



# Deployment Guide

for Version 11.0



## **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 EMC, 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 EMC.

## **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**

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

October 2017

# Contents

---

<b>NetWitness Suite Deployment .....</b>	<b>5</b>
Basic Deployment Process .....	6
Process .....	6
NetWitness Suite Deployment Diagram .....	7
RSA Physical Appliance Environment .....	8
<b>Deployment: Network Architecture and Ports .....</b>	<b>10</b>
NetWitness Suite Network Architecture Diagram .....	10
Comprehensive List of NetWitness Suite Host and Service Ports .....	10
NW Server Host .....	11
Archiver Host .....	11
Broker Host .....	12
Concentrator Host .....	13
Event Stream Analysis (ESA) Host .....	13
Log Collector Host .....	14
Log Decoder Host .....	16
Log Hybrid Host .....	17
Malware Host .....	18
Packet Decoder Host .....	19
Packet Hybrid Host .....	19
<b>Site Requirements and Safety .....</b>	<b>21</b>
Intended Application Uses .....	21
Service .....	21
Safety Information .....	21
Site Selection .....	21
Equipment Handling Practices .....	22
Power and Electrical Warnings .....	22
Rack Mount Warnings .....	22
Cooling and Air Flow .....	22
Antenna Placement .....	23

<b>Configure Group Aggregation .....</b>	<b>24</b>
RSA Group Aggregation Deployment Recommendations .....	24
Advantages of Using Group Aggregation .....	24
Configure Group Aggregation .....	26
Prerequisites .....	26
	28
Set up Group Aggregation .....	28

## NetWitness Suite Deployment

---

This guide describes the basic requirements of a NetWitness Suite deployment and outlines optional scenarios to address needs of your enterprise. You can use distributed networks to install Brokers, Concentrator, Decoders, and Log Decoders in diverse geographical locations before the NetWitness Server is installed and brought online. 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](#) for Version 11.0 to find NetWitness Suite 11.0 documents.

There are many factors you must consider before you deploy NetWitness Suite. 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 Suite).
- The volume of packets and logs you need to process.
- The performance each NetWitness Suite 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 Suite
  - RSA Appliances (software running on hardware supplied by RSA)  
See the *RSA NetWitness® Suite Physical Host Installation Guide* for detailed instructions on how to deploy RSA Appliances.
  - Software Only provided by RSA:
    - On-Premises (On-Prem) Virtual Hosts
    - VCloud:
      - Amazon Web Services (AWS)
      - Azure

## Basic Deployment Process

Before you can deploy NetWitness Suite 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 Suite deployment.

## Process

The components and topology of a NetWitness Suite 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.

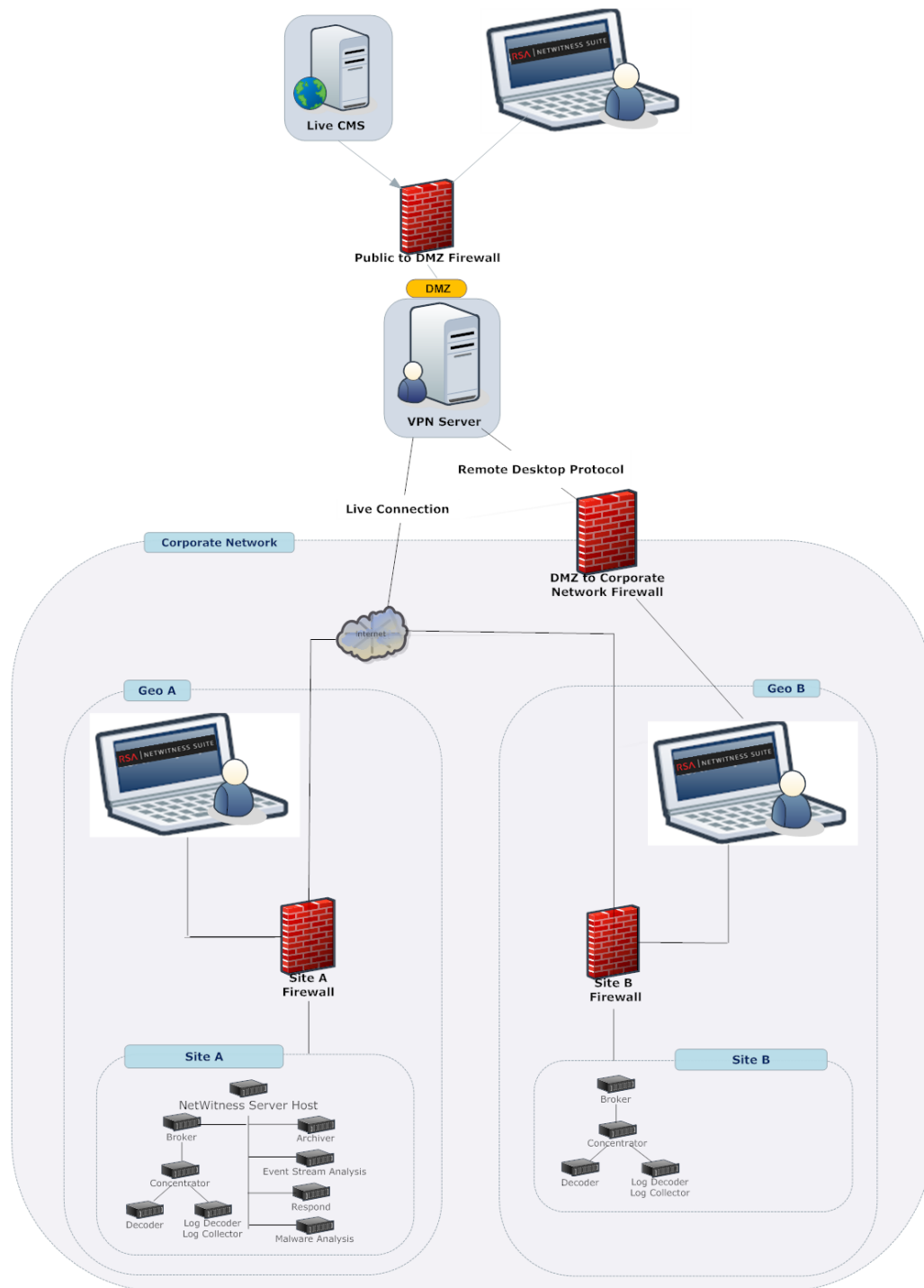
When ready to begin deployment, the general sequence is:

- For RSA Appliances:
  1. Install appliances and connect to the network as described in the RSA NetWitness® Suite Hardware Setup Guides and the *RSA NetWitness® Suite Physical Host Installation Guide*.
  2. Set up licensing for NetWitness Suite as described in the *RSA NetWitness® Suite Licensing Guide*.
  3. Configure individual appliances and services as described in *RSA NetWitness® Suite 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® Suite Virtual Host Setup Guide*.
- For AWS, follow the instructions in the *RSA NetWitness® Suite AWS Deployment Guide*.
- For Azure, follow the instructions in the *RSA NetWitness® Suite Azure Deployment Guide*.

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

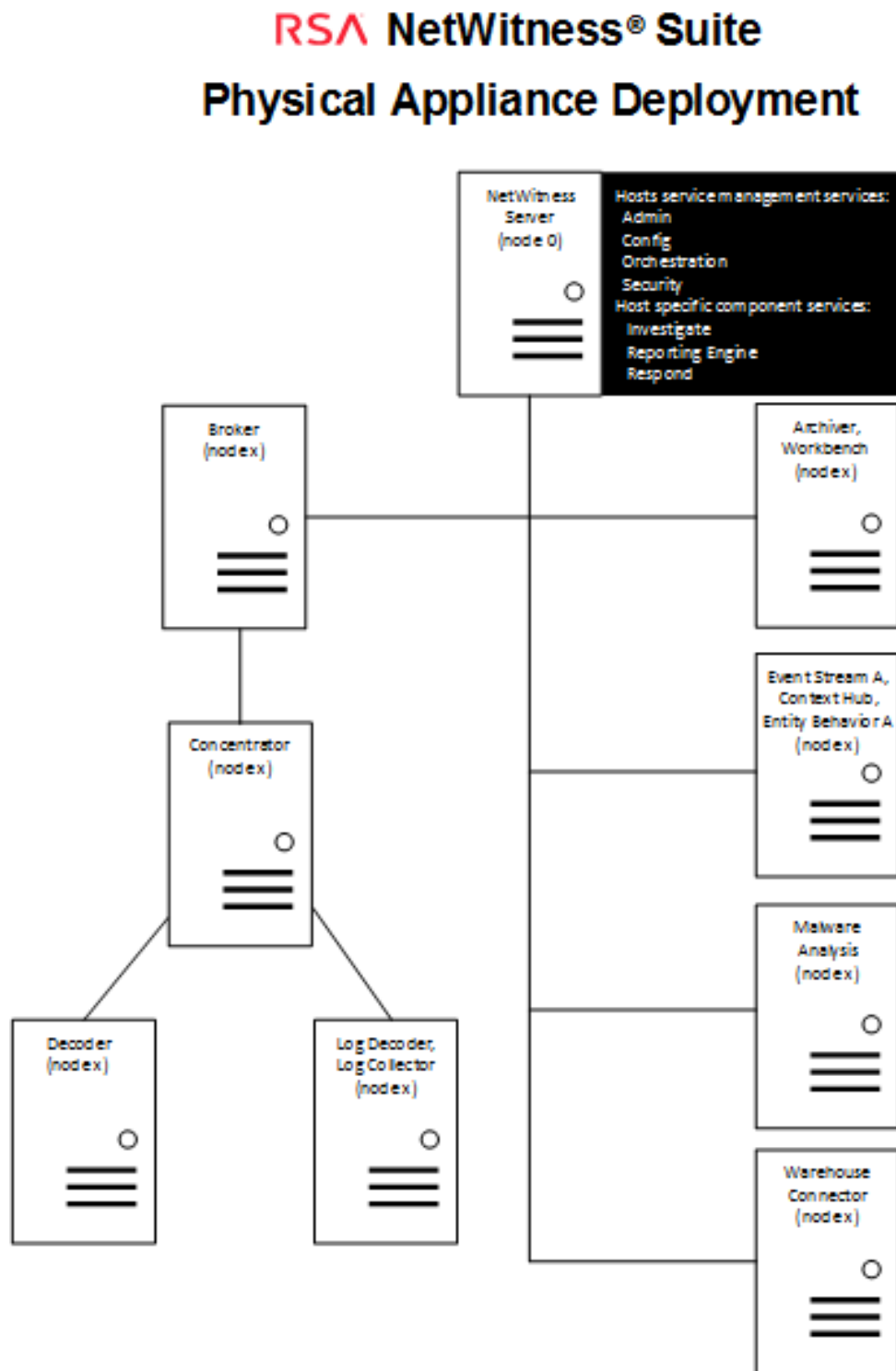
## NetWitness Suite Deployment Diagram

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



## RSA NetWitness Suite Physical Appliance Environment

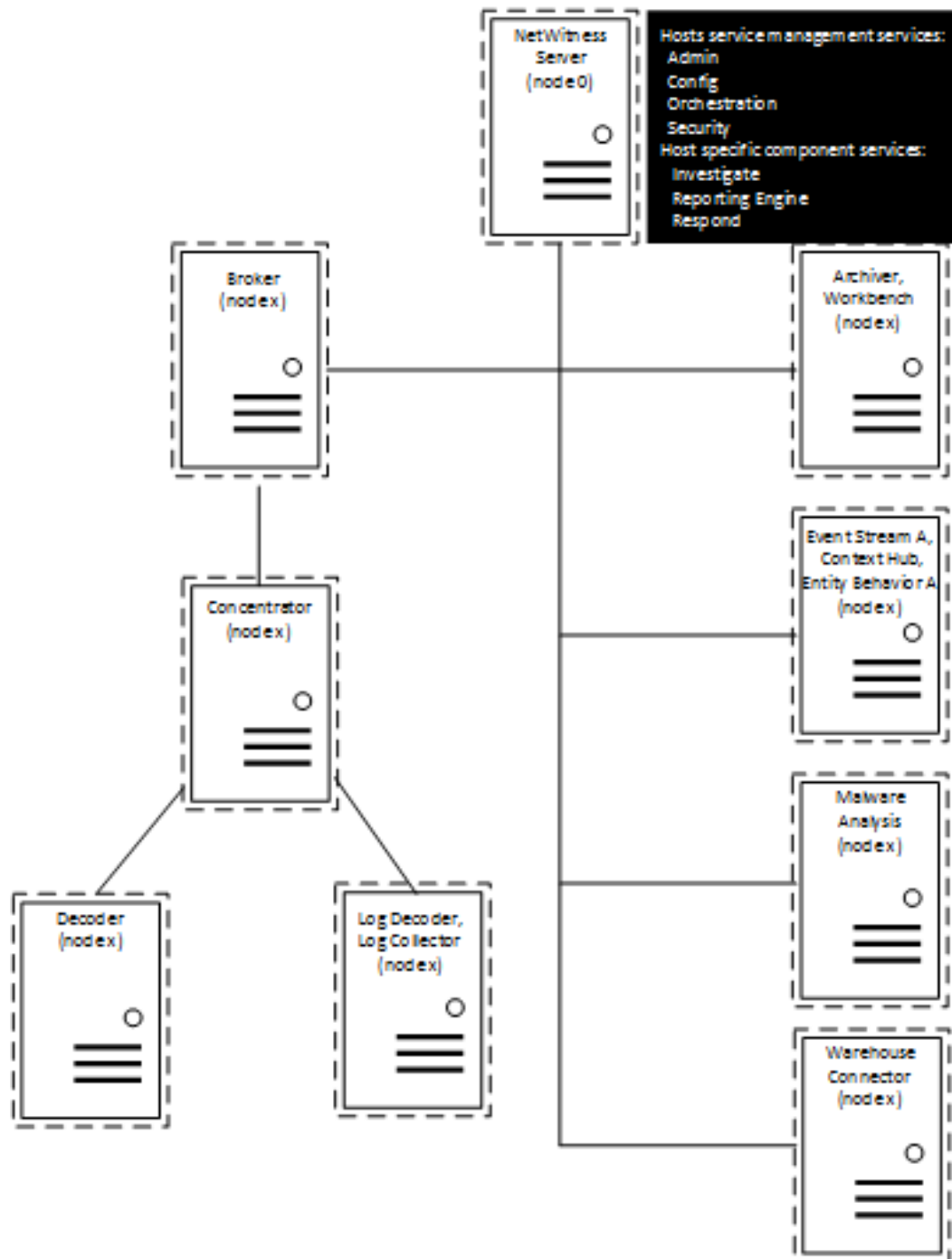
The following diagram illustrates a basic NetWitness Suite deployment hosted on RSA hardware.





The following diagram illustrates a basic NetWitness Suite deployment hosted virtually. See the RSA NetWitness® Suite On-Prem Virtual Host Setup Guide for details.

## RSA NetWitness® Suite On-Prem Virtual Deployment



## NetWitness Suite Network Architecture Diagram

**Note:** NetWitness Suite 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.

The diagram illustrates the NetWitness architecture, showing the flow of data from various sources through processing components to a central server and finally to a user interface.

**Data Sources and Initial Processing:**

- Packet Capture (TAP/SPAN):** Captures network traffic and sends it to the **PACKET DECODER**.
- Log Capture:** Captures logs from Syslog/Checkpoint LEA/SDEE/ODBC/File/SNMP/VMWare/WnRM/WnLegacy/NetFlow and sends them to the **Local Log Collector**.
- Remote Log Collector (Win/CentOS):** Collects logs from remote systems and sends them to the **Local Log Collector**.
- Remote Windows Legacy Log Collector:** Collects logs from remote Windows systems and sends them to the **Local Log Collector**.
- enVision LOCAL COLLECTOR:** A hardware device that collects logs and sends them to the **Local Log Collector**.

**Processing and Storage:**

- The **Local Log Collector** sends data to the **LOG DECODER**, which normalizes logs/session/log meta.
- The **LOG DECODER** sends data to the **WAREHOUSE**, which stores normalized logs, log meta, packet meta, and Pivotal HD, MapR.
- The **WAREHOUSE** feeds into the **ARCHIVER**, which stores normalized logs/session/log meta and includes a **DAC** (Data Access Control) and **Workbench**.
- The **ARCHIVER** sends data to the **(ARCHIVER) Broker**, which manages session/meta ID range.

**Analysis and Detection:**

- The **WAREHOUSE** feeds into the **CONCENTRATOR**, which manages session/packet meta.
- The **CONCENTRATOR** feeds into the **ESA** (session correlation/metadata/threat detection), which includes a **Context Hub**.
- The **ESA** feeds into the **CONCENTRATOR**, which manages session/log meta.
- The **CONCENTRATOR** feeds into the **Malware Analysis** component, which includes **suspect file analysis** and a **Broker**.

**NetWitness Server and External Systems:**

- The **NetWitness Server** is a central component that manages the following modules:
  - Respond**
  - Licensing (theserver)**
  - Reporting Engine**
  - Investigate**
  - RSA LIVE**
  - Admin Server**
  - Config Server**
  - Orchestration Server**
  - Security Server**
  - Local Update Repo**
- The **NetWitness Server** interacts with the **Malware Analysis** component and the **(ARCHIVER) Broker**.
- The **NetWitness Server** is connected to the **RSA Live Intelligence System** (cloud).

**User Interface and Endpoints:**

- The **NetWitness Server** is connected to the **NW Endpoint** (a device).
- The **NetWitness Server** is connected to the **NW SecOps** (a dashboard).
- The **NW SecOps** is accessible via a **user** (represented by a person icon).

**Traffic Types:**

- Analyst Traffic:** Represented by a dashed line.
- NW Server-component Traffic:** Represented by a red dotted line.
- Inter-component Traffic:** Represented by a green dotted line.
- External Traffic:** Represented by a blue dotted line.

**Note:** Respond, Investigate, Admin, Config, Orchestration, 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.

## Comprehensive List of NetWitness Suite Host and Service Ports

This section contains the port specifications for the following hosts.

[NW Server Host](#)[Log Decoder Host](#)[Archiver Host](#)[Log Hybrid Host](#)[Broker Host](#)[Malware Host](#)[Concentrator Host](#)[Packet Decoder Host](#)[Event Stream Analysis Host](#)[Packet Hybrid Host](#)[Log Collector Host](#)

## NW Server Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	NW Server	TCP 443, 80	nginx - NetWitness UI
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
Admin Workstation	NW Server	TCP 22	SSH
NW Hosts	NW Server	TCP 4505, 4506	Salt Master 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 111 204	iDRAC Installations

## Archiver Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Archiver	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
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	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

## Broker Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 15671	RabbitMQ Management UI
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

Source Host	Destination Host	Destination Ports	Comments
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
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
Admin Workstation	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
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 111 204	iDRAC Installations

### Event Stream Analysis (ESA) Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 22	SSH
NW Server, NW Endpoint, 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	cms.netwitness.com	TCP 443	Live
ESA	NFS Server	TCP 111 2049 UDP 111 2049	NTP

## Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
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> for Version 11.0 to find NetWitness Suite 11.0 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	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC installations

## Log Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Decoder	TCP 15671	RabbitMQ Management UI
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> for Version 11.0 to find NetWitness Suite 11.0 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.
Log Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations



## Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
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> for Version 11.0 to find NetWitness Suite 11.0 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 111 204	iDRAC Installations

### Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
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

Source Host	Destination Host	Destination Ports	Comments
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

### Packet Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Decoder	TCP 22	SSH
NW Server	Packet Decoder	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Decoder	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

### Packet Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Hybrid	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Hybrid	TCP 22	SSH
NW Server	Packet Hybrid	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Packet Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Hybrid	NFS Server	TCP 111 2049 UDP 111 204	iDRAC Installations

## 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

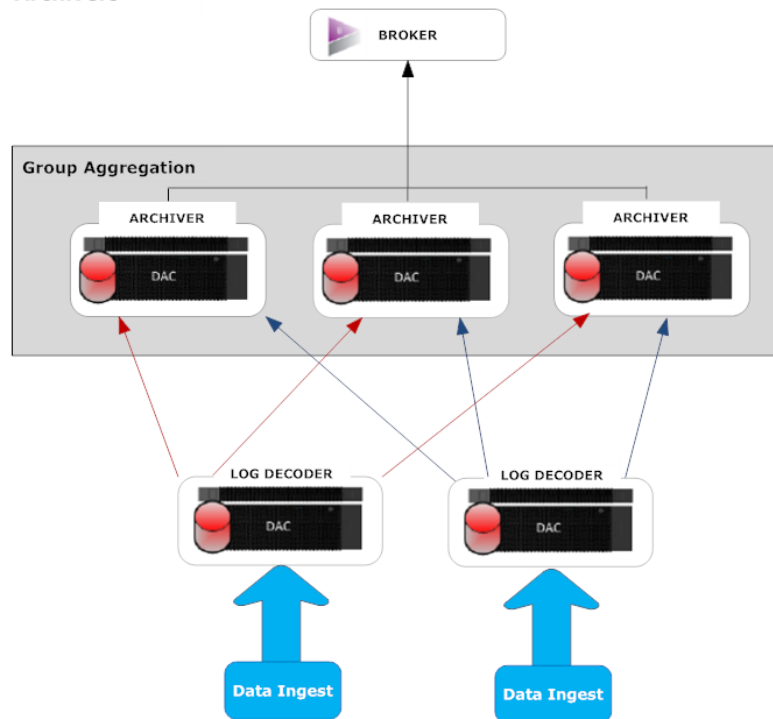
Group Aggregation:

- Increases the speed of Security Analytics 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.

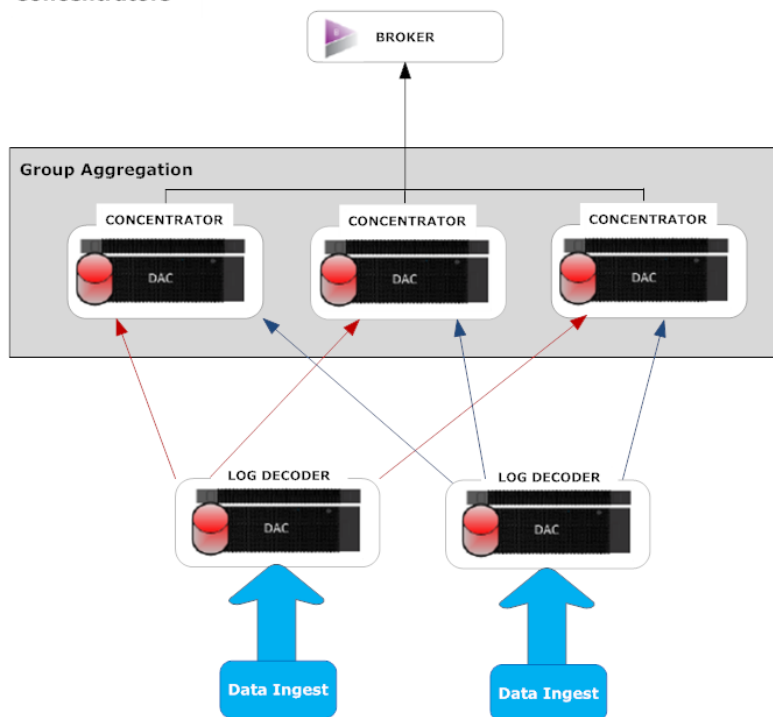
The following diagram illustrates Group Aggregation.



### Archivers



### Concentrators



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.

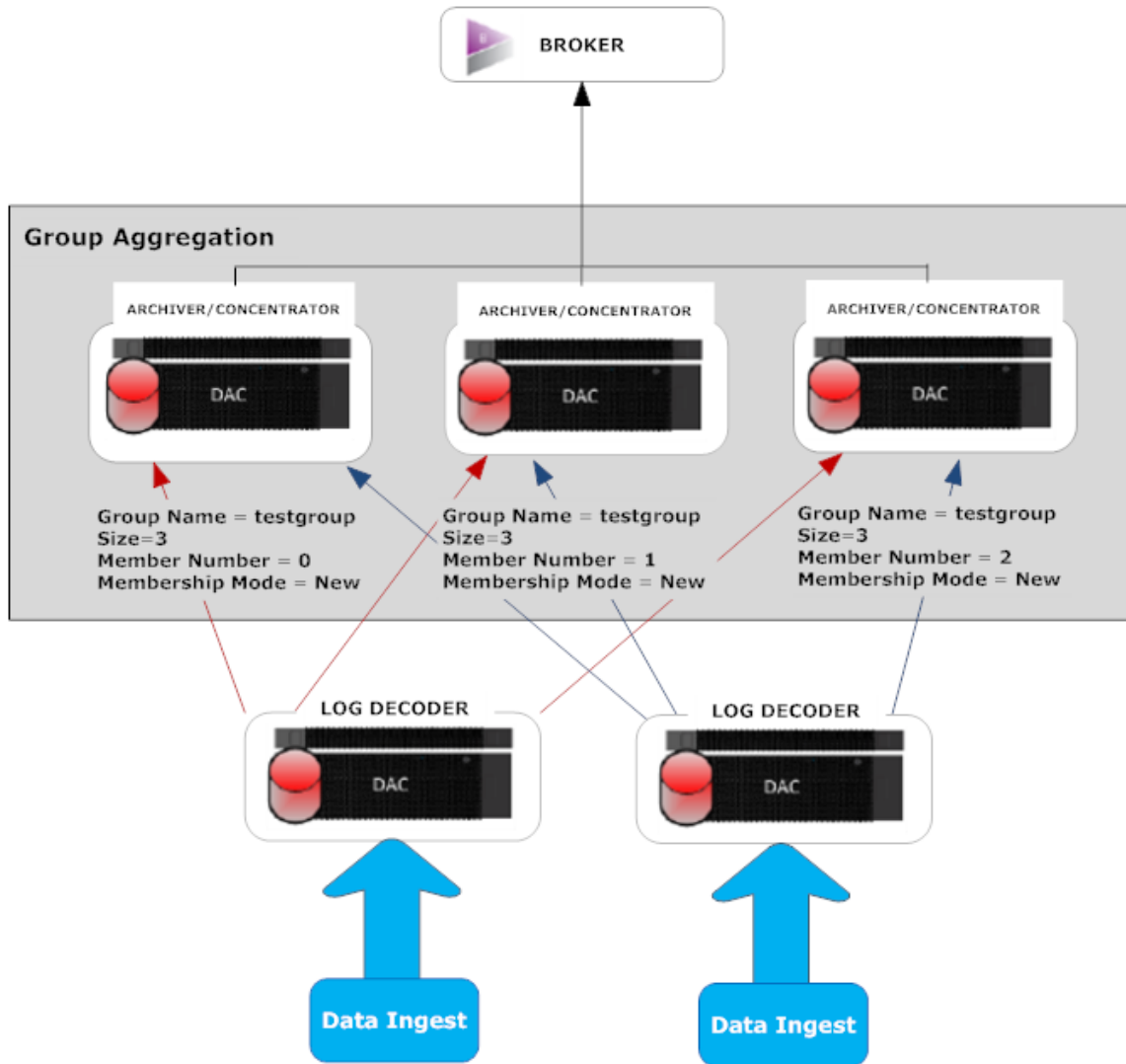
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

## Configure Group Aggregation

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

### Prerequisites

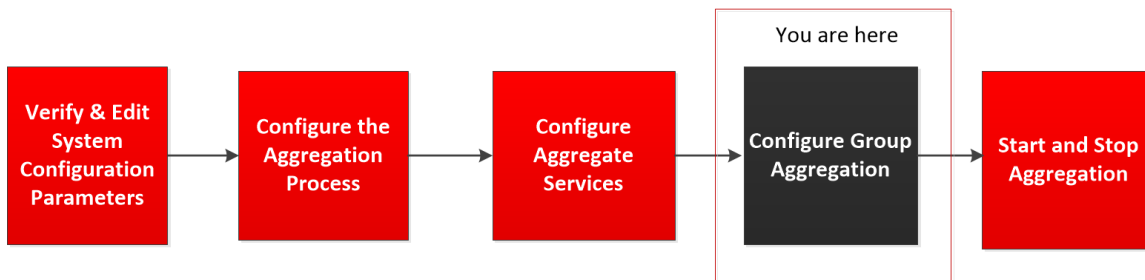
Plan the network design for group aggregation. The following figure is an example of a group aggregation setup.



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 Concentrators 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	<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: New and Replace.</p> <p>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.</p> <p>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.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This parameter has an effect only when no sessions have been aggregated from the service. After some sessions are aggregated, this parameter has no effect.</p> </div>



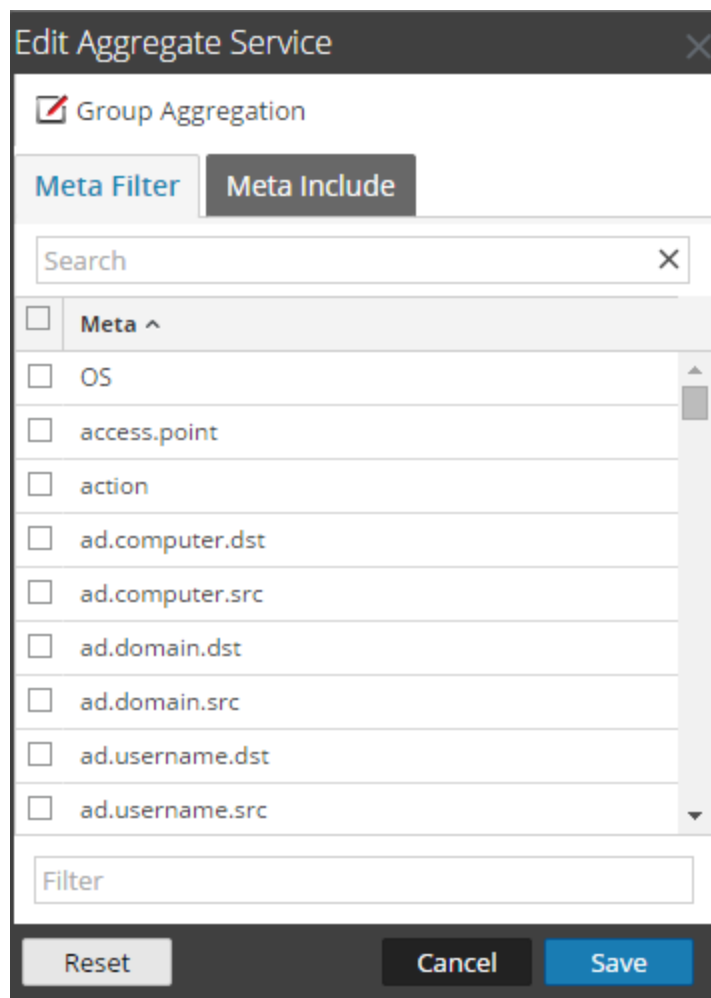
## Set up Group Aggregation

Complete the following procedure 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. In the **main menu**, select **ADMIN > Services**.
- b. Select the Archiver or Concentrator service, and in the **Actions** column, select **View > Config**.  
The Device Config view of the Archiver or Concentrator is displayed.
- c. Under **Aggregate Services** section, select the Log Decoder device.
- d. Click  **Toggle Service** to change the status of the Log Decoder to offline if it is online.
- e. Click .

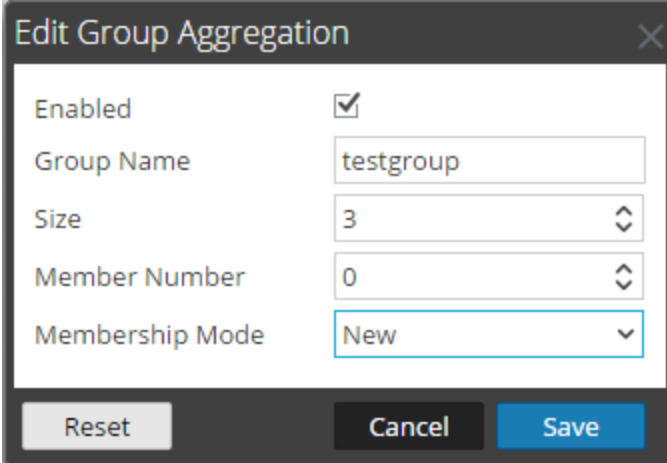
The **Edit Aggregate Service** dialog is displayed.



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

- f. Click  **Group Aggregation**.

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



**Edit Group Aggregation**

Enabled	<input checked="" type="checkbox"/>
Group Name	testgroup
Size	3
Member Number	0
Membership Mode	New

Reset Cancel 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 Device 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**.



