

RSA NetWitness

Version 11.7

Security Configuration Guide



Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

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

March 2022

Contents

Security Configuration Guide Overview	7
Security Configuration Settings	8
Access Control Settings	9
User Authentication	10
Multi-Factor Authentication	10
NetWitness Platform Core Trusted Connection	10
User Accounts	10
Configuring New Accounts	11
Authentication Configuration	11
User Passwords	12
NetWitness Users	12
NetWitness Core Service Users	12
Security Parameter Settings	12
Kibana Health and Wellness Interface	13
User Authorization	14
Access Roles	14
Component Authentication	15
Host Configuration and Service Authentication	15
Changing Credentials for Default Configuration Service Accounts	15
Configuring Live Account Authentication	16
Configuring Lockbox Authentication	16
Change Root Account Password On All NW Hosts	16
Display Logon Banner for Remote SSH Connections	16
Secure Boot Loader	17
Disable Interactive Startup	17
Log Settings	18
Log Description	18
Log Management and Retrieval	18
Communication Security Settings	20
Port Usage	20
NetWitness Network Architecture Diagram	21
NetWitness Network (Packets) Architecture Diagram with Ports	22
NetWitness Logs Architecture Diagram with Ports	23
Event Stream Analysis Network (Packets) Architecture Diagram with Ports	24
Event Stream Analysis (Logs) Architecture Diagram with Ports	25

NetWitness Firewall Requirements Summary	26
Comprehensive List of NetWitness Host, Service, and iDRAC Ports	30
NW Server Host (Primary and Warm Standby NW Server Host)	31
Analyst UI Host	32
Archiver Host	33
Broker Host	34
Concentrator Host	35
Endpoint Log Hybrid	36
Endpoint Relay Server	37
Event Stream Analysis (ESA) Host	38
New Health and Wellness	39
New Health and Wellness on Different Subnet	39
iDRAC Ports	40
Log Collector Host	41
Log Decoder Host	42
Log Hybrid Host	43
Log Hybrid - Retention Host	44
Malware Host	45
Network Decoder Host	46
Network Hybrid Host	47
UEBA Host	48
NetWitness Endpoint Architecture	49
NetWitness Endpoint 4.4 Integration with NetWitness Platform	50
NetWitness Endpoint Architecture with Ports	50
How to Change UDP Port for Endpoint Log Hybrid	51
Task 1 - Tell All Agents to Use a New UDP Port	51
Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment	51
Network Encryption	53
NetWitness Platform Web Server Communications	53
Reporting Engine, ESA and Warehouse Connector : External Communication	53
Log Collector Service	53
Enabling HTTPS on REST Interfaces for Core Services	55
Data Security Settings	56
Securing Data	56
Data Privacy	56
Default Storage Passwords	57
Alert System Settings	58
FIPS Compliance	59
NetWitness Platform Components working in FIPS mode	59

Common Criteria Compliance	60
Disabling Unencrypted Ports For NetWitness Core Services	60
STIG Compliance	61
Overview	61
STIG Limits Account Access	61
Other Security Considerations	62
Changing the RabbitMQ Management Password for Windows Legacy Collectors	62
Hardening the NetWitness Platform Core service	63
Example:	63
NFS Access Controls	64
Secure Deployment and Usage Settings	66
Security Controls Map	67
Secure Enclave	67
Secure Deployment Guidelines	68
Firewall Rules	69
DMZ to Corporate Network	69
Corporate Network to Site	69
Site to Site	70
Live CMS to DMZ	70
RSA Download Central to DMZ	70
External Email Server to DMZ	71
Syslog Server to Site	71
SNMP Server to Site	71
Secure Deployment Settings	72
Secure Maintenance	73
Security Patch Upgrade	73
Security Patch Management	73
Virus Scanning	73
Ongoing Monitoring and Auditing	73
Hardware Replacement	74
Physical Security Controls Recommendations	75
Supporting Users	76
Preventing Social Engineering Attacks	76
Confirming User Identities	76
Advice for Your Users	77
Appendix A: Customer Provided Certificates	78
Appendix B: Reissue Certificates	80
Introduction	80

CA Certificate Reissue	80
Service Certificate Reissue	80
Reissuing Service Certificate	81
When to Use the --host-key Argument	82
cert-reissue Arguments and Options for All Hosts	82
When to Use the Individual Host Arguments (--host-id <id>, --host-name <display-name>, --host-addr <ip/hostname>)	83
cert-reissue Arguments and Options for a Single Host	84
Reissuing Certificates for All Hosts Except Windows Legacy Collection (WLC) host	85
Running the Cert-Reissue Command for All Hosts	85
Running the Cert-Reissue Command for an Individual Host	85
Reissuing Certificates for a WLC Host	85
Successful Reissue Summary Report	86
Unsuccessful Reissue Summary Reports	86
Reissue Failed for Host and Aborted Command	86
Reissue Certificate Partially Executed	86
Appendix C. Troubleshooting Cert-Reissue Command	87
Argument Options Used for Troubleshooting	87
Problems and How to Troubleshoot Them	88

Security Configuration Guide Overview

This guide provides information about the security configuration settings and security best practices for NetWitness.

This guide applies to NetWitness version 11.0 or later. There will be periodic updates made to the content.

Anyone using this guide should possess experience as a network engineer, equivalent to at least that of a journeyman, and also have a strong understanding of network concepts and TCP/IP communications.

Security Configuration Settings

This topic describes information about various security configuration settings that are designed to help you securely operate RSA NetWitness.

You can adjust the following security configuration settings:

- Access Control Settings
- Log Settings
- Communication Security Settings
- Data Security Settings
- Alert System Settings
- Other Security Considerations

Access Control Settings

Access control settings are designed to enable the protection of resources against unauthorized access or by external components.

- [User Authentication](#)
- [User Authorization](#)
- [Component Authentication](#)

User Authentication

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing RSA NetWitness.

Multi-Factor Authentication

You can set up Multi-Factor Authentication (MFA) for NetWitness using one of the following methods:

- ADFS Log in to NetWitness with SecurID Passcode
- PAM SecurID Log in to NetWitness for AD Users

For more information, see "Set Up Multi-Factor Authentication" and "Set Up Single Sign-On Authentication" in the *System Security and User Management Guide*.

NetWitness Platform Core Trusted Connection

NetWitness Core 11.3 or later has the ability to connect and authenticate over SSL without having to provide user account information on the service itself. This feature is only available over the native port and not the REST interface. For more information on trusted connection, see *Host and Services Getting Started Guide*. Go to the [NetWitness Documents - All Versions](#) to find all RSA NetWitness Platform 11.x documents.

User Accounts

The following table identifies the default RSA NetWitness user roles including the Administrator (admin) account and several service accounts. When deploying, you must enter a password for the System Administrator account and all the service accounts. For more information on passwords and password strength, see "Settings Tab" in the *System Security and User Management Guide*.

Note: Custom roles can be added as required. For instructions, see "Add a Service User Role" in the *Host and Services Configuration Guides*.

User Roles	Description
Administrators	Full system access
Operators	Access to configurations but not to metadata and session content.
Analysts	Access to metadata and session content but not to configurations.
SOC_Managers	Same access as Analysts plus additional permission to handle incidents.
Malware_Analysts	Access to malware events and to metadata and session content.

User Roles	Description
Data_Privacy_ Officers	Access to metadata and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).
Respond_ Administrator	Access to all Respond server and Incidents permissions.
UEBA_ Analysts	Access to the User and Entity Behavior Analytics (UEBA) service in the Investigate > Users view. UEBA is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all entities in your network environment.
	<div style="border: 1px solid green; padding: 5px;"> <p>Note: You do not need to set up specific permissions for this role. You only need to assign this role to a user, and that user will have access to UEBA.</p> </div>

Configuring New Accounts

Each RSA NetWitness user must have an account to log on to the UI. For more information on how to add new user accounts, see "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Caution: RSA recommends that you ensure that users are approved by the company for logging on to the system before creating an account for them. Even if users are approved, RSA recommends that you only assign the minimum set of access permissions that enable the users to perform their jobs.

Authentication Configuration

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing NetWitness. For more information, see "Set Up System Security" in the *System Security and User Management Guide*.

Below are recommendations for some of the configurations:

- **Default System Administrator Account:** RSA recommends that you instruct RSA NetWitness administrators on your corporate IT policy and security best practices to generate and manage passwords for the default System Administrator account. RSA recommends that you change the default System Administrator password and the admin passwords for the service accounts per your company's password policy. For more information on password strength settings, see "Password Strength" in the *System Security and User Management Guide*. You should change the System Administrator password using the Admin user preferences. For instructions on how to change the password, see "Change the Default admin Passwords" in the *System Security and User Management Guide*.
- **External Authentication:** RSA NetWitness supports external authentication. For more information, see "Configure External Authentication" in the *System Security and User Management Guide*.

User Passwords

NetWitness Users

Administrators can set the appropriate level of password strength for the user and can force users to change their passwords when password strength policy changes. Administrators can specify the global default user password expiration period and the notification period for the password expiry. For more information, see "Configure System-Level Security Settings" in the *System Security and User Management Guide*.

The following table shows the default security parameters settings for passwords.

Caution: RSA recommends that you change these settings in accordance with your corporate policy. Users must ensure the idle period and session time-out is specified.

Parameter	Default Setting
Global Default User Password Expiration Period	0
Notify User <n> Days Prior to Password Expiry	5

NetWitness Core Service Users

Administrators can change the password of a service user and replicate the new password to all the NetWitness Core services with the defined user account. For more information, see "Change a Service User Password" in the *Host and Services Configuration Guide*.

You can also change your password from the Preferences panel in the Profile view. For more information, see "User Preferences" in the *NetWitness Getting Started Guide*.

Security Parameter Settings

The following table shows the default security parameters settings.

Caution: RSA recommends that you change these settings in accordance with your corporate policy.

Parameter	Default Setting
Lockout Period	20 minutes
Idle Period	10 minutes
Session Timeout	480 minutes
Max Login Failures	5

For more information on security parameter settings, see "Configure System-Level Security Settings" in the *System Security and User Management Guide*.

Kibana Health and Wellness Interface

You can change the default password of the Kibana UI. For more information, see the "Changing Kibana Password" in the *System Maintenance Guide*.

User Authorization

User authorization settings are designed to control rights or permissions that are granted to a user for accessing a resource managed by RSA NetWitness.

Access Roles

RSA NetWitness allows you to create access roles that you can assign to users. Each access role is mapped to a list of user authorization settings.

For more information, see the following NetWitness topics:

- "Role Permissions" in the *Alerting Using ESA Guide*.
- "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Note: RSA NetWitness recommends that you review users' task permissions on a routine basis to ensure that each user is granted the correct task permissions.

RSA NetWitness allows access roles to be assigned to users through external group membership or directly to user accounts. RSA recommends that you assign permissions through group membership and not assign permissions directly to user accounts. For more information, see "Map User Roles to External Groups" in the *System Security and User Management Guide*.

The user roles assigned also control permissions that are granted to accounts that need access to a specific component of NetWitness.

Component Authentication

This topic describes how component authentication settings control the process of verifying an identity claimed by an external or internal system or component.

Host Configuration and Service Authentication

When you install or upgrade to NetWitness 11.x, trusted connections are established by default with two settings:

1. SSL is enabled.
2. NetWitness is connected to core services using the encrypted SSL port.

RSA NetWitness allows secure authentication services for the following hosts as SSL is enabled by default:

- NetWitness Server
- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Archiver
- ESA
- Malware Analysis
- Endpoint
- UEBA

Note: By default all the services on the hosts have SSL enabled.

For more information, see the *Host and Service Configuration Guide*.

Changing Credentials for Default Configuration Service Accounts

For information on how to reset the password for an admin of the host service accounts, see "Users Tab" in the *Host and Services Configuration Guide*.

Note: The default user name of the host service accounts (admin) cannot be modified.

Configuring Live Account Authentication

RSA NetWitness supports secure authentication for the Live account connection to the Content Management System (CMS) as the SSL is enabled by default. The default communications port on the CMS is 443. For information on how to configure this setting, see "Configure Live Settings" in the *System Configuration Guide*.

Configuring Lockbox Authentication

Lockbox provides an encrypted file that Warehouse Connector or Log Collector uses to store and protect sensitive data. You need to create the lockbox by providing a lockbox password while configuring the Warehouse Connector or Log Collector for the first time. For more information on lockbox setup, see the following topics:

- "Log Collector - Set Up a Lockbox" in the *Log Collection Guide*.
- "Warehouse Connector - Create Lockbox" in the *Host and Services Configuration Guide*.

Change Root Account Password On All NW Hosts

You must change the default SSH root account password to a strong password in all the hosts in the NetWitness Deployment.

Display Logon Banner for Remote SSH Connections

RSA NetWitness allows you to customize the logon banner to display standard government or corporate warning signs for SSH remote connections to the hosts.

For example:

"This system is private. Use or misuse may be logged and invalid access pursued."

1. Log on to the appliance using root credentials.
2. Type `cd /etc/` to switch to the `/etc/` directory.
3. Edit the `/etc/issue.net` file with the required banner text.
4. Save the changes and exit.
5. Type `cd /etc/ssh` to switch to the `/etc/ssh` directory.
6. Edit the `/etc/ssh/sshd_config` file to remove the comment for the banner and provide the location of the banner text file (For example, `/etc/issue.net`).

The following file is an example of an `sshd.config` file before being modified:

```
# no default banner path
#Banner none
```

The following file is an example of an `sshd.config` file after being modified:

```
# no default banner
#Banner /etc/issue.net
```

7. Save the changes and exit.
8. Type `service sshd restart` in order to restart the `sshd` service.

Secure Boot Loader

A boot loader password is set to prevent unauthorized modification of boot menu entries. Change the default password to a strong password.

To change the boot loader password:

1. Run the `grub2-setpassword` command as root.

```
# grub2-setpassword
```

2. Enter and confirm the password:

```
Enter password:
```

```
Confirm password:
```

Disable Interactive Startup

To prevent users from starting up the system interactively, as root, disable the **PROMPT** parameter in the file:

```
"/etc/sysconfig/init"
```

```
PROMPT= no
```

Log Settings

A log is a chronological record of system activities that enables the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction.

Global Audit Logging provides NetWitness Auditors with consolidated visibility into user activities within NetWitness in real-time from one centralized location. NetWitness audit logs are collected in a centralized system that converts them into the required format and forwards them to an external syslog system. The external syslog system can be a third-party syslog server or a Log Decoder. For more information, see "Global Audit Logging Overview" in the *System Configuration Guide*.

Log Description

The following table shows the security-relevant logs provided by RSA NetWitness.

Component	Reference
Appliance and Service Logs	See the "Services Explore View" and "Services Logs View" in the <i>Host and Services Configuration Guides</i> and "Configure Log File Settings" in the <i>System Configuration Guide</i> .
Audit Logs	See "Configure Global Audit Logging" in <i>System Configuration Guide</i> .
Syslogs	See "Configure Syslog and SNMP Settings" in the <i>System Configuration Guide</i> .

Log Management and Retrieval

For more information on:

- Log settings, see "Configure Log File Settings" in the *System Configuration Guide*.

Note: RSA recommends that you set the maximum log file size in accordance to your corporate policy.

- Log forwarding, see "Set Syslog Forwarding" in the *Host and Services Configuration Guide*.
- Setting log overrides:
You may override the default logging levels if you want to include messages generated by specific modules.

Syntax: <module>=<level>

SDK-Language=none

Where level is one or more of "none|debug|info|warning|failure|audit|all", all options must be separated by a pipe |

none

and

all

are mutually exclusive with each other and all other options.

Overrides are useful for query auditing (that is, those modules that begin with SDK-) or for debugging by module (that is, Index). The following are the type of logs available :

- Data
- Engine
- Index
- Network
- Packet
- Parse
- Decoder
- Rules
- Concentrator
- Appliance
- SDK
- SDK-Query
- SDK-Values
- SDK-Language
- SDK-Info
- SDK-Session
- SDK-Timeline
- SDK-Content
- SDK-Search

Note: RSA recommends that you restrict permissions to the log files folder to the appropriate user.

Communication Security Settings

Communication security settings are designed to enable the establishment of secure communication channels between RSA NetWitness components, as well as between RSA NetWitness components and external systems or components.

Port Usage

To help ensure security, RSA recommends that you configure your firewall rules and access control lists to expose only the ports and protocols necessary for the operation of RSA NetWitness. The services, such as Reporting Engine, Respond Service, Malware, Log Collector, Live account, Broker, Concentrator, Decoder, and Log Decoder, use specific TCP ports to communicate with each other and the following:

- Web user client interfaces
- Live CMS
- LDAP synchronization
- Third-party email server
- NetWitness console

All communication from NetWitness uses the native NetWitness Core ports. The additional native NetWitness Core port per host allows an administrator to enable secure (SSL) network communications while still being able to use non-secure (HTTP and NetWitness Core native) connectivity methods for communication between services that are present on the same host system. Administrators can toggle the ports on and off to support only SSL, only non-SSL, or both.

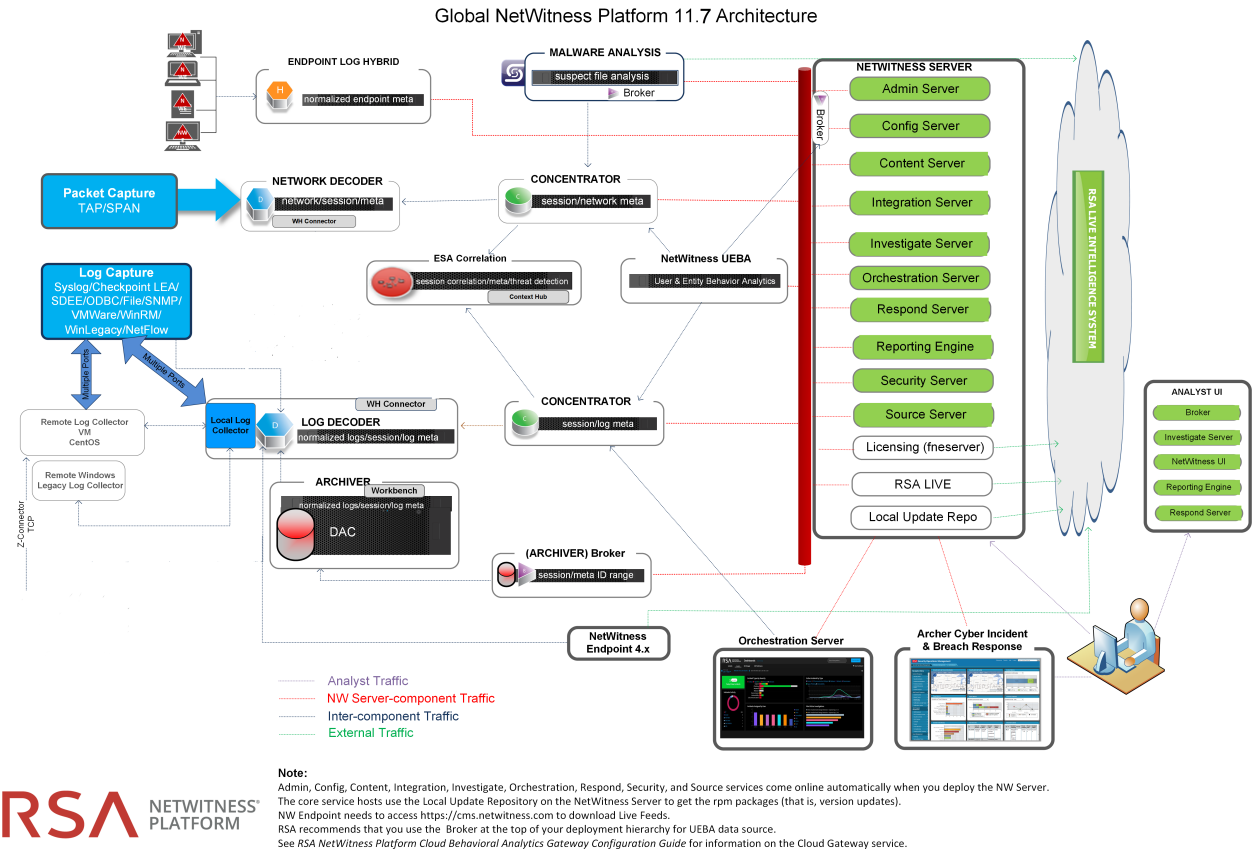
Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness deployment to communicate with each other.

For more information on individual Endpoint Architectural diagrams, see [NetWitness Endpoint Architecture](#) at the end of this topic.

Note: enVision Local Collector is not more supported in versions 11.x. Warehouse is supported from version 11.5 and earlier versions.

NetWitness Network Architecture Diagram

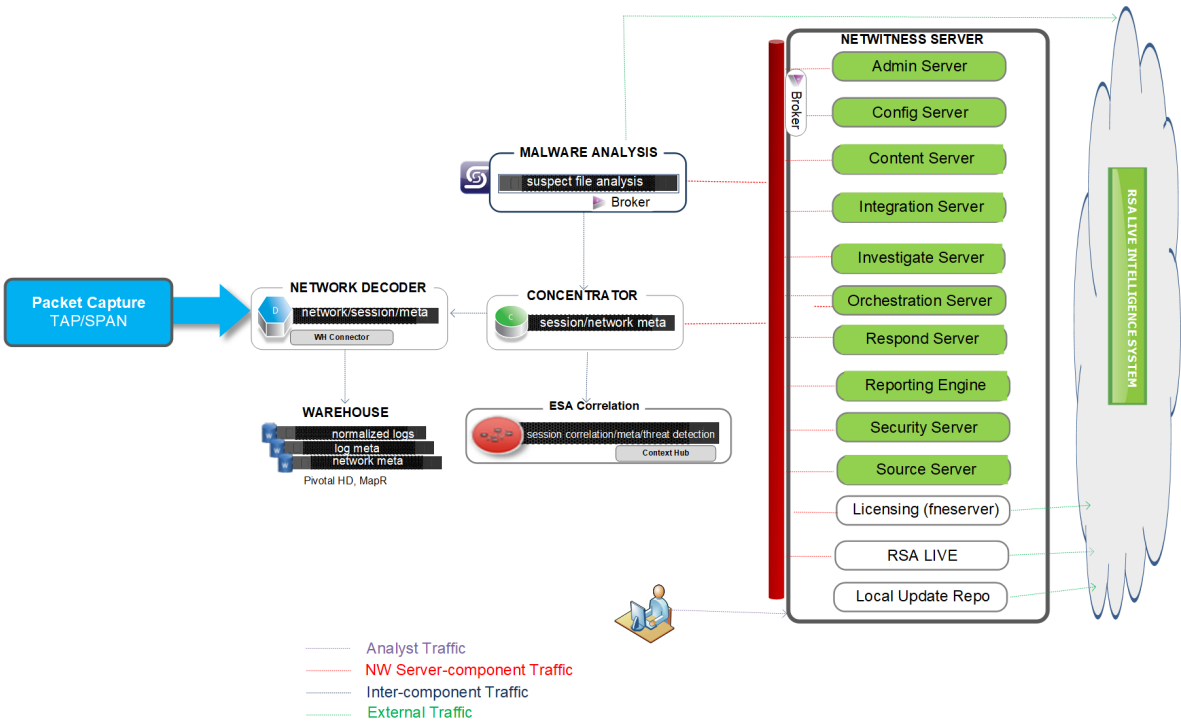
The following diagram illustrates the NetWitness network architecture including all of its component products.



Note: NetWitness core hosts must be able to communicate with the Netwitness Server through UDP port 123 for Network Time Protocol (NTP) time synchronization.

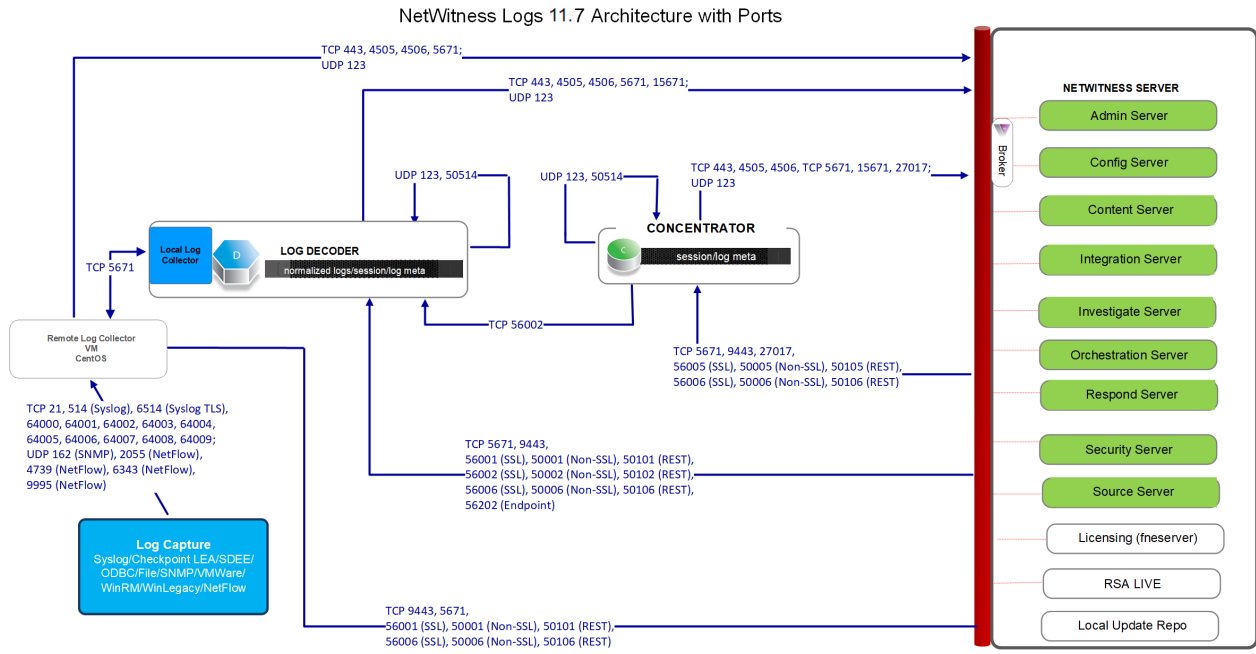
NetWitness Network (Packets) Architecture Diagram with Ports

NetWitness Network 11.7 Architecture



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

NetWitness Logs Architecture Diagram with Ports

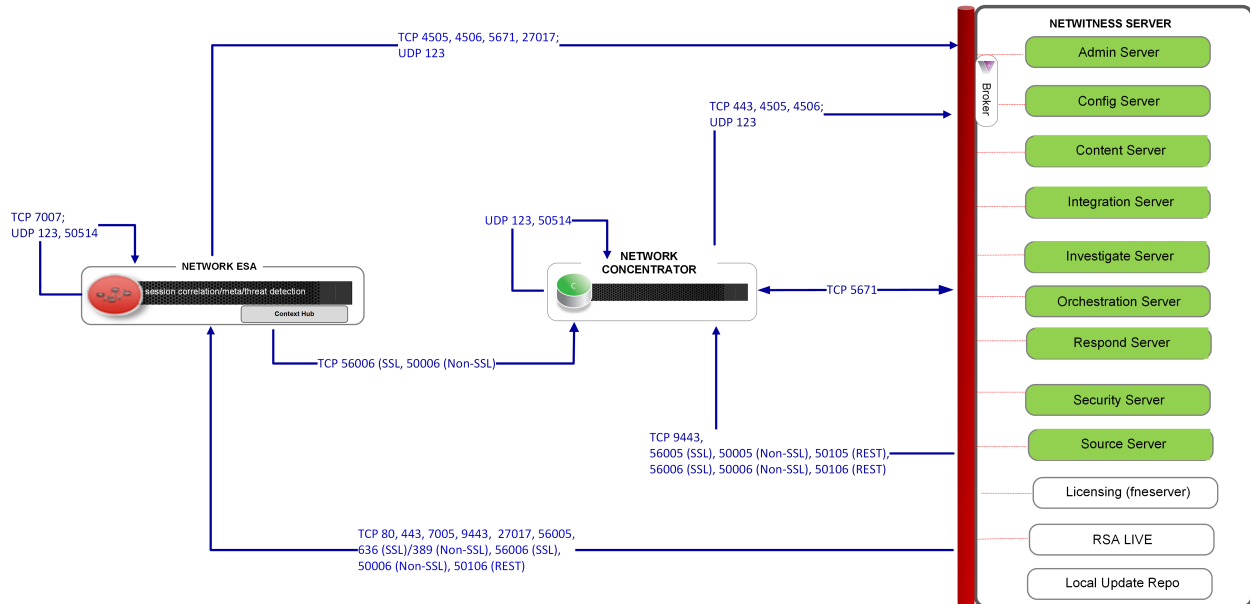


Note: Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

Event Stream Analysis Network (Packets) Architecture Diagram with Ports

The following diagram illustrates the Event Stream Analysis network architecture with packet capture.

Event Stream Analysis (ESA) Network 11.7 Architecture with Ports



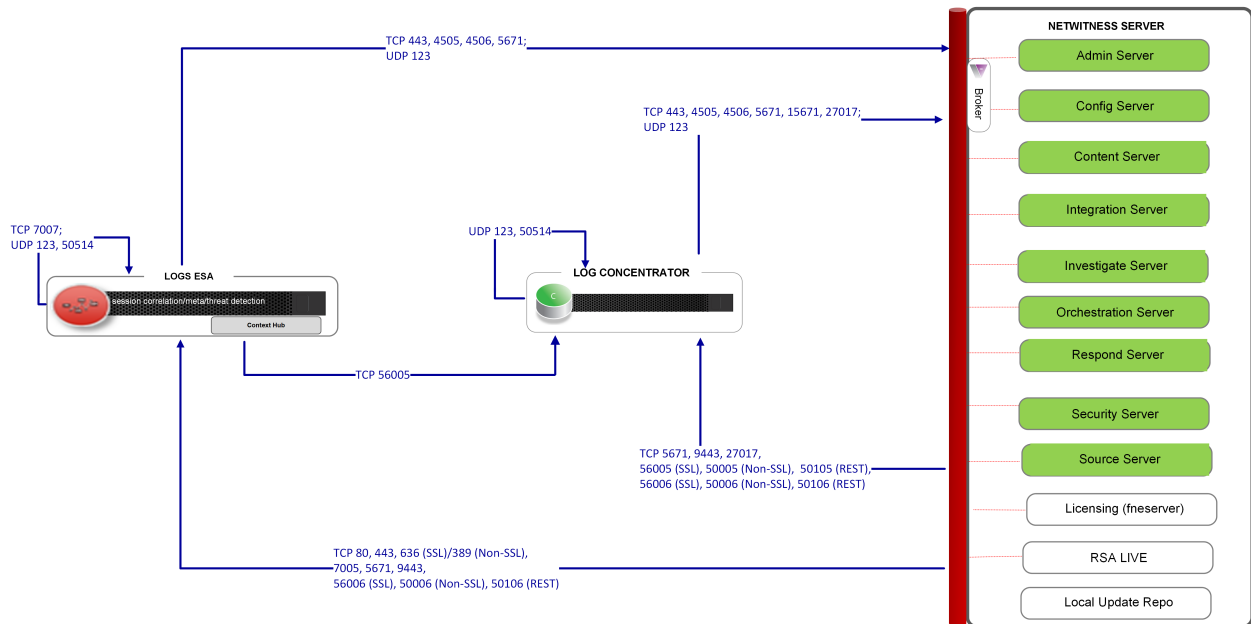
Notes:

Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates). Port 7005 is used by Context Hub as its HTTP port for REST calls, and is only installed on ESA Primary hosts.

Event Stream Analysis (Logs) Architecture Diagram with Ports

The following diagram illustrates the Event Stream Analysis network architecture with log collection.

Event Stream Analysis (ESA) Logs 11.7 Architecture with Ports



Note:
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates). Port 7005 is used by Context Hub as its HTTP port for REST calls, and is only installed on ESA Primary hosts.

NetWitness Firewall Requirements Summary

The following table lists all the ports that need to be open in your firewall by host.

Note: The "NW Server" host ports apply to both the Primary and Warm Standby NW Server. Synchronization between the Primary and Warm Standby is done through TCP Port 22.

Source Host	Destination Host	Ports
NW Server	ESA Primary	TCP: 22, 80, 443, 5671, 7005, 50030 (SSL), 50035 (SSL), 50036 (SSL) UDP: 123
NW Server	ESA	TCP: 22, 80, 443, 5671, 50035 (SSL), 50036 (SSL) UDP: 123
NW Server	Network Decoder	TCP: 22, 5671, 50004 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50106 (REST), 56004 (SSL), 56006 (SSL) UDP: 123
NW Server	Broker	TCP: 5671, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST) 56003 (SSL), 56006 (SSL) UDP: 123
NW Server	Concentrator (Network & Logs)	TCP: 22, 5671, 50005 (Non-SSL), 60006 (Non-SSL), 50105 (REST), 50106 (REST), 56005 (SSL), 56006 (SSL) UDP: 123
NW Server	Network Hybrid	TCP: 22, 5671, 50004 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50104 (REST), 50105 (REST), 50106 (REST), 56004 (SSL), 56005 (SSL), 56006 (SSL) UDP: 123
NW Server	Log Decoder	TCP: 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL) UDP: 123
NW Server	Log Hybrid	TCP: 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL) UDP: 123

Source Host	Destination Host	Ports
NW Server	Log Hybrid - Retention	TCP: 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL) UDP: 123
NW Server	Endpoint Log Hybrid	TCP: 22, 5671, 7050, 7054, 50001 (Non-SSL), 50002 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL), 56202 (Endpoint) UDP: 123
NW Server	VLC	TCP: 22, 5671, 50001 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50106 (REST), 56001 (SSL), 56006 (SSL) UDP: 123
NW Server	Archiver	TCP: 22, 514, 5671, 6514, 50006(Non-SSL), 50007 (Non-SSL), 50008 (Non-SSL), 50106 (REST), 50107 (REST), 50108 (REST), 56006 (SSL), 56007 (SSL), 56008 (SSL) UDP: 123, 514
NW Server	Malware	TCP: 22, 5671, 5432, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST), 56003 (SSL), 56006 (SSL), 60007 UDP: 123
NW Server	UEBA	TCP: 22 UDP: 123
ESA	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 123, 53
ESA	Active Directory	TCP: 389 (Non-SSL), 636 (SSL)
ESA	Archer	TCP: 80 (Non-SSL), 443 (SSL),
ESA Secondary	ESA Primary	TCP: 27017
ESA Primary or Secondary	Concentrator	TCP: 50005 (Non-SSL), 56005 (SSL)
Network Decoder	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017, UDP: 53, 123

Source Host	Destination Host	Ports
Concentrator (Network & Logs)	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 53, 123
Network Hybrid	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017) UDP: 53, 123
Log Decoder	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017 UDP: 53, 123
Log Hybrid	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123
Log Hybrid - Retention	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123
VLC	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671,15671, 27017 UDP: 53, 123
VLC	Log Collector	TCP: 5671
Log Collector	VLC	TCP: 5671
Endpoint Log Hybrid	NW Server	TCP: 53, 80, 443, 5671, 4505, 4506, 15671, 27017 UDP: 53, 123
Endpoint Log Hybrid	Log Decoder	TCP: 50202 (Non-SSL), 50102 (REST), 56202 (SSL) UDP: 514
Endpoint Agent	Log Decoder	TCP: 514, 6514 UDP: 514
Endpoint Agent	Endpoint Log Hybrid	TCP: 443 UDP: 444
UEBA	NW Server	TCP: 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 50003 (Broker-Non-SSL), 50103 (Broker/REST), 56003 (Broker/SSL) UDP: 53, 123
UEBA	Concentrator	TCP: 50005 (Non-SSL), 50105 (REST), 56005 (SSL)

www connections

Source Host	Destination Host	Ports
NW Server	cloud.netwitness.com cms.netwitness.com download.rsasecurity.com panacea.threatgrid.com quantum.subscribenet.com rsasecurity.subscribenet.com smcupdate.emc.com	TCP: 80, 443
ESA (Primary & Secondary)	cloud.netwitness.com cms.netwitness.com download.rsasecurity.com panacea.threatgrid.com quantum.subscribenet.com rsasecurity.subscribenet.com smcupdate.emc.com	TCP: 80, 443
Malware	panacea.threatgrid.com cloud.netwitness.com	TCP: 443

Comprehensive List of NetWitness Host, Service, and iDRAC Ports

Note: For ports used in event collection through the NetWitness Logs, see the "The Basics" in the *RSA NetWitness Platform Log Collection Deployment Guide*. Go to the [NetWitness Documents - All Versions](#) to find all RSA NetWitness Platform 11.x documents.

This section contains the port specifications for the following hosts.

NW Server Host	iDRAC Ports
Analyst UI Host	Log Collector Host
Archiver Host	Log Decoder Host
Broker Host	Log Hybrid Host
Concentrator Host	Log Hybrid - Retention
Endpoint Log Hybrid Host	Malware Host
Endpoint Relay Server	Network Decoder Host
Event Stream Analysis Host	Network Hybrid Host
New Health & Wellness	UEBA Host

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

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	NW Server	TCP 443, 80	nginx - NetWitness UI
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
Admin Workstation	NW Server	TCP 22	SSH Primary to Standby NW Server synchronization port.
NW Hosts	NW Server	TCP 53 UDP 53	DNS
NW Hosts	NW Server	TCP 15671	RabbitMQ Management UI
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Hosts	NW Server	TCP 443	RSA Update Repository
NW Hosts	NW Server	TCP 5671	RabbitMQ-amqp
NW Hosts	NW Server	UDP 123	NTP
NW Hosts	NW Server	TCP 27017	MongoDB
NW Server	cloud.netwitness.com	TCP 443	Live
NW Server	cms.netwitness.com	TCP 443	Live
NW Server	smcupdate.emc.com	TCP 443	Live
NW Server	NFS Server	TCP 111, 2049, UDP 111, 2049	iDRAC Installations
NW Server	NW Hosts	UDP 123	NTP
NW Server	NW Endpoint	TCP 443, 9443	For NW Endpoint 4.x integrations

Analyst UI Host

Source Host	Destination Host	Destination Ports	Comments
Analyst UI	NW Server	TCP 7006	The Content Server is listening on this port.
Analyst UI	NW Server	TCP 7009	The Admin Server is listening on this port.
Analyst UI	NW Server	TCP 7012	The Integration Server is listening on this port.
Analyst UI	NW Server	TCP 7015	The Source Server is listening on this port.
Analyst UI	NW Server	TCP 7016	The License Server is listening on this port.
NW Hosts	Analyst UI	TCP 5671	RabbitMQ-amqp
Analyst UI	NW Server	UDP 123	NTP

Note: Make sure you restrict DNS access on the Netwitness Server. You must allow access to DNS service on NetWitness Server only from NeWitness Hosts by adding the firewall rules in NetWitness Server.

Archiver Host

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

Broker Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 15671	RabbitMQ Management UI
Broker	Concentrator	TCP 50005 (Non-SSL), 56005	Concentrator Application Port
Broker	NW Server	TCP 15671	RabbitMQ Management UI
Broker	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Broker	TCP 22	SSH
NW Server	Broker	TCP 50003 (Non-SSL), 56003 (SSL), 50103 (REST)	Broker Application Ports
NW Server	Broker	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
Endpoint Broker	NW Server	TCP 443	RSA Update Repository

Concentrator Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Concentrator	TCP 15671	RabbitMQ Management UI
Concentrator	Log Decoder	TCP 50002 (Non-SSL), 56002 (SSL)	Log Decoder Application Port
Concentrator	Network Decoder	TCP 56004, 50004 (Non-SSL)	Network Application Port
Concentrator	NW Server	TCP 15671	RabbitMQ Management UI
Concentrator	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)	Concentrator Application Ports
Malware	Concentrator	TCP TCP 50005 (Non-SSL), 56005 (SSL)	Malware
NW Server	Concentrator	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Concentrator	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Concentrator	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint Agent	Endpoint Log Hybrid	TCP 443 UDP 444	NGINX HTTPS NGINX UDP. If UDP port 444 is not acceptable in your environment, see How to Change UDP Port for Endpoint Log Hybrid .
Endpoint Agent	Log Decoder or Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Log Hybrid	Log Decoder (External)	TCP 50102 (REST) 56202 (Protobuf SSL) 50202 (Protobuf)	To forward meta to an external Log Decoder
Endpoint Log Hybrid	NW Server	TCP 443	RSA Update Repository
NW Server	Endpoint Log Hybrid	TCP 7050	UI web traffic
Endpoint Log Hybrid	NW Server	TCP 5671	Message Bus
Endpoint Log Hybrid	NW Server	TCP 27017	MongoDB
NW Server	Endpoint Log Hybrid	TCP 7054	UI web traffic
NW Server	NFS Server	TCP 111, 2049 UDP 111, 2049	iDRAC Installations
NW Server	Endpoint Log Hybrid	TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)	Log Collector application ports
NW Server	Endpoint Log Hybrid	TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder application ports
Admin Workstation	Endpoint Log Hybrid	TCP 15671	RabbitMQ Management UI
Endpoint Log Hybrid	NW Server	TCP 15671	RabbitMQ Management UI

Endpoint Relay Server

Source Host	Destination Host	Destination Ports	Comments
Endpoint Agent	Relay Server	TCP 443	To forward host data to the Relay Server
Endpoint Log Hybrid	Relay Server	TCP 443	Pull host data from the Relay Server

Event Stream Analysis (ESA) Host

Note: The ports in this table are for the ESA Primary and ESA Secondary hosts. The Content Hub, Correlation and ESA Analytics services are co-located on the ESA Primary host. The Correlation and ESA Analytics services are co-located on the ESA Secondary host.

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 443	RSA Update Repository
Admin Workstation	ESA	TCP 22	SSH
NW Server, ESA Secondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 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

New Health and Wellness

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

New Health and Wellness on Different Subnet

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

Example:

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

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

iDRAC Ports

Port	Function	Comments
22*	SSH	Default, configurable port through which iDRAC listens for connections
443*	HTTP	Default, configurable port through which iDRAC listens for connections
5900*	Virtual Console keyboard and mouse redirection, Virtual Media, Virtual Folders, and Remote File Share.	Default, configurable port through which iDRAC listens for connections
111, 2049	TCP	NetWitness Platform hosts to NFS Server
111, 2049	UDP	NetWitness Platform hosts to NFS Server

Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI
Log Collector	NW Server	TCP 15671	RabbitMQ Management UI
Log Collector	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Collector	TCP 22	SSH
Log Collector	Log Event Sources	See <i>Log Collection Configuration Guide</i> . (missing or bad snippet)	
Log Event Sources	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Log Collection Ports
Log Event Sources	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Log Collection FTP/S Ports
NW Server	Log Collector	TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Collector	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Collector	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Collector	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC installations
Log Collector	Virtual Log Collector	TCP 5671	In Pull Mode
Virtual Log Collector	Log Collector	TCP 5671	In Push Mode

Log Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Decoder	TCP 15671	RabbitMQ Management UI
Log Decoder	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Log Event Sources	See <i>Log Collection Configuration Guide</i> . (missing or bad snippet)	
Log Event Sources	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Decoder	TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Decoder	TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Decoder	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
Log Decoder	NW Server	TCP 15671	RabbitMQ Management UI

Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
Log Hybrid	NW Server	TCP 15671	RabbitMQ Management UI
Log Hybrid	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Log Event Sources	See <i>Log Collection Configuration Guide</i> . Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.	
Log Event Sources	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid	TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid	TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Hybrid	TCP TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Log Hybrid	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Log Hybrid - Retention Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid - Retention	TCP 15671	RabbitMQ Management UI
Log Hybrid - Retention	NW Server	TCP 15671	RabbitMQ Management UI
Log Hybrid - Retention	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Log Hybrid - Retention	TCP 22	SSH
Log Collector	Log Event Sources	See <i>Log Collection Configuration Guide</i> . Go to the NetWitness Documents - All Versions to find all RSA NetWitness Platform 11.x documents.	
Log Event Sources	Log Hybrid - Retention	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Hybrid - Retention	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid - Retention	TCP 50001 (Non-SSL), 56001 (SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid - Retention	TCP 50002 (Non-SSL), 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder Application Ports
NW Server	Log Hybrid - Retention	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Hybrid - Retention	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Hybrid - Retention	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
Malware	NW Server	TCP 15671	RabbitMQ Management UI
Malware	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malware Application Ports
NW Server	Malware	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Malware	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Malware	TCP 5432	Postgresql
NW Server	Malware	TCP 56003 (SSL), 50103 (REST)	Broker Application Ports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Network Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Network Decoder	TCP 15671	RabbitMQ Management UI
Network Decoder	NW Server	TCP 15671	RabbitMQ Management UI
Network Decoder	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Network Decoder	TCP 22	SSH
NW Server	Network Decoder	TCP 56004 (SSL), 50104 (REST), 50004 (Non-SSL)	Network Decoder Application Ports
NW Server	Network Decoder	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Network Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Network Decoder	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Network Hybrid Host

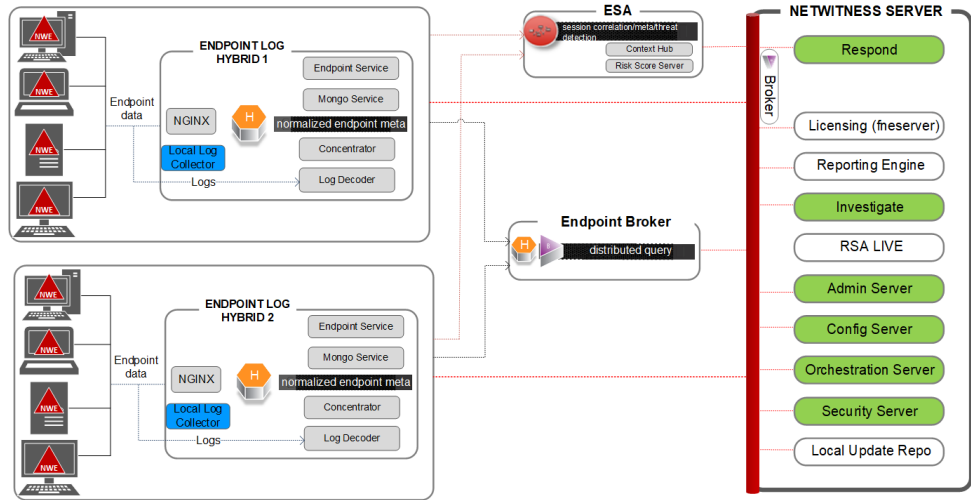
Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Network Hybrid	TCP 15671	RabbitMQ Management UI
Network Hybrid	NW Server	TCP 15671	RabbitMQ Management UI
Network Hybrid	NW Server	TCP 443	RSA Update Repository
Admin Workstation	Network Hybrid	TCP 22	SSH
NW Server	Network Hybrid	TCP 56004 (SSL), 50104 (REST), 50004 (Non-SSL)	Network Decoder Application Ports
NW Server	Network Hybrid	TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Network Hybrid	TCP 56006 (SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Network Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Network Hybrid	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

UEBA Host

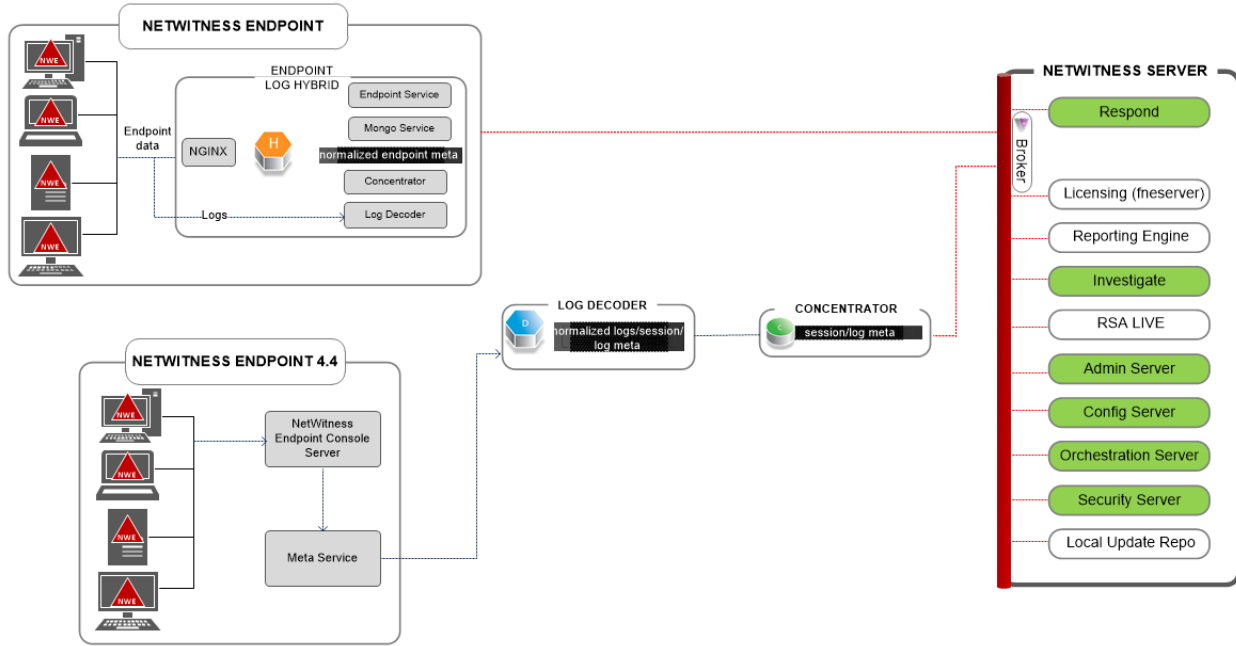
Source Host	Destination Host	Destination Ports	Comments
UEBA Server	NW Server	TCP 443	RSA Update Repository
UEBA Server	Broker	TCP 56003 (SSL), 50103 (REST)	Broker Application Ports
UEBA Server	Concentrator	TCP TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)	Concentrator Application Ports
Admin Workstation	UEBA Server	443	UEBA Monitoring
Admin Workstation	UEBA Server	22	SSH
UEBA Server	NW Server	15671	UEBA Alerts forwarding to Respond
NW Server	NFS Server	TCP 111, 2049 UDP 111, 2049	iDRAC Installations

NetWitness Endpoint Architecture

NetWitness Endpoint Architecture

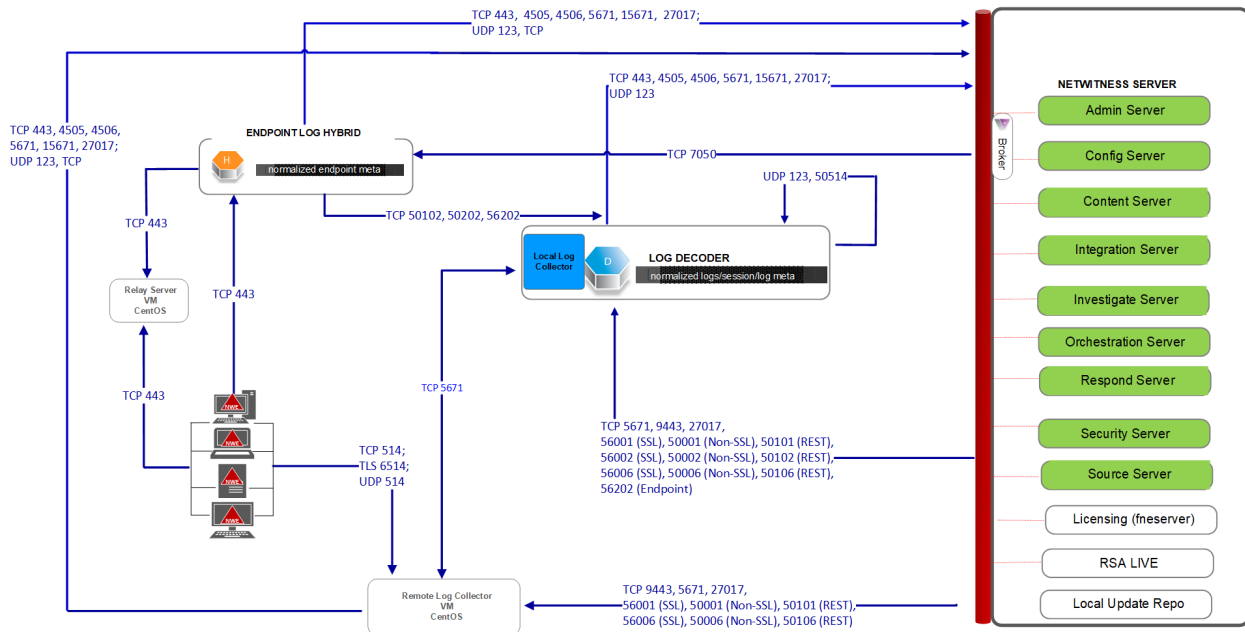


NetWitness Endpoint 4.4 Integration with NetWitness Platform



NetWitness Endpoint Architecture with Ports

NetWitness Endpoint Architecture with Ports



For more information on the services running on Endpoint Log Hybrid, see *RSA NetWitness Endpoint Configuration Guide*.

How to Change UDP Port for Endpoint Log Hybrid

The following steps tell you how to change the Endpoint Log Hybrid default UDP port 444 if it is not acceptable in your environment. 555 is the example this procedure uses as a replacement for 444 UDP port.

There are two tasks you need to do to change the Endpoint Log Hybrid default UDP port 444:

[Task 1 - Tell All Agents to Use a New UDP Port](#)

[Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment](#)

Note: If you did not select the custom firewall rules option when you ran the `nwsetup-tui`, NetWitness platform overwrites the firewall rules after a period of time. Please refer to the following Knowledge Base Article 00036446 (<https://community.netwitness.com/t5/netwitness-knowledge-base/how-to-add-custom-firewall-rules-after-nwsetup-tui-has-completed/ta-p/5900>) if this is the case.

Task 1 - Tell All Agents to Use a New UDP Port

Complete the following steps to update the UDP port in the default Enterprise Data Replication (EDR) policy, and all other policies you have, to tell all agents to use a new UDP port.

1. In the **NetWitness** menu, select **(missing or bad snippet) > Endpoint Sources > Policies**. The **Policies** view is displayed.
2. Select the **Default EDR Policy** and click **Edit** from the toolbar.
3. roll down to find the **UDP PORT** and change the value (for example, change from **444** to **555**).
4. Click **Publish Policy** at the bottom of the view.

Task 2 - Update the Port on All Endpoint Log Hybrid Hosts in Your Environment

SSH to each Endpoint Log Hybrid host in your environment with `admin` credentials and make the following updates.

1. Update the `iptables` rules to allow 555 in place of 444.

- a. Replace 444 with 555 in the following file.

```
vi /etc/sysconfig/iptables
```

- b. Restart `iptables` with the following command string.

```
systemctl restart iptables
```

- c. Verify the change with the following command string.

```
iptables -L -n
```

The following is an example of what is displayed for a correct change.

```
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /*  
EndpointNginxPort */ ctstate NEW
```

2. Update the SELinux policy. 555 is a privileged port, so you must update SELinux policy to allow this port.
 - a. Run the following command string.

```
semanage port -a -t http_port_t -p udp 555
```

If you received any python errors or warnings, ignored them.
 - b. Verify the change with the following command string.

```
semanage port -l | grep http_port_t
```

The following is an example of what is displayed for a correct change.

```
http_port_t udp 555, 444
```
 - c. (Optional) Remove 444.
3. Update nginx config.
 - a. Edit the following file.

```
vi /etc/nginx/nginx.conf
```
 - b. Search for the following string.

```
listen 444 udp;
```
 - c. Replace 444 with 555.
 - d. Restart nginx with the following command string.

```
systemctl restart nginx
```
4. Verify that agents are communicating over the new port.
 - a. Run the following command string.

```
tcpdump -i eth0 port 555
```
 - b. Wait for 30 seconds because the port sends out a beacon every 30 seconds. If everything is working correctly, information similar to the following will be displayed.

```
09:20:12.571316 IP 10.40.15.103.60807 > EPS1.rsa.lab.emc.com.dsf: UDP,
length 20
09:20:12.572433 IP EPS1.rsa.lab.emc.com.dsf > 10.40.15.103.60807: UDP,
length 1
```

Both lines must be returned. One is the size request (20 bytes) and the other is the response size (1 byte).

Note: For the latest architecture and port usage information, see "Network Architecture and Ports" topic in the *Deployment Guide*.

Network Encryption

You can configure RSA NetWitness Platform to send or receive data from external data sources.

Note: RSA recommends that whenever you have the option to choose between unsecured and secured versions of a communication protocol, you choose the secured version.

NetWitness Platform Web Server Communications

The RSA NetWitness Platform UI or web server communicates with the Live Service (CMS) over port 443 using the HTTPS protocol.

Note: During installation, the system is engineered to set the default communication protocol to HTTPS over port 443.

Reporting Engine, ESA and Warehouse Connector : External Communication

RSA recommends that you use the secure TCP protocol and enable an SSL connection while configuring Reporting Engine, ESA, Warehouse Connector, Licensing, and Malware.

For more information on Reporting Engine, see "Configure Output Actions" in the *Host and Services Configuration Guide*.

For more information on Malware external communication, see "Configure Malware Analysis Operating Environment" in the *Host and Services Configuration Guide*.

For more information on ESA, see "Notification Methods" in the *Alerting Using ESA Guide*.

For more information on the Warehouse Connector, see "Configure Warehouse Connector" in the *Host and Services Configuration Guide*.

For more information on Licensing, see "Configure NetWitness Platform Notifications" in the *Licensing Management Guide*.

Log Collector Service

To help secure communication between the Log Collector service running on the Log Decoder and the event sources, RSA recommends the following protocols.

Event Source	Protocol	Resources
File	SFTP, SCP, FTPS	For more information, see "File Collection Protocol Configuration" in the <i>Log Collection Guide</i> .

Event Source	Protocol	Resources
ODBC	ODBC	<p>For more information on configuring an ODBC event source, see "ODBC Collection Configuration" in the <i>Log Collection Guide</i>.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Note: Depending on the event source, administrators can configure additional progress driver parameter for secure connections. For more information, see the Progress document at https://www.progress.com/odbc/resources/documentation/books-and-readme-file.</p> </div> <p>For more information on using a certificate, see the certificate creation kit at http://openssl.org/.</p> <p>For more information on securing communication with SQL Server, Oracle, and ODBC, see the URLs: http://technet.microsoft.com/en-us/library/105%29.as http://technet.microsoft.com/en-us/library/cc754431.aspx http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html http://www.psdn.progress.com/progress...92/odr/odr.pdf</p>
Windows	HTTPS	For more information on configuring a Windows event source to use certificates and enable HTTPS, see the NetWitness Platform 11.7 help topics in the <i>Windows Collection Configuration Guide</i> .
Check Point	OPSEC LEA	For more information on configuring a Check Point event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>Check Point Collection Configuration Guide</i> .
Netflow	Netflow	For more information on configuring a Netflow event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>Netflow Collection Configuration Guide</i> .
SDEE	SDEE	For more information on configuring a SDEE event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>SDEE Collection Configuration Guide</i> .
SNMP	SNMP	For more information on configuring a SNMP event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>SNMP Collection Configuration Guide</i> .
VMware		For more information on configuring a VMware event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>VMware Collection Configuration Guide</i> .
Legacy Windows and NetApp		For more information on configuring a Legacy Windows event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>Legacy Windows and NetApp Collection Configuration Guide</i>

Event Source	Protocol	Resources
Amazon Web Services (AWS) Cloud Trail	HTTPS	For more information on configuring an AWS Cloud Trail event source to use certificates, see the NetWitness Platform 11.7 help topics in the <i>AWS (CloudTrail) Collection Configuration Guide</i> .

Note: For more information on enabling SSL for component communications, see [Component Authentication](#).

Enabling HTTPS on REST Interfaces for Core Services

To enable HTTPS on REST interfaces:

1. Log in to REST interface.
2. Go to the **rest > config** node.
3. Set **SSL** config to **on**.
4. Restart the service.

Data Security Settings

Data security settings are designed to enable the definition of controls to prevent data permanently stored by RSA NetWitness from being disclosed in an unauthorized manner.

Securing Data

To help protect online data, such as current database, log, and configuration files, RSA recommends that you restrict access to the files, database and configure permissions so that only trusted administrators are allowed to access them.

RSA recommends that you back up your sensitive data, encrypt it, and keep it in a secure physical location in accordance with your corporate disaster recovery and business continuity policies.

The backup can be done in the following ways:

- Regular backup of Configuration and Data files – You can back up and restore data and configuration files for the core host and services and all the modules of NetWitness. For more information, see the *NetWitness Recovery Tool User Guide*.
- Regular backup of critical configuration – You can export configurations using the Export option available on the UI. For example, you can take a backup of critical rules, reports, alerts, ESA rules, dashboards, investigation profiles, metadata groups, event sources, global notifications, and so on. For more information, see topics:
 - "Export a Rule, Export an Alert and Export a Report" in the *Reporting Guide*.
 - "Rule Library View and Dashboard" in the *Alerting using ESA Guide*.
 - "Manage Profiles Dialog and Export a Meta Group" in the *Investigation and Malware Analysis Guide*.
 - "Events View and Export Event Sources" in the *Event Source Management Guide*.
 - "Global Notifications Panel Toolbar" in the *System Configuration Guide*.

Data Privacy

Data Privacy is very integral and helps you manage privacy-sensitive data. You can achieve data privacy using the Data Privacy Officer (DPO) role. The DPO can configure NetWitness to limit the exposure of metadata and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness include:

- Data Obfuscation
- Data Retention Enforcement
- Auditing Logging

For more information, see topics in the *Data Privacy Management*.

Default Storage Passwords

The default storage passwords for database accounts that store alerts in ESA, and Respond Service can be changed. For more information, see "Change Default Storage Passwords" in the *Host and Services Configuration Guide*.

Alert System Settings

For instructions on configuring NetWitness to send alerts or notifications, see the following topics in the *System Configuration Guide*:

- "Email Configuration Panel"
- "Global Audit Logging Configurations Panel"
- "Global Notifications Panel"

FIPS Compliance

This topic provides information on the Federal Information Processing Standards (FIPS) compliant mode for RSA NetWitness. The FIPS publications are guidelines that set best practices for software and hardware security products for the protection of valuable and sensitive information.

When the FIPS compliant mode is used, products that support one or more FIPS standards can be set into a mode where the product uses FIPS approved algorithms and methods only.

NetWitness supports both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

NetWitness Platform Components working in FIPS mode

The table below lists the NetWitness components that work in FIPS mode. The method you use to activate or deactivate FIPS depends on the type of security library used by your NetWitness services. Your NetWitness services use the security libraries, as mentioned in the following table.

Services	Security Library
Event Stream Analysis (ESA), Malware Analysis, Reporting Engine, NetWitness Host, Respond Service, Context Hub and Endpoint	BSAFE
Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, Archiver, and Workbench	BSAFE

FIPS 140-2 Certified Cryptographic Modules are enabled for all services that perform cryptographic operations. For the following services, although the FIPS Cryptographic Module is leveraged, the use of FIPS cipher suites is not being enforced:


- NTP: UDP Port 123
- TCP: SSH Port 22
- TCP: Salt API Loopback Port 8000
- CollectD
- Log Collector
- Log Decoder

Common Criteria Compliance

This topic provides information on Common Criteria Compliance for RSA NetWitness. To support this requirement, you must ensure that only a secure communication is configured for the core services. To achieve this you must disable the unencrypted ports for the NetWitness core services.

Disabling Unencrypted Ports For NetWitness Core Services

To disable an unencrypted port for a NetWitness core service:

1. Log in to NetWitness UI.
2. Go to **(Admin) > Services**.
The Services page is displayed.
Select a core service to configure.
3. Click  and select **View > Config**.
.
4. Select the General tab.
5. In the Port field under the System Configuration section, replace the existing value with **0**.
6. Now click the Appliance Service Configuration tab.
7. In the Port field, replace the existing value with **0**.
.
8. Click **Apply** and restart the service, if prompted.

Note: After you apply the changes only the SSL port is configured for the service and no unencrypted interfaces are available to interact with the service.

STIG Compliance

Overview

Note: Security Technical Implementation Guide (STIG) Compliance is available in NetWitness.

This topic provides information on Security Technical Implementation Guide (STIG) Compliance.

STIG Limits Account Access

NetWitness 11.3.1 and later, is STIG compliant which helps to lock down information, systems, and software, which might otherwise be vulnerable to a malicious computer attack by limiting account access to a system.

For example, STIG:

- Ensures that the account password has a length, complexity, expiration period, and lockout period that are in accordance with DISA's best practices.
- Applies auditing and logging of user actions on the appliance.

To be STIG compliant, your organization must implement policies that ensure strong passwords. For more information about STIG and STIG exceptions, see DISA STIG in the *System Maintenance Guide*.

Other Security Considerations

This topic describes various other security configuration settings that are not covered in previous sections.

Changing the RabbitMQ Management Password for Windows Legacy Collectors

For Windows Legacy Log Collectors (WLCs), a default password is used for the "logcollector" username to access the RabbitMQ broker on that machine. RSA recommends that you change the password for WLCs, per the procedure outlined, which involves changing the RabbitMQ password for the Log Collector and for the RabbitMQ broker.

Note: For CentOS, changing the RabbitMQ password is not supported.

If you are using a Log Collector, you may have to initialize the "lockbox". For instructions, see "Set Up a Lockbox" in the *Log Collection Guide*.

To change the RabbitMQ password:

1. Change the RabbitMQ password in Log Collector:
 - a. Go to the Explore view for the Log Collector service.
 - b. Right-click the **event-broker** node and select **config**.
 - c. Type the new password in the **amqp_password** field. The password is encrypted by a key that is managed through the lockbox of this Log Collector. This only changes the password on the Log Collector side.

Note: Most of the settings should not be changed. Ensure you do NOT change the Message Queue User Name "amqp_username" because it is referred to in some certificate checks.

2. Change the RabbitMQ password for the RabbitMQ broker:
 - a. Go to the Explore view for the Log Collector service.
 - b. Right-click the **event-broker** node and select **properties**.
 - c. Select **passwd** in the drop-down list.
 - d. In the **Parameters** field, type the old and new password.
Ensure you remember your old password. If it was never changed, it should be "netwitness" by default.
Example: Parameters: oldpw=<netwitness> newpw=<YourNewPasswordHere>
 - e. Click **Send**.

Hardening the NetWitness Platform Core service

By default, all NetWitnessCore services ship with a default username and password and with SSL turned off. To harden the service, you have to run it with the command line option `-s harden=true`

Using a Decoder, here's an example command line:

```
NwDecoder -s harden=true -s defaultUsername=<username> -s
defaultPassword=<password>
```

The above command does the following:

1. Removes the default admin account (with caveats, see below).
2. Creates a new account `<username>` with a password of `<password>` (thus meeting the password requirements below).
3. Enables SSL on both the native and REST ports.
4. Strengthens default password requirements:
 - `/users/config/account.lockout.time = 60`
 - `/users/config/password.alpha.lowercase.min = 1`
 - `/users/config/password.alpha.uppercase.min = 1`
 - `/users/config/password.length.min = 8`
 - `/users/config/password.numeric.min = 1`
 - `/users/config/password.symbol.min = 1`
5. Sets `/rest/config/user.agent.whitelist = Apache-HttpClient\d\.\d\.\d`

Note: This setting prevents the browsers to connect to the REST port.

The caveat for changing the default user account is that there cannot be an already existing configuration file. This is always true the first time the service is run or before the service is licensed. To harden a service, you must run it before a configuration is written or delete whatever configuration file exists and then harden.

To alter the command line for a service that writes its own upstart script without actually SSHing into the box and modifying the script, there is a new parameter that you can pass to either the `/sys shutdown` or `/decoder reset` command (substitute decoder for the actual service name) and this parameter is called "cl" for command line. What you do is pass name=value pairs to the "cl" parameter and those parameters will take affect on the next restart of the service.

Example:

```
/sys shutdown reason="Restart because license was applied"
cl="harden=true default
Username=<username> defaultPassword=<password>"
```

The above command shuts down the service (which should be restarted by Linux upstart) and the command line parameters will be applied on the restart. This command line exactly matches the command line given above for the decoder service. If you want to do a configuration reset, you can use the following:

```
/broker reset config=true cl="harden=true defaultUsername=<username>
defaultPassword=<password>"
```

This will delete the broker configuration file and create a new default configuration that is automatically hardened with the given default account and credentials. The admin account will not exist when the broker restarts, only the <username> account exists.

NFS Access Controls

By default, the NFS mounts are wide open. To lock them down to a specific address, you must edit the exports file and specify the IP addresses that are allowed to interact with the SAW.

The SAW NFS service is managed from the command line using *mapr-nfsserver*.

```
[root@saw-nodel ~]# service mapr-nfsserver
Usage: /etc/init.d/mapr-nfsserver {start|stop|status|restart|}
[root@saw-nodel ~]# service mapr-nfsserver status
nfsserver (pid 5692 5691) is running...
[root@saw-nodel ~]#
```

If *nfs-utils* is installed on the node, you can execute a *showmount* on the localhost to see the exposed exports.

```
[root@saw-nodel ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
[root@saw-nodel ~]#
```

Exports are controlled using the exports file in the */opt/mapr/conf* directory.

```
[root@saw-nodel ~]# cat /opt/mapr/conf/exports
# Sample Exports file
# for non /mapr exports
# <Path> <comma separated cldb addresses=host:port> <exports_
control>
# for /mapr exports
# <Path> <exports_control>
#access_control -> order is specific to default
# list the hosts before specifying a default for all
# a.b.c.d,1.2.3.4(ro) d.e.f.g(ro) (rw)
# enforces ro for a.b.c.d & 1.2.3.4 and everybody else is rw
# special path to export clusters in mapr-clusters.conf. To disable
exporting,
```



```
# comment it out. to restrict access use the exports_control
#
/mapr (rw)
#to export only certain clusters, comment out the /mapr & uncomment.
# Note: this will cause /mapr to be unexported
#/mapr/clustername (rw)
#to export /mapr only to certain hosts (using exports_control)
#/mapr a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster1 rw to a.b.c.d & ro to e.f.g.h (denied for
others)
#/mapr/cluster1 a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster2 only to e.f.g.h (denied for others)
#/mapr/cluster2 e.f.g.h(rw)
# export /mapr/cluster3 rw to e.f.g.h & ro to others
#/mapr/cluster2 e.f.g.h(rw) (ro)
[root@saw-node1 ~]#
```

To restrict the SAW exports to a certain IP address or group of IPs, you must first edit the exports file and then restart the *mapr-nfsserver* service.

```
[root@saw-node1 ~]# vi /opt/mapr/conf/exports
[root@saw-node1 ~]# cat /opt/mapr/conf/exports | grep ^/mapr
/mapr 10.42.1.87(rw)
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
[root@saw-node1 ~]# service mapr-nfsserver restart
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr 10.42.1.87
/mapr/saw 10.42.1.87
[root@saw-node1 ~]# mount -t nfs -o nolock,tcp localhost:/mapr/saw
/saw
mount.nfs: access denied by server while mounting
localhost:/mapr/saw
[root@saw-node1 ~]#
```

Note: Trying to mount the export on the localhost will fail as only a specific host IP is now allowed to use the NFS mount.

Secure Deployment and Usage Settings

This topic describes the settings for secure deployment and usage. It is very important to protect all physical, local, and remote access to the RSA NetWitness appliances. It is also important to restrict all access methods to the absolute minimum required to maintain RSA NetWitness.

Note: RSA recommends that you do not set up the test environments to be exact copies of the full production environment. If the test environment is identical to the production environment, you should take the same precautions to protect the test environment as you do in the production environment.

Security Controls Map

This topic describes the security controls map. An RSA NetWitness deployment can consist of the following components:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Context Hub
- Malware
- ESA
- Archiver
- NetWitness Server
- Endpoint
- UEBA Server

NetWitness supports integration with products such as RSA NetWitness 4.x and RSA Archer.

RSA recommends that you access the host on secure client machines within the network. If you must access the host through remote access, RSA recommends that you connect to the network through a secure VPN connection. Only allow remote access to NetWitness hosts for secure maintenance using the Remote Desktop Protocol (RDP) through a secure VPN connection.

Caution: RSA recommends that you deploy the hosts in a secure location, where physical access to the hosts are restricted only to the personnel who manage the hosts.

Secure Enclave

To help protect NetWitness against unauthorized authentication and access by end users or machines, RSA recommends that you deploy NetWitness hosts such as Broker, Concentrator, and Decoder.

You can help create a secure enclave by separating the low security corporate network from the high security network with firewalls. To help create a secure enclave, RSA recommends that you:

- Implement basic physical security elements, policies, procedures, and processes for the low security network.
- Provide access to the hosts within the secure enclave through a secure virtual private network (VPN) tunnel only, such as IPsec tunnel, to establish encryption and authentication of all network traffic to and from the hosts.

Note: The client machines through which you access NetWitness can be present outside of the Secure Enclave.

Secure Deployment Guidelines

To help ensure a secure deployment, RSA recommends that you:

- Deploy multiple hosts in the corporate network. The multiple hosts in the example are in two geographic locations and include the following components:
 - NetWitness
 - Broker
 - Packet Decoder
 - Log Decoder
 - Concentrator
 - ESA
 - Archiver
 - NetWitness Warehouse
 - Malware Analysis
 - Endpoint
 - UEBA Server
- Ensure that all the components are connected to the same subnetwork.
- Deploy firewalls at each site to ensure the secure transfer of data from an instance of NetWitness at one site to another instance of NetWitness located at a different site.
- Configure firewall rules to control all communication between different sites and other components in the network as depicted in the previous figure.
- Implement data transfer between sites using a secure tunnel IPSec.

The following figures show the deployment of multiple sites within a corporate network:

Firewall Rules

It is important that you use a firewall to restrict network traffic between RSA NetWitness and external systems. RSA NetWitness recommends that you configure firewall rules to help ensure secure communication for the following connections:

- Demilitarized zone (DMZ) to corporate network
- Corporate network to site sub network
- Site to site
- Live CMS to DMZ
- External email server to DMZ

Note: RSA recommends that you restrict access from client hosts to only known IP addresses. For example, if you set up the NetWitness Client UI on IP address 192.168.0.1, configure your firewall to allow only the IP address 192.168.0.1 to connect to the NetWitness host.

Note: The firewall rules should be configured on an external firewall and not on any of the NetWitness host.

RSA recommends that you configure firewall rules as described in the sections below. These recommendations are based on the following assumptions:

- You have a stateful firewall, indicating that only the establishment of TCP ports is considered.
- You specify the direction of communication for the UDP ports because the connections are sessionless.
- You deploy NetWitness as shown in the Security Controls Map.
- The firewall processes the rules top to bottom, finishing with a generic drop of all the packets.

DMZ to Corporate Network

RSA recommends that you:

- Configure whitelist communication from the VPN server in the DMZ to the client machines on which you run RSA NetWitness applications such as NetWitness Web UI.
- Create firewall rules for all the machines from which you intended to remotely access the corporate network through Remote Desktop Protocol (RDP).

Corporate Network to Site

RSA recommends that the firewall at each RSA NetWitness site allow access only from designated client machines through a whitelisted IP address and port.

RSA recommends that you secure the following ports to ensure secure communication between the client machine that is set as the RSA NetWitness Web UI and the NetWitness site:

- TCP 443

For more information, see [Communication Security Settings](#). To help ensure secure communication between the client machines that access the NetWitness UI and a site, you must set up the firewall rules as shown below:

ALLOW \$nwclient_IP to \$nwsite_IP on port 443/tcp

DROP all from * to *

where **nwclient_IP** is the IP address assigned to the client machine that is set as the NetWitness web UI and **nwsite_IP** is the IP address assigned to the Broker host within which the RSA NetWitness web server is running.

Site to Site

RSA NetWitness may run in multiple sub-networks within your corporate network, called sites. You can configure RSA NetWitness to allow the hosts located in one site to communicate with the hosts in another site.

For this scenario, RSA recommends that you do the following:

- Ensure that the firewall at each RSA NetWitness site allows communication between two sites only through a whitelisted IP address and port. For a graphical depiction of the site-to-site security control map showing the site firewalls, see the above figure.
- NetWitness system update uses port 80. That means NetWitness site to another site (where brokers, decoders exist), port 80 should be open.

Live CMS to DMZ

To ensure secure communication between the RSA NetWitness site and Live CMS, set up the firewall rules as shown below:

ALLOW \$nw_site_IP to \$Live_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Live_IP** are the IP addresses assigned to the NetWitness site and the Live CMS respectively.

Note: If you are using proxy server with self-signed certificate, you must add exception in proxy server rule to allow traffic between Live CMS server (cms.netwitness.com, port 443) and NetWitness.

RSA Download Central to DMZ

To ensure secure communication between the RSA NetWitness site and RSA Download Central, set up the firewall rules as shown below:

ALLOW \$nw_site_IP to \$rsa_DLC_IP on port 80/tcp

DROP all from * to *

where **nw_site_IP** and **rsa_DLC_IP** are the IP addresses assigned to the NetWitness site and RSA Download Central respectively.

External Email Server to DMZ

To ensure secure communication between the RSA NetWitness site and the External Email Server, set up the firewall rules as shown below:

ALLOW \$nw_site_IP to \$Email_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Email_IP** are the IP addresses assigned to the NetWitness site and the external email server respectively.

Syslog Server to Site

If you have enabled the syslog port, to ensure secure communication between the RSA NetWitness site and the Syslog Server, set up the firewall rules as shown below:

ALLOW \$nw_site_IP to \$Syslog_IP on port 514/udp

DROP all from * to *

where **nw_site_IP** and **Syslog_IP** are the IP addresses assigned to the NetWitness site and the syslog server respectively.

SNMP Server to Site

If you have enabled the SNMP port, to ensure secure communication between the RSA NetWitness site and the SNMP Server, set up the firewall rules as shown below:

ALLOW \$nw_site_IP to \$SNMP_IP on port 1610/SNMP

DROP all from * to *

where **nw_site_IP** and **SNMP_IP** are the IP addresses assigned to the NetWitness site and the SNMP server respectively.

Secure Deployment Settings

The following table shows the security controls that RSA recommends putting in place to help secure the deployment.

Default Deployment Setting	Secure Deployment Settings	Pros of Secure Deployment Settings	Cons of Secure Deployment Settings	Instructions on how to configure secure deployment settings
HTTPS is enabled by default between the NetWitness client and the server	For the best possible security between the client and the server, use certificates from CA.	Provides a high level of protection for the communication between client and server by avoiding tampering, spoofing, and man-in-the middle attacks.	May have impact on performance	For instructions on installing external certificates, see SSL Certificate Guidance for NetWitness

Secure Maintenance

This topic describes some common solutions to help ensure secure maintenance.

Security Patch Upgrade

To apply security patches to any of the required release, see the *Upgrade Guide* for the specific upgrade version.

Security Patch Management

All security patches for RSA NetWitness originate at RSA and are available for you via the NetWitness User Interface. For more information, see "Manage NetWitness Updates" in the *System Maintenance Guide*.

The following table lists the third-party components for which patches are needed.

Third-party Component for which patch is needed	Frequency of Patch	EMC Responsibility (Y/N)	Customer Responsibility (Y/N)	Reference to instructions for Applying Patch
NetWitness Hosts	Monthly and Quarterly	Y	Y	Based on EMC RSA recommendations

Virus Scanning

RSA recommends that you:

- Deploy anti-virus client software on the deployed servers in accordance with your enterprise requirements.
- Run anti-virus and anti-malware tools with the most current definition files on the deployed servers.
- Scan all files/drivers before uploading on the deployed server.
- Follow best practices for patch management and regularly review available patches for all anti-virus and anti-malware software.

Ongoing Monitoring and Auditing

As with any critical infrastructure component, RSA NetWitness recommends that you constantly monitor your system and perform periodic and random audits (for example, configuration, permissions, and security logs). You should ensure that the configurations and user access settings match your company policies and needs. For more information, see "Global Audit Logging Configurations Panel" in the *System Configuration Guide*.

Hardware Replacement

If RSA NetWitness hardware fails or is faulty, order a replacement by contacting RSA Customer Support. While awaiting a replacement, the Redundant Array of Independent Disks (RAID) configuration is designed to ensure that there is no data loss due to a hardware failure.

The RAID configuration on NetWitness:

- Hosts are RAID 1.
- Direct Attach Capacity (DAC) disk shelves is RAID 5.

Physical Security Controls Recommendations

Physical security controls help to enable the protection of resources against unauthorized physical access and physical tampering. RSA recommends that the physical devices and servers for RSA NetWitness are deployed in a secure data center leveraging the organization's best practices for physically securing a data center, server rack, and/or server.

Supporting Users

This topic describes well-defined policies around help desk procedures for your RSA NetWitness installation.

It is important to have well-defined policies around help desk procedures for your RSA NetWitness installation. RSA recommends that your help desk administrators understand the importance of password strength and the sensitivity of data, such as user logon names and passwords. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and help desk administrators to request, the least amount of information needed in each situation.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. RSA recommends that you use the following guidelines to help reduce the likelihood of a successful social engineering attack:

- Help desk administrators should only ask for User IDs over the phone when receiving help desk calls. Help desk administrators should never ask for user passwords.
- The help desk telephone number should be well known to all users.
- Help desk administrators should perform an action to authenticate the user's identity before performing any administrative action on a user's behalf. For example, ask users one or more questions to which only they know the answer.
- If help desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call the help desk back at a well-known help desk telephone number to ensure that the original request is legitimate.

Confirming User Identities

It is critical that your help desk administrators verify end users' identities before performing any help desk operations on their behalf. RSA recommends that you verify user identity using the following methods:

- Call the end user back on a phone owned by the organization and on a number that is already stored in the system.

Caution: Be wary of using mobile phones for identity confirmation, even if they are owned by the company because mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

- Send the user an email to a company email address. If possible, use encrypted email.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.

- Use multiple open-ended questions from employee records. For example, "Name one person in your group" or "What is your badge number?" Avoid yes or no questions.

Advice for Your Users

RSA recommends that you instruct your users to do the following:

- Never give passwords to anyone.
- Change passwords at regular intervals.
- Inform your users of what information requests to expect from help desk administrators.
- Always log off from the web interface when finished.
- Always lock their desktops when stepping away from their computers.
- Regularly close their browser and clear their cache of data.

Note: Consider regular training to communicate this guidance to users.

Appendix A: Customer Provided Certificates

The procedure tells you how to replace the internally generated NetWitness web server certificate (NGINX front-door) with a customer issued certificate. This enables client browsers to establish a trusted SSL connection.


Caution: The cert files and key files must be .pem format. All the files must have the same name and permissions as the original files generated by NetWitness.

1. Rename your certificate files and save them in for NGINX.
 - Rename the customer provided `cert.pem` certificate pem file to `web-server-cert.pem`.
 - Rename the customer provided `key.pem` key pem file to `web-server-key.pem`.
 - Rename customer provided `cert.chain` certificate chain file to `web-server-cert.chain`.
 - Rename `cert.p7b` certificate p7b file to `web-server-cert.p7b`.
2. SSH to the NW Server.
3. Replace the existing NetWitness Platform generated `/etc/pki/nw/web/web-server-cert.pem`, `/etc/pki/nw/web/web-server-key.pem`, `/etc/pki/nw/web/web-server-cert.chain` and `/etc/pki/nw/web/web-server-cert.p7b` files with the files you renamed in step 1.
4. Restart NGINX service.

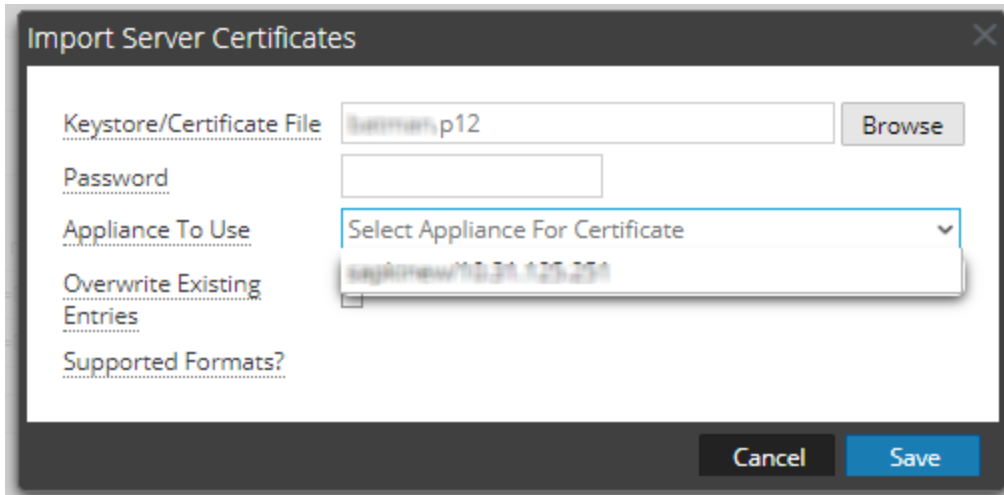
```
service nginx restart
```

To add Custom Server Certificate in PFX, P12 and JKS format.



1. Go to  (Admin) > Security.
The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.


- In the **Server Certificates** section, click  .
The Import Server Certificates dialog is displayed.




- In the **Keystore/Certificate File** field, click **Browse** and select the keystore.
- In the **Password** field, enter the keystore password.
- In the **Appliance To Use** field, select the appliance for which you want to use this certificate.
- (Optional) Select the **Overwrite Existing Entries** checkbox to overwrite the entries of the certificate that is already added.
- Click **Save**.

The NetWitness Server certificate with its private key is successfully added to NetWitness.

Note: When the certificate is being applied on the selected appliance, no other operation on PKI can be performed until the process is completed.
Double-click on the added entries to view the details of the certificate.

- To apply the server certificate on a server, select a certificate and click  .

Note: Uploading a keystore will add the server certificate and its private key locally. To apply a server certificate on a server, you need to select a server certificate and click the synchronization button  .
All server certificates are also synchronized on the appliances when PKI is enabled.

Appendix B: Reissue Certificates

Introduction

For a secure deployment, NetWitness has installed internal RSA-issued certificates such as CA Certificate and Service certificates.

The validity for NetWitness certificates are as follows:

- CA root certificate for 11.x deployment is valid for 10 years
- CA root certificate for 10.6.x deployment is valid for 5 years
- Service certificates are valid for 1000 days

When these certificates are about to expire or have expired, you must renew and reissue the certificates as soon as possible to avoid any issues with your NetWitness deployment.

Note: You can view the expiration details, by executing the `ca-expire-test-sh` script on the NetWitness Server. For more information, see [Reissue root CA security certificates on RSA NetWitness Platform 11.x](#) and download the script.

CA Certificate Reissue

To renew the CA certificates, do the following:

- Before you upgrade from 10.6.x to 11.x, check the expiry and reissue those certificates. For more information, see the [Reissue root CA security certificates on RSA NetWitness Platform 11.x](#).
- If you are on 10.6.x, check the expiry and reissue all the certificates. For more information, see the [Reissuing security certificates on RSA NetWitness Platform 10.6.x](#).

Note: If you have Windows Legacy Collectors (WLC) in your deployment, renew the CA certificate of the WLC after renewing the CA certificate of the NetWitness Admin Server.

Service Certificate Reissue

To renew the Service certificates, do the following:

- In case of a fresh installation of 11.3 or later, you must use the `cert-reissue` script. For more information, see the [Reissuing Service Certificate](#).
- In case of a fresh installation of 11.1 or 11.2 or if you upgrade from 10.6.x to 11.x, you must use the `nw-root-ca-update` script. For more information, see the [Reissue root CA security certificates on RSA NetWitness Platform 11.x](#).

Note: If you have a host that is decommissioned or plan to remove, do not renew the certificate for that host.

Reissuing Service Certificate

You can reissue service certificates in the following two ways.

- All at once
Reboot NW Server host after the `cert-reissue --host-key` command completes.
- One at a time
Reissue the NW Server host certificates first, restart the host, then reissue each component host.

IMPORTANT: If you are reissuing certificates for each host individually (one at a time), you must reissue the certificate for the NW Server host before you can reissue certificates for any other host.

When to Use the `--host-key` Argument

Use the `cert-reissue --host-key` command string if you have a large number of hosts. Make sure that:

- All your hosts are running 11.4.0.0 or later.
- All your hosts are online.
- The NW Server host run time services are running.

`cert-reissue` Arguments and Options for All Hosts

The following table lists the argument you can use to reissue certificates for all hosts at one time. See [Appendix C. Troubleshooting Cert-Reissue Command](#) for additional options you can use with Customer Support to troubleshoot errors.

Arguments	Description
<code>--host-key</code>	Reissues certificates for all hosts at one time applying system health checks and restarts services.

Note: If even one host is not online, this command fails. If you have numerous hosts in your deployment, make sure that all hosts are up and running.

Caution: Make sure you do not run this argument on a node or host that you plan to remove or decommission.

When to Use the Individual Host Arguments (`--host-id <id>`, `--host-name <display-name>`, `--host-addr <ip/hostname>`)

The `cert-reissue --host-id <id>`, `cert-reissue --host-name <display-name>`, or `cert-reissue --host-addr <ip/hostname>` reissues a certificate for an individual host. You may want to reissue certificates for an individual host if you have a small number of hosts.

Make sure that:

- Each host is running 11.4.0.0 or later.
- Each host is online.
- The NW Server host run time services are running
- You reissue certificates for the NW Server host first.

cert-reissue Arguments and Options for a Single Host

The following tables lists the arguments and options you can use to reissue certificates for a single host (one host at a time). For more information, see the [Appendix C. Troubleshooting Cert-Reissue Command](#) section on the additional options you can use with Customer Support to troubleshoot errors.

Note: You must run the command for the NW Server host first and reboot that host before you run the command for each component host.

Arguments	Description
<code>--host-id <id></code>	Reissues certificate for the host identified by <id> (host identification code).
<code>--host-name <display-name></code>	Reissues certificate for host identified by <display-name>. <display-name> is the value shown under Name in the (missing or bad snippet) > Hosts View in the NetWitness Platform Interface.
<code>--host-addr <Hostname-in UI></code> or <code>--host-addr <hostname></code>	Reissues certificate for the host identified by the value shown under Hostname in the (missing or bad snippet) > Hosts > Edit dialog in the NetWitness Platform Interface. This value can be an ip-address (default) or a user-specified name.

Reissuing Certificates for All Hosts Except Windows Legacy Collection (WLC) host

Use the `cert-reissue` command to reissue certificates for all hosts except the WLC host with the following procedures.

Running the Cert-Reissue Command for All Hosts

1. SSH to the NW Server host.
2. Submit the appropriate command string.
`cert-reissue --host-key`

Running the Cert-Reissue Command for an Individual Host

1. SSH to the NW Server host.
2. Submit the appropriate command string (that is `cert-reissue --host-id` or `--host-name` or `--host-addr`). Each of the following command strings is an example of how you reissue certificates for a specific host.
 - `--host-id <host-identification-code>`
 - `--host-name <named-displayed-under-Name-in-Hosts-view>`
 - `--host-addr <ip-address-default-hostname-or-user-specified-hostname>`

Reissuing Certificates for a WLC Host

You must use the `wlc-cli-client` utility to reissue certificates for a WLC host (you cannot use the `cert-reissue` command). You also need to specify a number of WLC identification parameters with this utility.

Note: The certificates for a Windows Legacy Server host are stored in the following directories on the host.

C:\ProgramData\netwitness\ng\logcollector_cert.pem

C:\ProgramData\netwitness\ng\logcollector_dh2048.pem

The validity period of WLC certificates can range from 2 to 20 years. If you rename or remove the files and restart **NwLogCollector** Service, NetWitness regenerates them.

/ssl/truststore.pem - is no longer used in 11.x

Every reissue of a certificate on the Windows Legacy server creates a new private key.

To reissue certificates on a WLC host.

1. SSH to the NW Server host.

2. Submit the following command string.

```
wlc-cli-client --cert-renew --host <wlc-host-ip-address> --port 50101 --  
use-ssl false --username <wlc-username> --password <wlc-password> --ss-  
username <deploy-admin-username> --ss-password <deploy-admin-password>
```

Successful Reissue Summary Report

When you run `cert-reissue --host-key`, the following summary report will be displayed if all hosts are online, all run time services are running, and all hosts on version 11.4.0.0 or later.

Unsuccessful Reissue Summary Reports

You must contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) to troubleshoot problems. You know there is a problem if any `<host-id>` does not return a `SuccessStatus`. `Success` indicates that certificates were reissued for a host. The following examples illustrate unsuccessful reissues.

Reissue Failed for Host and Aborted Command

The following three examples illustrate the failure of certificate reissuing for any hosts.

Reissue Certificate Partially Executed

The NW Server Host certificates were reissued but failed to properly distribute the reissued certificates to one or more component hosts.

Appendix C. Troubleshooting Cert-Reissue Command

You must contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) to troubleshoot problems. You know there is a problem if any `<host-id>` does not return a `SuccessStatus`. `Success` indicates that certificates were reissued for a host.

Argument Options Used for Troubleshooting

You use the following argument options with `cert-reissue --host-all` to troubleshoot problems.

You can run `cert-reissue --host--all<arguments>` multiple times without an adverse effect.

Note: Use the following Argument Options with caution. They force the `cert-reissue` command to execute for all the hosts.

Argument Option	Description
<code>--skip-health-checks</code>	<p>Reissues certificates for all hosts at one time without applying system health checks (force Reissue). This means that the command does not:</p> <ul style="list-style-type: none"> • verify that all hosts are online line. • verify that all services are running. <p>Use case: You have numerous hosts and you know that a small minority of them will fail. This updates all the hosts that conform to the checking rules and you can reissue certificates for the others subsequently with the help of Customer Support.</p>
<code>--skip-version-checks</code>	<p>Do not verify that hosts are running version 11.3.0.0 or later.</p> <p>Use Case: You have numerous hosts and your know that some of them are not updated to 11.3 or later. This reissues certificates for all the hosts that are at 11.3 or later and you can reissue certificates for the others subsequently with the help of Customer Support.</p>
<code>--ignore-trigger-errors</code>	<p>Ignore any errors that trigger failures. This option forces the cert reissue process to continue disregarding the errors instead of aborting or failing the cert reissue command quickly.</p> <p>When a cert reissue for a host succeeds, the reissued certificates on that host are not provisioned to other dependent hosts (referred to as trusts). In this case, the:</p> <ul style="list-style-type: none"> • host with reissued certificates is reported as “Partial.” • the hosts with trusts that failed to update are listed separately in the summary table to tell you that these hosts may require a refresh using the new <code>--refresh-trusts-only</code> option.
<code>--refresh-trusts-only</code>	<p>Refreshes trusts exclusively for host identified by <code><id></code> (does not reissue certificates for that host).</p>

Problems and How to Troubleshoot Them

This section describes solutions to problems that you may encounter when running the `cert-reissue` command to reissue certificates with suggested causes and solutions.

Status Failed!

Error ...

Message 2019-02-06 13:34:39.646 INFO 8540 --- [main]
c.r.n.i.o.client.OrchestrationClient : Checking host connections...
...
2019-02-06 13:34:57.861 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator :
Host '192.168.200.99' (nw-platform-esa-primary) verification failed!
...
2019-02-06 13:34:57.862 INFO 8540 --- [main]
c.r.n.i.o.client.OrchestrationClient : Checking status of services...
2019-02-06 13:35:57.931 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator :
Service 'nw-platform-node-zero - Investigate Server' not available!
...

Cause `cert-reissue --host-all` failed because one or more hosts are offline or one or more run time services are unreachable. You can force this command to run in spite of this error by specifying the `--skip-health-checks` option, that is:
`cert-reissue --host-all--skip-health-checks`

Solution

1. Bring appropriate hosts back online or make sure the NW Server hosts run time services are running.
2. Run `cert-reissue` for the hosts affected.

Status Failed!

Error ...

Message 2019-02-06 13:34:39.643 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator
: Host '192.168.200.102' (nw-platform-decoder) version '11.2.0.0' not
supported, minimum required version: 11.3.0.0
2019-02-06 13:34:39.644 ERROR 8540 --- [main] c.r.n.i.o.client.HostValidator
: Host '192.168.200.101' (nw-platform-concentrator) version '11.2.0.0' not
supported, minimum required version: 11.3.0.0
...

Cause cert-reissue -host-all command string failed because one or more hosts are
running a version earlier than 11.3.0.0

Note: You can force the reissue of certificates for the remaining hosts using the `-skip-version-checks` argument.

Solution Update the host to 11.3 or later and run `cert-reissue` for that host again.

Status Partial

Error

Message

```
...
2019-02-06 02:27:09.078 ERROR 20647 --- [ main]
c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '<IP-address>'
(nw-platform-decoder)

2019-02-06 02:27:09.079 ERROR 20647 --- [ main]
c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '<IP-address>'
(nw-platform-concentrator)

...
2019-02-06 02:27:09.118 WARN 20647 --- [ main]
c.r.n.i.o.client.OrchestrationClient : One or more host(s) may require manual
refresh due to failed triggers:
```

Cause cert-reissue command completed on NW Server host however one or more triggers failed. This aborted the cert-reissue command for other hosts.

Solution Address all the errors and run the cert-reissue --host--all<arguments> command string again.

Status Partial

Error ...

Message

```
2019-02-06 14:18:03.208 ERROR 17800 --- [ main]
c.r.n.i.o.client.OrchestrationClient : Trigger failed for host '192.168.200.82'
(nw-platform-node-x)
...
...
2019-02-06 14:29:05.200 WARN 17800 --- [ main]
c.r.n.i.o.client.OrchestrationClient : One or more host(s) may require manual
refresh due to failed triggers:
```

Cause One or more hosts did not pass system health checks. In addition, one or more of the unhealthy hosts are running core services, which will result in the NW Server host `cert-reissue` to fail (because of failed triggers explained above). By disabling health checks and trigger errors, you can continue the process and reissue certificates for the remaining hosts. The NW Server host **Status** is reported as `Partial` because the `cert-reissue` command completed for the NW Server but downstream triggers failed for other hosts.

Solution Manually refresh the failed core hosts (to synchronize trust peers).

Submit the following command string to reissue certificates for healthy hosts.

```
cert-reissue --host-all --skip-health-checks --ignore-trigger-errors
```