



Deployment Guide

for RSA NetWitness® Platform 11.3



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

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

April 2019

Contents

The Basics	5
Basic Deployment	6
Process	6
NetWitness Platform High-Level Deployment Diagram	7
RSA NetWitness Platform Detailed Host Deployment Diagram	8
Deployment Options	9
Deployment Optional Setup Procedures	10
Group Aggregation	10
RSA Group Aggregation Deployment Recommendations	10
Advantages of Using Group Aggregation	10
Configure Group Aggregation	12
Hybrid Categories on NW Server	15
Second Endpoint Server	16
Warm Standby NW Server Host	17
Procedures	17
Planned Fail-Over Scenario	18
Required Fail-Over Scenario without Hardware Replacement	18
Required Fail-Over Scenario with Hardware Replacement	18
Set Up Secondary NW Server in Standby Role	19
Fail Over Primary NW Server to Secondary NW Server	32
Fail Back Secondary NW Server to Primary NW Server	33
Network Architecture and Ports	34
NetWitness Platform Network Architecture Diagram	34
NetWitness Network (Packets) Network Architecture Diagram	35
NetWitness Logs Network Architecture Diagram	36
Comprehensive List of NetWitness Platform Host, Service, and iDRAC Ports	37
NW Server Host	38
Archiver Host	39
Broker Host	40
Concentrator Host	41
Endpoint Log Hybrid	42
Event Stream Analysis (ESA) Host	43
iDRAC Ports	44
Log Collector Host	45
Log Decoder Host	46

Log Hybrid Host	47
Malware Host	48
Network Decoder Host	49
Network Hybrid Host	50
UEBA Host	51
NetWitness Endpoint Architecture	52
NetWitness Endpoint 4.4 Integration with NetWitness Platform	52
How to Change UDP Port for Endpoint Log Hybrid	53
Task 1 - Tell All Agents to Use a New UDP Port	53
Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment	53
Site Requirements and Safety	55
Intended Application Uses	55
Service	55
Safety Information	55
Site Selection	55
Equipment Handling Practices	55
Power and Electrical Warnings	56
Rack Mount Warnings	56
Cooling and Air Flow	56

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 NetWitness Platform Logs & Network 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:

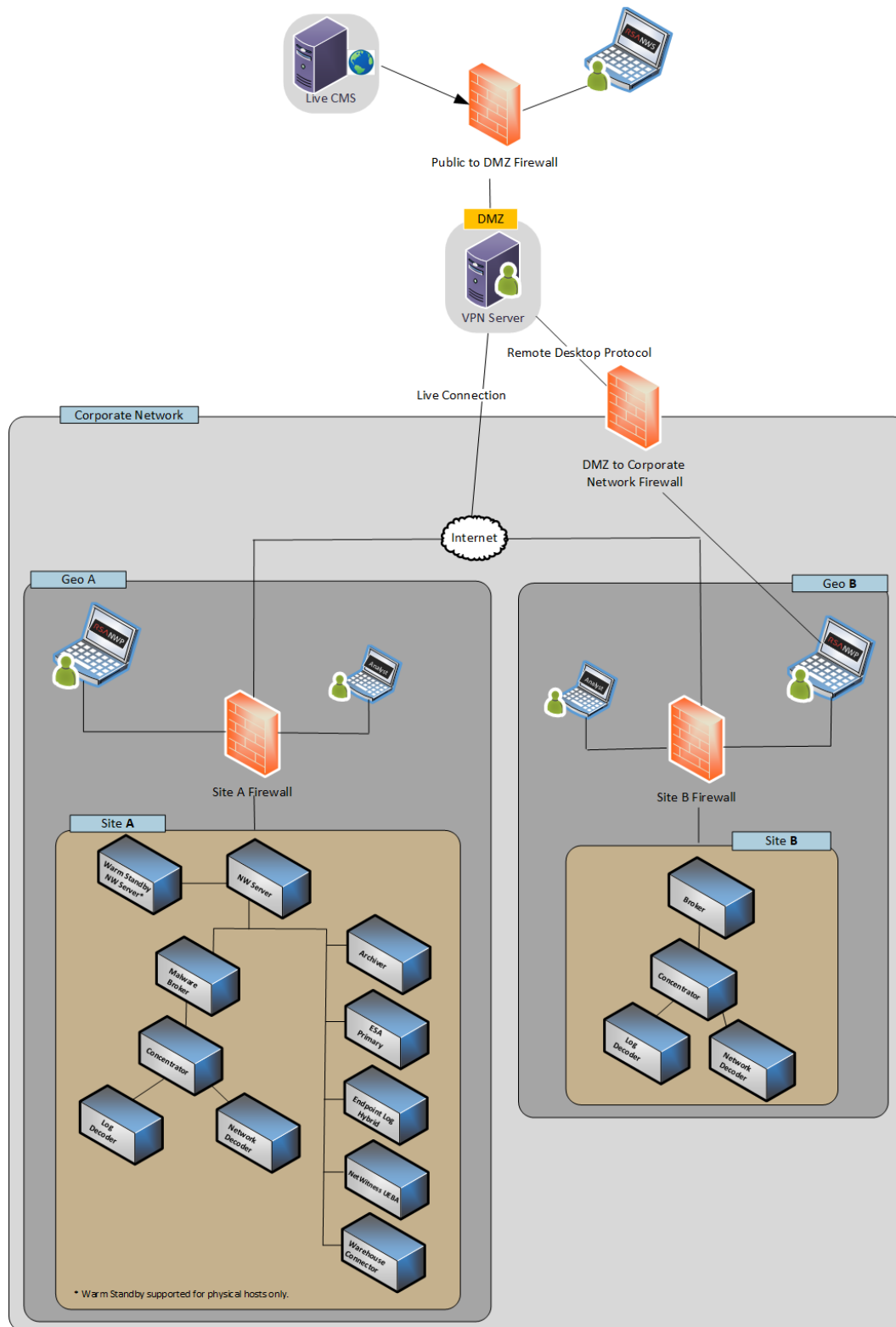
- For RSA Physical Hosts:
 1. Install physical hosts and connect to the network as described in the RSA NetWitness® Platform Hardware Setup Guides and the *RSA NetWitness® Platform Physical Host Installation Guide*.
 2. Set up licensing for NetWitness Platform as described in the *RSA NetWitness® Platform 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*.

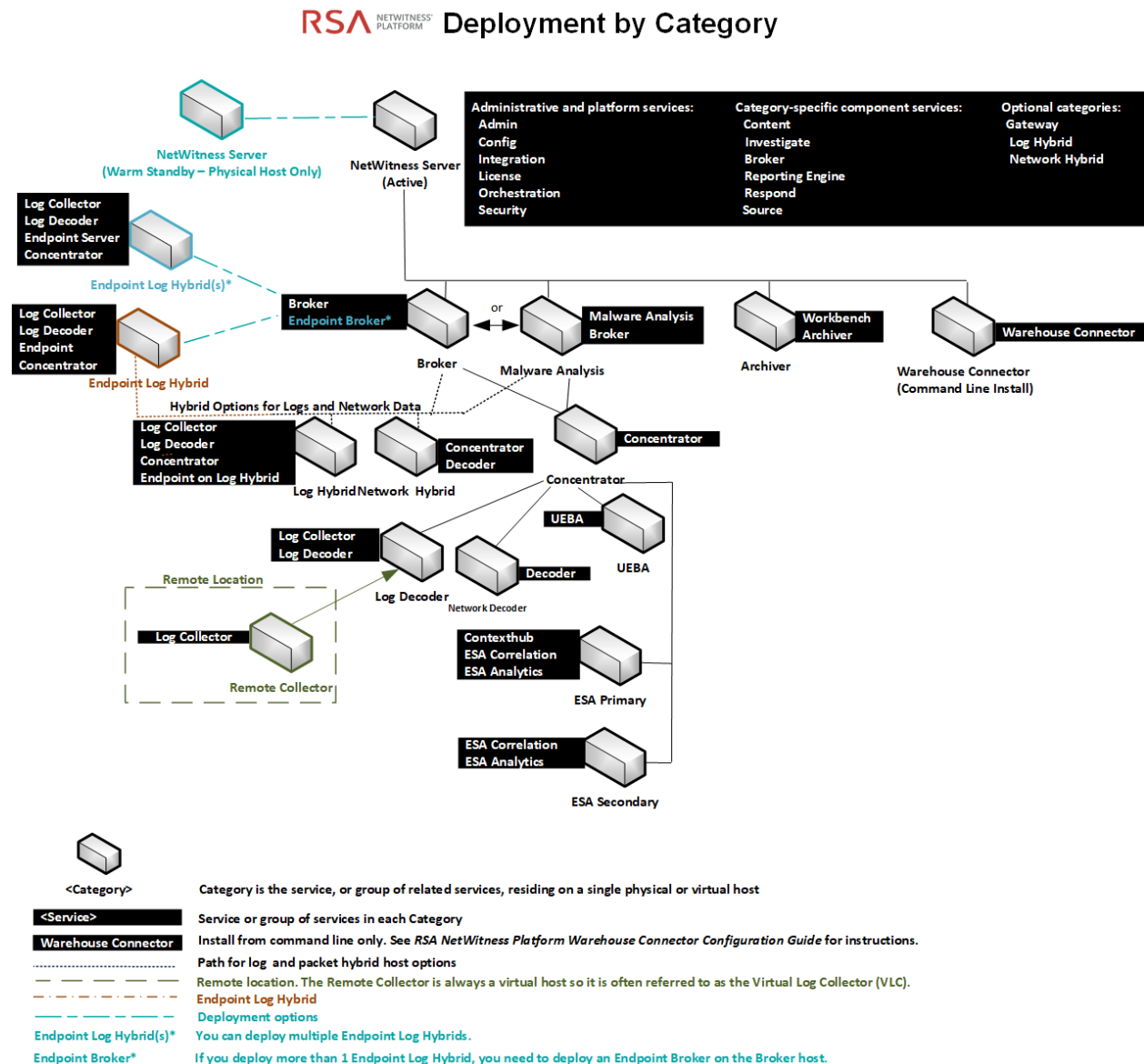
NetWitness Platform High-Level Deployment Diagram

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 NetWitness Platform Logs & Network 11.x documents.



Deployment Options

You deploy RSA NetWitness Platform with the following options.

- Group Aggregation
- Second Endpoint Server
- Warm Standby NW Server Host
- Hybrid Categories on the NW Server

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

Deployment Optional Setup Procedures

[Group Aggregation](#)

[Hybrid Categories on the NW Server](#)

[Second Endpoint Server](#)

[Warm Standby NW Server](#)

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

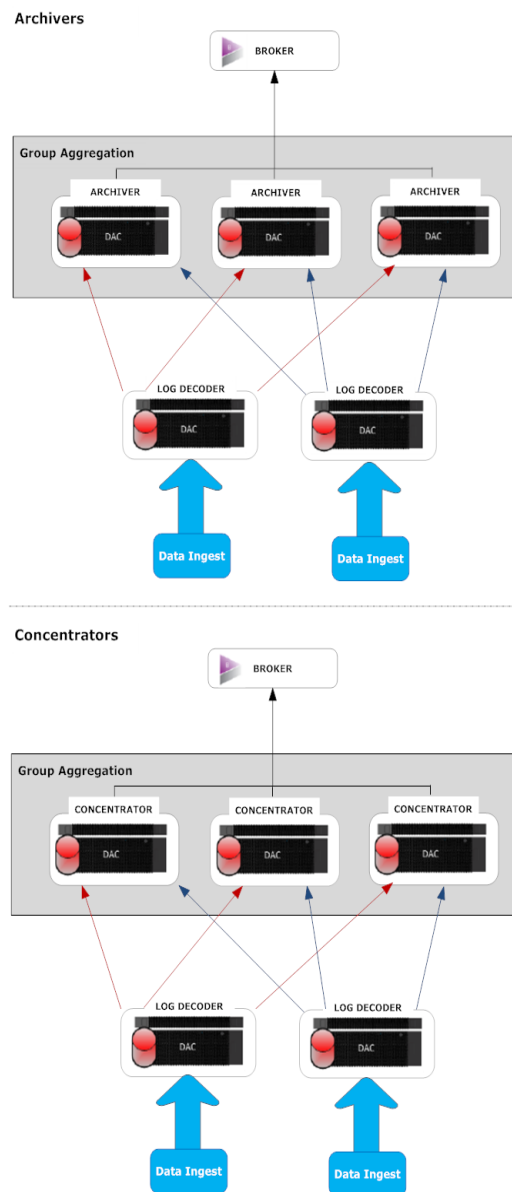
RSA recommends the following deployment for Group Aggregation:

- 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.

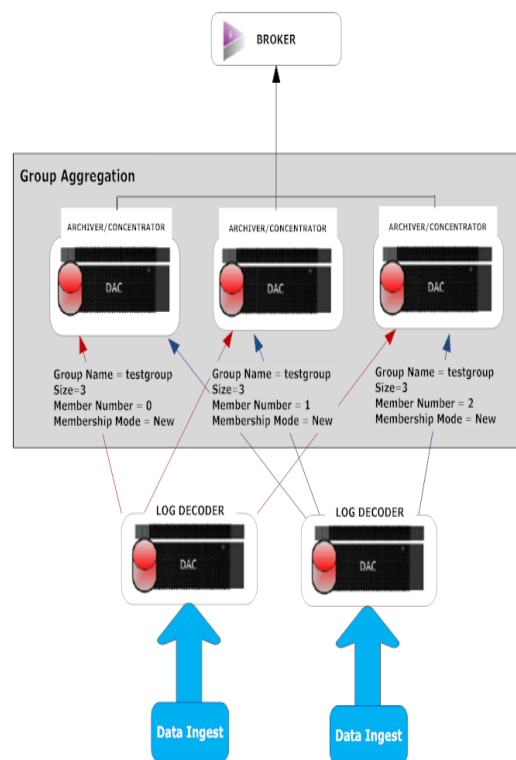
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

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.



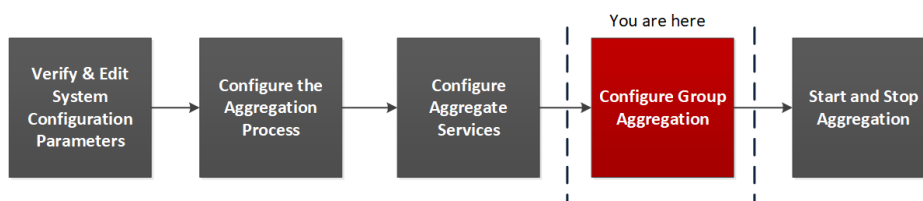
Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

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.

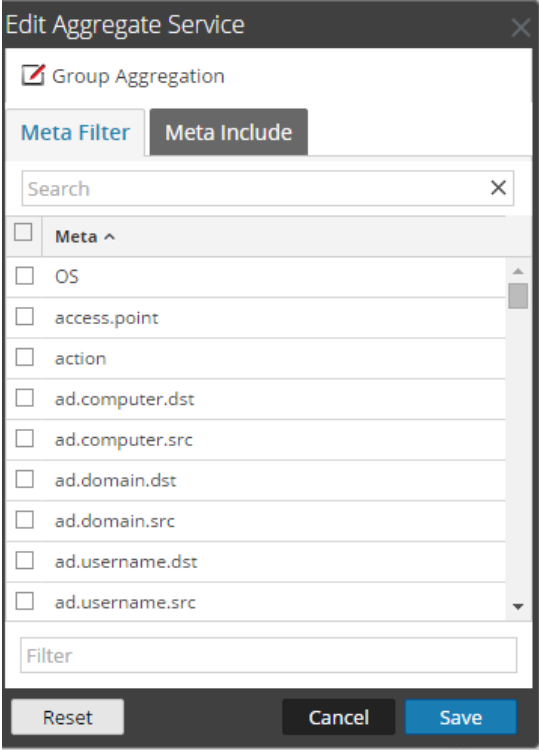


Complete the following steps to set up group aggregation.


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 .

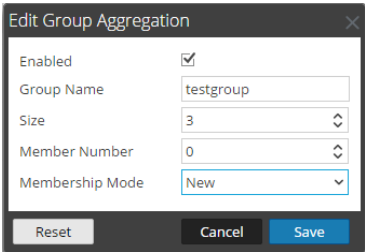
The **Edit Aggregate Service** dialog is displayed.



The **Edit Aggregate Service** dialog is shown. It has a title bar with a close button. Below the title bar is a checkbox labeled **Group Aggregation** which is checked. There are two tabs: **Meta Filter** (selected) and **Meta Include**. Below the tabs is a search bar with the text "Search" and a clear button (X). A list of meta items follows, each with a checkbox and a label: **Meta ^**, **OS**, **access.point**, **action**, **ad.computer.dst**, **ad.computer.src**, **ad.domain.dst**, **ad.domain.src**, **ad.username.dst**, and **ad.username.src**. At the bottom of the list is a **Filter** input field. At the very bottom are three buttons: **Reset**, **Cancel**, and **Save**.

- f. Click .

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



The **Edit Group Aggregation** dialog is shown. It has a title bar with a close button. Below the title bar are several fields: **Enabled** (checkbox, checked), **Group Name** (text input, value "testgroup"), **Size** (spin box, value "3"), **Member Number** (spin box, value "0"), and **Membership Mode** (dropdown menu, value "New"). At the bottom are three buttons: **Reset**, **Cancel**, and **Save**.

- 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 console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar shows the 'SERVICES' section with sub-tabs for Hosts, Event Sources, Health & Wellness, System, and Security. The main content area is titled 'Aggregate Services' and contains a table with columns: Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. Two services are listed: 10.31.125.245 (Port 50004, Rate 0, Max 0, Behind 0, Meta Fields, Filter, Meta Include no, Grouped consuming) and 10.31.125.246 (Port 50002, Rate 0, Max 0, Behind 0, Meta Fields, Filter, Meta Include yes, Grouped offline). Below this table is the 'System Configuration' section with a table listing various settings like Compression, Port, SSL FIPS Mode, etc. The 'Aggregation Configuration' section on the right contains a table with settings for Aggregate Settings (Aggregate Autostart, Aggregate Hours, Aggregate Interval) and Service Heartbeat (Heartbeat Error Restart, Heartbeat Next Attempt, Heartbeat No Response). The 'Aggregate Max Sessions' is set to 10000. An 'Apply' button is located at the bottom of the page.

Hybrid Categories on NW Server

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.

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 11.3 on Other Component Hosts" under "Installation Tasks" of the *Physical Host Installation Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.
 - For a virtual host, follow the instructions in the *Virtual Host Installation Guide* in "Task 2 - Install 11.3 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

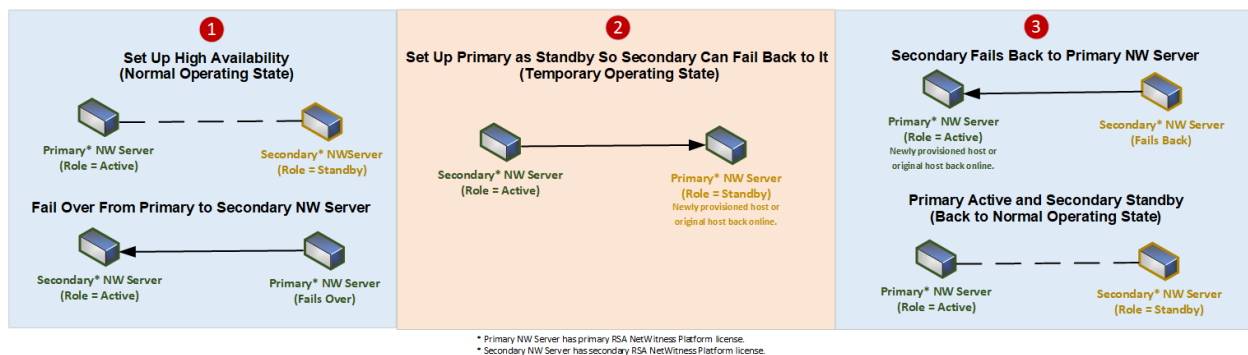
The Warm Standby NW Server duplicates the critical components and configurations of your active NW Server Host to increase reliability.

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 allowing 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, 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, you must assign the same IP address as the primary NW Server to the secondary NW Server so it can assume the active role.

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 (<https://community.rsa.com/docs/DOC-1294>) 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

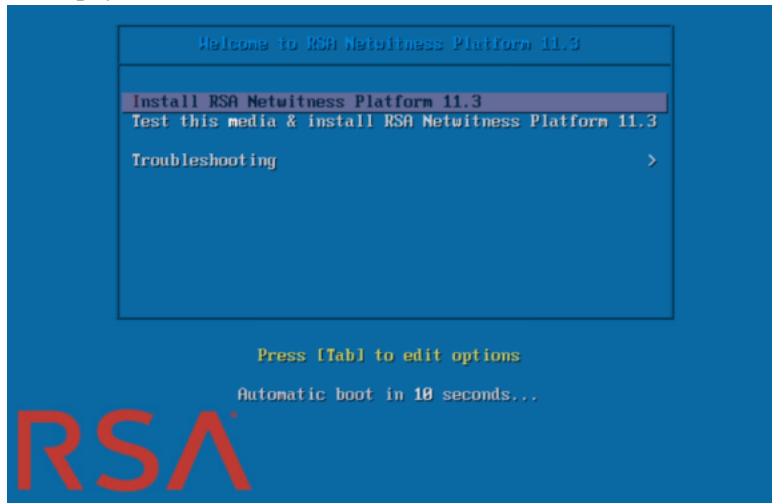
This scenario occurs when the active NW Server completely fails and the hardware requires replacement, for example you receive a Return Merchandise Authorization (RMA). You need to run `nwsetup-tui` and contact Customer Support (<https://community.rsa.com/docs/DOC-1294>) to reestablish licensing. If 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

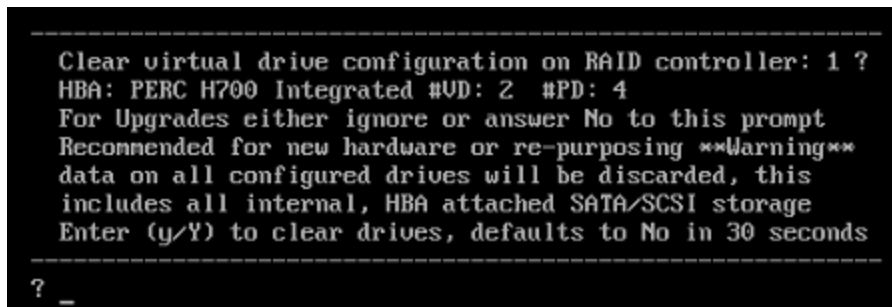
1. Before you install a secondary NW Server host for the standby role, make sure that your:
 - a. primary NW Server is running 11.3.
 - b. All your component hosts are running 11.3
If you are:
 - Installing NetWitness Platform 11.3, follow the instructions in the *RSA NetWitness Platform Physical Host Installation Guide for Version 11.3*.
 - Upgrading from 10.6.x to 11.3, follow the instructions in the *RSA NetWitness Platform Physical Host Upgrade Guide for Version 10.6.6.x to 11.3*.
 - Updating from 11.x to 11.3, follow the instructions in *RSA NetWitness Platform Update Guide for Version 11.x to 11.3*.
Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 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 etch an 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 11.3** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



- d. Select **Install RSA NetWitness Platform 11.3** (default selection) and press **Enter**. The Installation program runs and stops at the **Enter (y/Y) to clear drives** prompt that asks you to format the drives.



- 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.

```
Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

- f. Press **Enter** to reboot the host.

The Installation program asks you to clear the drives again.

```
-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations 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
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----
```

- g. Type **N** because you already cleared the drives.

The Enter **Q (Quit)** or **R (Reinstall)** prompt is displayed.

```
-----
No root level logical volumes found for Migration
Assuming this system is new or being reinstalled
Migration cannot proceed, system will be reimaged
If you had intended to migrate please quit and
contact support for assistance.
-----
Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

- h. Type **R** to install the base image.

The installation program displays the components as they are installed, which varies depending on the appliance, and reboots.

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

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

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

- i. 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
```

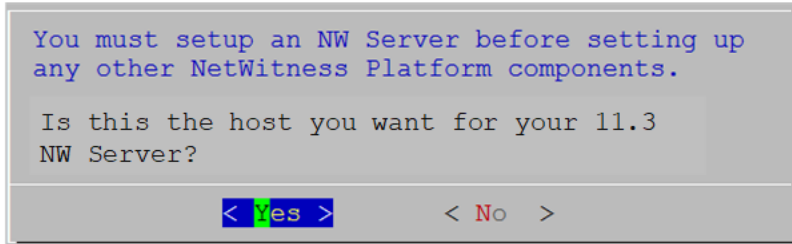
92%

`<Accept >`

`<Decline>`

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

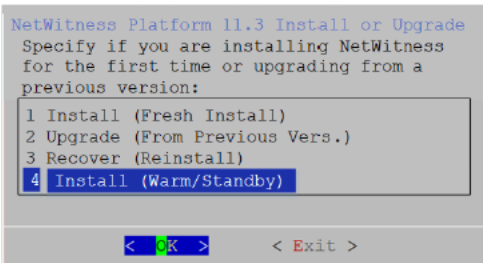
The **Is this the host you want for your 11.3 NW Server** prompt is displayed.



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).

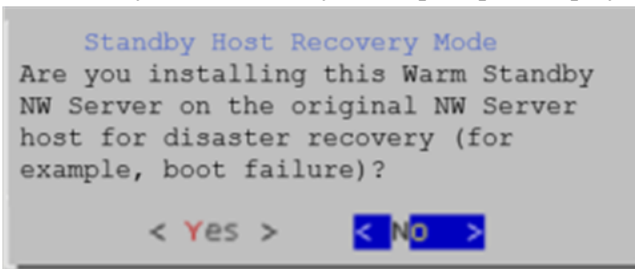
4. Tab to **Yes** and press **Enter**.

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



5. Tab to **4 Install (Warm Standby)** and press **Enter**.

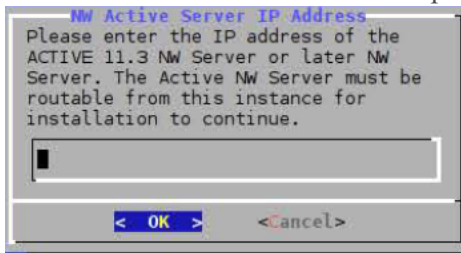
The **Standby Host Recovery Mode** prompt is displayed.



6. Tab to:

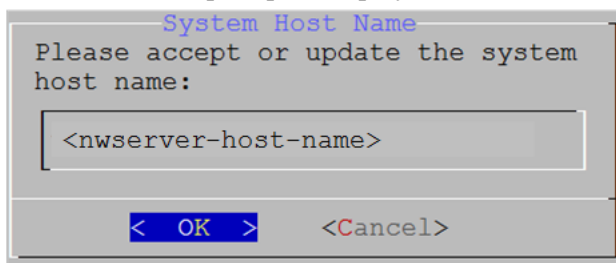
- **No** and press **Enter** to set up a secondary NW Server with the standby role (most common scenario).
- **Yes** and press **Enter** to set up a host that was previously used as a primary NW Server with the standby role so you can execute a fail-over and fail-back (less common scenario).

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 { } [] () / \ ' " ` ~ ; : . < > -

The screenshot shows a dialog box titled "Master Password" in blue text. The main text in blue explains that the master password is used for the system recovery account and the NetWitness UI "admin" account, and that it should be safely stored. Below this, it says "Enter a Master Password." in black. There are two input fields: "Password" and "Verify". Both fields contain masked characters (asterisks). The "Password" field has a red cursor at the end. The "Verify" field has a green cursor at the end. At the bottom of the dialog, there are three buttons: "< OK >" and "<Cancel>".

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

The screenshot shows a dialog box titled "Deployment Password" in blue text. The main text in blue explains that the deployment password is used when deploying NetWitness hosts and needs to be safely stored. Below this, it says "Enter a Deploy Password." in black. There are two input fields: "Password" and "Verify". Both fields contain masked characters (asterisks). The "Password" field has a red cursor at the end. The "Verify" field has a green cursor at the end. At the bottom of the dialog, there are three buttons: "< OK >" and "<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.

```

IP Address <IP-address> is
currently assigned to this
host. Do you still want to
change network settings?

< Yes >    < No >

```

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.

```

NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >

```

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.

```

NetWitness Platform Network Configuration
The IP address of the NW Server is used by all other NetWitness
Platform components. RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP. After the
IP address is assigned, record it for future use. You need this
address to set up other components.

Select an IP address configuration for the NW Server.

1 Static IP Configuration
2 Use DHCP

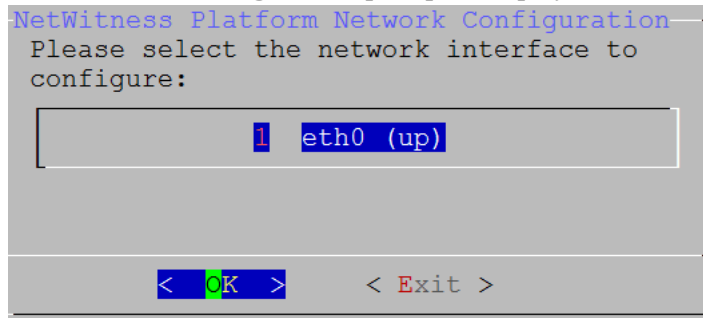
< OK >    < Exit >

```

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.



NetWitness Platform Network Configuration

Please select the network interface to configure:

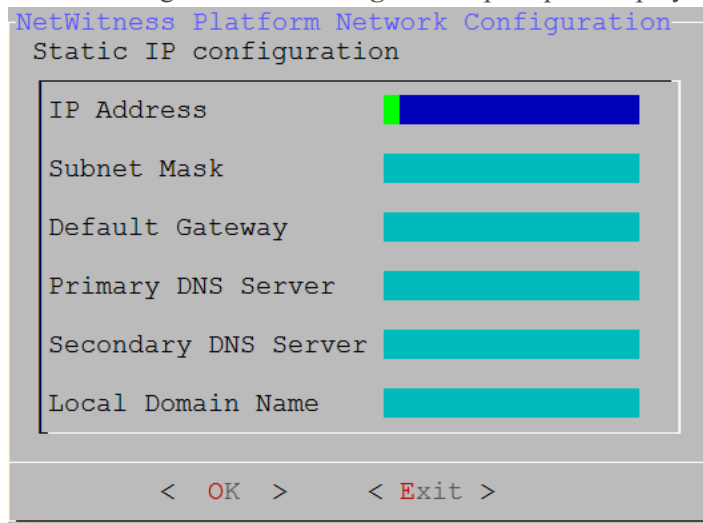
1 eth0 (up)

< OK > < Exit >

This is a terminal-style dialog box. The title bar reads 'NetWitness Platform Network Configuration'. The main text says 'Please select the network interface to configure:'. Below this is a list box containing one item, '1 eth0 (up)', where '1' is highlighted in blue. At the bottom, there are two buttons: '< OK >' and '< Exit >'. The 'OK' button has a green highlight on the 'O'.

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.



NetWitness Platform Network Configuration

Static IP configuration

IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
Local Domain Name	

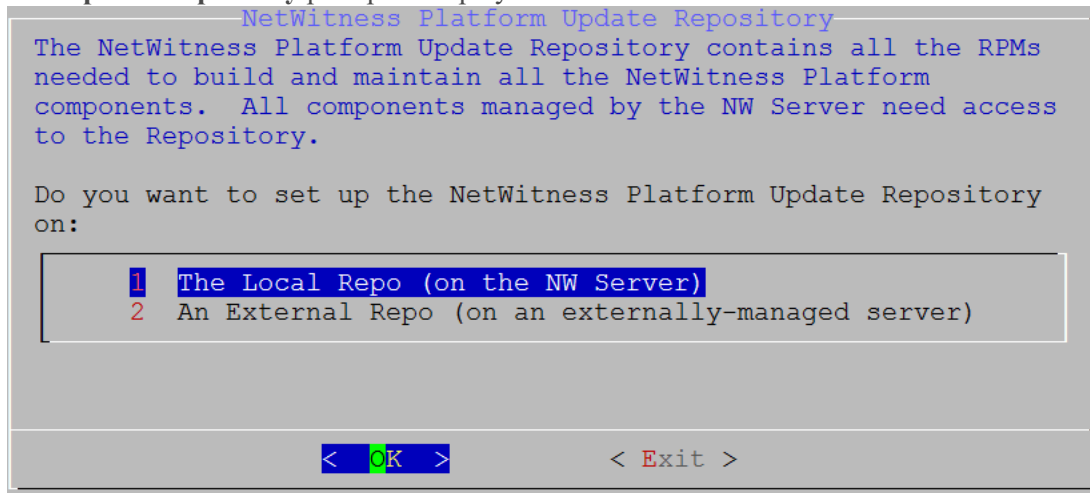
< OK > < Exit >

This is a terminal-style dialog box. The title bar reads 'NetWitness Platform Network Configuration'. The main text says 'Static IP configuration'. Below this is a table with six rows, each with a label and an empty input field. The labels are 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS Server', 'Secondary DNS Server', and 'Local Domain Name'. The first input field has a green cursor. At the bottom, there are two buttons: '< OK >' and '< Exit >'. The 'OK' button has a red highlight on the 'O'.

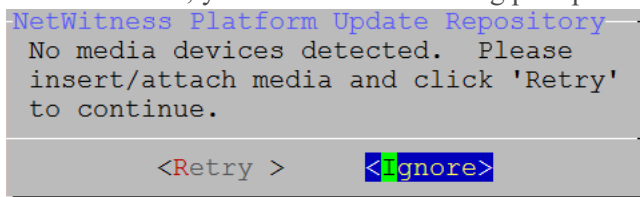
13. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an All fields are required error message is displayed (**secondary DNS Server** and **Local Domain Name** fields are not required). 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.

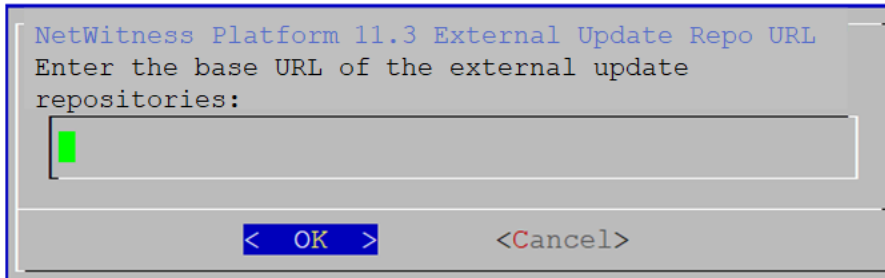
The **Update Repository** prompt is displayed.



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 11.2.0.0. If the program cannot find the attached media, you receive the following prompt.



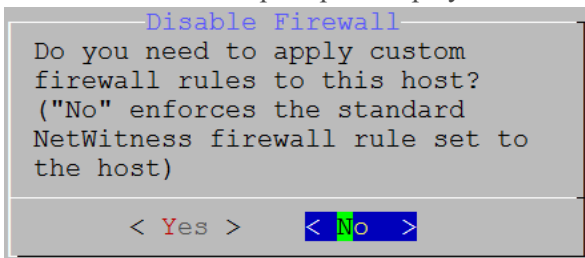
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to [Appendix B. Create an External Repo](#) for instructions on how to create this repo and its external repo URL so you can 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.

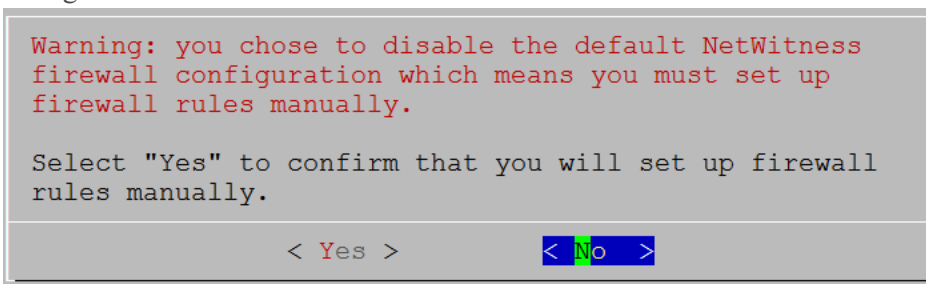
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for instructions. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

The Disable firewall prompt is displayed.

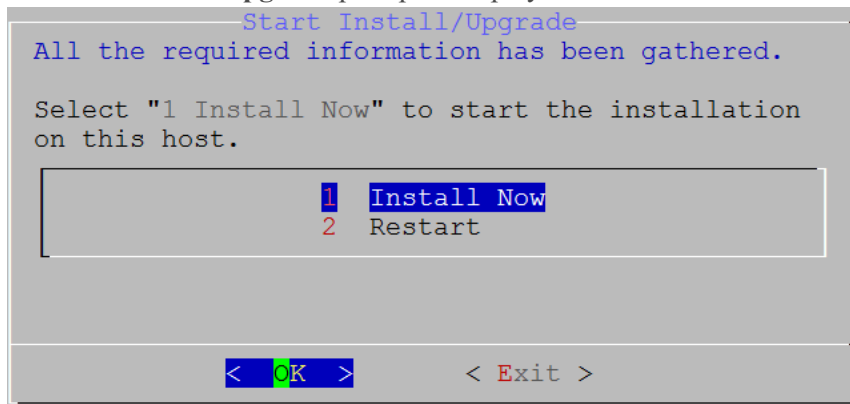


15. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

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 11.3 on the NW Server.

When **Installation complete** is displayed, you have installed the 11.3 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 back 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: '0 0 1,10 * *'
<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

Initially, the primary NW Server fails over to the secondary NW Server. A subsequent fail-over that is the secondary NW Server to the primary NW Server and that is referred to as a fail-back. 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 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.

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

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

Global NetWitness Platform 11.3 Architecture

The diagram illustrates the Global NetWitness Platform 11.3 Architecture, showing the flow of data from various sources through processing and storage components to a central NetWitness Server and external systems.

Data Sources and Ingestion:

- Endpoint Log Hybrid:** Collects logs from endpoints (represented by laptop icons) and sends them to the NetWitness Server via a Broker.
- Malware Analysis:** Analyzes suspect files and sends results to the NetWitness Server via a Broker.
- Packet Capture TAP/SPAN:** Captures network traffic and sends it to the Network Decoder.
- Log Capture:** Captures logs from Syslog/Checkpoint LEA/SDE/ODBC/File/SNMP/VMWare/WinRM/WinLegacy/NetFlow and sends them to the Local Log Collector.
- Remote Log Collector:** Collects logs from Remote Log Collector VM (CentOS) and Remote Windows Legacy Log Collector.
- enVision LOCAL COLLECTOR:** Collects logs from the enVision LOCAL COLLECTOR (SSH) and sends them to the Local Log Collector.

Processing and Storage:

- Network Decoder:** Processes network/session/meta data and sends it to the Concentrator.
- Concentrator:** Processes session/network/meta data and sends it to the Warehouse.
- Warehouse:** Stores normalized logs, log meta, and network meta. It sends data to the Log Decoder and the Archiver.
- Log Decoder:** Processes normalized logs/session/log meta and sends it to the Archiver.
- Archiver:** Stores normalized logs/session/log meta and sends it to the NetWitness Server via a Broker.
- ESA Correlation:** Performs session correlation/meta/threat detection and sends results to the NetWitness Server via a Broker.
- NetWitness UEBA:** Performs User & Entity Behavior Analytics and sends results to the NetWitness Server via a Broker.

NetWitness Server Components:

- Admin Server
- Config Server
- Content Server
- Integration Server
- Investigate Server
- Orchestration Server
- Respond Server
- Reporting Engine
- Security Server
- Source Server
- Licensing (fserver)
- RSA LIVE
- Local Update Repo

External Systems and Interfaces:

- NetWitness Endpoint 4.x:** Connects to the NetWitness Server.
- Orchestration Server:** Connects to the NetWitness Server.
- Archer Cyber Incident & Breach Response:** Connects to the NetWitness Server.
- RSA LIVE INTELLIGENCE SYSTEM:** Connects to the NetWitness Server.

Legend:

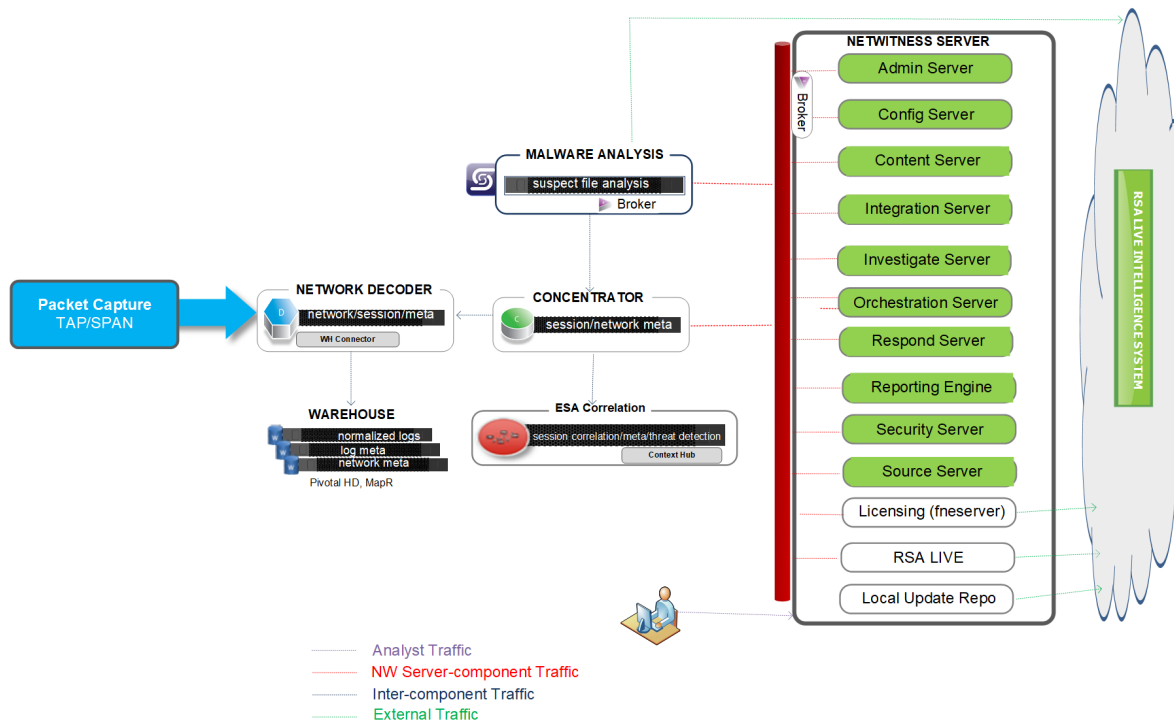
- Analyst Traffic (Blue line)
- NW Server-component Traffic (Red line)
- Inter-component Traffic (Green line)
- External Traffic (Yellow line)



NetWitness Network (Packets) Network Architecture Diagram

The following diagram illustrates the NetWitness Network (Packets) network architecture.

NetWitness Network 11.3 Architecture



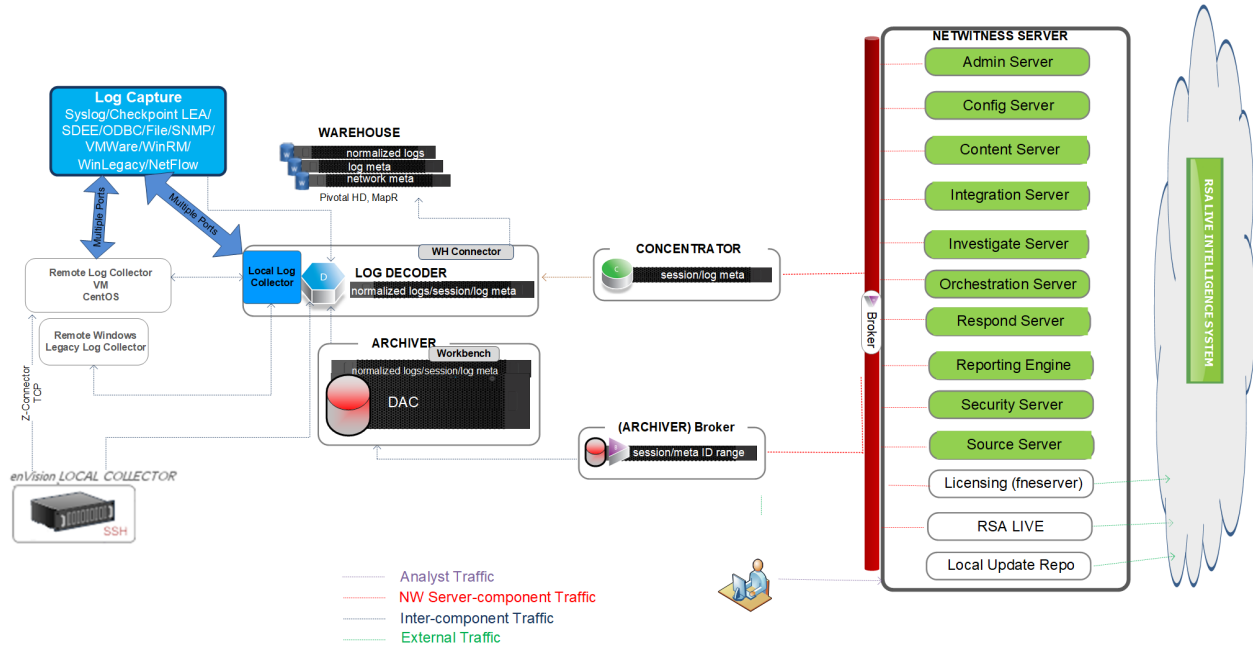
Notes:

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 Network Architecture Diagram

The following diagram illustrates the NetWitness Logs network architecture.

NetWitness Logs 11.3 Architecture



RSA NETWITNESS[™] LOGS

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).

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 NetWitness Platform Logs & Network 11.x documents.

This section contains the port specifications for the following hosts.

NW Server Host	Log Collector Host
Archiver Host	Log Decoder Host
Broker Host	Log Hybrid Host
Concentrator Host	Malware Host
Endpoint Log Hybrid Host	Network Decoder Host
Event Stream Analysis Host	Network Hybrid Host
iDRAC Ports	UEBA Host

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
NW Hosts	NW Server	TCP 53 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, 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

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 514, 6514, 50007 (Non-SSL) 56007 (SSL), 50107 (REST), UDP 514	Workbench Application Ports
Archiver	NFS Server	TCP 111 2049 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 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)	Concentrator Application Port
Concentrator	Network Decoder	TCP 56004	Concentrator 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 UDP 111 2049	iDRAC Installations

Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Agent	Endpoint Log Hybrid	TCP 443 UDP 444	NGINX HTTPS NGINX UDP. If UDP port 444 is not acceptable in your environment, see How to Change UDP Port for Endpoint Log Hybrid .
Endpoint Agent	Log Decoder or Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Log Hybrid	Log Decoder (External)	TCP 50102 (REST) 56202 (Protobuf SSL) 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 UDP 111, 2049	iDRAC Installations

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 50030 (SSL)	ESA Application Port
NW Server	ESA	TCP 50035 (SSL)	ESA Application Port
NW Server	ESA	TCP 50036 (SSL)	ESA Application Port
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 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

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 Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.	
Log Event Sources	Log Collector	TCP 514 (Syslog) 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 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 Master Table of Contents to find all NetWitness Platform Logs & Network 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 UDP 111 2049	iDRAC Installations

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 Master Table of Contents to find all NetWitness Platform Logs & Network 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
NW Server	Log Hybrid	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid	NFS Server	TCP 111 2049 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), 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), 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 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)	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 UDP 111 2049	iDRAC Installations

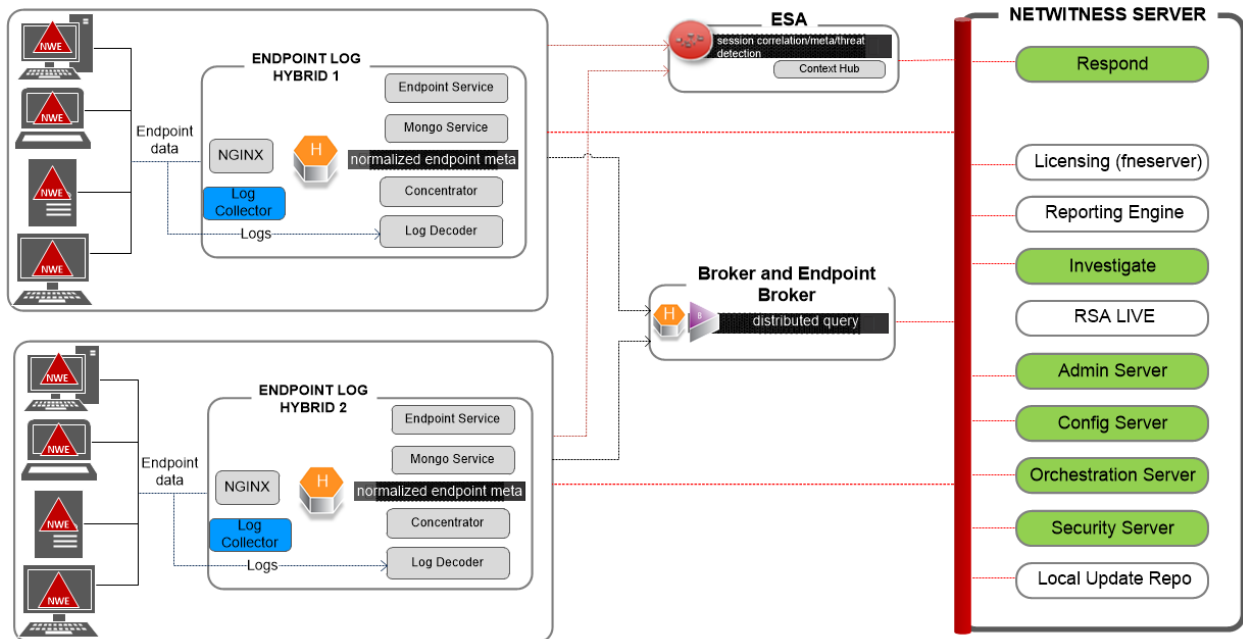
Network Hybrid Host

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)	Network Decoder Application Ports
NW Server	Network Hybrid	TCP 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 UDP 111 2049	iDRAC Installations

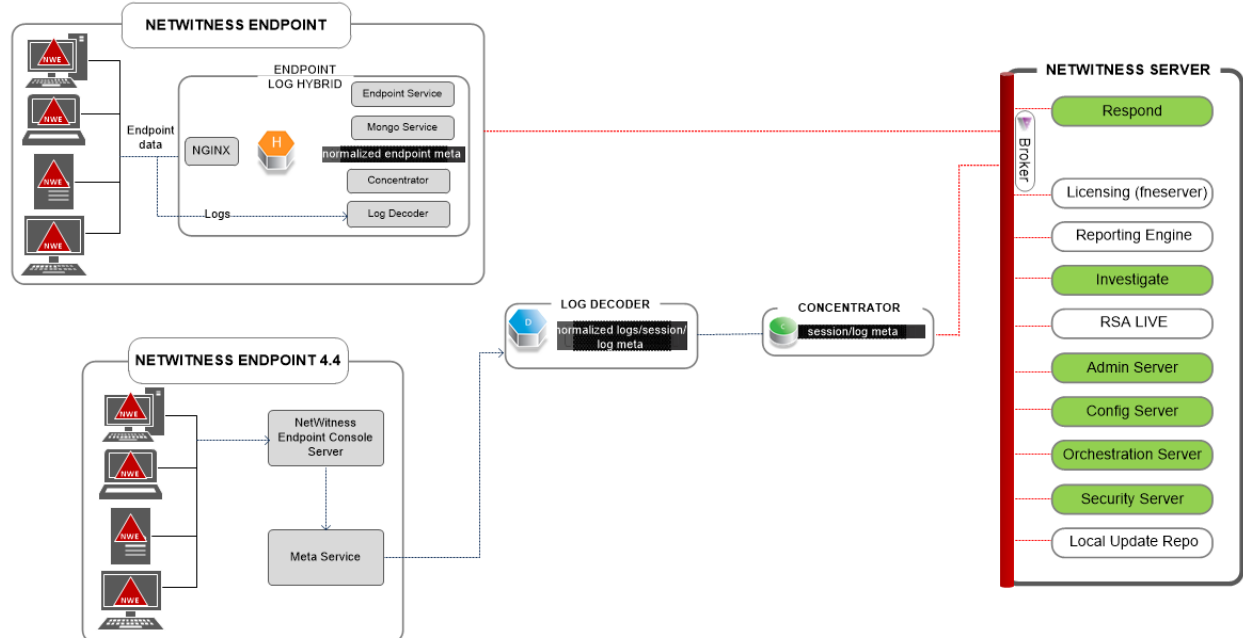
UEBA Host

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
UEBA Server	NW Server	15671	UEBA Alerts forwarding to Respond
NW Server	NFS Server	TCP 111, 2049 UDP 111, 2049	iDRAC Installations

NetWitness Endpoint Architecture



NetWitness Endpoint 4.4 Integration with NetWitness Platform



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 >
```

```
NiranjanEPS1.rsa.lab.emc.com.dsrf: UDP, length 20
```

```
09:20:12.572433 IP NiranjanEPS1.rsa.lab.emc.com.dsrf >
```

```
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.