDP port.

1. In the **NetWitness Platform** menu, select **ADMIN > Endpoint Sources > Policies**. The **Policies** view is displayed.
2. Select the **Default EDR Policy** and click **Edit** from the toolbar.
3. roll down to find the **UDP PORT** and change the value (for example, change from **444** to **555**).
4. Click **Publish Policy** at the bottom of the view.

## Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment

SSH to each Endpoint Log Hybrid host in your environment with `admin` credentials and make the following updates.

1. Update the `iptables` rules to allow 555 in place of 444.
  - a. Replace 444 with 555 in the following file.  

```
vi /etc/sysconfig/iptables
```
  - b. Restart `iptables` with the following command string.  

```
systemctl restart iptables
```
  - c. Verify the change with the following command string.  

```
iptables -L -n
```

The following is an example of what is displayed for a correct change.

```
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /*
EndpointNginxPort */ ctstate NEW
```
2. Update the SELinux policy. 555 is a privileged port, so you must update SELinux policy to allow this port.
  - a. Run the following command string.  

```
semanage port -a -t http_port_t -p udp 555
```

If you received any python errors or warnings, ignored them.
  - b. Verify the change with the following command string.  

```
semanage port -l | grep http_port_t
```

The following is an example of what is displayed for a correct change.

```
http_port_t udp 555, 444
```
  - c. (Optional) Remove 444.
3. Update `nginx` config.
  - a. Edit the following file.  

```
vi /etc/nginx/nginx.conf
```
  - b. Search for the following string.  

```
listen 444 udp;
```
  - c. Replace 444 with 555.
  - d. Restart `nginx` with the following command string.  

```
systemctl restart nginx
```

4. Verify that agents are communicating over the new port.

- a. Run the following command string.

```
tcpdump -i eth0 port 555
```

- b. Wait for 30 seconds because the port sends out a beacon every 30 seconds. If everything is working correctly, information similar to the following will be displayed.

```
09:20:12.571316 IP 10.40.15.103.60807 > EPS1.rsa.lab.emc.com.dsf: UDP,
length 20
```

```
09:20:12.572433 IP EPS1.rsa.lab.emc.com.dsf > 10.40.15.103.60807: UDP,
length 1
```

Both lines must be returned. One is the size request (20 bytes) and the other is the response size (1 byte).

# Site Requirements and Safety

---

Make sure that you read this topic thoroughly and observe all warnings and precautions prior to installing or maintaining your RSA devices.

## Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE) that may be installed in offices, schools, computer rooms, and similar indoor commercial type locations. This device is not intended for any connection to an outdoor type cable.

## Service

There are no user-serviceable components inside of this device. Please contact Customer Care in the event of a malfunction. In a fault condition, high temperatures may arise inside the system causing an alarm signal. In the event of the alarm signal, immediately disconnect the device from the power source and contact Customer Care. Further operation of the device will be unsafe and may cause personal injury or property damage.

## Safety Information

### Site Selection

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean, dry, and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat, including direct sunlight and radiators.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cords, because they serve as the product's main power disconnect.

### Equipment Handling Practices

Reduce the risk of personal injury or equipment damage by:

- Conforming to local occupational health and safety requirements when moving and lifting equipment.
- Using mechanical assistance or other suitable assistance when moving and lifting equipment.

- Reducing the weight for easier handling by removing any easily detachable components.

## Power and Electrical Warnings

**Caution:** The power button, indicated by the standby power marking, DOES NOT completely turn off the system AC power; 5V standby power is active whenever the system is plugged in. To remove power from system, you must unplug the AC power cord(s) from the wall outlet.

- Do not attempt to modify or use an AC power cord if it is not the exact type required. A separate AC cord is required for each system power supply.
- This product contains no user-serviceable parts. Do not open the system.
- When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing it from the server.

## Rack Mount Warnings

- The equipment rack must be anchored to an unmovable support to prevent it from tipping when a server or piece of equipment is extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.
- Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Extend only one piece of equipment from the rack at a time.
- To avoid risk of potential electric shock, a proper safety ground must be implemented for the rack and each piece of equipment installed in it.

## Cooling and Air Flow

Installation of the equipment should be such that the amount of air flow required for safe operation of the equipment is not compromised.