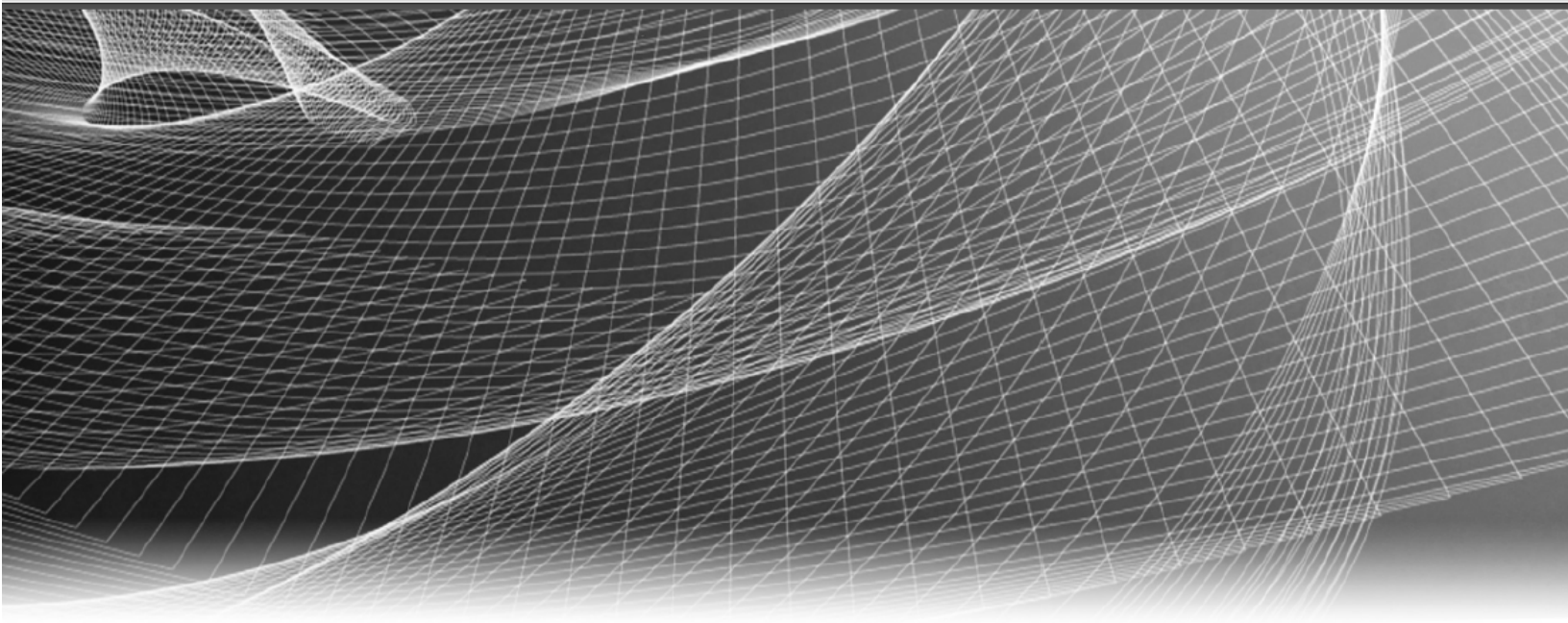


RSA Security Analytics

Deployment Guide

for Version 10.6.5

RSA

EMC²

Contact Information

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

Trademarks

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

License Agreement

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

Deployment Guide

This guide describes the basic requirements of a Security Analytics 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 Security Analytics 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.

There are many factors you must consider before you deploy Security Analytics. 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 Security Analytics.
- The volume of packets and logs you need to process.
- The performance each Security Analytics user role needs to do their jobs effectively.
- The prevention of downtime (that is, how to avoid a single point of failure).

Terminology Changes

The following terminology changes were made 10.6 that affect this guide.

10.6.0.0	Prior to 10.6.0.0	Description
Security Analytics Server Host	SA host, SA appli-ance	**Note:** Abbreviated to **Security Analytics Server Host** for messaging and in graphics where space is an issue. Host on which the Security Analytics Server resides. The Security Analytics Server contains the User Interface and Service Management Service (SMS). When you are updating to a new version, the Security Analytics Server must be updated first. If you have a mixed-version Security Analytics deployment, the Security Analytics Server must have the latest version in your deployment. Depending on your deployment, you may host the following services on the Security Analytics Server host in addition to the Security Analytics server and SMS: • Event Source Management • Reporting Engine • Malware Analysis • IPDBExtractor • Incident Management • Broker
non-Security Analytics Server host	non-SA host	Any host in your Security Analytics deployment other than an Security Analytics Server Host. See **Security Analytics Server Host**.

Primary Security Analytics Server	Primary SA Host	Security Analytics Server that you designate as primary. This is the Security Analytics Server host that you must update first in a multi-SA Server-host deployment. You use the Primary Security Analytics Server to monitor all the hosts in your Security Analytics deployment. See Multiple Security Analytics Server Deployment.
Secondary Security Analytics Server	Secondary SA Host	Any Security Analytics Server not designated as primary in a multi-Security Analytics Server deployment. You must update Secondary Security Analytics Servers after you update the primary Security Analytics Server. Secondary Security Analytics Servers help you balance the Security Analytics load of activity to improve performance. Each Secondary Security Analytics Server manages a standalone subset of Security Analytics functionality (that is services) to improve performance. See Multiple Security Analytics Server Deployment.

Note: Refer to the *RSA Security Analytics Virtual Host Setup Guide* for instructions on how to deploy Security Analytics hosts in a virtual environment.

Basic Deployment Process

Before you can deploy Security Analytics 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 Security Analytics deployment.

Process

The components and topology of a Security Analytics network can vary greatly between installations, and should be carefully planned before the process begins. As part of your initial planning you need to:

- Consider Site Requirements and Safety.
- Review the Deployment: Network Architecture and Ports.
- Examine specialized deployment considerations such as multiple Security Analytics Server hosts, support of group aggregation on Archivers and Concentrators, and virtual hosts.

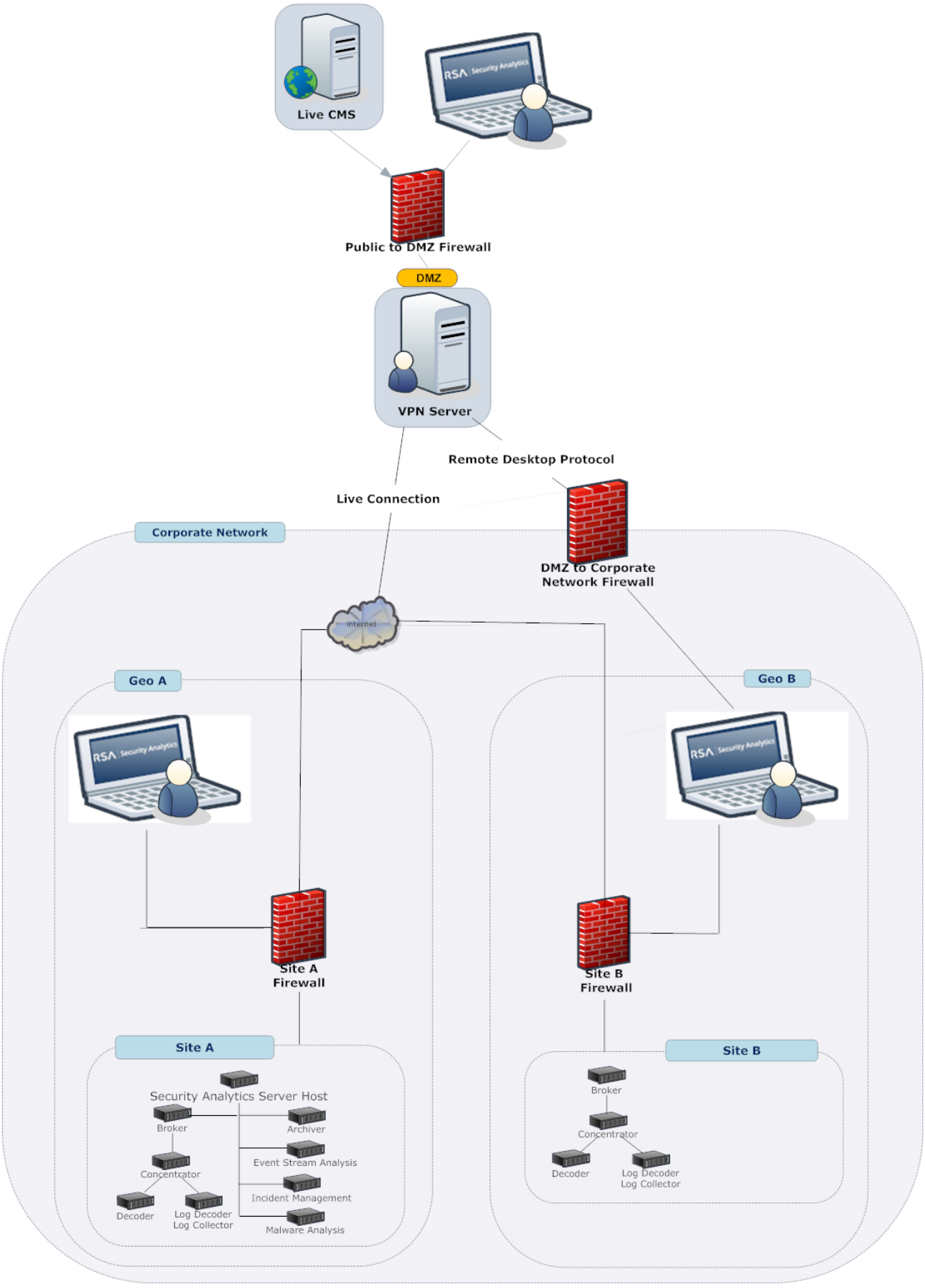
When ready to begin deployment, the general sequence is:

1. Install appliances and connect to the network as described in the Hardware Setup Guides.
2. Set up licensing for Security Analytics as described in the Security Analytics Licensing Guide.
3. Configure individual appliances and services as described in *RSA Security Analytics Host and Services Configuration Guide*. These guides also describe the procedures for applying updates and preparing for version upgrades.

Note: When updating appliance hosts and services, follow recommended guidelines under the "**Update Hosts in Correct Sequence**" topic in the *RSA Security Analytics Host and Services Configuration Guide*.

Security Analytics Deployment Diagram

The following diagram illustrates a basic, multi-site Security Analytics Deployment.


Live CMS
Public to DMZ Firewall
DMZ
VPN Server
Remote Desktop Protocol
Live Connection
DMZ to Corporate Network Firewall
Corporate Network
Internet
Geo A
Geo B
Site A Firewall
Site B Firewall
Site A
Site B
Security Analytics Server Host
Broker
Archiver
Concentrator
Event Stream Analysis
Incident Management
Decoder
Log Decoder
Log Collector
Malware Analysis
Broker
Concentrator
Decoder
Log Decoder
Log Collector

Multiple Security Analytics Server Deployment

Warning: Customers must contact Customer Care and arrange for a Professional Services Engagement to Deploy Multiple Security Analytics Servers.

You deploy multiple Security Analytics Servers to minimize risk of a single point of failure in your deployment. Multiple Security Analytics Servers can also limit the downtime you would experience in a single Security Analytics Server deployment. Finally, a multiple Security Analytics Server deployment helps you distribute the load of Security Analytics activity resulting in improved performance.

Sample Use Cases

The following use cases improve Security Analytics performance for high-volume, multi-site, deployments that are made up of a large number of hosts and services.

Improve Investigation Efficiency - Designate one or more Secondary Security Analytics Servers to handle Investigation to speed up investigations, data export, and reporting.

Eliminate Single Point of Failure - Deploy multiple Security Analytics Servers (that is, a Primary Security Analytics Server and Secondary Security Analytics Servers) to continue some or all Security Analytics activity if a Security Analytics Server fails. For example, you can send the packets and logs you collect to multiple Secondary Security Analytics Servers and if one fails, you will not lose any data.

Segregate User Interface Functionality - Similar to the Improve Investigation Efficiency use case, designate one or more Secondary Security Analytics Servers to handle individual Security Analytics functions for which you want to improve performance.

Components

If you deploy multiple Secondary Security Analytics Servers, you must determine which Secondary Security Analytics Server is the Primary Server and which Secondary Security Analytics Servers are the Secondary Servers.

Note: You must perform all administrative functions from Primary Security Analytics Server because secondary Security Analytics Servers perform a subset of all the Security Analytics functions or even a single function.

Primary Security Analytics Server

The Primary Security Analytics Server has all the functionally including:

- Fully functional Hosts view including the version update functionality.
- Access to Health & Wellness views.
- Full use of the trusted connections feature.

Secondary Security Analytics Servers

Secondary Security Analytics Servers can be in offline and online mode. You can connect to Security Analytics through a secondary Security Analytics Server even if it is not designated as the Primary Security Analytics Server.

Secondary Security Analytics Servers improve performance (for example, Analysts can leverage designated Security Analytics Servers to improve Investigation and Reporting efficiency).

A Secondary Security Analytics Server has the following limitations:

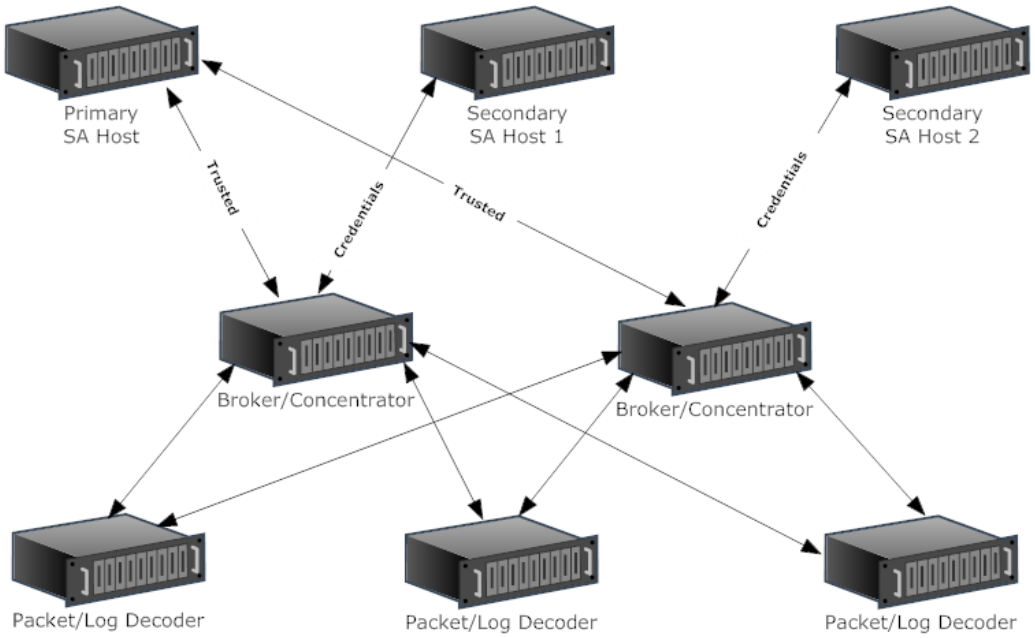
- The version update functionality on the Hosts view only applies to hosts connected to the Security Analytics Server using the trust model. Each Security Analytics Server can update itself and any core appliances connected to it using the trust model. See. the "**Apply Updates**" topic in the *RSA Security Analytics Host and Services Configuration Guide* for detailed instructions on how update a host to a new version.
- You cannot use the following features.
  - Health & Wellness views
  - Trusted connections feature
  - Event Source Management
  - Incident Management
- You cannot modify rules.

Sample Deployment Eliminating Single Point of Failure

The following diagram illustrates how a multiple Security Analytics Server deployment that eliminates a single point of failure.

The communication connections between the:

- Primary Security Analytics Server Host and the non-SA Server Hosts are trusted connections.
- Secondary Security Analytics Server Hosts and the non-SA Server Hosts required login credentials.


Primary
SA Host
Secondary
SA Host 1
Secondary
SA Host 2
Trusted
Credentials
Trusted
Credentials
Broker/Concentrator
Broker/Concentrator
Packet/Log Decoder
Packet/Log Decoder
Packet/Log Decoder

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

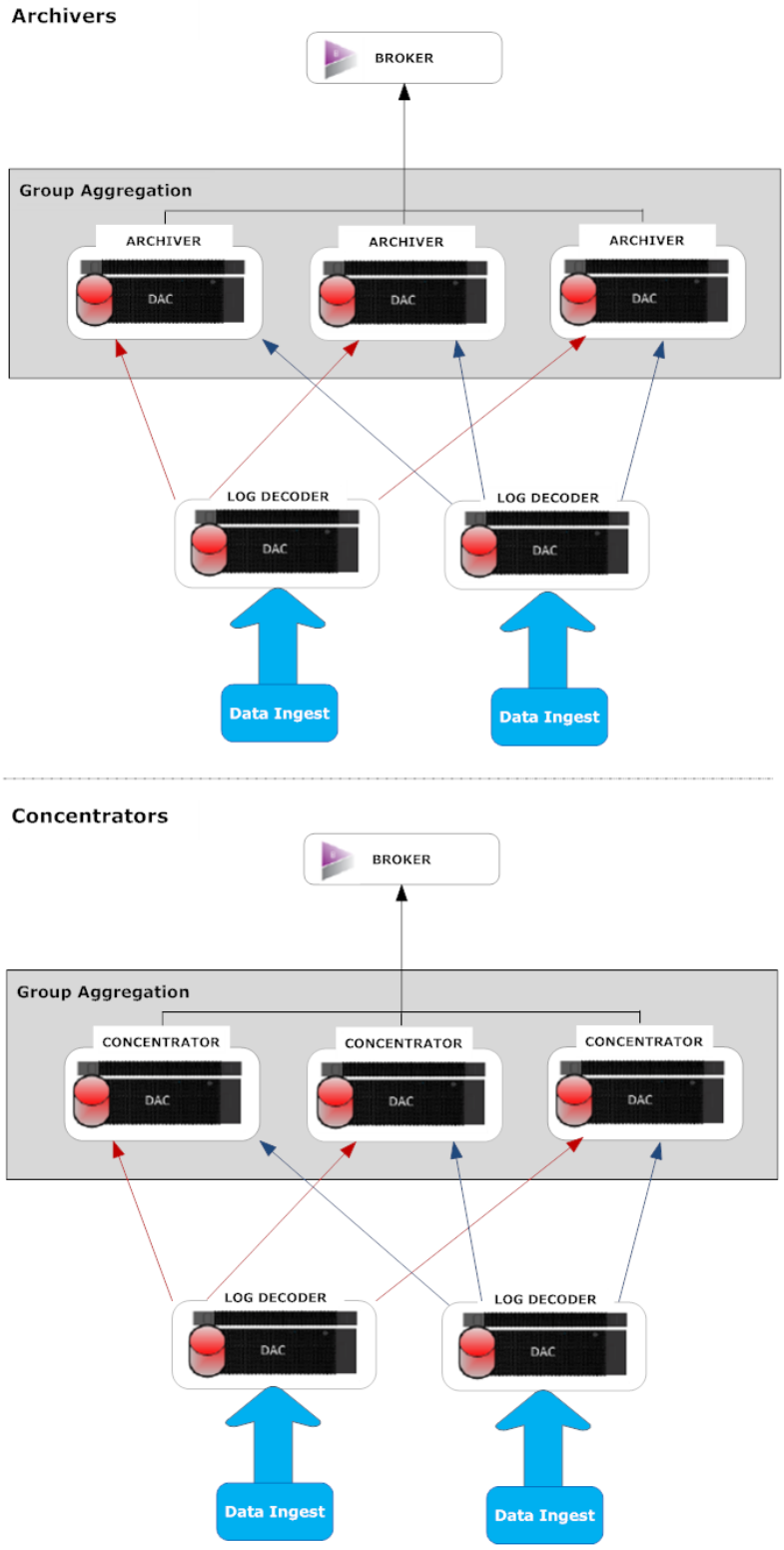
Advantages of Using Group Aggregation

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.

Note: To achieve the best performance, the total amount of data stored on the group of nodes should not increase compared to the amount of data stored on the original nodes. For example, if you had one node at 90% capacity then created a three-node group, and all three nodes were at 90% capacity, you would increase the storage, but the performance gain would be minimal.

The following diagram illustrates Group Aggregation.


Archivers
BROKER
Group Aggregation
ARCHIVER
ARCHIVER
ARCHIVER
DAC
DAC
DAC
LOG DECODER
LOG DECODER
DAC
DAC
Data Ingest
Data Ingest
Concentrators
BROKER
Group Aggregation
CONCENTRATOR
CONCENTRATOR
CONCENTRATOR
DAC
DAC
DAC
LOG DECODER
LOG DECODER
DAC
DAC
Data Ingest
Data Ingest

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.

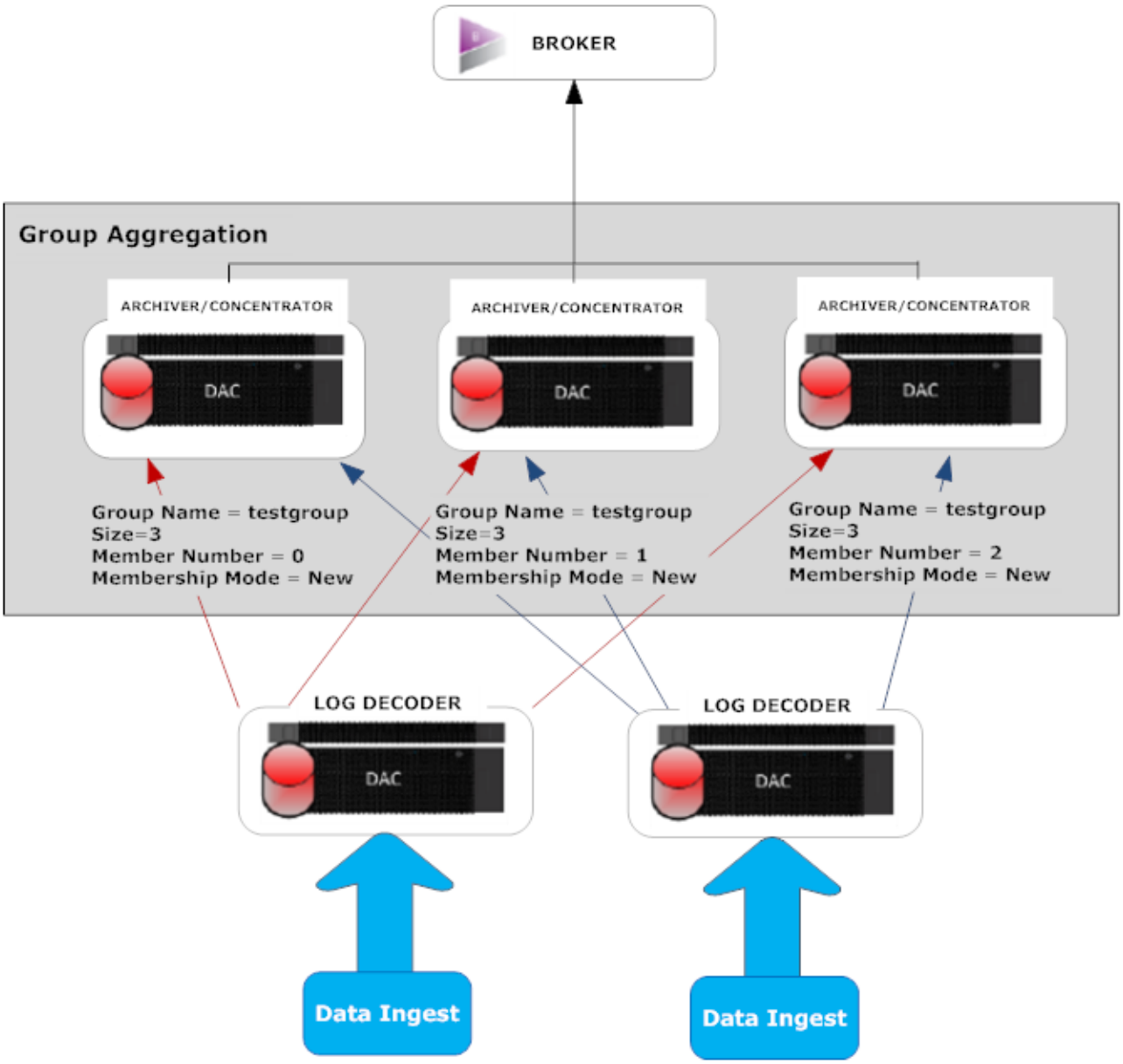
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

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.

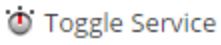


Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

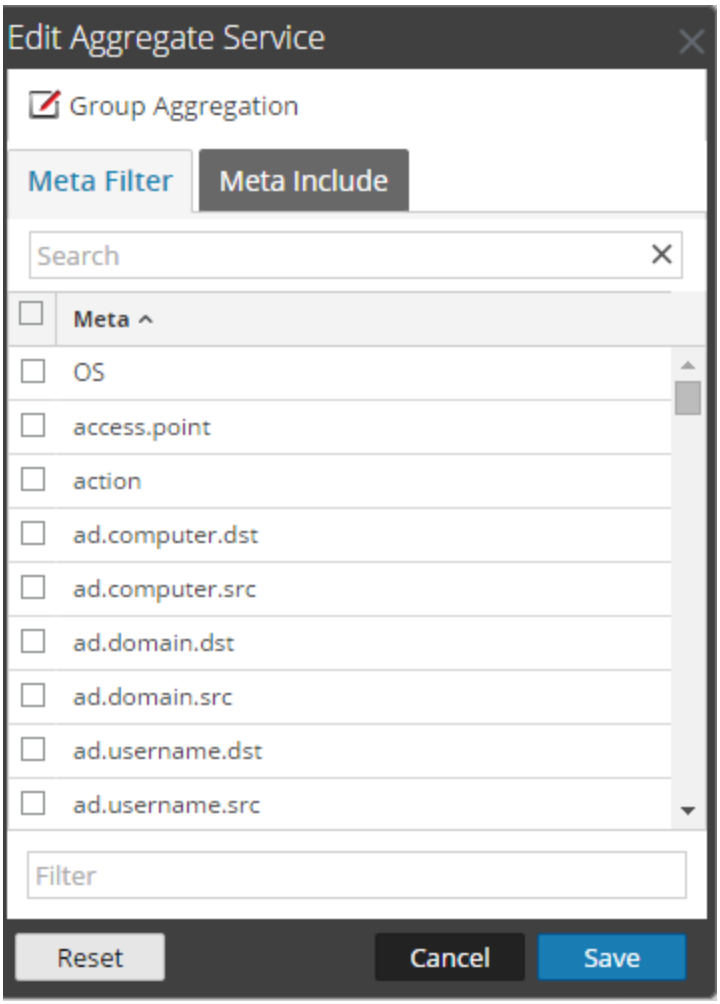
Parameter	Description
Group Name	It determines the group to with the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All 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	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: New and Replace. 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:** 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.

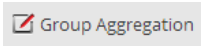
Set up Group Aggregation

Complete the following procedure to set up group aggregation.

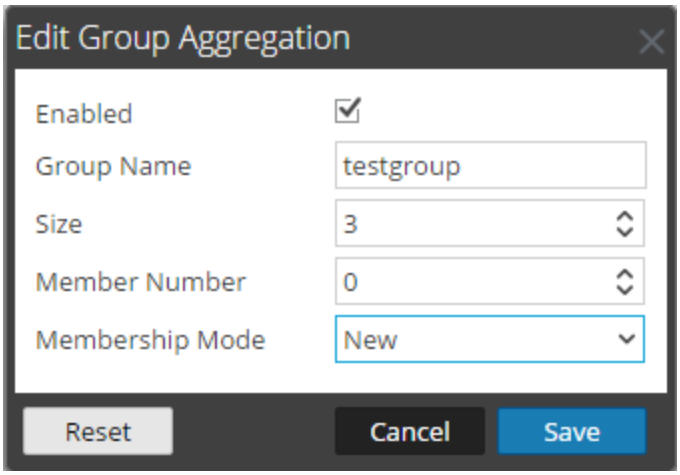
1. Configure multiple Archiver or Concentrator services in your environment. For instructions, see the "**Configure Archiver**"topic in the *RSA Security Archiver Configuration Guide* or "**Broker and Concentrator Configuration**" topic in the *RSA Security Analytics Broker and Configuration Guide*.
   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 **Security Analytics** menu, select **Administration > 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 

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:

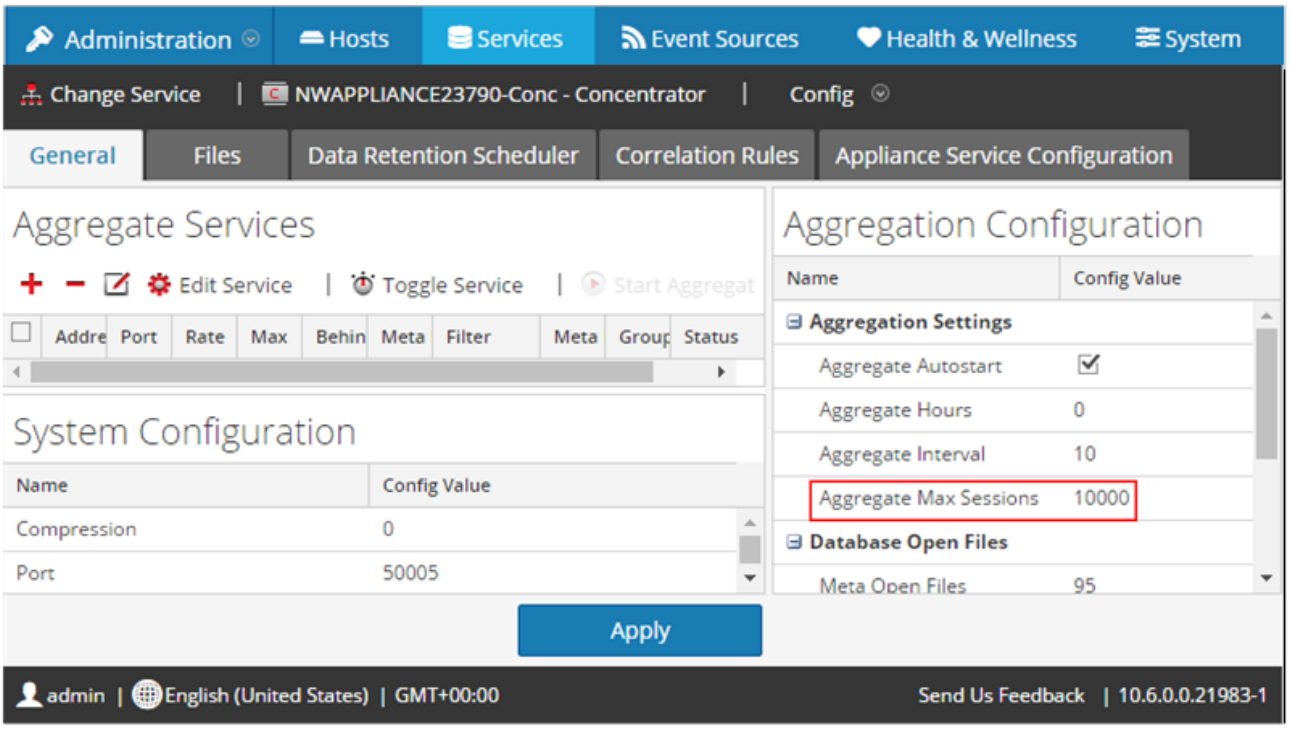
In the **Group Name** field, type the group name.
In the **Size** field, select the number of Archiver or Concentrator services in the aggregation group.
In the **Member Number** field, select the position of the Archiver or Concentrator in the aggregation group.
In the **Membership Mode** drop-down menu, select the mode.

h. Click **Save**.

i. In the 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 **Aggregate Max Sessions** parameter set to **10000**.



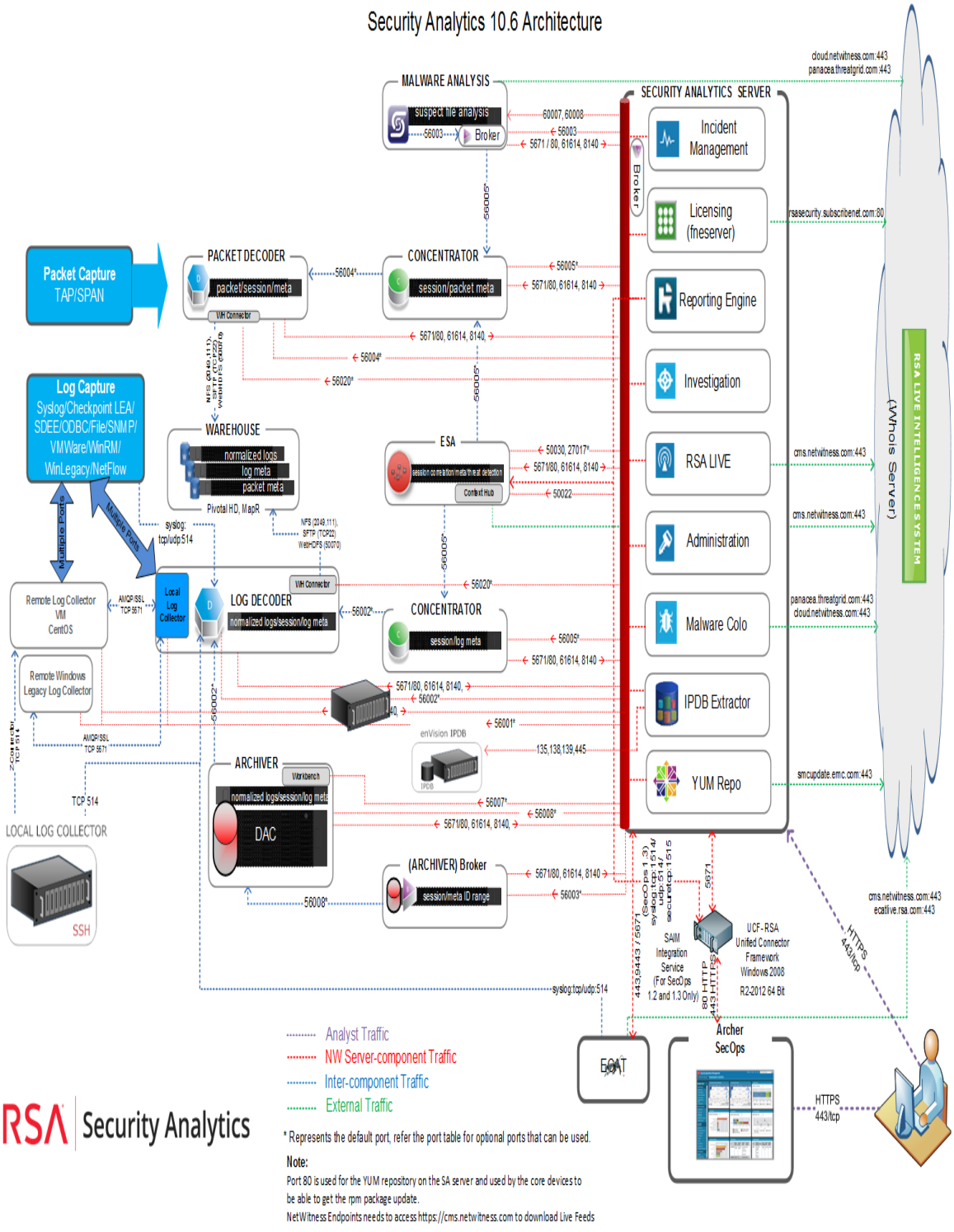
Deployment: Network Architecture and Ports

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

Security Analytics Network Architecture

The following diagram illustrates the Security Analytics network architecture with ports used for communications in Security Analytics 10.6.

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


Security Analytics 10.6 Architecture
MALWARE ANALYSIS
suspect file analysis
Broker
SECURITY ANALYTICS SERVER
Incident Management
Licensing (fneserver)
Reporting Engine
Investigation
RSA LIVE
Administration
Malware Colo
IPDB Extractor
YUM Repo
Broker
cloud.netwitness.com:443
panacea.threatgrid.com:443
rsasecurity.subscribenet.com:80
cms.netwitness.com:443
panacea.threatgrid.com:443
cloud.netwitness.com:443
smcupdate.emc.com:443
RSA LIVE INTELLIGENCE SYSTEM
(Whois Server)
Packet Capture
TAP/SPAN
PACKET DECODER
packet/session/meta
VIH Connector
CONCENTRATOR
session/packet meta
Log Capture
Syslog/Checkpoint LEA/
SDEE/ODBC/File/SNMP/
VMWare/WinRM/
WinLegacy/NetFlow
WAREHOUSE
normalized logs
log meta
packet meta
Pivotal HD, MapR
ESA
session correlation meta threat detection
Context Hub
Multiple Ports
Multiple Ports
syslog: tcp/udp:514
Remote Log Collector
VM
CentOS
AMQP/SSL TCP 5671
Local Log Collector
LOG DECODER
normalized logs/session/log meta
CONCENTRATOR
session/log meta
Remote Windows Legacy Log Collector
AMQP/SSL TCP 5671
TCP 514
LOCAL LOG COLLECTOR
SSH
ARCHIVER
Workbench
normalized logs/session/log meta
DAC
(ARCHIVER) Broker
session/meta ID range
enVision IPDB
IPDB
135,138,139,445
syslog:tcp/udp:514
SAIM Integration Service (For SecOps 1.2 and 1.3 Only)
UCF-RSA Unified Connector Framework Windows 2008 R2-2012 64 Bit
443,9443 / 5671 (SecOps 1.3) syslog:tcp:514/ secure tcp:1515
5671
80 HTTP 443 HTTPS
HTTPS 443/tcp
cms.netwitness.com:443
ecative.rsa.com:443
Archer SecOps
HTTPS 443/tcp
EOAT
Analyst Traffic
NW Server-component Traffic
Inter-component Traffic
External Traffic
RSA Security Analytics
* Represents the default port, refer the port table for optional ports that can be used.
Note:
Port 80 is used for the YUM repository on the SA server and used by the core devices to be able to get the rpm package update.
NetWitness Endpoints needs to access https://cms.netwitness.com to download Live Feeds

Security Analytics Host and Service Ports

In versions prior to Security Analytics 10.4, an administrator was able to use the native protocol for fast non-SSL communications like aggregation and REST API for SSL between Security Analytics and the hosts. All communications from Security Analytics moved from REST API to the native Security Analytics Core ports. As a result a second native Security Analytics Core port per host service was added so that administrators can enable secure (SSL) network communications while still being able to use non-secure (HTTP and Security Analytics Core (native)) connectivity methods for communication between services on the same system. Administrators can toggle the ports on and off to support only SSL, only non-SSL, or both.

The following table lists the Security Analytics hosts and their respective service ports:

From Host	To Host	To Ports (Protocol)	Comments
Any host	Security Analytics Server	80 (TCP)	Yum/HTTP: All SA hosts receive RPM package updates from Yum repository located in Security Analytics Server over HTTP. This is a two-way communication from any host to the Security Analytics Server.
Any host	Security Analytics Server	8140 (TCP)	Puppet-master.HTTPS: All communication from any host to the Security Analytics Server (Puppet master) is over HTTPS.
Any host	Security Analytics Server	61614 (STOMP/TCP)	rabbitmq-server (Mcollective/STOMP): All communication from any host to the Security Analytics Server (rabbitmq-server) is over Mcollective/STOMP.
Security Analytics Server	Any host	5671 (AMQPS/TCP)	rabbitmq-server(RabbitMQ/AMQPS): All communication from Security Analytics server (rabbitmq-server) to any host is over RabbitMQ/AMQPS. **Note:** Port 5671 must be open both ways between the SA Server and the other hosts for version updates.

From Host	To Host	To Ports (Protocol)	Comments
Security Analytics Server	Log Decoder	56002 (SSL / TCP)	50002 (non-SSL / TCP) 50102 (REST / TCP) - For Security Analytics 10.3 and earlier only
Security Analytics Server	Broker	56003 (SSL / TCP)	50003 (non-SSL / TCP) 50103 (REST / TCP) - For Security Analytics 10.3 and earlier only
Security Analytics Server	Concentrator	56005 (SSL / TCP)	50005 (non-SSL / TCP) 50105 (REST / TCP) - For Security Analytics 10.3 and earlier only
Security Analytics Server	Packet Decoder	Service: 56004 (SSL / TCP)	50004 (non-SSL / TCP) 50104 (REST / TCP)
Security Analytics Server	Log Collector (Local, Remote and Windows Legacy)	56001 (SSL / TCP)	50001 (non-SSL / TCP) 50101 (REST / TCP) - For Security Analytics 10.3 and earlier only
Security Analytics Server	Archiver	56008 (SSL / TCP)	50008 (non-SSL / TCP) 50108 (REST / TCP)
Security Analytics Server	ESA	50030 (SSL / TCP) 27017 (SSL / TCP) (Default)	27017 is for one ESA host only.
Security Analytics Server	ESA - Context Hub	50022 (SSL / TCP)	
Security Analytics Server	Malware (Malware-colocated on Security Analytics Server)	60007 (TCP)	
Security Analytics Server	Reporting Engine (rsa-re on Security Analytics Server)	51113 (SSL / TCP)	

From Host	To Host	To Ports (Protocol)	Comments
Security Analytics Server	Incident Management (rsa-im on Security Analytics Server)	50040 (TCP)	
Security Analytics Server (IPDB Extractor)	enVision IPDB	135,138,139,445 (TCP / UDP)	
Security Analytics Server	IPDB Extractor	56025 (SSL / TCP)	50025 (non-SSL / TCP) 50125 (REST / TCP)
Security Analytics Server	Warehouse Connector (on Packet Decoder/Log Decoder)	56020 (SSL)	50020 (non-SSL) 50120 (REST)
Security Analytics Server	ECAT	443 (TCP)	
Security Analytics Server	Host Service (Log Decoder, Packet Decoder, Concentrator, Broker, Warehouse Connector, Archiver,)	56006 (SSL / TCP)	50006 (non-SSL / TCP) 50106 (REST / TCP) - For Security Analytics 10.3 and earlier only
Security Analytics Server	Workbench (Archiver)	56007 (SSL / TCP)	50007 (non-SSL / TCP) 50107 (REST / TCP)
Security Analytics Server	Audit Log Syslog Receiver This can be a third-party syslog receiver or a Log Decoder	514 (TCP / UDP)	Required only if SA audit logs are sent to Log Decoder/third-party syslog receiver to be parsed.

From Host	To Host	To Ports (Protocol)	Comments
Security Analytics Server	cms.netwitness.com	443, 80 (TCP)	RSA LIVE content
Security Analytics Server	smcupdate.emc.com	443 (TCP)	RSA Update Repo to Local Update Repo
Concentrator	Packet Decoder	56004	
Concentrator	Log Decoder	56002	
Broker	Concentrator	56005	
Broker	Archiver	56008	
Archiver	Log Decoder	56002	
ESA	Concentrator	56005	
ESA	RSA LIVE Whois Server	443	
Malware	Broker	56003	
Warehouse Connector	Warehouse	NFS (2049,111), SFTP (TCP22) WebHDFS (50070)	
In the Pull mode: Log Collector (on Log Decoder)	Virtual Log Collector Windows Legacy Collector	5671 (TCP)	:
In the Push Mode: Virtual Log Collector Windows Legacy Collector	Log Collector (on Log Decoder)	5671 (TCP)	

From Host	To Host	To Ports (Protocol)	Comments
enVision Local Collector	Remote Collector (VM)	514 (TCP)	
enVision Local Collector	Log Decoder	514 (TCP)	
ECAT	Log Decoder	514 (TCP/UDP)	
ECAT	Security Analytics Server	5671 (TCP)	ECAT alerts are sent to SAIM on this port.
Security Analytics Server (RE alerts, ESA and Business Context Live Feeds)	Archer SecOps 1.3	Security Analytics Server To UCF:syslog 1514 (TCP)/ 514 UDP/ 1515 STCP UCF to Archer Sec Ops : 80/ 443 Security Analytics Server to UCF:9090 HTTP / 8443 HTTPS (Business context live feeds)	.

From Host	To Host	To Ports (Protocol)	Comments
Security Analytics Server (IM alerts)	Archer SecOps 1.2/1.3	SAIM Integration Service to on Security Analytics Server : 5671 SAIM Integration Service to Archer Sec Ops: 80/ 443	SAIM Integration service is present on UCF and integrates with SecOps 1.3 and 1.2.
Security Analytics-Web Browser	Security Analytics Server UI	443 (HTTPS)	
External	All hosts	22 (TCP)	SSH provides shell access to the device, for emergency host management. On hosts with the LogCollector installed, ssh provides sftp and scp support for devices that upload log files for consumption by Security Analytics.

Note: When you update to a new version, open firewall ports 8140 and 61614 from all non-Security Analytics Server hosts to Security Analytics Server so that the Security Analytics Server can discover all of your non-Security Analytics Server hosts and services.

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.