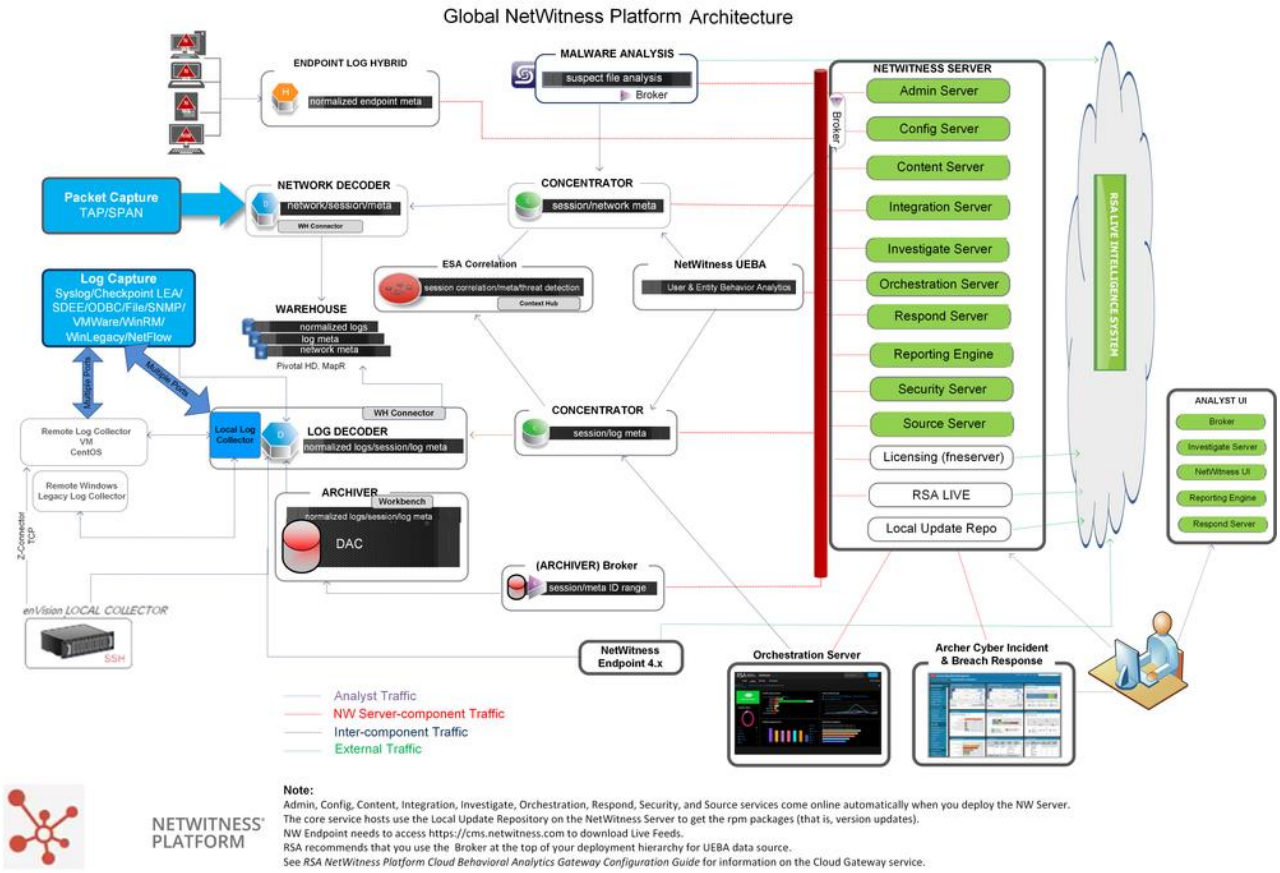
Network Architecture and Ports

Refer to the following diagrams and port tables to ensure that all the relevant ports are opened for components in your NetWitness deployment to communicate with each other. See NetWitness Endpoint Architecture at the end of this topic for individual Endpoint Architectural diagrams.

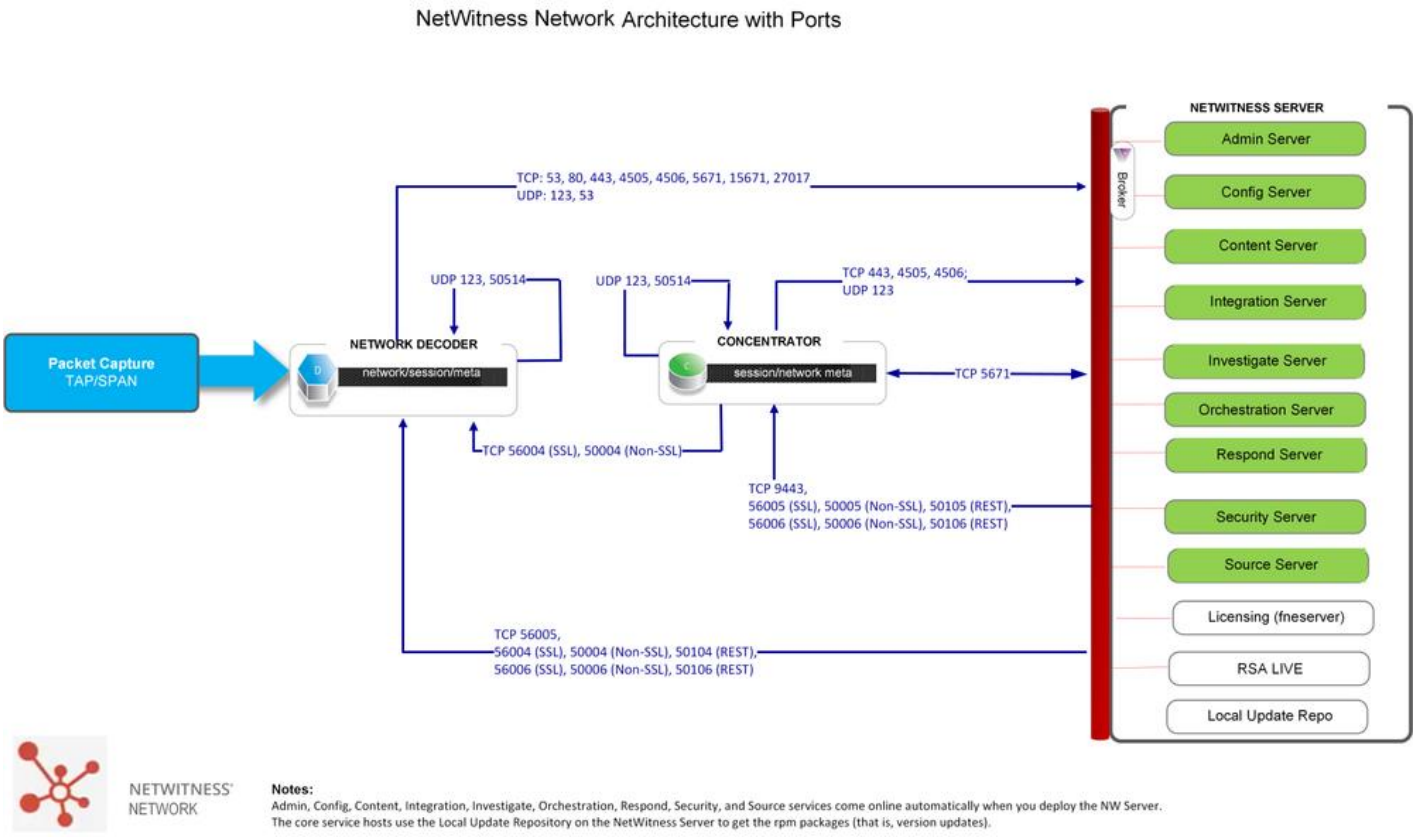
NetWitness Network Architecture Diagram

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

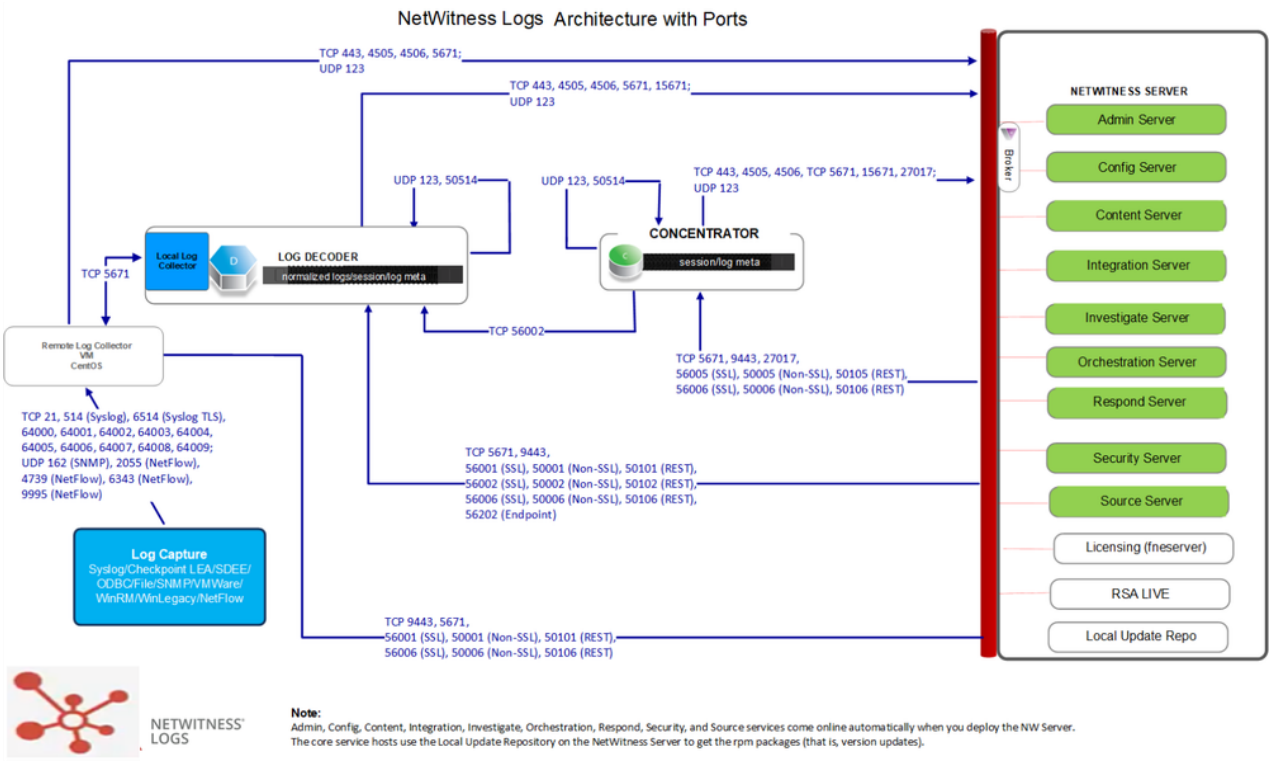
Note: NetWitness core hosts must be able to communicate with the NetWitness Server (Primary Server in a multiple server deployment) through UDP port 123 for Network Time Protocol (NTP) time synchronization.



NetWitness Network (Packets) Architecture Diagram with Ports

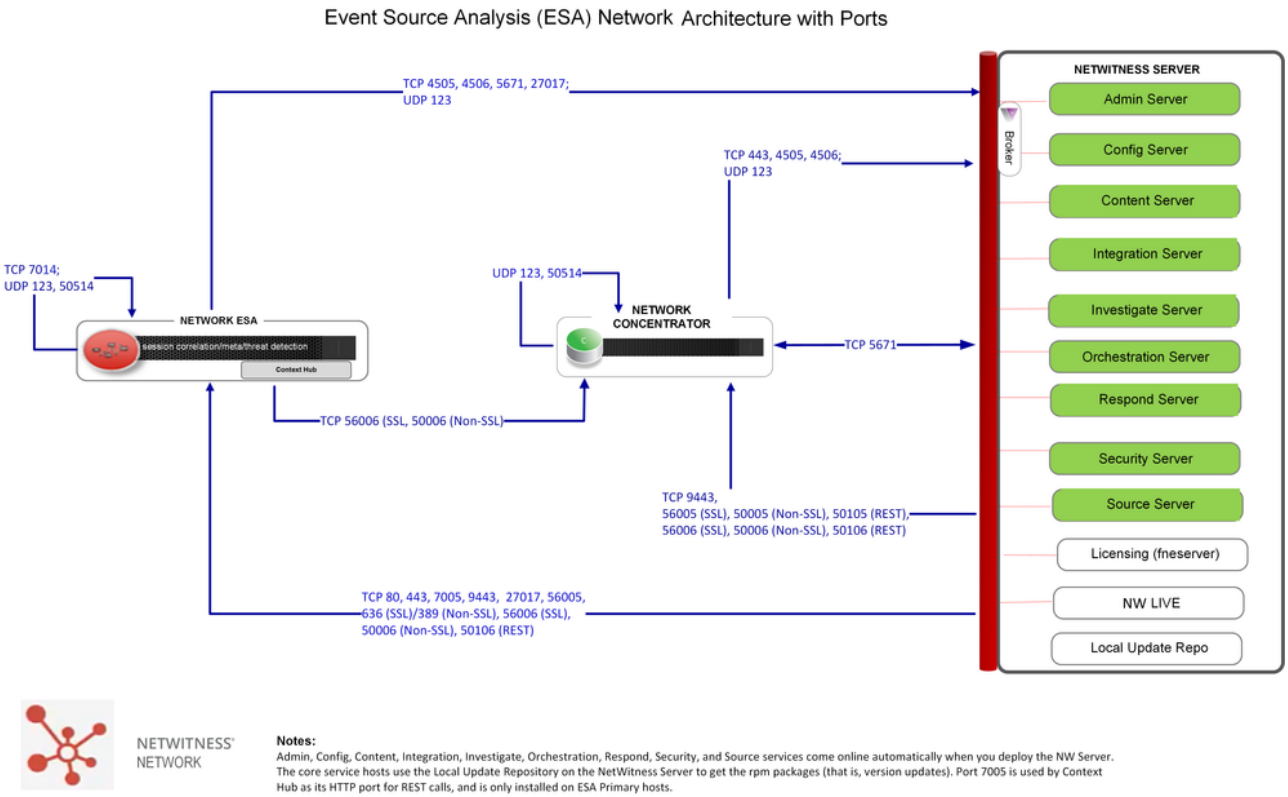


NetWitness Logs Architecture Diagram with Ports



Event Stream Analysis Network (Packets) Architecture Diagram with Ports

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

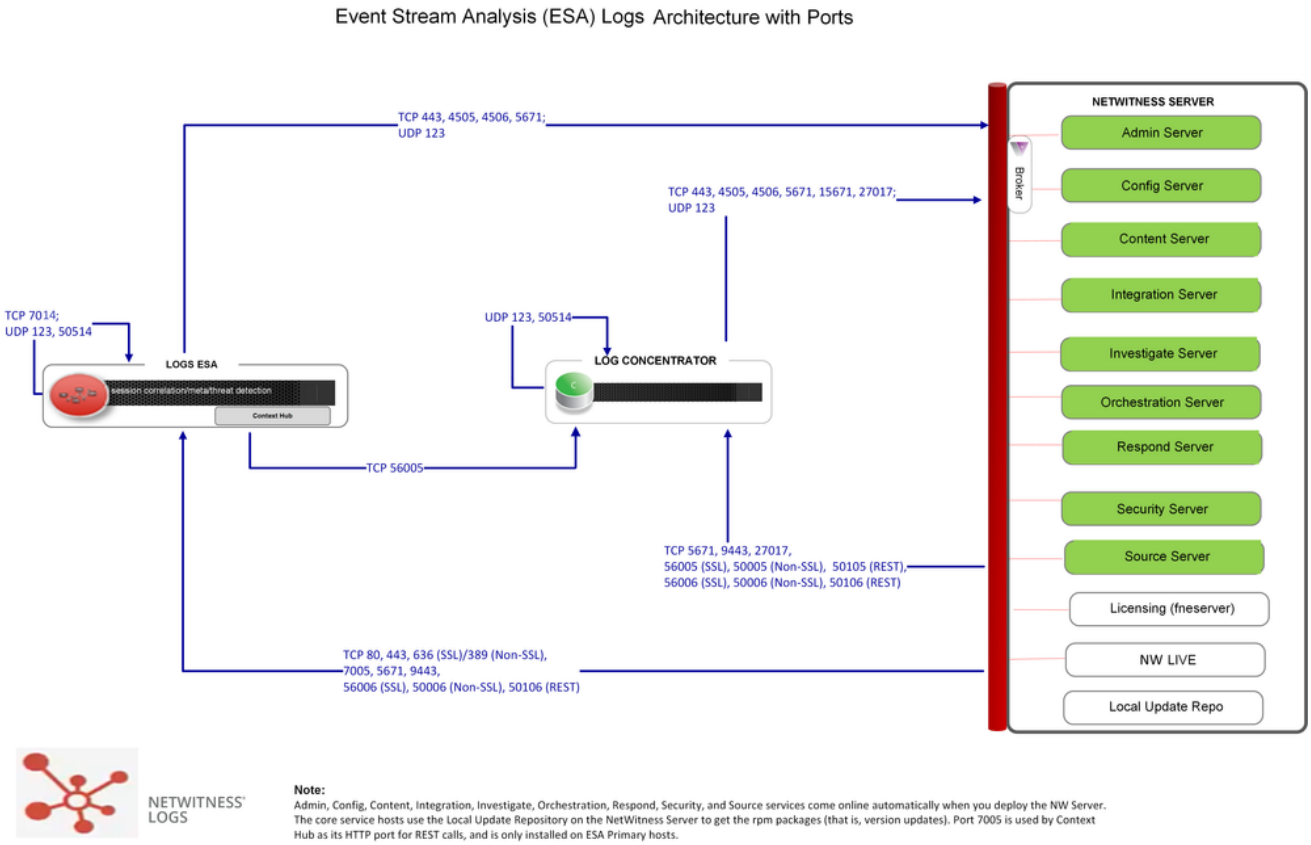


NETWITNESS
NETWORK

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.



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 Stanby is done through TCP Port 22.

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

Source Host	Destination Host	Ports
		56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL) **UDP:** 123
NW Server	Log Hybrid - Retention	**TCP:** 22, 5671, 50001 (Non-SSL), 50002 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56006 (SSL) **UDP:** 123
NW Server	Endpoint Log Hybrid	**TCP:** 22, 5671, 7050, 7054, 50001 (Non-SSL), 50002 (Non-SSL), 50005 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50102 (REST), 50105 (REST), 50106 (REST), 56001 (SSL), 56002 (SSL), 56005 (SSL), 56006 (SSL), 56202 (Endpoint) **UDP:** 123
NW Server	VLC	**TCP:** 22, 5671, 50001 (Non-SSL), 50006 (Non-SSL), 50101 (REST), 50106 (REST), 56001 (SSL), 56006 (SSL) **UDP:** 123
NW Server	Archiver	**TCP:** 22, 514, 5671, 6514, 50006(Non-SSL), 50007 (Non-SSL), 50008 (Non-SSL), 50106 (REST), 50107 (REST), 50108 (REST), 56006 (SSL), 56007 (SSL), 56008 (SSL) **UDP:** 123, 514
NW Server	Malware	**TCP:** 22, 5671, 5432, 50003 (Non-SSL), 50006 (Non-SSL), 50103 (REST), 50106 (REST), 56003 (SSL), 56006 (SSL), 60007 **UDP:** 123
NW Server	UEBA	**TCP:** 22, 15671, 5671, 443 **UDP:** 123
ESA	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 444 **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

Source Host	Destination Host	Ports
ESA Primary or Secondary	Concentrator	**TCP:** 50005 (Non-SSL), 56005 (SSL)
Network Decoder	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 444 **UDP:** 53, 123
Concentrator (Network & Logs)	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 444 **UDP:** 53, 123
Network Hybrid	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 444 **UDP:** 53, 123
Log Decoder	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671, 15671, 27017, 444 **UDP:** 53, 123
Log Hybrid	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671,15671, 27017, 444 **UDP:** 53, 123
Log Hybrid - Retention	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671,15671, 27017, 444 **UDP:** 53, 123
Broker	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671,15671, 27017, 444 **UDP:** 53, 123
VLC	NW Server	**TCP:** 53, 80, 443, 4505, 4506, 5671,15671, 27017, 444 **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, 444 **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, 444, 4505, 4506, 5671, 15671, 27017, 50003 (Broker-

Source Host	Destination Host	Ports
		Non-SSL), 50103 (Broker/REST), 56003 (Broker/SSL) **UDP:** 53, 123
UEBA	Concentrator	**TCP:** 50005 (Non-SSL), 50105 (REST), 56005 (SSL)
www connections		
NW Server	cms.netwitness.com download.rsasecurity.com rsasecurity.subscribenet.com update.netwitness.com	**TCP:** 443
ESA (Primary & Secondary)	cms.netwitness.com	**TCP:** 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 *Log Collection Configuration Guide for RSA NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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 sy nchronization port.
NW Hosts	NW Server	TCP 444	Node-infra-server check
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	cms.netwitness.com	TCP 443	Live Content Management System (CMS) Library
NW Server	download.rsasecurity.com	TCP 443	RSA Licensing
NW Server	rsasecurity.subscribenet.com	TCP 443	RSA Licensing
NW Server	update.netwitness.com	TCP 443	NetWitness Software Updates
NW Server	NFS Server	TCP 111, 2049, UDP 111, 2049	iDRAC Installations
NW Server	NW Hosts	UDP 123	NTP
NW Server	NW Endpoint	TCP 443, 9443	For NW Endpoint 4.x integrations
NW Hosts	NW Server	TCP 444	nw-node-infra service failover check

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 Hosts	TCP 5671	RabbitMQ-amqp
Analyst UI	NW Server	UDP 123	NTP
Analyst UI	NW Server	TCP 444	nw-node-infra service failover check
Analyst UI	Log Collector	TCP 56001	Log Collector application ports

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.

Source Host	Destination Host	Destination Ports	Comments
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
Archiver	NW Server	TCP 444	nw-node-infra service failover check

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
Broker	NW Server	TCP 444	nw-node-infra service failover check

Concentrator Host

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

Source Host	Destination Host	Destination Ports	Comments
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
Concentrator	NW Server	TCP 444	nw-node-infra service failover check

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)	To forward meta to an external Log Decoder

Source Host	Destination Host	Destination Ports	Comments
		50202 (Protobuf)	
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 Log Hybrid	NW Server	TCP 444	nw-node-infra service failover check

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 an ESA Secondary hosts. The Content Hub, Correlation and ESA Analytics services are co-located on the ESA Primary host. The Correlation and ESA Analytics services are co-located on the ESA Secondary host.

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	ESA	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 15671	RabbitMQ Management UI
ESA Primary and Secondary	NW Server	TCP 443	RSA Update Repository
Admin Workstation	ESA	TCP 22	SSH
NW Server, ESA Secondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
ESA Primary and Secondary	cms.netwitness.com	TCP 443	Live
ESA Primary and Secondary	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
ESA Primary and Secondary	Active Directory	636 (SSL)/389 (Non-SSL)	
NW Server	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Non-SSL)	
ESA Primary	ESA Primary	TCP 7014	Launch Port
ESA Primary and Secondary	NW Server	TCP 444	nw-node-infra service failover check

New Health and Wellness

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

New Health and Wellness on Different Subnet

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

Example:

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

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

iDRAC Ports

Port	Function	Comments
22*	SSH	Default, configurable port through which iDRAC listens for connections
443*	HTTP	Default, configurable port through which iDRAC listens for connections

Port	Function	Comments
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 *Log Collection Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.	
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

Source Host	Destination Host	Destination Ports	Comments
			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 Collector	NW Server	TCP 444	nw-node-infra service failover check

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 *Log Collection Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.	
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

Source Host	Destination Host	Destination Ports	Comments
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 Decoder	NW Server	TCP 444	nw-node-infra service failover check

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 *Log Collection Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.	
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

Source Host	Destination Host	Destination Ports	Comments
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	NW Server	TCP 444	nw-node-infra service failover check

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 *Log Collection Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.	
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

Source Host	Destination Host	Destination Ports	Comments
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
Log Hybrid - Retention	NW Server	TCP 444	nw-node-infra service failover check

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

Source Host	Destination Host	Destination Ports	Comments
Malware	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
Malware	NW Server	TCP 444	nw-node-infra service failover check

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 Decoder	NW Server	TCP 444	nw-node-infra service failover check

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

Source Host	Destination Host	Destination Ports	Comments
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
Network Hybrid	NW Server	TCP 444	nw-node-infra service failover check

UEBA Host

Source Host	Destination Host	Destination Ports	Comments
UEBA Server	NW Server	TCP 443	RSA Update Repository
UEBA Server	Broker	TCP 56003 (SSL), 50103 (REST)	Broker Application Ports
UEBA Server	Concentrator	TCP TCP 50005 (Non-SSL), 56005 (SSL), 50105 (REST)	Concentrator Application Ports
Admin Workstation	UEBA Server	443	UEBA Monitoring
Admin Workstation	UEBA Server	22	SSH
Admin Workstation	UEBA Server	TCP 15671	RabbitMQ Management UI
UEBA Server	NW Server	TCP 15671	UEBA Alerts forwarding to Respond
NW Server	NFS Server	TCP 111, 2049 UDP 111, 2049	iDRAC Installations
NW Server	UEBA Server	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts
UEBA Server	NW Server	TCP 444	nw-node-infra service failover check

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	UEBA Server	8100	Airflow UI

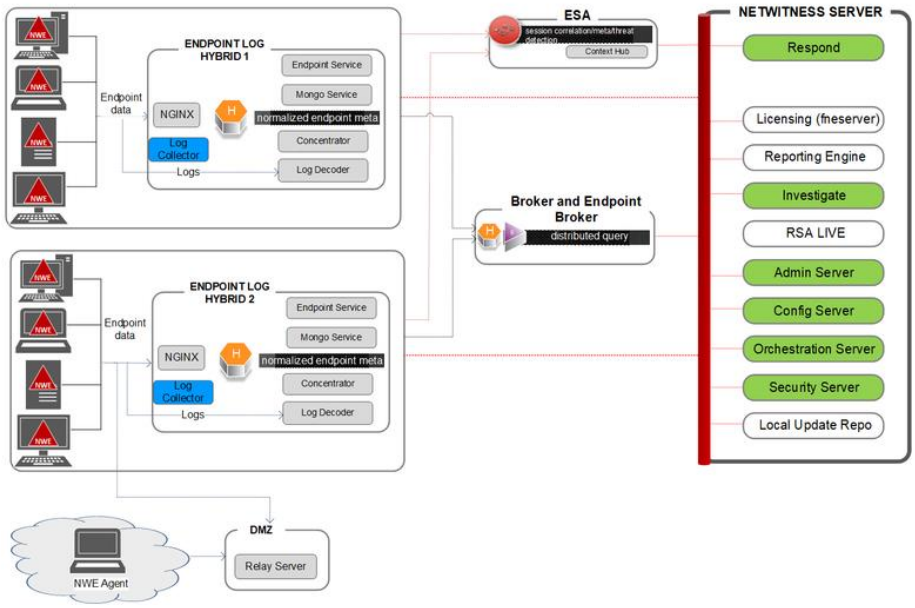
Recommended Network Bandwidth Between NetWitness Components

To ensure optimal performance and reliability of the NetWitness deployment, it is crucial to maintain adequate network bandwidth between various components. The table below outlines the recommended network bandwidth for key connections between NetWitness components.

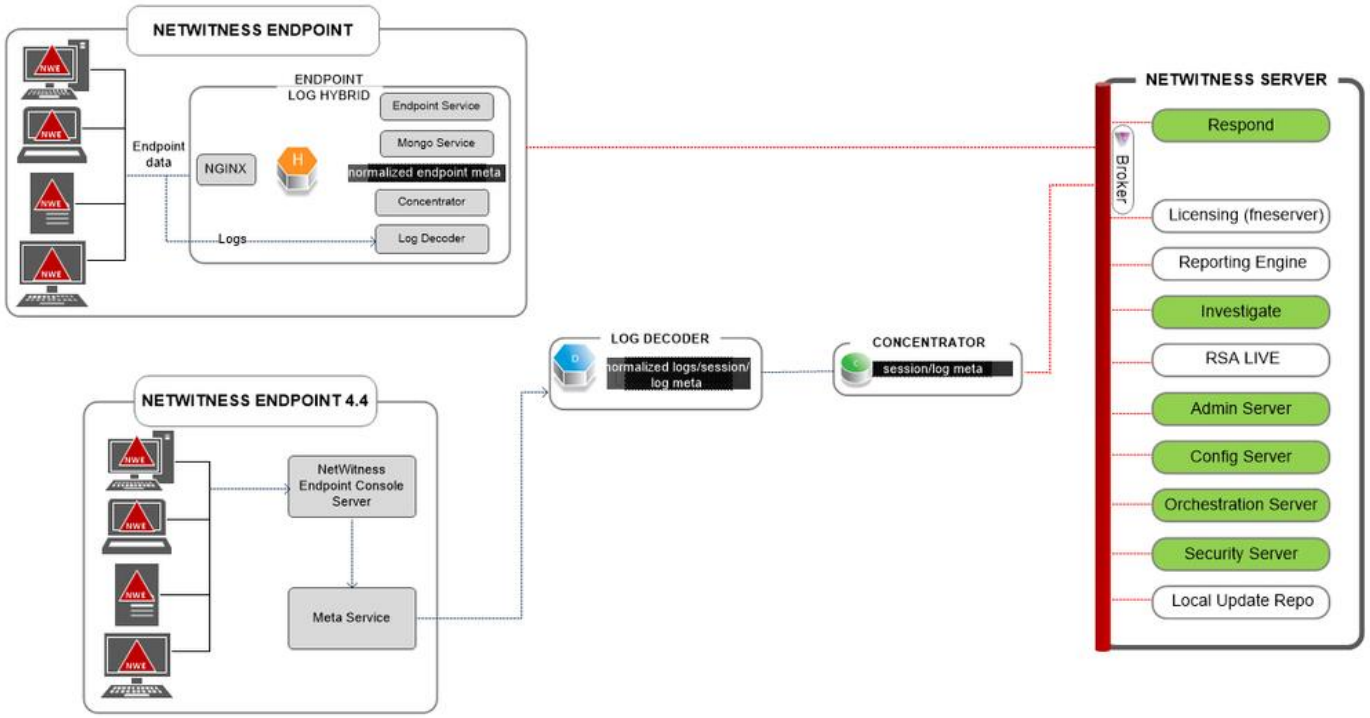
Components	Recommended Network Bandwidth
Between Concentrator and ESA	100 Mbps
Between Log Decoder and Concentrator	100 Mbps
Between Packet Decoder and Concentrator	100 Mbps
Between Admin Server and ESA	100 Mbps
Between Concentrator and Broker	100 Mbps

NetWitness Endpoint Architecture

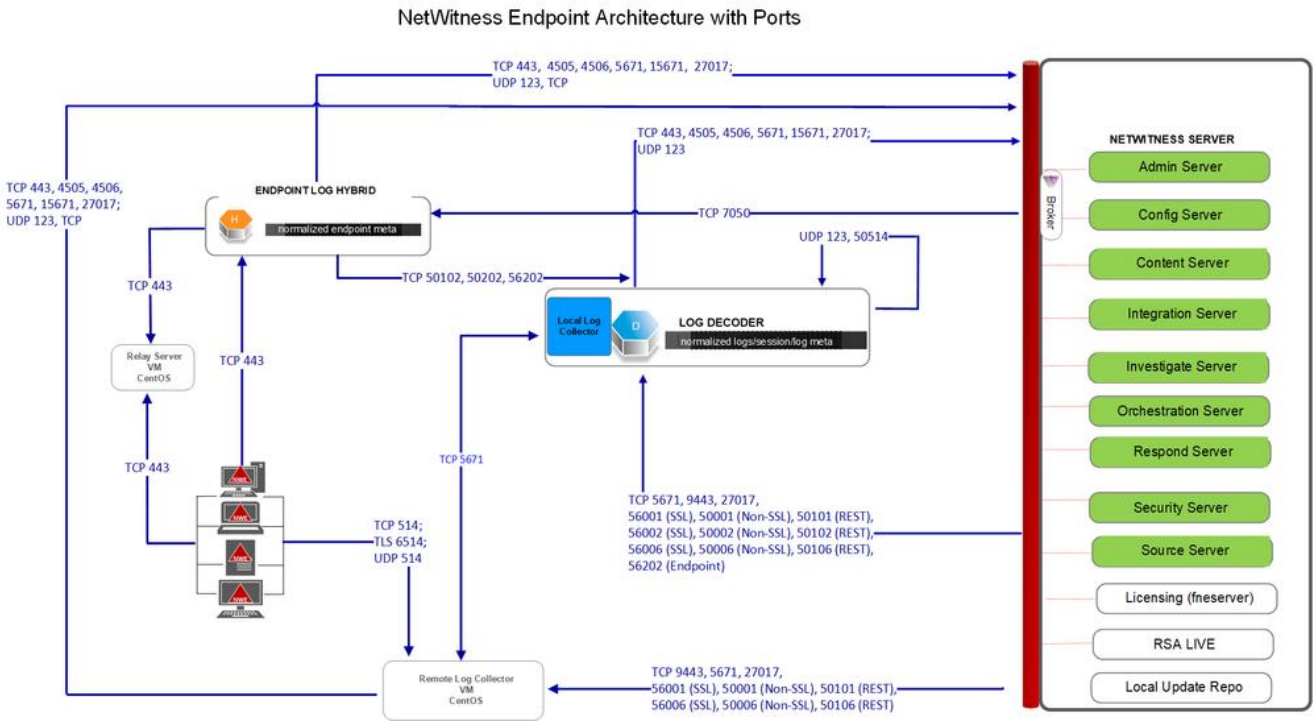
NetWitness Endpoint Architecture



NetWitness Endpoint 4.4 Integration with NetWitness Platform



NetWitness Endpoint Architecture with Ports



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

How to Change UDP Port for Endpoint Log Hybrid

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

There are two tasks you need to o 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 are overwritten 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  (Admin) > Endpoint Sources > Policies. The Policies view is displayed.

2. Select the Default EDR Policy and click Edit from the toolbar.

3. roll down to find the UDP PORT and change the value (for example, change from 444 to 555).

4. Click Publish Policy at the bottom of the view.

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

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

1. Update the `iptables` rules to allow `555` in place of `444`.
    a. Replace `444` with `555` in the following file.
    `vi /etc/sysconfig/iptables`
    b. Restart `iptables` with the following command string.
    `systemctl restart iptables`

c. Verify the change with the following command string.
   `iptables -L -n`
   The following is an example of what is displayed for a correct change.
   `ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /* EndpointNginxPort */ ctstate NEW`

2. Update the SELinux policy. 555 is a privileged port, so you must update SELinux policy to allow this port.
   a. Run the following command string.
      `semanage port -a -t http_port_t -p udp 555`
      If you received any python errors or warnings, ignored them.
   b. Verify the change with the following command string.
      `semanage port -l | grep http_port_t`
      The following is an example of what is displayed for a correct change.
      `http_port_t udp 555, 444`
   c. (Optional) Remove `444`.

3. Update nginx config.
   a. Edit the following file.
      `vi /etc/nginx/nginx.conf`
   b. Search for the following string.
      `listen 444 udp;`
   c. Replace `444` with `555`.
   d. Restart nginx with the following command string.
      `systemctl restart nginx`

4. Verify that agents are communicating over the new port.
   a. Run the following command string.
      `tcpdump -i eth0 port 555`
   b. Wait for 30 seconds because the port sends out a beacon every 30 seconds. If t everything is working correctly, information similar to the following will be displayed.
      ```
      09:20:12.571316 IP 10.40.15.103.60807 >
      EPS1.rsa.lab.emc.com.dsf: UDP, length 20
      09:20:12.572433 IP EPS1.rsa.lab.emc.com.dsf >
      10.40.15.103.60807: UDP, length 1
      ```
      Both lines must be returned. One is the size request (`20` bytes) and the other is the response size (`1` byte).