



# Deployment Guide

for Version 11.2



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

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

## **Trademarks**

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

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

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

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

## **Third-Party Licenses**

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

## **Note on Encryption Technologies**

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

## **Distribution**

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

September 2018

# Contents

---

<b>The Basics</b>	<b>5</b>
Basic Deployment	6
Process	6
NetWitness Platform High-Level Deployment Diagram	7
RSA NetWitness Platform Detailed Host Deployment Diagram	8
<b>Network Architecture and Ports</b>	<b>9</b>
NetWitness Platform Network Architecture Diagram	9
Comprehensive List of NetWitness Platform Host and Service Ports	10
NW Server Host	11
Archiver Host	12
Broker Host	13
Concentrator Host	14
Endpoint Hybrid or Endpoint Log Hybrid	15
Endpoint Hybrid or Endpoint Log Hybrid with NetWitness Endpoint 4.4	15
Event Stream Analysis (ESA) Host	16
Log Collector Host	18
Log Decoder Host	20
Log Hybrid Host	22
Malware Host	24
Network Decoder Host	25
Network Hybrid Host	26
UEBA Host	27
NetWitness Endpoint Insights Architecture	28
NetWitness Endpoint Insights 11.2	28
NetWitness Endpoint Insights 11.2 with Log Decoder	29
NetWitness Endpoint 4.4 Integration with NetWitness Endpoint Insights 11.2	29
<b>Site Requirements and Safety</b>	<b>31</b>
Intended Application Uses	31
Service	31
Safety Information	31
Site Selection	31

Equipment Handling Practices .....	31
Power and Electrical Warnings .....	32
Rack Mount Warnings .....	32
Cooling and Air Flow .....	32
Antenna Placement .....	32
<b>Configure Group Aggregation .....</b>	<b>33</b>
RSA Group Aggregation Deployment Recommendations .....	33
Advantages of Using Group Aggregation .....	33
Configure Group Aggregation .....	36
Prerequisites .....	36
Set up Group Aggregation .....	38

## The Basics

---

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

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

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

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

## Basic Deployment

Before you can deploy NetWitness Platform you need to:

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

## Process

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

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

When ready to begin deployment, the general sequence is:

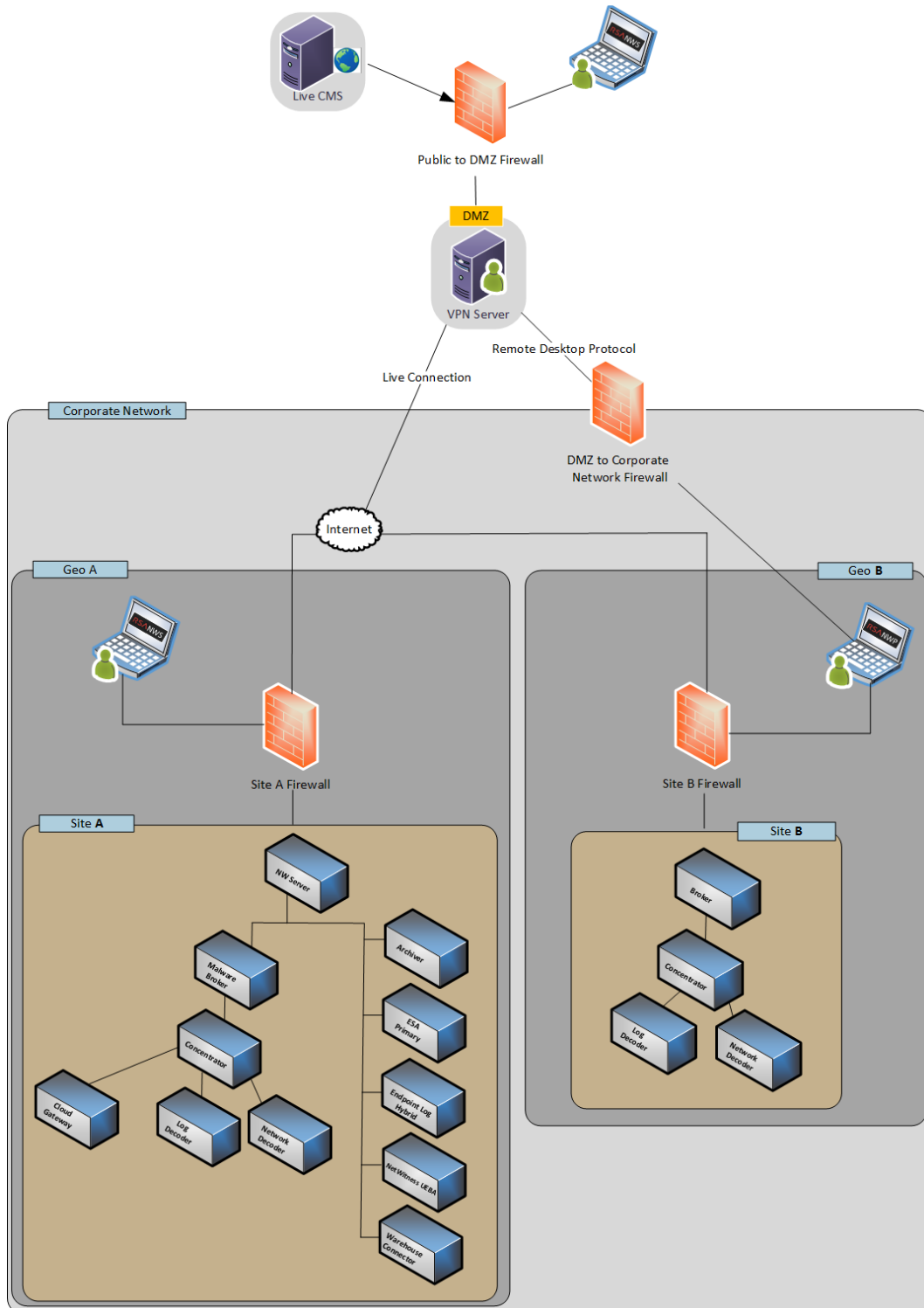
- For RSA Physical Hosts:
  1. Install physical hosts and connect to the network as described in the *RSA NetWitness® Platform Hardware Setup Guides* and the *RSA NetWitness® Platform Physical Host Installation Guide*.
  2. Set up licensing for NetWitness Platform as described in the *RSA NetWitness®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

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

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

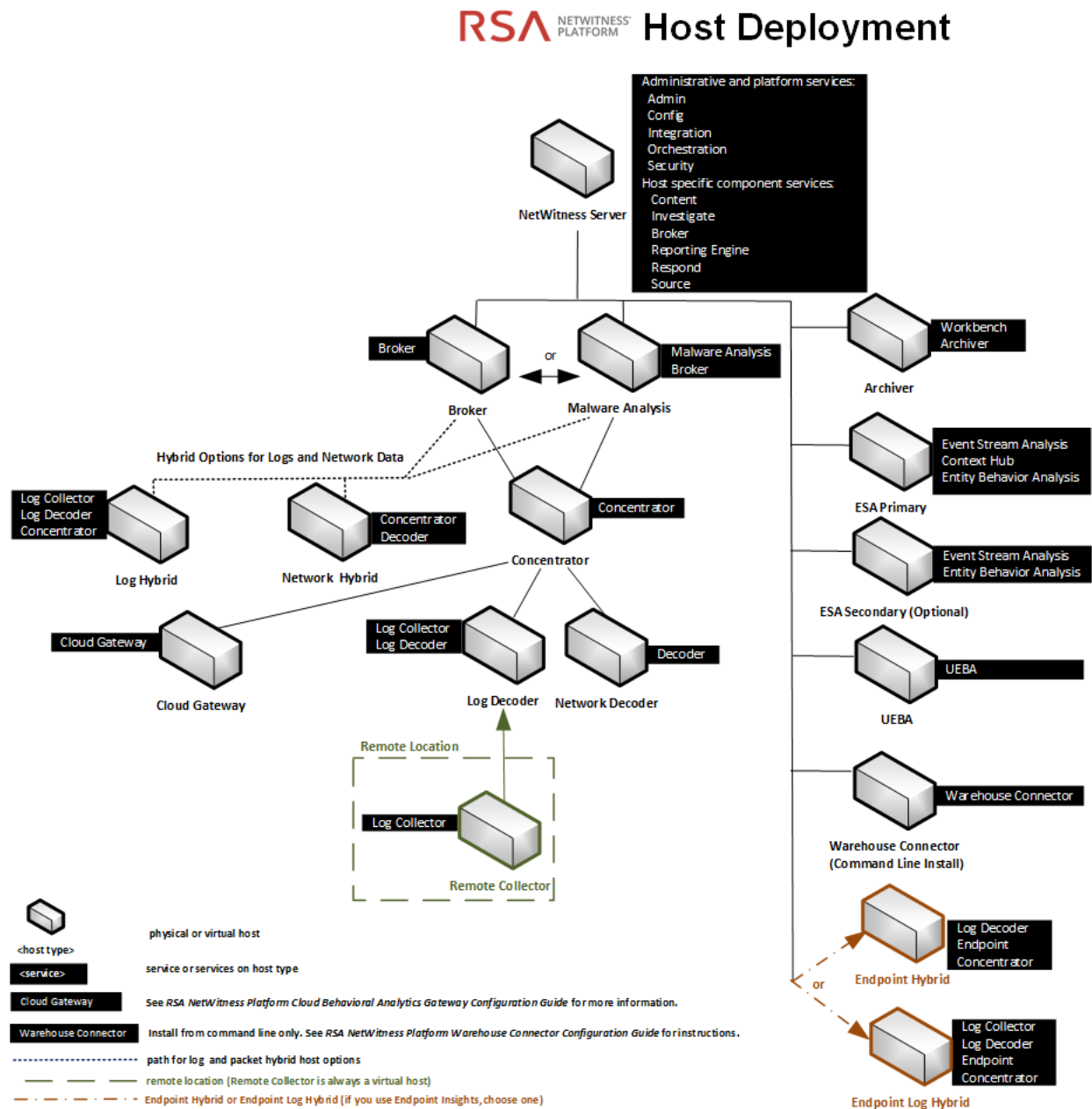
## NetWitness Platform High-Level Deployment Diagram

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



## RSA NetWitness Platform Detailed Host Deployment Diagram

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





## Network Architecture and Ports

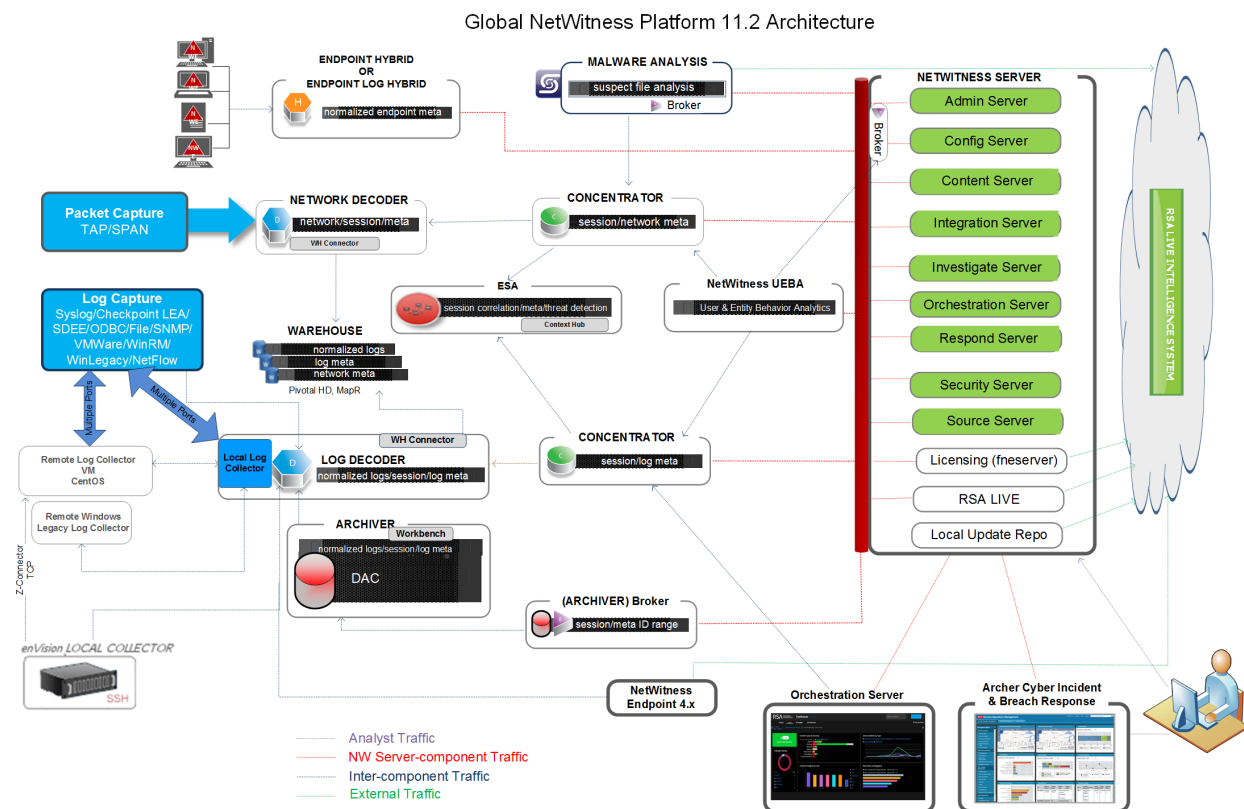
Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness Platform deployment to communicate with each other.

See [NetWitness Endpoint Insights 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.



**RSA** NETWITNESS<sup>®</sup> PLATFORM

**Note:**  
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, and Security 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.

## Comprehensive List of NetWitness Platform Host and Service Ports

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

This section contains the port specifications for the following hosts.

<a href="#">NW Server Host</a>	<a href="#">Log Collector Host</a>
<a href="#">Archiver Host</a>	<a href="#">Log Decoder Host</a>
<a href="#">Broker Host</a>	<a href="#">Log Hybrid Host</a>
<a href="#">Concentrator Host</a>	<a href="#">Malware Host</a>
<a href="#">Endpoint Hybrid/Endpoint Log Hybrid Host</a>	<a href="#">Network Decoder Host</a>
<a href="#">Event Stream Analysis Host</a>	<a href="#">Network Hybrid Host</a>
	<a href="#">UEBA Host</a>

## NW Server Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	NW Server	TCP 443, 80	nginx - NetWitness UI
NW Hosts	NW Server	TCP 443	RSA Update Repository
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
NW Hosts	NW Server	TCP 15671	RabbitMQ Management UI
Admin Workstation	NW Server	TCP 22	SSH
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 5671	RabbitMQ-amqp
NW Server	NW Server	UDP 50514	Audit Ports
NW Hosts	NW Server	UDP 123	NTP
NW Hosts	NW Server	TCP 27017	MongoDB
NW Server	NW Server	UDP 123	NTP
NW Server	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
NW Server	NW Endpoint	TCP 443, 9443	For NW Endpoint 4.x integrations

## Archiver Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Archiver	TCP 15671	RabbitMQ Management UI
Archiver	NW Server	TCP 15671	RabbitMQ Management UI
Archiver	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Archiver	TCP 22	SSH
NW Server	Archiver	TCP 56008 (SSL), 50008 (Non-SSL), 50108 (REST)	Archiver Application Ports
NW Server	Archiver	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Archiver	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Non-SSL), 50107 (REST), UDP 514	Workbench Application Ports
Archiver	Archiver	UDP 50514	Audit Data
Archiver	Archiver	UDP 123	NTP
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	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 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
NW Server	Broker	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Broker	Broker	UDP 50514	Audit Data
Broker	Broker	UDP 123	NTP
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

## Concentrator Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Concentrator	TCP 15671	RabbitMQ Management UI
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 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW Server	Concentrator	TCP 56006 (SSL), 50006 (Non-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
Concentrator	Concentrator	UDP 50514	Audit Data
Concentrator	Concentrator	UDP 123	NTP

## Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint 11.2 Agent	Endpoint Hybrid or Endpoint Log Hybrid	TCP 443	NGINX HTTPS
Endpoint 11.2 Agent	Log Decoder or Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Server	Log Decoder (External)	TCP 50102, 56202, 50202	To forward meta to an external Log Decoder
Endpoint Server	NW Server	TCP 443	RSA Update Repository
NW Server	Endpoint Hybrid or Endpoint Log Hybrid	TCP 7050	UI web traffic
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5671	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

## Endpoint Hybrid or Endpoint Log Hybrid with NetWitness Endpoint 4.4

Source Host	Destination Host	Destination Ports	Comments
NW Console Server (4.4.0.2 or later)	Endpoint Hybrid	TCP 443	NGINX HTTPS
Meta Service	Log Decoder	TCP 50102, 56202, 50202	NGINX HTTPS To forward meta to a Log Decoder Endpoint Hybrid or Endpoint Log Hybrid with NWE 4.4

## Event Stream Analysis (ESA) Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 443	RSA Update Repository
Admin Workstation	ESA	TCP 22	SSH
NW Server, ESA Secondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 50030 (SSL)	ESA Application Port
NW Server	ESA	TCP 50035 (SSL)	ESA Application Port
NW Server	ESA	TCP 50036 (SSL)	ESA Application Port
NW Server	ESA	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
ESA Primary and Secondary	cms.netwitness.com	TCP 443	Live
ESA Primary and Secondary	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
ESA Primary and Secondary	Active Directory	636 (SSL)/389 (Non-SSL)	
NW Server	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Non-SSL)	
ESA Primary	ESA Primary	TCP 7007	Launch Port
ESA Primary	ESA Primary	UDP 50514	Audit Data



Source Host	Destination Host	Destination Ports	Comments
ESA Primary	ESA Primary	UDP 123	NTP

## Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI
Log Collector	NW Server	TCP 15671	RabbitMQ Management UI
Log Collector	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Collector	TCP 22	SSH
Log Collector	Log Event Sources	See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all NetWitness Platform Logs & Network 11.x documents.	
Log Event Sources	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Log Collection Ports
Log Event Sources	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Collector	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Collector	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Collector	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Collector	Log Collector	UDP 50514	Audit Data

Source Host	Destination Host	Destination Ports	Comments
Log Collector	Log Collector	UDP 123	NTP
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 15671	RabbitMQ Management UI
Log Decoder	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Log Event Sources	See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all NetWitness Platform Logs & Network 11.x documents.	
Log Event Sources	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Decoder	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Decoder	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.

Source Host	Destination Host	Destination Ports	Comments
Log Decoder	Log Decoder	UDP 50514	Audit Data
Log Decoder	Log Decoder	UDP 123	NTP
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

## Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
Log Hybrid	NW Server	TCP 15671	RabbitMQ Management UI
Log Hybrid	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Log Event Sources	See <i>Log Collection Configuration Guide</i> . Go to the <a href="#">Master Table of Contents</a> to find all NetWitness Platform Logs & Network 11.x documents.	
Log Event Sources	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid	TCP 56002 (SSL), 50002 (Non-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Log Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

## Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
Malware	NW Server	TCP 15671	RabbitMQ Management UI
Malware	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malware Application Ports
NW Server	Malware	TCP 56006 (SSL), 50006 (Non-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), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	Malware	UDP 50514	Audit Data
Malware	Malware	UDP 123	NTP
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), 50004 (Non-SSL), 50104 (REST)	Network Decoder Application Ports
NW Server	Network Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Network Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Network Decoder	Network Decoder	UDP 50514	Audit Data
Network Decoder	Network Decoder	UDP 123	NTP
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), 50004 (Non-SSL), 50104 (REST)	Network Decoder Application Ports
NW Server	Network Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Network Hybrid	TCP 56006 (SSL), 50006 (Non-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

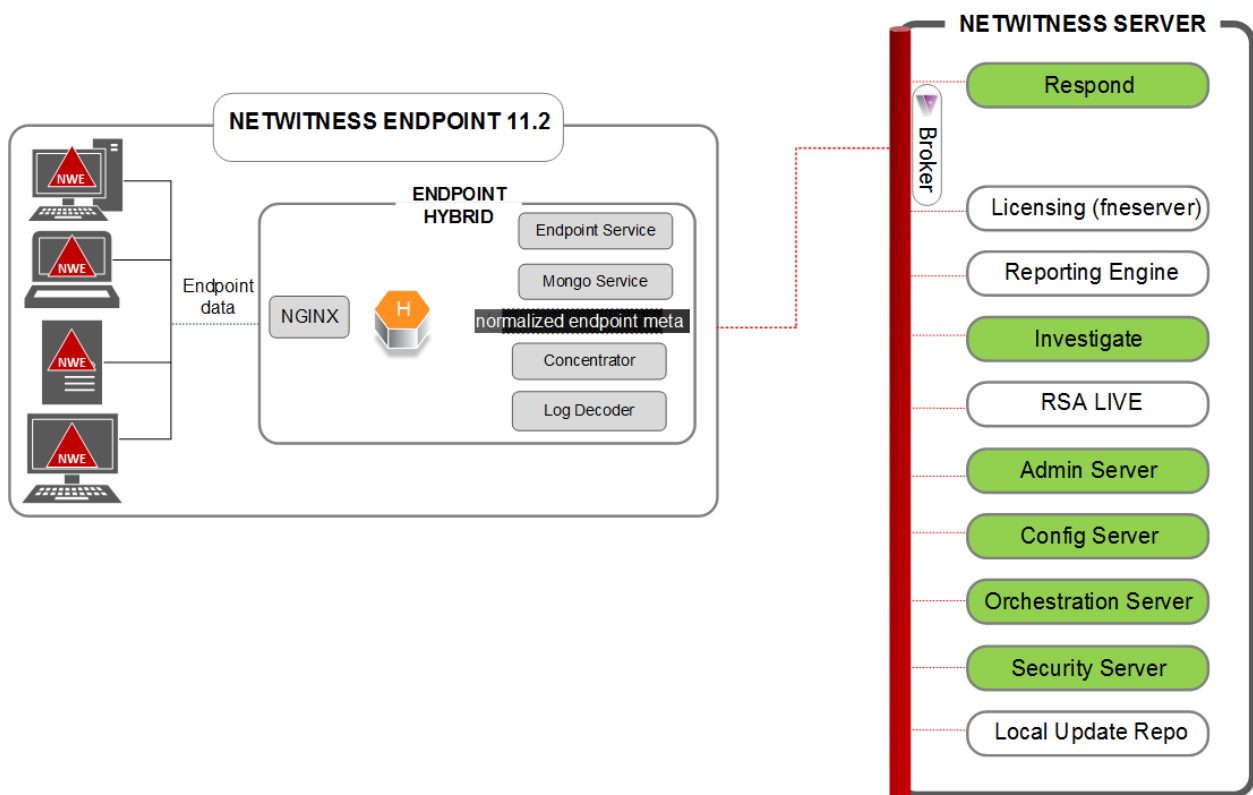
Source Host	Destination Host	Destination Ports	Comments
UEBA Server	NW Server	TCP 443	RSA Update Repository
UEBA Server	NW Server	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
UEBA Server	NW Server	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
Admin Workstation	UEBA Server	443	UEBA Monitoring
Admin Workstation	UEBA Server	22	SSH
UEBA Server	NW Server	15671	UEBA Alerts forwarding to Respond

## NetWitness Endpoint Insights Architecture

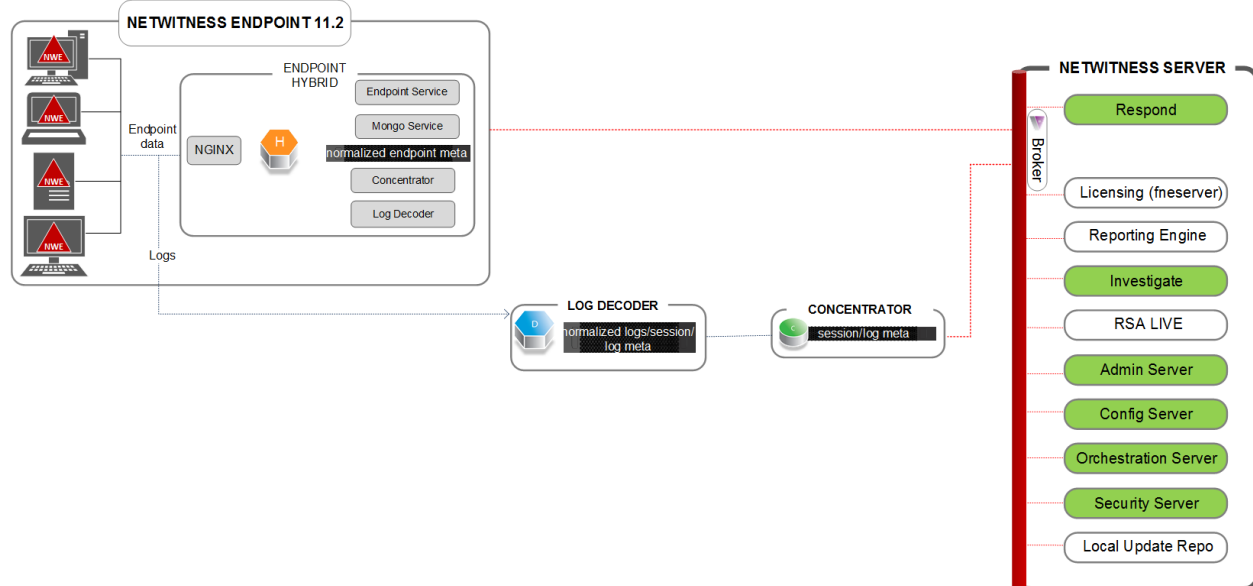
The following diagrams illustrate the NetWitness Endpoint Insights network architecture.

### NetWitness Endpoint Insights 11.2

#### NetWitness Endpoint Architecture

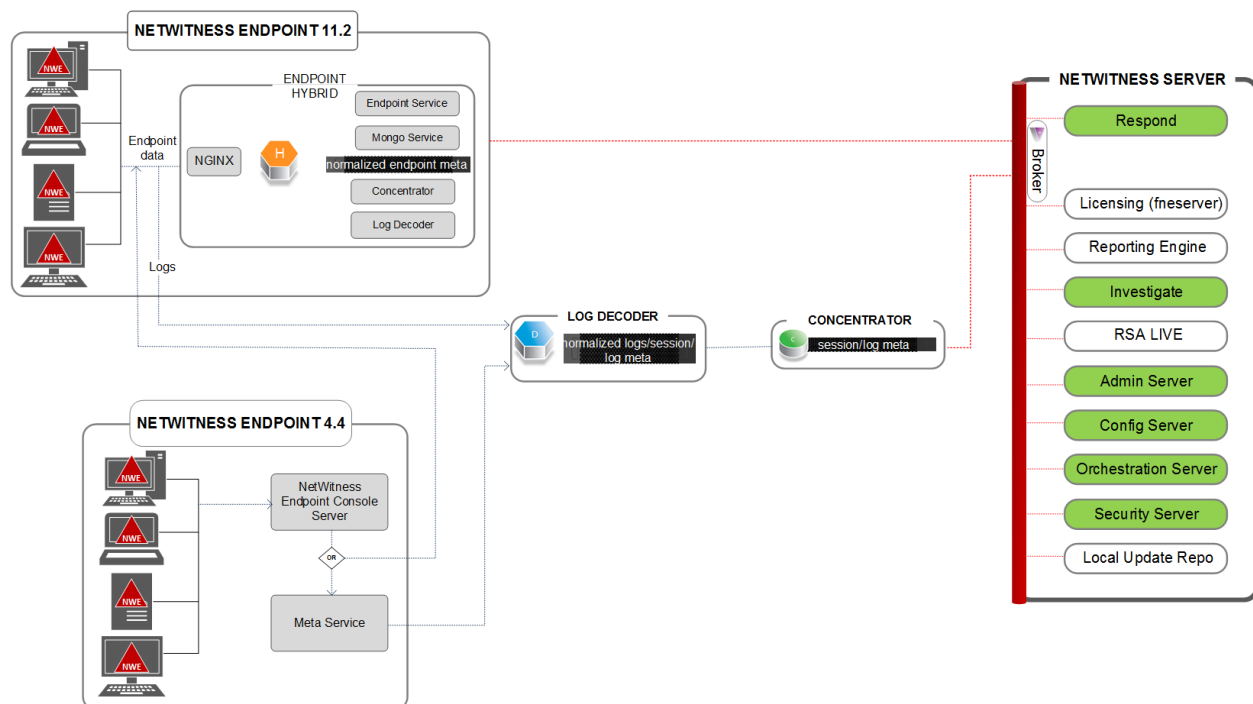


## NetWitness Endpoint Insights 11.2 with Log Decoder



## NetWitness Endpoint 4.4 Integration with NetWitness Endpoint Insights 11.2

### NetWitness Endpoint Architecture



For more information on the services running on Endpoint Hybrid, see *RSA NetWitness Endpoint Insights Configuration Guide*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.



## 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.

## Antenna Placement

This equipment should be installed and operated with a minimum distance of 7cm between the radiator and your body. The antennas used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



## Configure Group Aggregation

---

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

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

### RSA Group Aggregation Deployment Recommendations

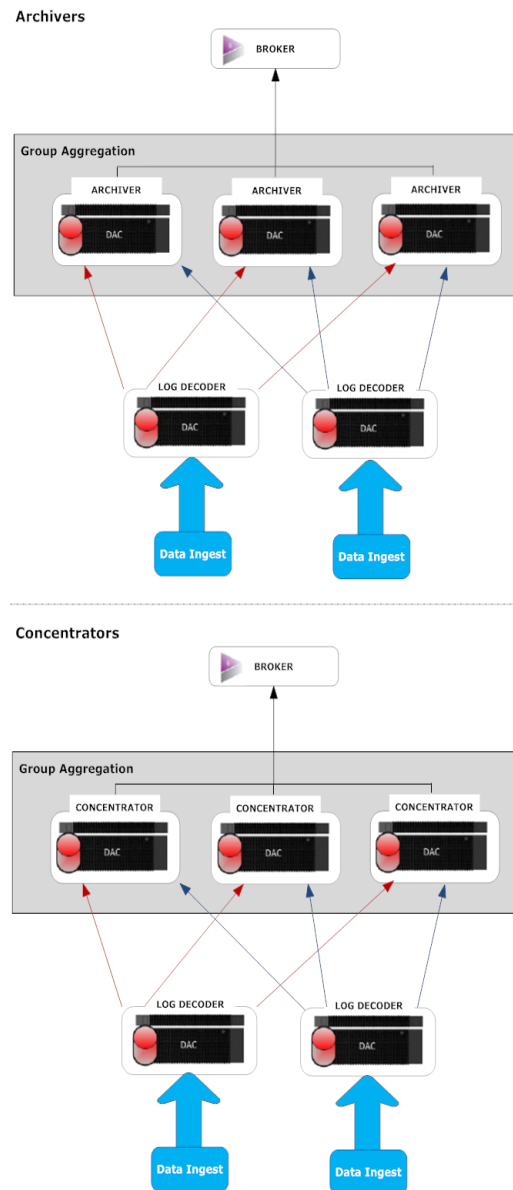
RSA recommends the following deployment for Group Aggregation:

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

### Advantages of Using Group Aggregation

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

The following diagram illustrates Group Aggregation.



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

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

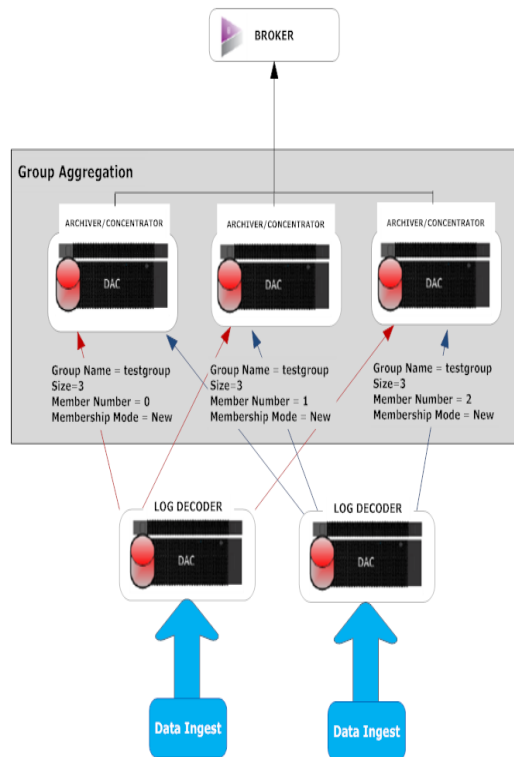
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

## Configure Group Aggregation

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

### Prerequisites

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



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

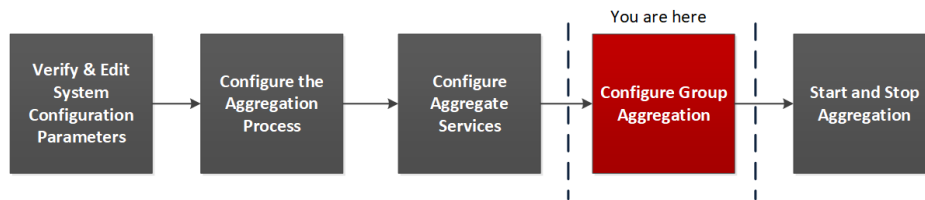
Parameter	Description
Group Name	It determines the group to which the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All Archiver or Concentrator services in the group should have the same group name.
Size	It determines the number of Archiver or Concentrator services in the aggregation group.

Parameter	Description
Member Number	<p>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.</p> <p>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.</p>
Membership Mode	<p>There are two membership modes:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>



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

## Set up Group Aggregation

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



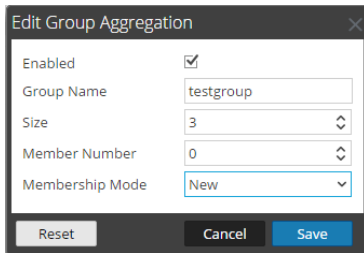
### To set up group aggregation:

1. Configure multiple Archiver or Concentrator services in your environment. Make sure that you add the same Log Decoder as data source to all the services.
2. Perform the following on all the Archiver or Concentrator services that you want to be part of aggregation group:
  - a. Go to **ADMIN > Services**.
  - b. Select the Archiver or Concentrator service, and in the **Actions** column, select **View > Config**. The Service Config view of the Archiver or Concentrator is displayed.
  - c. In the **Aggregate Services** section, select **Log Decoder**.
  - d. Click  **Toggle Service** to change the status of the Log Decoder to offline if it is online.
  - e. Click .

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

- f. Click  **Group Aggregation**.

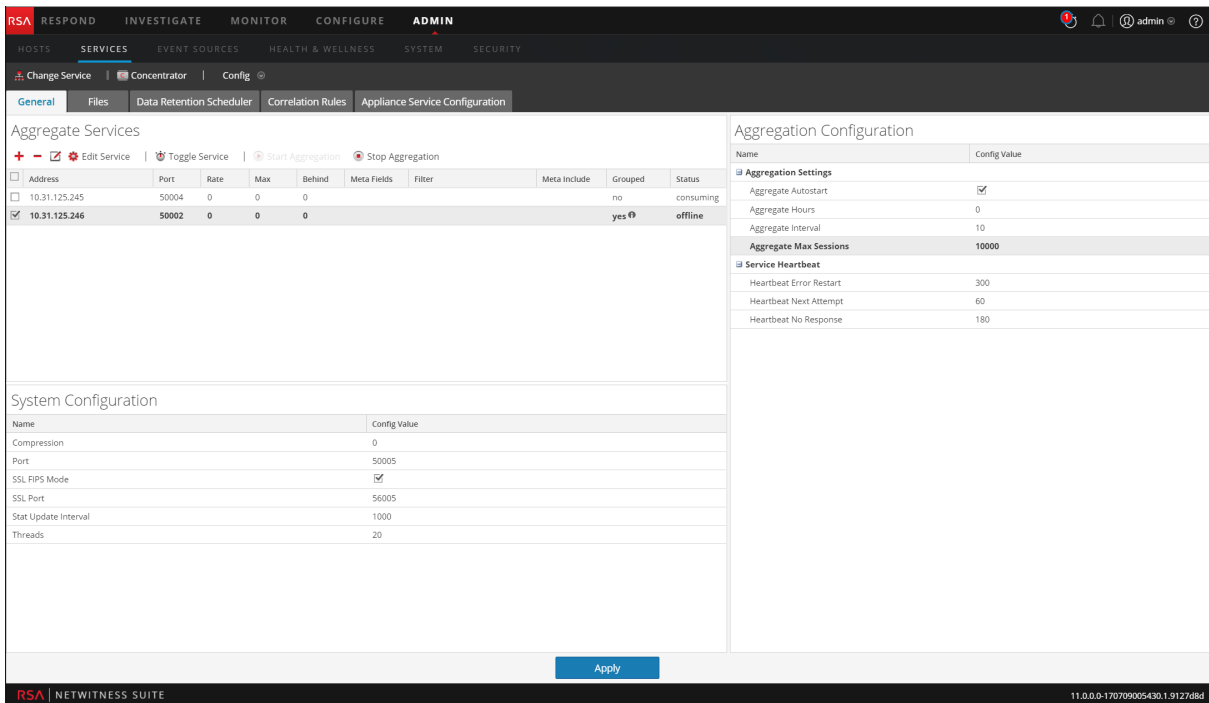
The **Edit Group Aggregation** dialog is displayed.



The dialog box titled "Edit Group Aggregation" contains the following fields and controls:

- Enabled:** A checked checkbox.
- Group Name:** A text field containing "testgroup".
- Size:** A spinner field set to "3".
- Member Number:** A spinner field set to "0".
- Membership Mode:** A drop-down menu set to "New".
- Buttons at the bottom: "Reset", "Cancel", and "Save".

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



The screenshot shows the RSA NetWitness Suite Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar shows the "Services" section with a "Config" button. The main content area is divided into two panels:

- Aggregate Services:** A table listing services with columns for Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. Two services are listed: 10.31.125.245 (status: consuming) and 10.31.125.246 (status: offline, grouped: yes).
- Aggregation Configuration:** A table with two columns: Name and Config Value. It contains settings for Aggregation Settings (Aggregate Autostart, Aggregate Hours, Aggregate Interval, Aggregate Max Sessions) and Service Heartbeat (Heartbeat Error Restart, Heartbeat Next Attempt, Heartbeat No Response).

The "Aggregate Max Sessions" value is set to 10000. At the bottom of the console, there is an "Apply" button and a footer with the RSA NetWitness Suite logo and version information.

