



Deployment Guide

for RSA NetWitness® Platform 11.5



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

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

June 2021

Contents

- The Basics 6**
 - Basic Deployment 7
 - Process 7
 - NetWitness Platform High-Level Deployment Diagrams 8
- Deployment Optional Setup Procedures 9**
 - Analyst User Interface 9
 - Features and Limitations 9
 - Use Case 10
 - Deployment 10
 - Group Aggregation 12
 - RSA Group Aggregation Deployment Recommendations 12
 - Advantages of Using Group Aggregation 12
 - Configure Group Aggregation 14
 - Prerequisites 14
 - Set up Group Aggregation 15
 - New Health and Wellness 18
 - Hybrid Categories on Series 6 (R640) Hardware 21
 - NW Server Deployment on ESA Hardware 21
 - Second Endpoint Server 22
 - Warm Standby NW Server Host 23
 - Procedures 23
 - Planned Fail-Over Scenario 24
 - Required Fail-Over Scenario without Hardware Replacement 24
 - Required Fail-Over Scenario with Hardware Replacement 24
 - Set Up Secondary NW Server in Standby Role 25
 - 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
 - SSO 41
 - Reporting Engine 42
 - UCF 43
 - PAM 43
 - ECAT 43
 - RSA NetWitness Orchestrator (By Demisto) 46
 - Audit Logging 47
 - Health and Wellness 47
 - Malware Analysis 47

| | |
|---|-----------|
| Windows Legacy Collection | 48 |
| Fail Back Secondary NW Server to Primary NW Server | 49 |
| Network Architecture and Ports | 50 |
| NetWitness Platform Network Architecture Diagram | 50 |
| NetWitness Network (Packets) Architecture Diagram with Ports | 51 |
| NetWitness Logs Architecture Diagram with Ports | 52 |
| Event Stream Analysis Network (Packets) Architecture Diagram with Ports | 53 |
| Event Stream Analysis (Logs) Architecture Diagram with Ports | 54 |
| NetWitness Platform Firewall Requirements Summary | 55 |
| Comprehensive List of NetWitness Platform Host, Service, and iDRAC Ports | 59 |
| NW Server Host (Primary and Warm Standby NW Server Host) | 60 |
| Analyst UI Host | 61 |
| Archiver Host | 62 |
| Broker Host | 63 |
| Concentrator Host | 64 |
| Endpoint Log Hybrid | 65 |
| Endpoint Relay Server | 66 |
| Event Stream Analysis (ESA) Host | 67 |
| New Health and Wellness | 68 |
| New Health and Wellness on Different Subnet | 68 |
| iDRAC Ports | 69 |
| Log Collector Host | 70 |
| Log Decoder Host | 71 |
| Log Hybrid Host | 72 |
| Log Hybrid - Retention Host | 74 |
| Malware Host | 75 |
| Network Decoder Host | 76 |
| Network Hybrid Host | 77 |
| UEBA Host | 78 |
| NetWitness Endpoint Architecture | 79 |
| NetWitness Endpoint 4.4 Integration with NetWitness Platform | 79 |
| NetWitness Endpoint Architecture with Ports | 80 |
| How to Change UDP Port for Endpoint Log Hybrid | 80 |
| Task 1 - Tell All Agents to Use a New UDP Port | 80 |
| Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment | 81 |
| Site Requirements and Safety | 83 |
| Intended Application Uses | 83 |
| Service | 83 |
| Safety Information | 83 |
| Site Selection | 83 |

| | |
|-------------------------------------|----|
| Equipment Handling Practices | 83 |
| Power and Electrical Warnings | 84 |
| Rack Mount Warnings | 84 |
| Cooling and Air Flow | 84 |

The Basics

This guide describes the basic requirements of a NetWitness Platform deployment and outlines optional scenarios to address the 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)
 - 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.
 - Google Cloud Platform (GCP)
See the *RSA NetWitness® Platform Google Cloud Platform Installation Guide* for detailed instructions on how to deploy virtual hosts in Google Cloud.

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*.
- For Google Cloud, follow the instructions in the *RSA NetWitness® Platform Google Cloud Platform 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*.

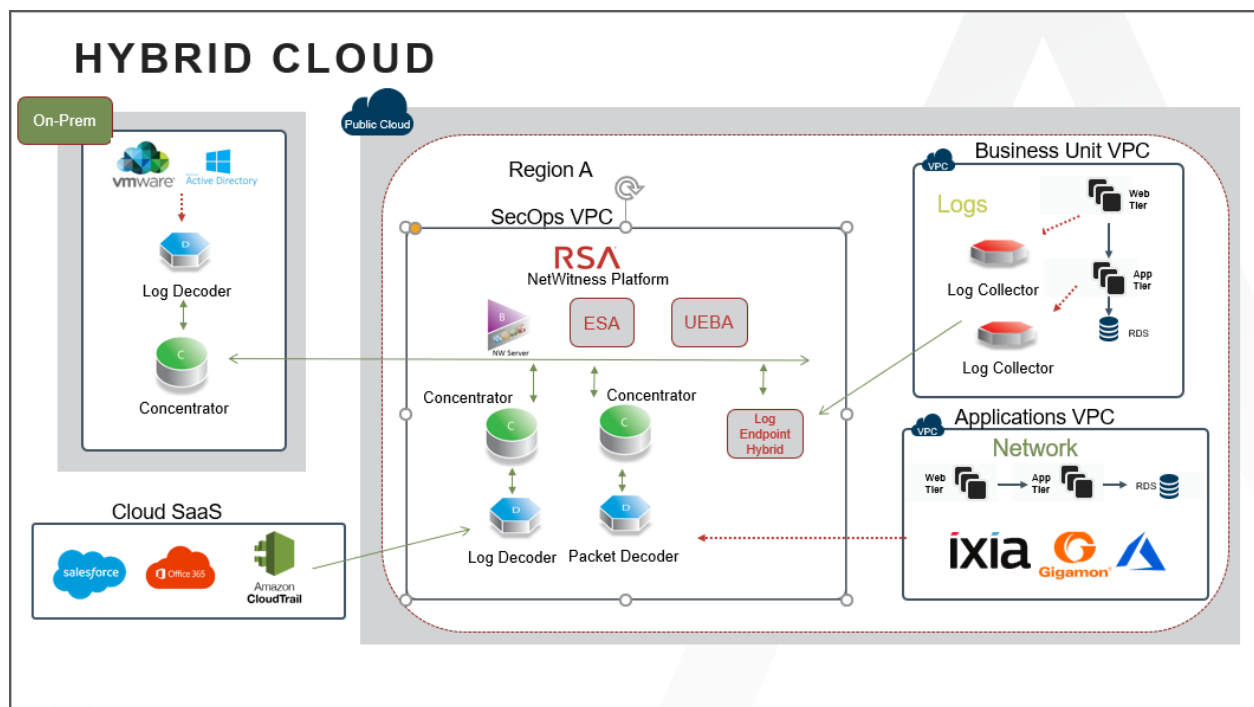
NetWitness Platform High-Level Deployment Diagrams

NetWitness Platform is inherently modular. Whether organizations are looking to deploy on-premise or in the cloud, the NetWitness components are decoupled in a way which allows flexible deployment architectures to satisfy a variety of use cases.

The following figure is an example of a hybrid cloud deployment, where the base of the components are residing within the SecOps VPC. Centralizing these components make management easier while keeping network latency to a minimum.

Network, log, and endpoint traffic could then be aggregated up to the SecOps VPC. The on-premise location would function just like a normal physical deployment and would be accessible for investigations and analytics.

Cloud SaaS visibility could be captured from a Log Decoder residing in either the cloud or on-premise locations.



Deployment Optional Setup Procedures

You can deploy NetWitness Platform with the following options.

[Analyst User Interface](#)

[Group Aggregation](#)

[New Health and Wellness Search](#)

[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 11.5 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.

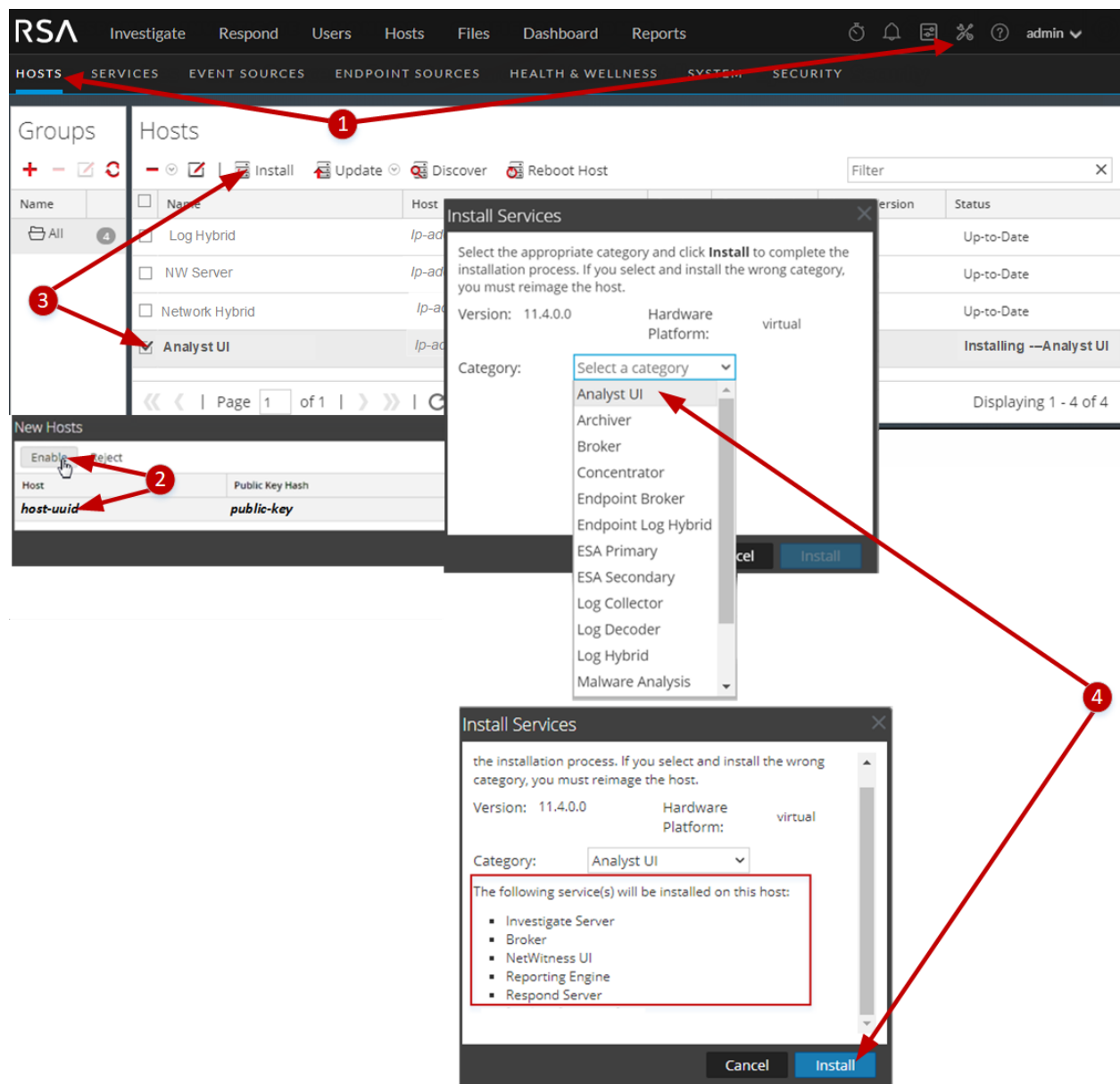
After you provision the Analyst UI host (that is after you run the nwsetup-tui for the component host designated for the Analyst UI), complete the following steps to install the Analyst UI service category on the provisioned host.

1. Log in to **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**.



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* 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* 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* 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

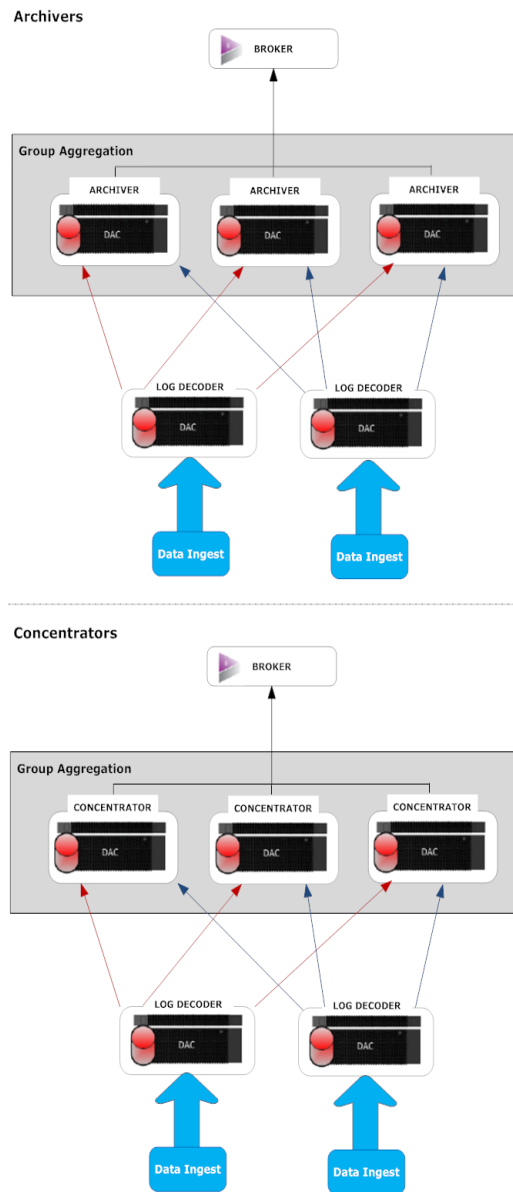
RSA recommends the following deployment for Group Aggregation:

- 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 sessions 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 10,000, the services would divide the session between themselves as illustrated in the following table.

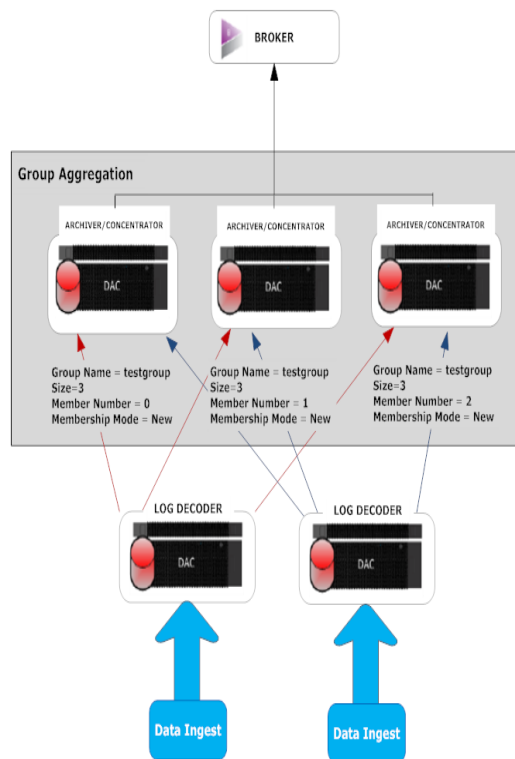
| Archiver 0 or Concentrator 0 | Archiver 1 or Concentrator 1 |
|------------------------------|------------------------------|
| 1 - 9,999 | 10,000 - 19,999 |
| 20,000 - 29,999 | 30,000 - 39,999 |
| 40,000 - 49,999 | 50,000 - 59,999 |

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.



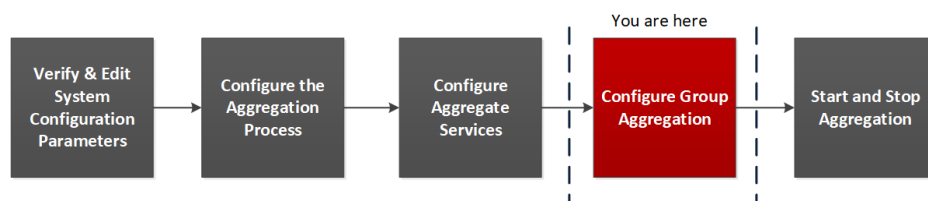
Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

| 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: The 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.

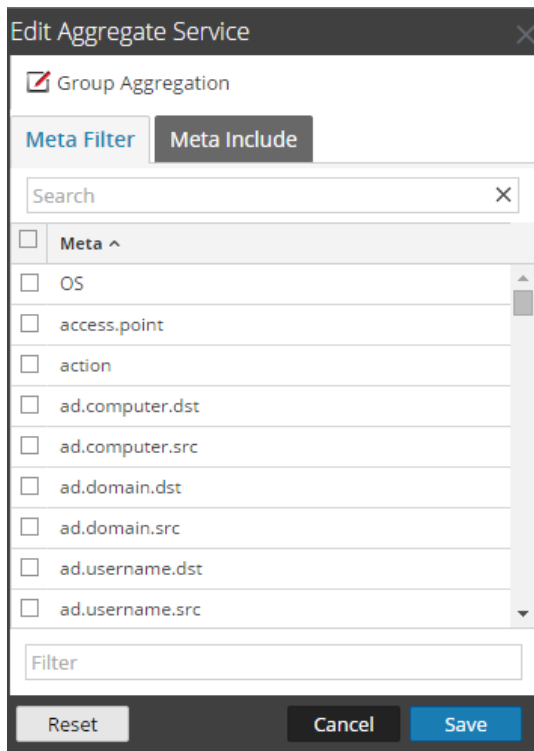


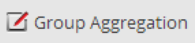
Complete the following steps to set up group aggregation.

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:

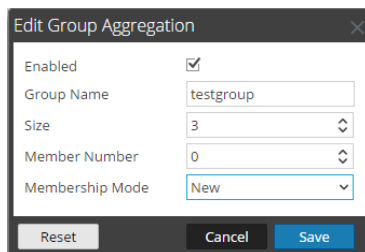
- a. Go to  (Admin) > Services.
- b. Select the Archiver or Concentrator service, and select  > View > Config.
The Service Config view of the Archiver or Concentrator is displayed.
- c. In the **Aggregate Services** section, select **Log Decoder**.
- d. Click  **Toggle Service** to change the status 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, 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 shows the RSA Archer interface for configuring a Concentrator service. The main area displays a table of 'Aggregate Services' with columns for Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. Two services are listed: 'decoder' (Port 50004, Rate 0, Max 11, Behind 0) and 'logdecoder' (Port 50002, Rate 0, Max 5814, Behind 0). Both are grouped and consuming.

Below the table is the 'System Configuration' section with a table of parameters:

| Name | Config Value |
|----------------------|--------------|
| Compression | 0 |
| Port | 50005 |
| SSL Port | 56005 |
| Stat Update Interval | 1000 |
| Threads | 20 |

On the right side, the 'Aggregation Configuration' panel is visible, showing a table of parameters:

| Name | Config Value |
|-------------------------------|-------------------------------------|
| Aggregation Settings | |
| Aggregate Autostart | <input checked="" type="checkbox"/> |
| Aggregate Hours | 0 |
| Aggregate Interval | 10 |
| Aggregate Max Sessions | 10000 |
| Service Heartbeat | |
| Heartbeat Error Restart | 300 |
| Heartbeat Next Attempt | 60 |
| Heartbeat No Response | 180 |

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

New Health and Wellness

New Health and Wellness is an advanced monitoring and alerting system that provides insights on the operational state of the host and services in your deployment, and helps identify potential issues.

System Requirements

The following tables list the memory, disk, and CPU recommended for the New Health and Wellness based on the size of the deployment.

Note: The recommended values might differ when you install and try the new features and enhancements.

Caution: If the New Health and Wellness node is on a different subnet, you must open the respective NetWitness Platform hosts port. For more information, see [New Health and Wellness on Different Subnet](#) section in the [Network Architecture and Ports](#).

Standalone Virtual Host

Minimum memory for a standalone virtual host is 16 GB.

Each NetWitness platform host writes 150 MB of New Health and Wellness metrics data into Elasticsearch data per day. For example, if you have 45 NetWitness Platform hosts then 6.6 GB of metrics data is written to Elasticsearch per day.

| CPU | Memory |
|---------|--------|
| 4 cores | 16 GB |

Physical Host

| Deployment Size | Memory | CPU | DISK per day |
|---|--------|-----|--------------|
| Small (~5-10 hosts / 20-40 services) | 16 GB | 15% | 1.5 GB |
| Medium (~150-200 hosts / 300- 400 services) | 18 GB | 15% | 29 GB |
| Large (~250-300 hosts / 500-600 services) | 22 GB | 15% | 44 GB |

Based on the resources available, you can deploy the 11.5 New Health and Wellness feature on any one of the following, listed in the order of preferred deployment method with most preferred first:


- Standalone virtual host (Most preferred recommendation to ensure no performance impact on any other functionality of deployed nodes)

- Physical host:
 - Broker
 - Admin Server
 - ESA

Installing New Health and Wellness enables all hosts in your deployment to start sending metrics to monitor New Health and Wellness. After you deploy New Health and Wellness, see the "Monitor New Health and Wellness" topic in the *System Maintenance Guide* for instructions on how to configure and use this feature.

Please direct any New Health and Wellness feedback to nw.health.wellness.feedback@rsa.com.



After you provision the New Health and Wellness host, complete the following steps to install the **New Health and Wellness** service category on the provisioned host.

1. Log in to NetWitness Platform and go to  (Admin) > **Hosts**.

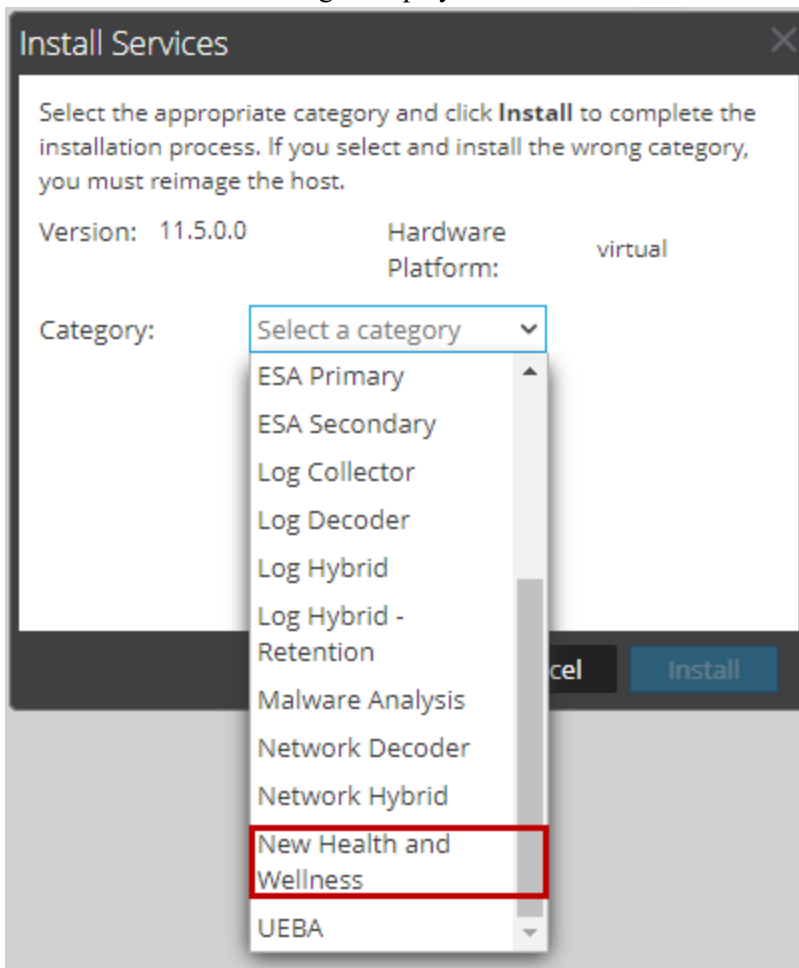
The **New Hosts** dialog is displayed with the **Hosts** view grayed out in the background.

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

Note: If you are not installing New Health and Wellness on a standalone virtual host ignore step 2.

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 on which New Health and Wellness should be installed in the **Hosts** view (for example, **New Health and Wellness**) and click  **Install** .

The **Install Services** dialog is displayed.



4. Select **New Health and Wellness** 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-key <Admin-serverIP>`

IMPORTANT: Make sure you wait for the above command to finish before you run the subsequent command.

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

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

Note: (For Standalone Virtual host only) 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*.

Note: After you have installed New Health and Wellness, for some reason, if you want to uninstall New Health and Wellness, you must refer to "Uninstall New Health and Wellness" in the *Upgrade 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 16 in "Install RSA NetWitness Platform" under "Installation Tasks" in the *Physical Host Installation Guide for NetWitness Platform 11.5*.
 - For a virtual host, complete steps 1 to 6 in "Step 4. Install RSA NetWitness Platform" in the *Virtual Host Installation Guide for NetWitness Platform 11.5*.

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

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 in to 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.

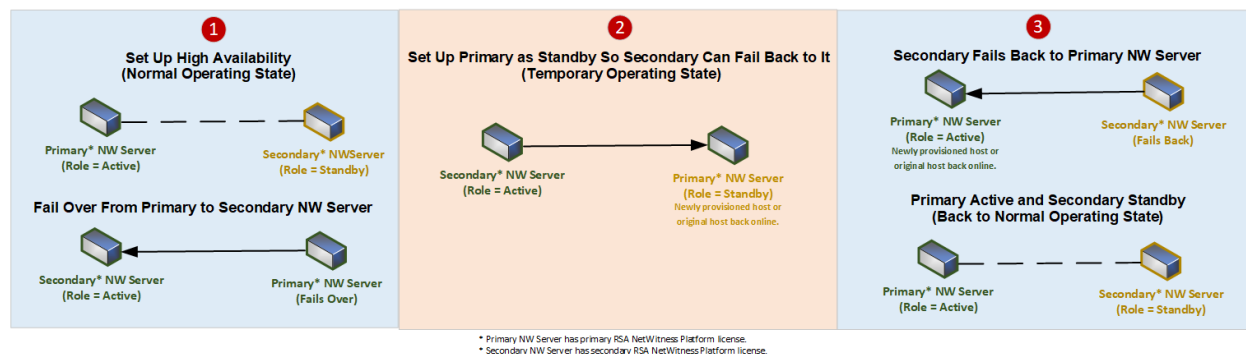
A secondary NW Server remains in the standby role and, when configured, receives backups of the primary NW Server in the active role at regular intervals. If the primary NW Server fails (goes offline), the fail-over procedure must be executed allowing the secondary NW Server to assume the active role.

In version 11.5 and later, we support a secondary NW Server that has a different IP address from the primary NW Server. Having the same IP address for both the primary NW Server and secondary NW Server is no longer necessary.

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.



Note: When you set up the secondary NW Server, follow the same administrative procedures, for example, for upgrade and maintenance, as the procedures for the primary active NW Server.

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

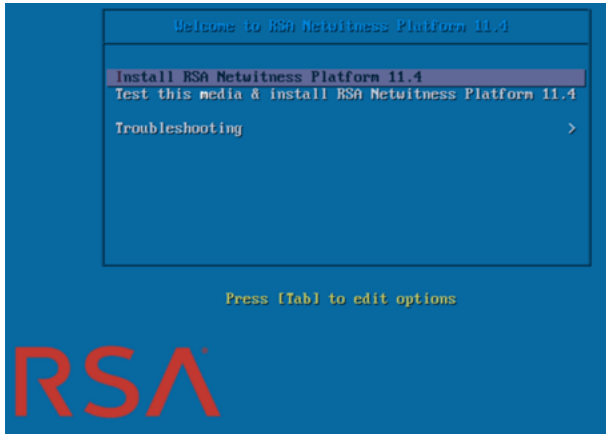
This scenario occurs when the active NW Server completely fails and the hardware requires replacement, for example you receive a Return Merchandise Authorization (RMA). You need to run reconfigure the host with the `nwsetup-tui` and contact Customer Support (<https://community.rsa.com/docs/DOC-1294>) 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:
 - a. The primary NW Server is running 11.5.
 - b. All component hosts are running 11.5
If you are:
 - Installing NetWitness Platform 11.5, follow the instructions in the *RSA NetWitness Platform Physical Host Installation Guide for Version 11.5*.
 - Updating from 11.x to 11.5, follow the instructions in *RSA NetWitness Platform Update Guide for Version 11.x to 11.5*.
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 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 11.5** installation menu is displayed. The menu graphics will render differently if you use a physical USB flash media.



- d. Select **Install RSA NetWitness Platform 11.5** (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
```

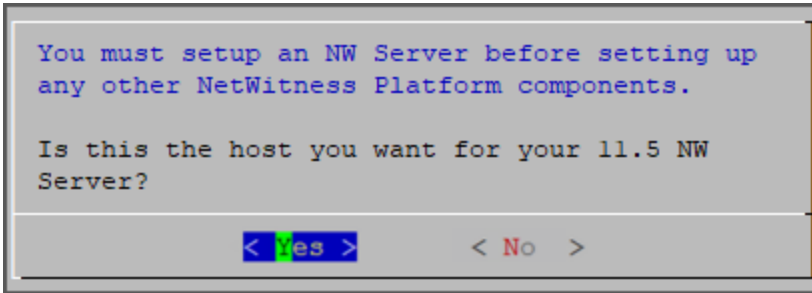
92%

<Accept >

<Decline>

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

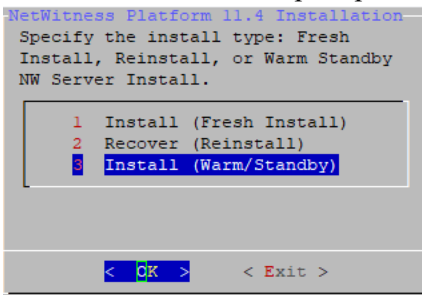
The **Is this the host you want for your 11.5 NW Server** prompt is displayed.



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).

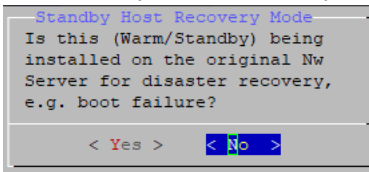
4. Tab to **Yes** and press **Enter**.

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



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

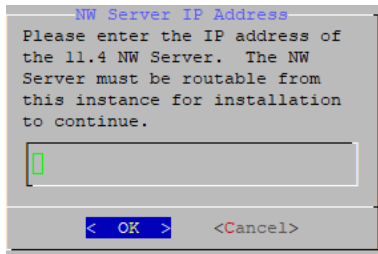
The **Standby Host Recovery Mode** prompt is displayed.



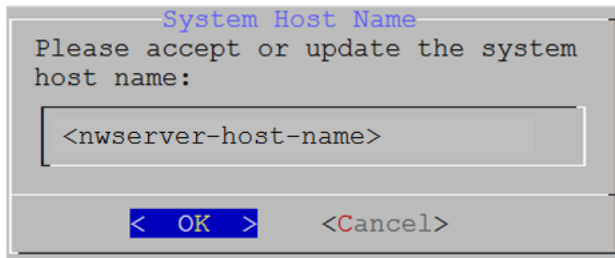
6. Tab to:

- **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.

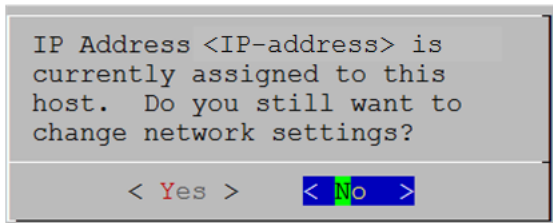
Password

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.

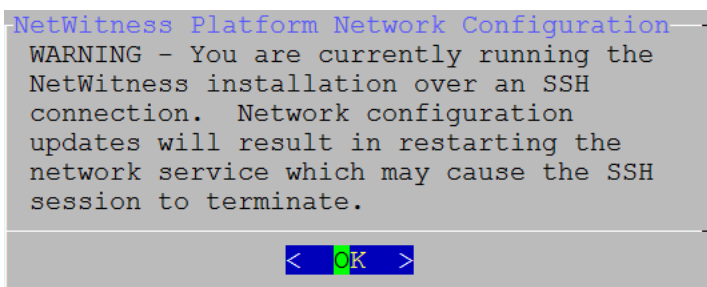
- If the Setup program finds a valid IP Address for this host, the following prompt is displayed.



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.

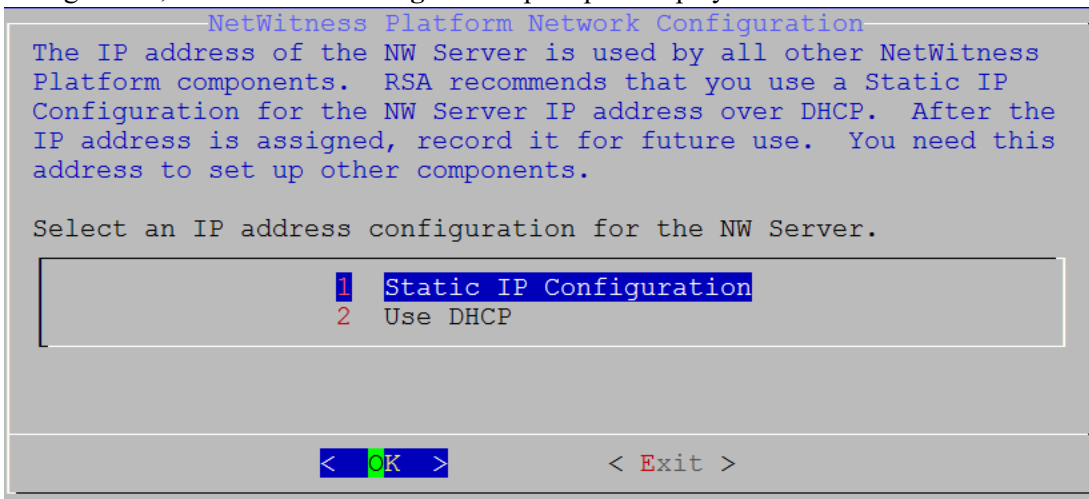
- If you are using an SSH connection, the following warning is displayed.

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

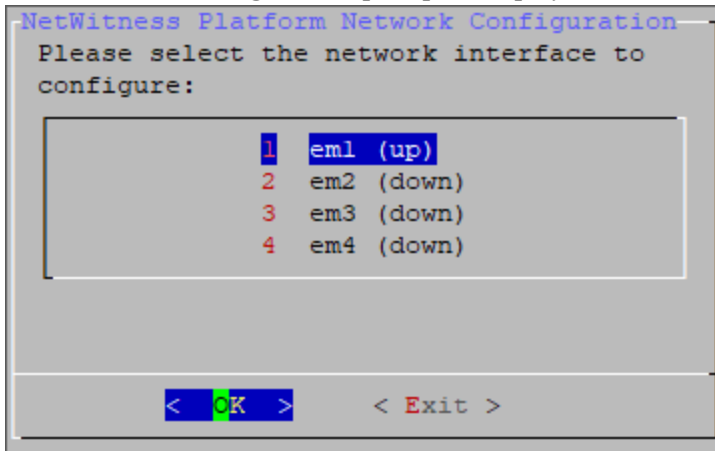


Press **Enter** to close warning prompt.

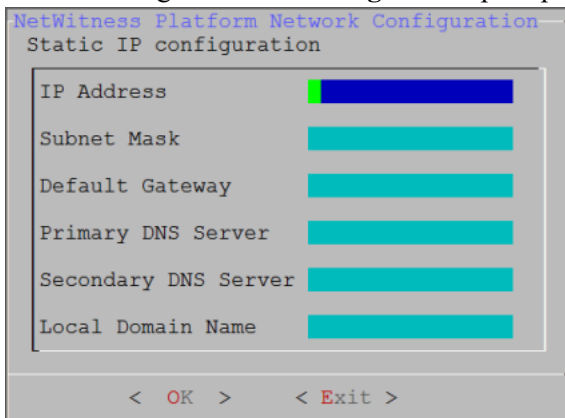
- If the Setup Program found an IP configuration and you chose to use it, the **Update Repository** prompt is displayed. Go to step 12 to and complete the installation.
- If the Setup Program did not find an IP configuration or if you chose to change the existing IP configuration, the **Network Configuration**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



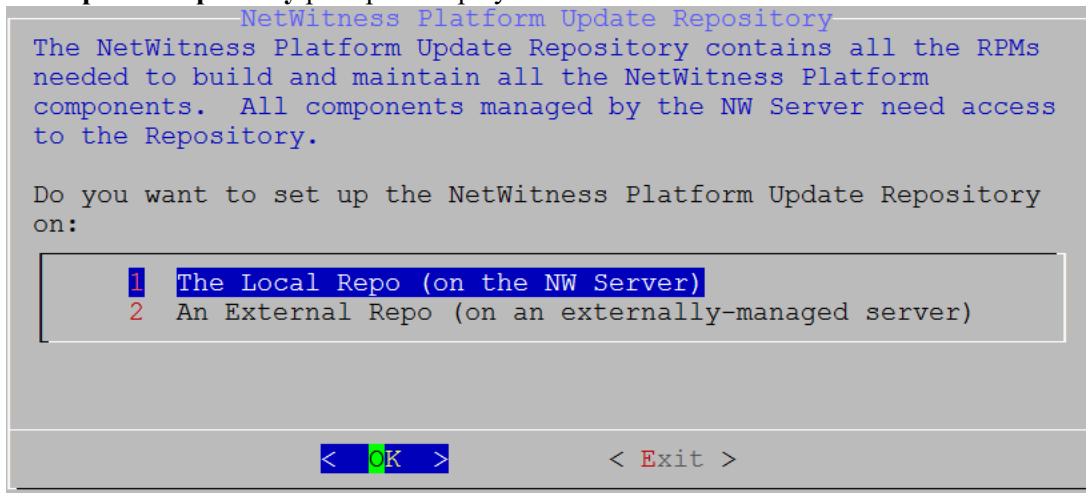
12. Down arrow to the network interface you want, tab to **OK**, and press **Enter**. If you do not want to continue, tab to **Exit**.
The following **Static IP Configuration** prompt is displayed.



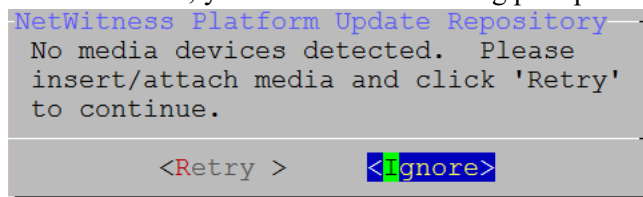
13. Type the configuration values (using the down arrow to move from field to field), tab to **OK**, and press **Enter**. If you do not complete all the required fields, an All fields are required error message is displayed (**secondary DNS Server** and **Local Domain Name** fields are not required).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

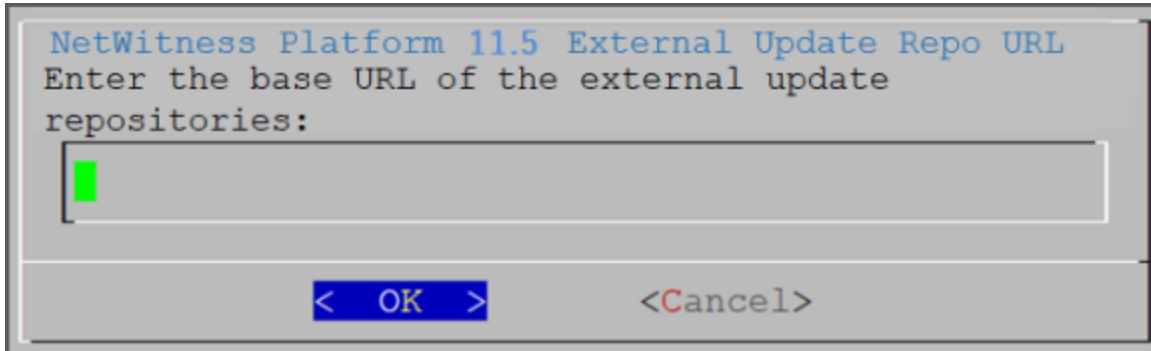
The **Update Repository** prompt is displayed.



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



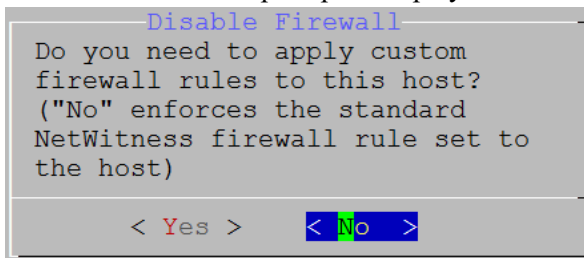
- If you select **2 An External Repo (on an externally-managed server)**, the UI prompts you for a URL. The repositories give you access to RSA updates and CentOS updates. Refer to "Appendix B. Create an External Repo" in the *Physical Host Installation Guide* for instructions on how to create this repo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

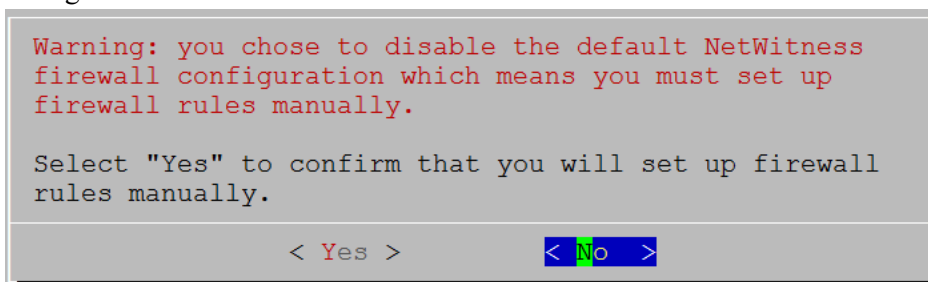
See "Set Up an External Repository with RSA and OS Updates" under "Hosts and Services Procedures" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for instructions. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

The Disable firewall prompt is displayed.

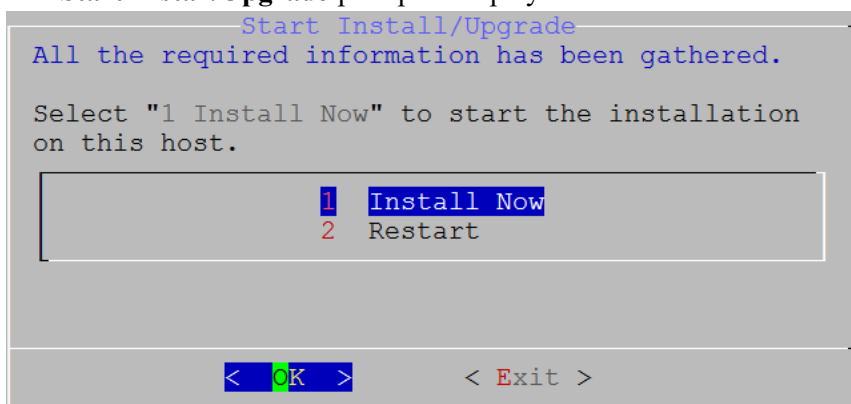


15. Tab to **No** (default), and press **Enter** to use the standard firewall configuration. Tab to **Yes**, and press **Enter** to disable the standard firewall configuration.

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 11.5 on the NW Server.

When **Installation complete** is displayed, you have installed the 11.5 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/flexnetlms/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>
```

Note: If the Warm Standby server becomes active, and if it will be accessed by any NW host with a NAT IP address, the NAT IP address must be added to the command:

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

| | |
|--|---|
| -h, --help | Display Help |
| -d, --daily | Schedule daily data synchronization |
| -w, --weekly | Schedule weekly data synchronization |
| -c, --custom <crontab formatted> | Schedule custom data synchronization i.e. to schedule for midnight on 1st and 10th of the month: '0 0 1,10 * *' |
| -i, --standby-ip <IP address> | (required) IP address of standby NW Server |
| -p, --standby-ip-public <NAT IP address> | (optional) NAT-based IP address of standby NW Server |
| -v, --verbose | 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.

IMPORTANT: If you have installed New Health & Wellness on Admin Server, perform the following:

- Install New Health & Wellness on Standby NW server.
- Back up the Search category (New Health and Wellness) from Primary NW server to standby NW server using the NRT:

```
nw-recovery-tool --export --dump-dir /root --category Search
```

You must manually copy files from Primary NW server to Standby NW server after running the above command.

2. Run the `nw-failover` script with the `--make-active` argument:


```
nw-failover --make-active
```
3. Complete the following steps for planned and required fail-over.
 - a. SSH to the primary NW Server.
 - b. Run the fail-over script with the `--make-standby` argument to assign the standby role to the primary NW Server:


```
nw-failover --make-standby
```
 - c. Shut down the primary 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 that you can fail back to it.

4. Validate that the component hosts have connected to the new active NW Server by running the following command on the new active NW Server:


```
nw-manage --check-hosts-status
```

Note: Do not continue to the next step until all component hosts have successfully connected to the new active NW Server. Rerun `nw-manage --check-hosts-status` as needed to continue verification.

5. Follow the IP address change procedures for the now-active NW Server in "Change Host Network Configuration" in the *System Maintenance Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

Note: If the primary NW Server is going to remain online, you must update its IP address so that it no longer conflicts with the Warm Standby NW Server IP address when it is changed. Follow the IP address change procedures for the now-active NW Server in "Change Host Network Configuration" in the *System Maintenance Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

6. Shut down the primary NW Server, or reboot the primary NW Server and set it up as the new secondary NW Server by completing the steps in [Set Up Secondary NW Server in Standby Role](#) for this host to create a new primary NW Server, so that you can fail back to this host.

IMPORTANT: After successful fail over to Standby NW server, restore the Search category (New Health & Wellness) using NRT:

```
nw-recovery-tool --import --dump-directory <Backup_directory_path> --  
category Search
```

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

If your secondary NW Server will maintain a different IP address from your primary NW Server after a fail-over event, for example, if the secondary NW Server is located in a different data center 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.

IMPORTANT: If you have installed New Health & Wellness on Admin Server, perform the following:

- Install New Health & Wellness on Standby NW server.
- Back up the Search category (New Health and Wellness) from Primary NW server to standby NW server using the NRT:

```
nw-recovery-tool --export --dump-directory <Backup_directory_path> --  
category Search
```

You must manually copy files from Primary NW server to Standby NW server after running the above command.

2. Run the failover script:

```
nw-failover --make-active
```
3. Complete the following steps for planned and required fail-over.
 - a. SSH to the primary NW Server.
 - b. Run the fail-over script with the `--make-standby` argument to assign the standby role to the primary NW Server:

```
nw-failover --make-standby
```
 - c. Shut down the primary 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 that you can fail back to it.

- If you are running in a mixed-version environment, log in to each component host that is still on a version prior to 11.5 and execute the following:

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

Note: If you have a component host that uses a NAT IP address to reach the NW Server, substitute the <NAT-IP-address> for the <active-nw-server-ip-address> in both bullet items above.

- Shut down the primary NW Server, or reboot the primary NW Server and set it up as the new secondary NW Server by completing the steps in [Set Up Secondary NW Server in Standby Role](#) for this host to create a new primary NW Server, so that you can fail back to this host.

IMPORTANT: After successful fail over to Standby NW server, restore the Search category (New Health & Wellness) using NRT:

```
nw-recovery-tool --import --dump-directory <Backup_directory_path> --category Search
```

Note: If the secondary NW Server had any custom certificates, you must re-apply them after failover. For information about how to re-apply custom certificates, see "(Optional) Use a Custom Server Certificate" in the *System Security and User Management Guide*. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

Note: After upgrading the NW Server host or a component host to 11.5, review the contents of the `/etc/hosts.user` file for any obsolete host entries. The `/etc/hosts.user` file contains system and user-generated entries that are not managed by NetWitness Platform. However, entries from `/etc/hosts.user` are merged with NetWitness Platform-generated host mappings to create and update `/etc/hosts`. To avoid conflicts with NetWitness Platform-generated mappings, and to avoid generating connectivity errors resulting from an IP address change, RSA recommends that you remove any entries in `/etc/hosts.user` that include a non-loopback IP address of a NetWitness Platform host. After updating `/etc/hosts.user`, you must refresh the system by running the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

Follow the steps in the sections that apply to your environment.

- [SSO](#)
- [Reporting Engine](#)
- [UCF](#)
- [PAM](#)
- [ECAT](#)
- [RSA NetWitness Orchestrator \(By Demisto\)](#)
- [Audit Logging](#)

- [Health and Wellness](#)
- [Malware Analysis](#)
- [Windows Legacy Collection](#)

SSO

Update Configuration for Single Sign-On

Note: You must disable SSO configurations ONLY when NW Server IP is changed.

When the host network is configured with a new IP address, the SSO configurations also must be updated.

To do this:

1. Disable the SSO configuration using `nw-shell` after failover from new IP.
To resolve this issue you must disable SSO manually, using the following commands:
 - a. SSH to admin server node.
 - b. Connect to `nw-shell`.
 - c. Connect to admin server service using the `connect --service admin-server` command.
 - d. Log in to admin server using the `login` command.
 - e. Enter the admin username and password.
 - f. Execute the following commands:
 - `cd /rsa/security/authentication/web/saml/sso-enabled`
 - `set false`
 - `logout`
 - `exit`

- `systemctl restart rsa-nw-admin-server`

```

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

```

2. Change the host IP address to the new IP.
3. 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.

For more information, see the "Troubleshooting" topic in the *System Security and User Management Guide*.


Reporting Engine

Update Configuration for Reporting Engine

Note: You must update the Reporting Engine configurations ONLY when NW Server IP is changed.

When the host network is configured with a new IP address, you must update and verify the Reporting Engine configurations. The hostname for NetWitness Platform configurations under the Output Actions must be updated with the new IP.

To manually configure the new IP, perform the following steps:

1. Log in to NetWitness Platform.
2. Navigate 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**.

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

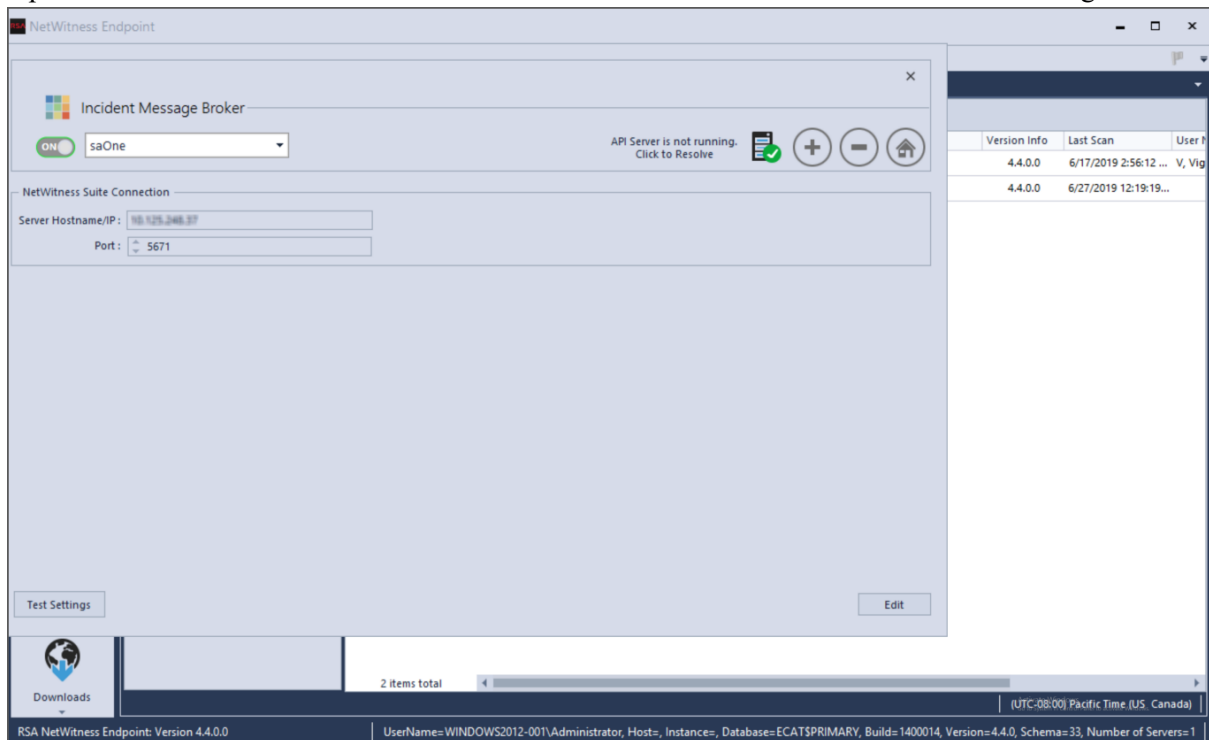
Update the following services:

- [Incident Message Broker](#)
- [NetWitness Suite](#)
- [Syslog Server Settings](#)

Incident Message Broker

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

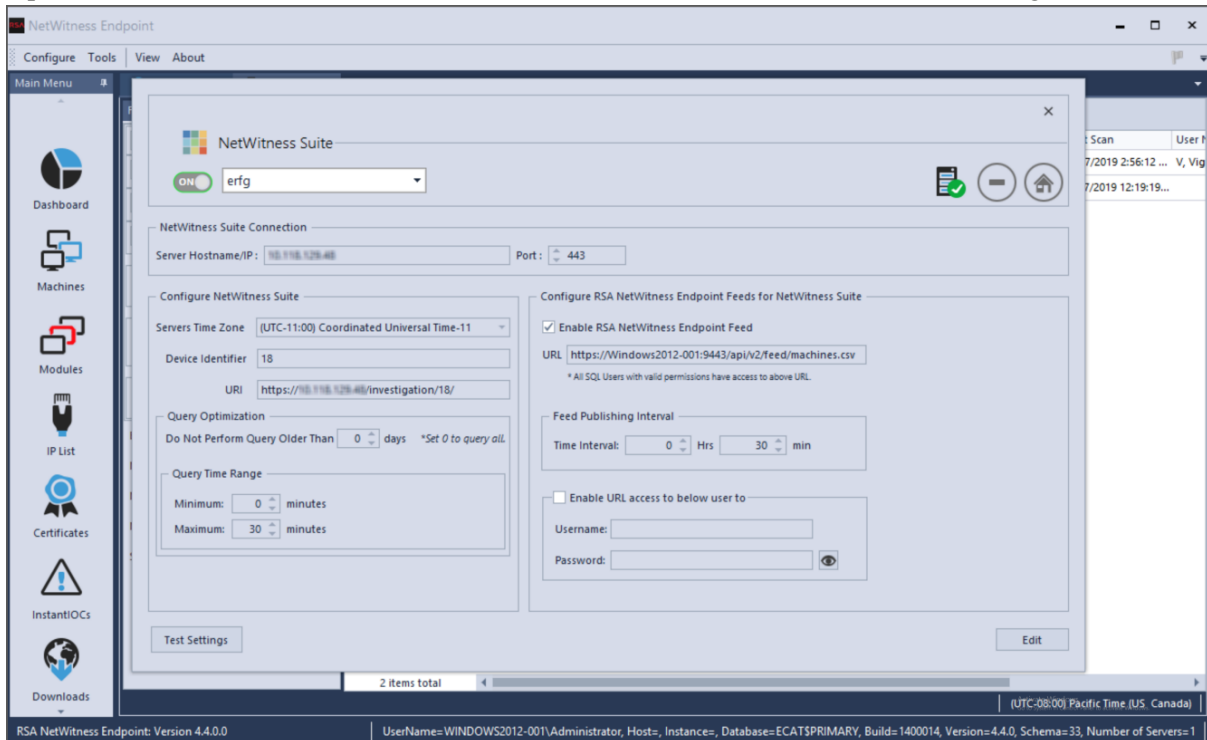
2. Update the server Hostname and IP Address to the current active server and test the settings.



NetWitness Suite

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

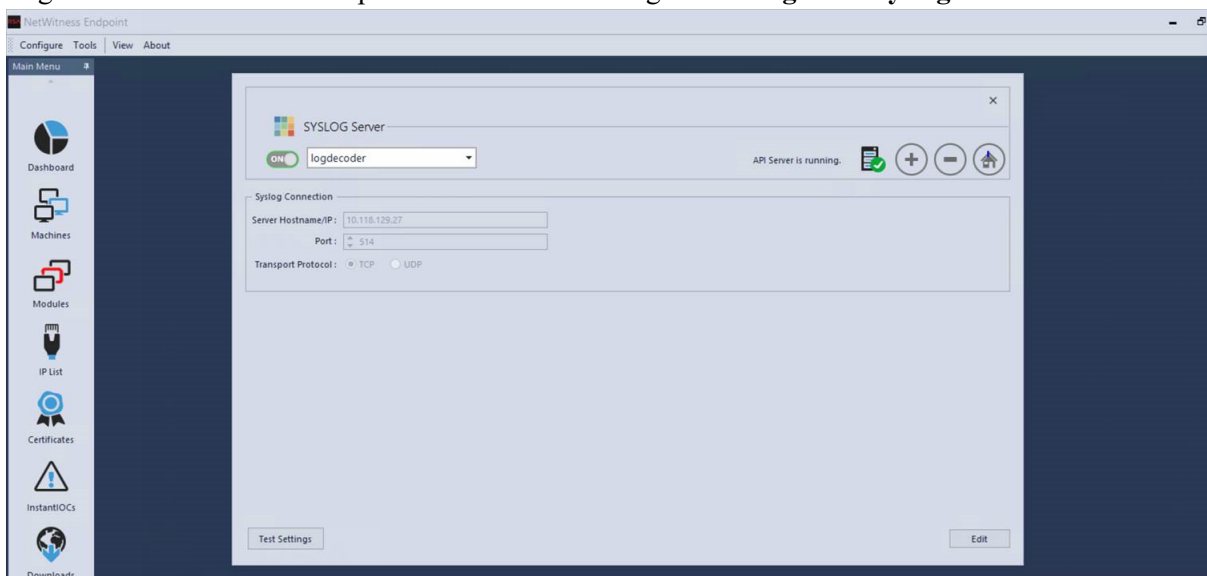
- Update the server Hostname and IP address to the current active server and test settings.



Syslog Server Settings

If you are forwarding syslog messages to a NetWitness Platform Log Decoder, update the syslog server settings to point to the new IP address of the Log Decoder host.

- Log in to the NetWitness Endpoint user interface and go to **Configure > Syslog Server**.

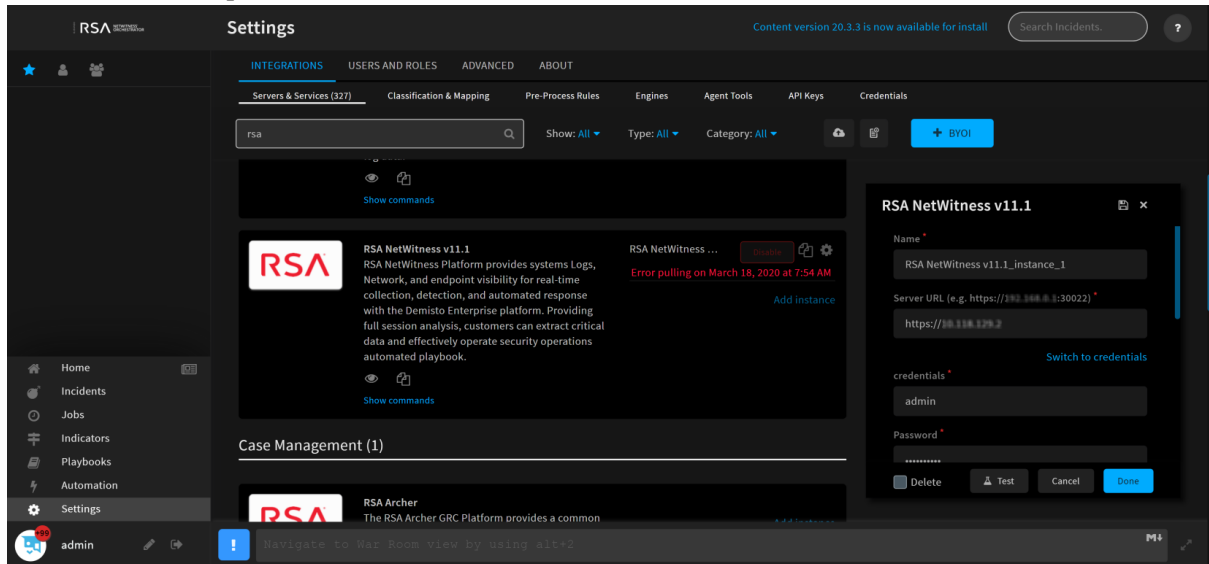


- Select **logdecoder**, and in **Server Hostname/IP**, enter the new IP address of the Log Decoder host.

RSA NetWitness Orchestrator (By Demisto)

Update the Current Active NW Server to Fetch Respond Incidents and Alerts

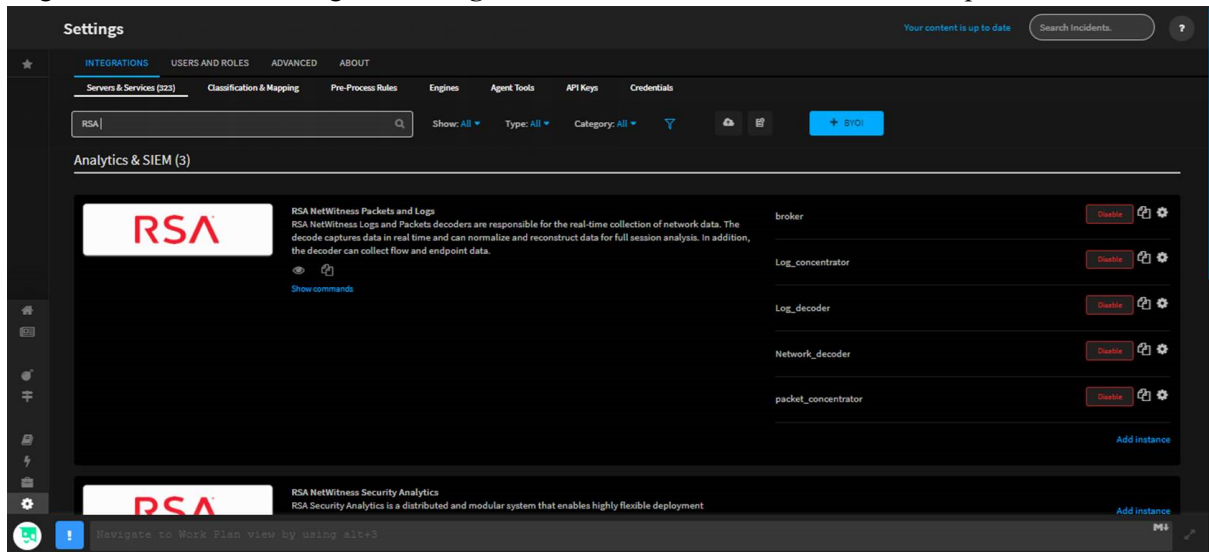
1. Log in to Orchestrator and go to **Settings** > **server&services**.
2. Edit the RSA NetWitness V11.1 instance by updating the server URL to the current active NW Server to fetch respond incidents and alerts.



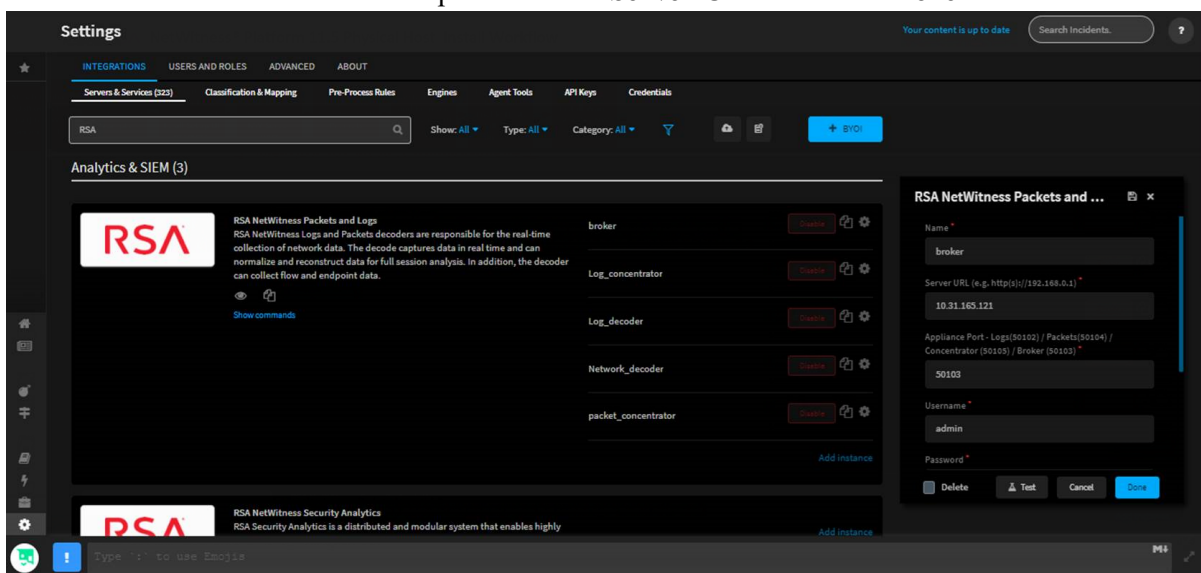
Update Component Hosts Acting as Data Sources

If you change the IP address of a component host, for example, a Concentrator, Network or Log Decoder, or Broker, that is acting as data source to the Orchestrator, update the following settings to point to the new IP address of the host.

1. Log in to Orchestrator and go to **Settings** > **server&services** and select the component host.



2. Enter the new IP address of the component host in **Server URL** and click **Done**.



Audit Logging

If you have changed the IP address of the NW Server, you must reconfigure audit logging. For instructions, see "Configure Global Audit Logging" in the *System Configuration Guide*.

Health and Wellness

If you have any Health and Wellness rules that contain IP addresses that have been changed, you must update those rules with the new IP addresses. For information about managing Health and Wellness rules, see "Monitor Health and Wellness using NetWitness Platform UI" in the *System Maintenance Guide*.

Malware Analysis

Source host IP address changes are not updated in the NetWitness Platform user interface for Malware Analysis continuous scan configurations. You must manually update this configuration in the Malware Analysis Config view > **General** > **Continuous Scan Configuration** and update the source host IP address to the new host IP address.

The screenshot shows the configuration interface for Malware Analytics. It is divided into several sections:

- Continuous Scan Configuration:** A table with columns 'Name' and 'Config Value'. The 'Source Host' row is highlighted with a red border and contains the value '172.16.0.0'. Other rows include 'Enabled', 'Query', 'Query Expiry', 'Query Interval', 'Meta Limit', 'Time Boundary', 'Source Port (NwPort)', 'Username', 'User Password', 'SSL', and 'Denial of Service (DOS) Prevention'.
- Repository Configuration:** A table with columns 'Name' and 'Config Value'. Rows include 'Directory Path', 'File Sharing Protocol', and 'Retention (in days)'.
- Miscellaneous:** A table with columns 'Name' and 'Config Value'. The 'Maximum File Size (MB)' row is visible.
- Modules Configuration:** A table with columns 'Name' and 'Config Value'. It is organized into sections:
 - Static:** Includes 'Enabled', 'Bypass PDF', 'Bypass Office', 'Bypass Executable', and 'Validate Windows PE Authenticate Settings ...'.
 - Community:** Includes 'Enabled', 'Bypass PDF', 'Bypass Office', and 'Bypass Executable'.
 - Sandbox:** Includes 'Enabled', 'Bypass PDF', 'Bypass Office', 'Bypass Executable', and 'Preserve Original File Name when Performin...'. Below this is a sub-section for 'GFI Sandbox (Local)' with 'Enabled', 'Server Name' (localhost), and 'Server Port' (80).

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

Windows Legacy Collection

On occasion, you may need to change the IP address of your Windows Legacy Collector. You may also need to edit any Destination Groups that you have configured.

Change WLC IP Address

The following procedure describes how to change the IP address for your system.

1. Log onto the Windows Legacy Collector system and manually change the IP address on the system.
2. In the UI, confirm that the Log Collector service corresponding to the WLC system shows up in error (Red). It might take some time for it to reflect the changed status.
3. On the NetWitness Server, use the **nw-manage** utility to view the host information for the WLC using the following command:

```
nw-manage --list-hosts
```

Sample output from running the command is shown here:

```
{
  "id" : "fdb8150c-e040-459e-8cc5-3c60ec2c65ae",
  "displayName" : "WLC-HOST-104",
  "hostname" : "10.101.216.102",
  "ipv4" : "10.101.216.102",
  "ipv4Public" : null
} ]
```

You use the value of **"id"** from your output in the following step.

4. Use the **nw-manage** utility to change the IP address of the WLC. For the **host-id** argument, use the value for the **"id"** that you noted from step 3. For the **ipv4** value, use the new IP Address to which you are changing.

```
nw-manage --update-host --host-id "fdb8150c-e040-459e-8cc5-3c60ec2c65ae" --  
ipv4 10.101.216.105
```

5. After you see the message that the previous command ran successfully, go to the NetWitness Server UI and verify that the WLC service is running without any errors.

Edit Destination Groups For Log Collectors and VLCs

The Windows Legacy Collector is often configured with Destination Groups to forward events to Log Collectors or Virtual Log Collectors. If the IP address of any such Destination LC or VLC is changed, the Windows Legacy Collector can no longer forward events. To remediate this, you must edit the Destination groups for the WLC, making sure to select the new LC or VLC IP Address.

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

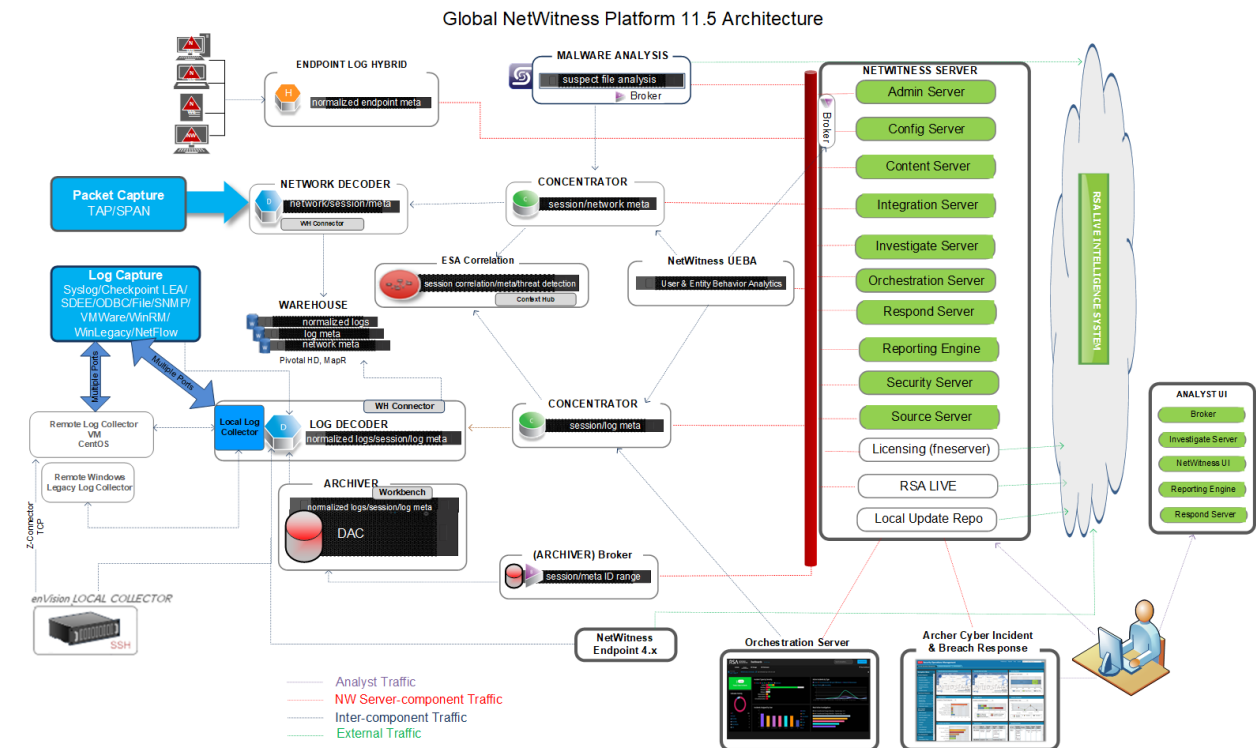
Refer to the following diagrams and port tables to ensure that all the relevant ports are opened for components in your NetWitness Platform deployment to communicate with each other.

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.

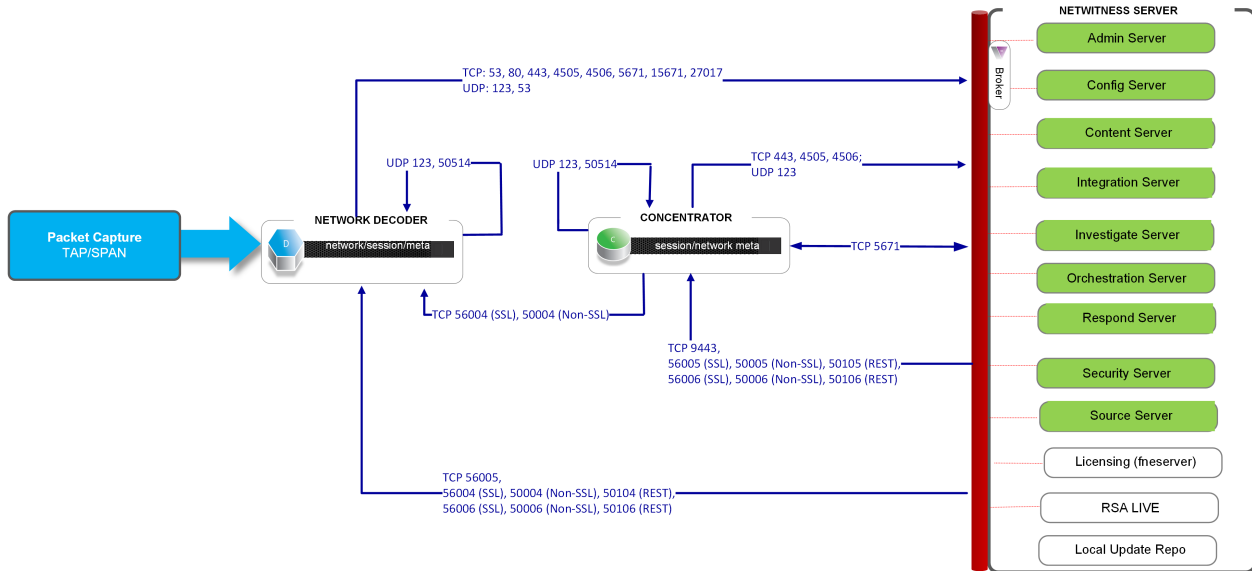


Note:
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server.
 The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).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



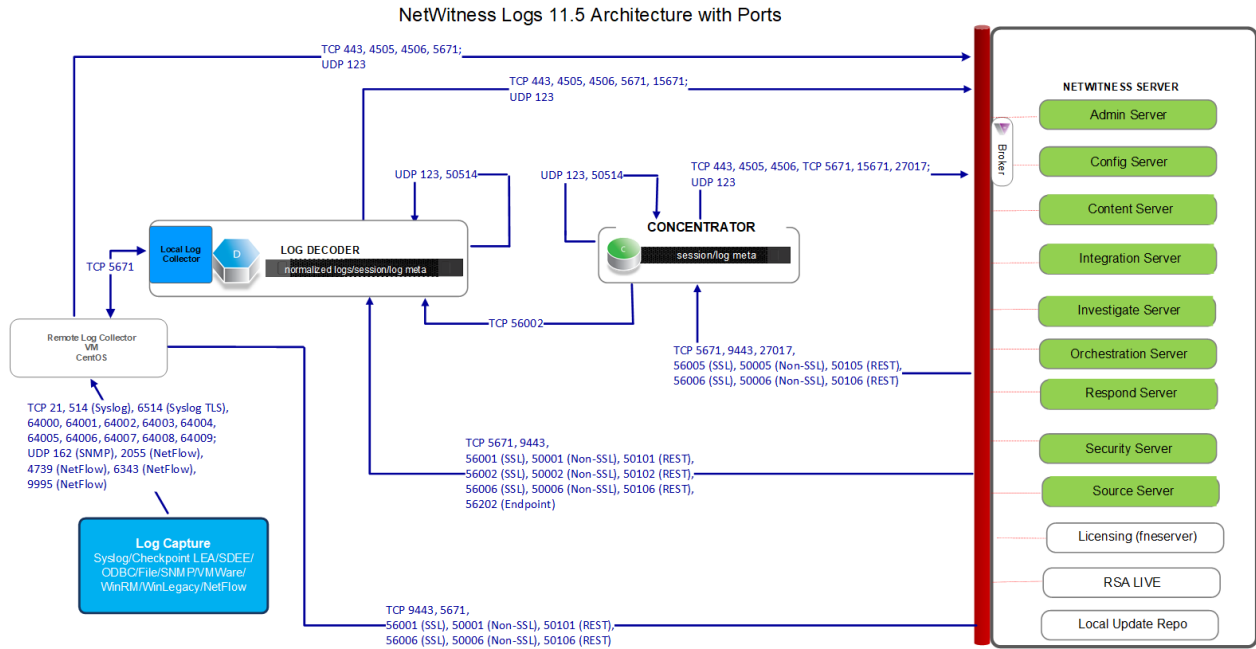
NetWitness Network (Packets) Architecture Diagram with Ports

NetWitness Network 11.5 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).

NetWitness Logs Architecture Diagram with Ports

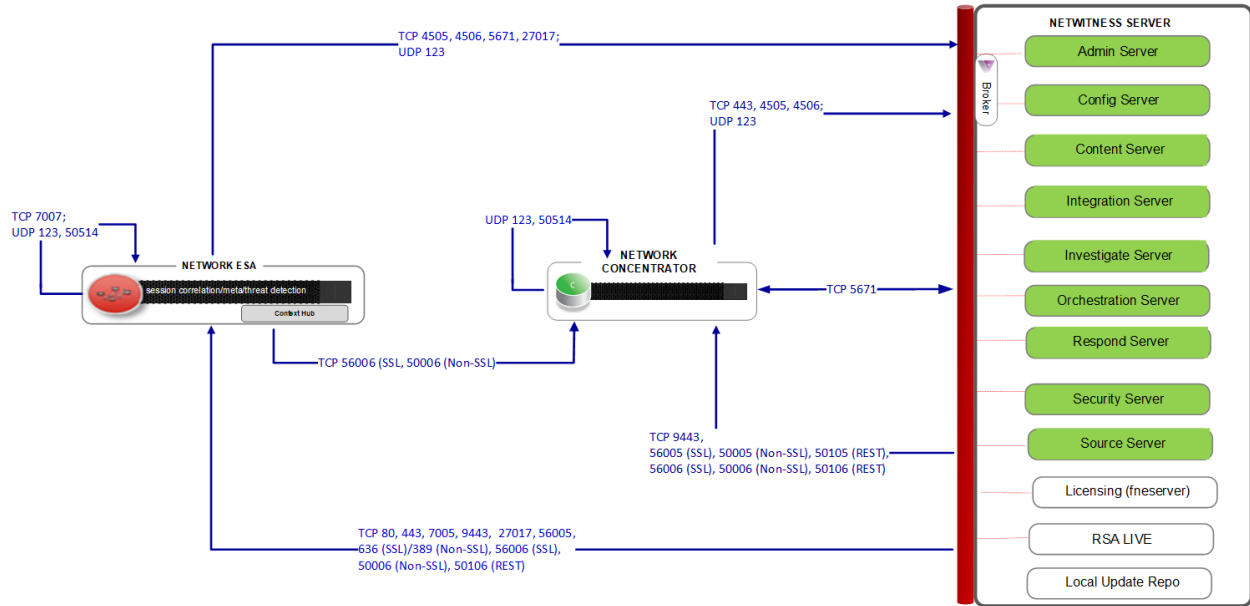


Note: Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

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

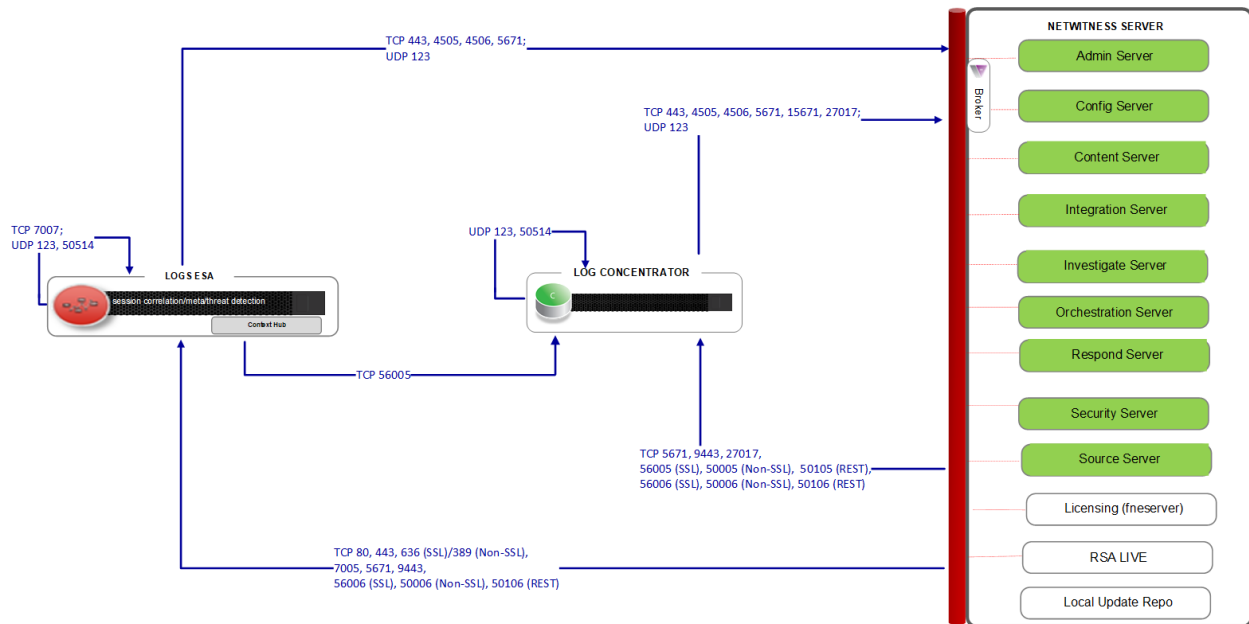


Notes:
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates). 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 | TCP: 22, 80, 443, 5671, 7005 UDP: 123 |
| NW Server | ESA | TCP: 22, 80, 443, 5671 UDP: 123 |
| NW Server | Network Decoder | TCP: 22, 5671, 50004 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50106 (REST), 56004 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Broker | TCP: 5671, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST) 56003 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Concentrator (Network & Logs) | TCP: 22, 5671, 50005 (Non-SSL), 50006 (Non-SSL), 50105 (REST), 50106 (REST), 56005 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Network Hybrid | TCP: 22, 5671, 50004 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50105 (REST), 50106 (REST), 56004 (SSL), 56005 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Log Decoder | TCP: 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Log Hybrid | TCP: 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) UDP: 123 |

| Source Host | Destination Host | Ports |
|-------------------------------------|------------------------|---|
| NW Server | Log Hybrid - Retention | TCP: 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) UDP: 123 |
| NW Server | Endpoint Log Hybrid | TCP: 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) UDP: 123 |
| NW Server | VLC | TCP: 22, 5671, 50001 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50106 (REST), 56001 (SSL), 56006 (SSL) UDP: 123 |
| NW Server | Archiver | TCP: 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) UDP: 123, 514 |
| NW Server | Malware | TCP: 22, 5671, 5432, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST), 56003 (SSL), 56006 (SSL), 60007 UDP: 123 |
| NW Server | UEBA | TCP: 22, 15671, 5671, 443 UDP: 123 |
| ESA | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 123, 53 |
| ESA | Active Directory | TCP: 389 (Non-SSL), 636 (SSL) |
| ESA | Archer | TCP: 80 (Non-SSL), 443 (SSL), |
| ESA Primary or Secondary | Concentrator | TCP: 50005 (Non-SSL), 56005 (SSL) |
| Network Decoder | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017, UDP: 53, 123 |
| Concentrator (Network & Logs) | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 53, 123 |

| Source Host | Destination Host | Ports |
|------------------------|---|---|
| Network Hybrid | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 53, 123 |
| Log Decoder | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 53, 123 |
| Log Hybrid | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123 |
| Log Hybrid - Retention | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123 |
| VLC | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123 |
| VLC | Log Collector | TCP: 5671 |
| Log Collector | VLC | TCP: 5671 |
| Endpoint Log Hybrid | NW Server | TCP: 53, 80, 443, 5671, 4505, 4506, 15671, 27017 UDP: 53, 123 |
| Endpoint Log Hybrid | Log Decoder | TCP: 50202 (Non-SSL), 50102 (REST), 56202 (SSL) UDP: 514 |
| Endpoint Agent | Log Decoder | TCP: 514, 6514 UDP: 514 |
| Endpoint Agent | Endpoint Log Hybrid | TCP: 443 UDP: 444 |
| UEBA | NW Server | TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 50003 (Broker-Non-SSL), 50103 (Broker/REST), 56003 (Broker/SSL) UDP: 53, 123 |
| UEBA | Concentrator | TCP: 50005 (Non-SSL), 50105 (REST), 56005 (SSL) |
| www connections | | |
| NW Server | cloud.netwitness.com cms.netwitness.com download.rsasecurity.com panacea.threatgrid.com quantum.subscribenet.com rsasecurity.subscribenet.com smcupdate.emc.com | TCP: 80, 443 |

| Source Host | Destination Host | Ports |
|---------------------------------|--|--------------|
| ESA (Primary & Secondary) | cms.netwitness.com smcupdate.emc.com | TCP: 80, 443 |
| Malware | panacea.threatgrid.com cloud.netwitness.com | TCP: 443 |

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

Note: For ports used in event collection through the NetWitness Logs, see the *Log Collection Configuration Guide for RSA NetWitness Platform*. 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 |
| New Health & Wellness | UEBA Host |

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

Note: Primary or Secondary Server is a type of appliance, while Active or Standby refers to an appliance's state, whether active or standby.

| 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 Primary to Standby NW Server synchronization port. |
| Admin Workstation | NW Server | TCP 22 | SSH Active to Standby NW Server synchronization port. |
| 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 |
| NW Server | Active Directory | TCP 3268, TLS 3269 | For NW User Authentication |

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 | Log Decoder | TCP 50002 (Non-SSL), 56002 (SSL) | Log Decoder Application Ports |
| 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 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 | Archiver | TCP 50008 (Non-SSL), 56008 (SSL) | Archiver Application Ports |
| 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) | 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 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 |
| NW Server | Endpoint Log Hybrid | TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST) | Log Collector application ports |
| NW Server | Endpoint Log Hybrid | TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (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 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 |

New Health and Wellness

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

New Health and Wellness on Different Subnet

If the New Health and Wellness is on a different subnet, you must open the respective NetWitness Platform hosts port.

Example:

New Health and Wellness is on subnet A: 10.10.1.0/24 and LogHybrid host is on subnet B: 10.10.2.0/24. In this case, you must open ports for Log Decoder, Log Collector, Concentrator on Metrics Server (New Health and Wellness host) to allow ports in the firewall for communication.

| Source Host | Destination Host | Destination Ports | Comments |
|-------------------------|------------------|---------------------------|---------------------------------|
| New Health and Wellness | Log Decoder | 50002(Non-SSL),56002(SSL) | Log Decoder Application Ports |
| New Health and Wellness | Log Collector | 50001(Non-SSL),56001(SSL) | Log Collector Application Ports |
| New Health and Wellness | Concentrator | 50005(Non-SSL)/56005(SSL) | Concentrator Application Ports |

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 RSA NetWitness Platform 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 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 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 Master Table of Contents 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), 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 |

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 Master Table of Contents 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 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), 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 UDP 111 2049 | iDRAC Installations |

Network Hybrid Host

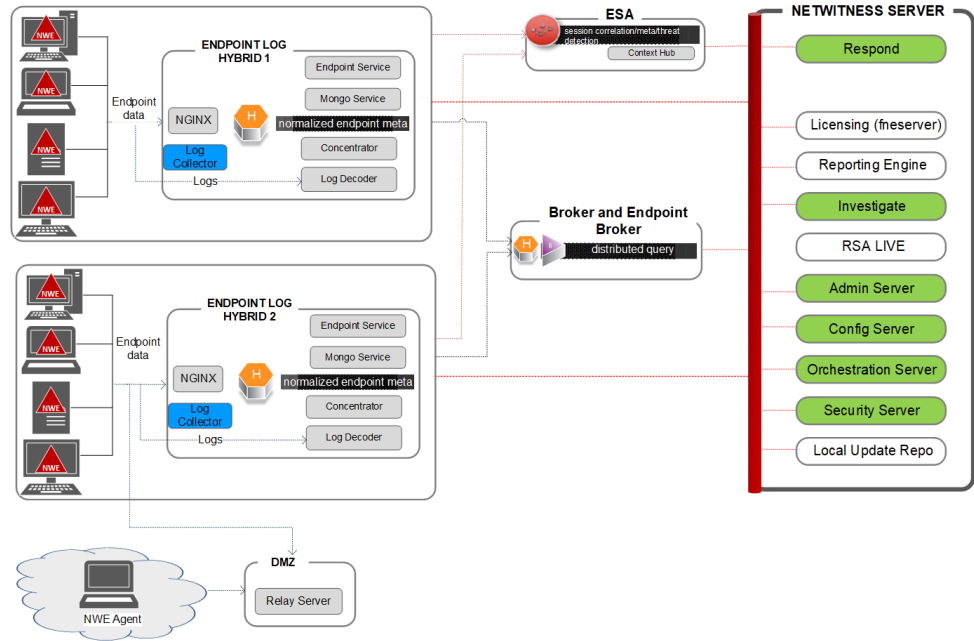
| Source Host | Destination Host | Destination Ports | Comments |
|-------------------|------------------|--|--|
| Admin Workstation | Network Hybrid | TCP 15671 | RabbitMQ Management UI |
| Network Hybrid | NW Server | TCP 15671 | RabbitMQ Management UI |
| Network Hybrid | NW Server | TCP 443 | RSA 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 UDP 111 2049 | iDRAC Installations |

UEBA Host

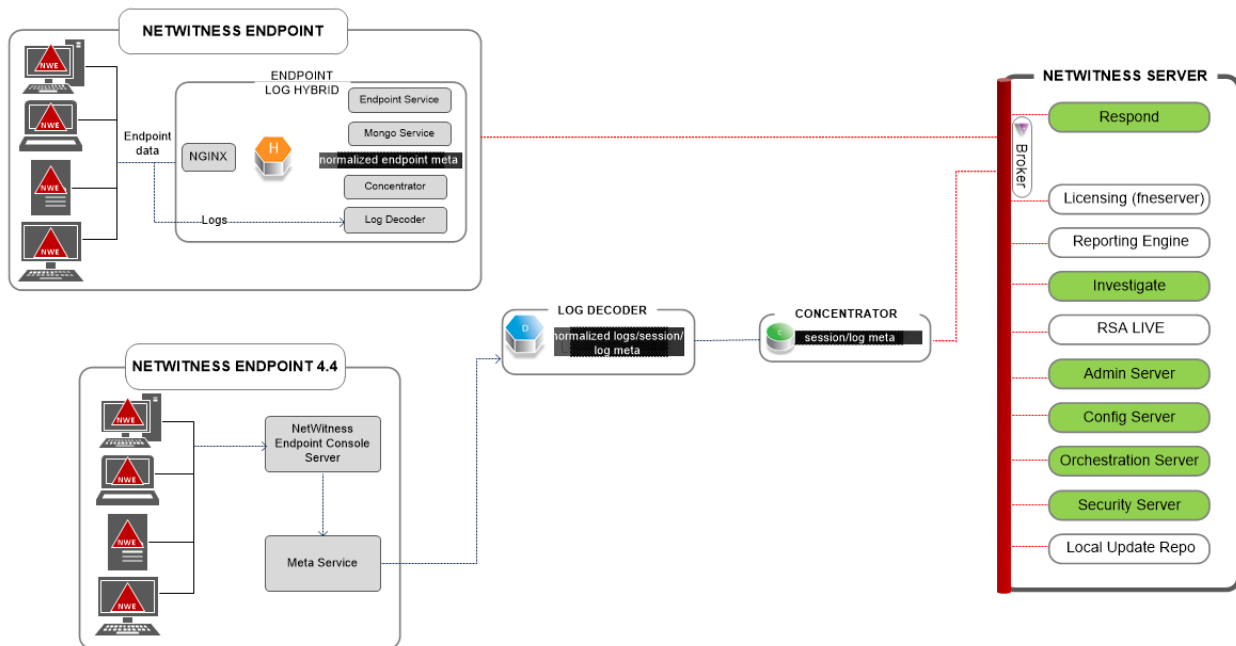
| Source Host | Destination Host | Destination Ports | Comments |
|-------------------|------------------|--|---|
| UEBA Server | NW Server | TCP 443 | RSA Update Repository |
| UEBA Server | Broker | TCP 56003 (SSL), 50103 (REST) | Broker Application Ports |
| UEBA Server | Concentrator | TCP TCP 50005 (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 UDP 111, 2049 | iDRAC Installations |
| NW Server | UEBA Server | TCP 5671 | RabbitMQ (AMQPS) message bus for all NW hosts |

NetWitness Endpoint Architecture

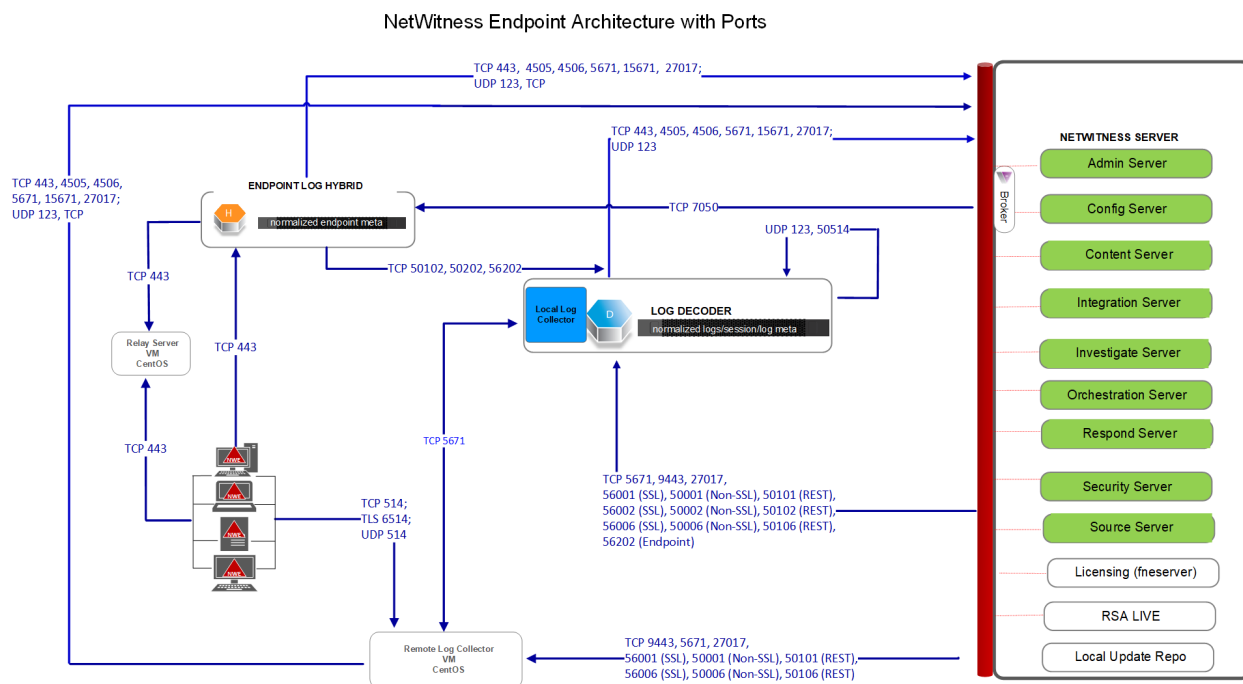
NetWitness Endpoint Architecture



NetWitness Endpoint 4.4 Integration with NetWitness Platform



NetWitness Endpoint 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 t 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.