



Leitfaden zur Bereitstellung

für Version 11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Kontaktinformationen

RSA Link unter <https://community.rsa.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens Dell ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2019

Inhalt

Die Grundlagen	5
Einfache Bereitstellung	6
Prozess	6
Allgemeines Bereitstellungsdiagramm für NetWitness Platform	8
Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Platform	9
Netzwerkarchitektur und Ports	10
Diagramm der NetWitness Platform-Netzwerkarchitektur	10
Umfassende Liste der Host- und Serviceports von NetWitness Platform	11
NW-Serverhost	12
Archiver-Host	13
Broker-Host	14
Concentrator-Host	15
Endpoint Hybrid oder Endpoint Log Hybrid	16
Endpoint Hybrid oder Endpoint Log Hybrid mit NetWitness Endpoint 4.4	16
Event Stream Analysis (ESA)-Host	17
Log Collector-Host	18
Log Decoder-Host	20
Log Hybrid-Host	22
Malware-Host	24
Network Decoder-Host	25
Network Hybrid-Host	26
UEBA-Host	27
NetWitness Endpoint Insights-Architektur	28
NetWitness Endpoint Insights 11.2	28
NetWitness Endpoint Insights 11.2 mit Log Decoder	29
Integration von NetWitness Endpoint 4.4 in NetWitness Endpoint Insights 11.2	29
Anforderungen an den Standort und Sicherheit	31
Vorgesehene Anwendung	31
Service	31
Sicherheitsinformationen	31
Standortauswahl	31
Vorgehensweise zur Handhabung des Geräts	31
Warnhinweise für Strom und Elektronik	32
Warnhinweise für Rackmontage	32
Kühlung und Luftstrom	32

Antennenpositionierung	32
Konfiguration der Gruppenaggregation	33
Empfehlungen zur Bereitstellung der RSA-Gruppenaggregation	33
Vorteile bei Verwendung der Gruppenaggregation	33
Konfiguration der Gruppenaggregation	36
Voraussetzungen	36
Einrichten der Gruppenaggregation	38

Die Grundlagen

In diesem Handbuch werden die grundlegenden Anforderungen einer NetWitness Platform-Bereitstellung beschrieben und optionale Szenarien zur Erfüllung der Anforderungen Ihres Unternehmens dargestellt. Selbst in kleinen Netzwerken kann durch gute Planung dafür gesorgt werden, dass alles reibungslos verläuft, wenn Sie bereit sind, die Hosts online zu schalten.

Hinweis: In diesem Dokument wird auf mehrere zusätzliche Dokumente Bezug genommen, die in RSA Link verfügbar sind. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Es gibt viele Faktoren, die Sie berücksichtigen müssen, bevor Sie NetWitness Platform bereitstellen. Die folgenden Elemente sind nur einige dieser Faktoren. Sie müssen bei der Berücksichtigung dieser Faktoren das Wachstum und die Speicheranforderungen abschätzen

- Größe Ihres Unternehmens (d. h. die Anzahl der Standorte und Personen, die NetWitness Platform verwenden werden)
- Menge der Netzwerkdaten und Protokolle, die Sie verarbeiten müssen
- Performance, die jede einzelne NetWitness Platform-Benutzerrolle benötigt, um ihre Jobs effektiv ausführen zu können
- Vermeidung von Ausfallzeiten (d. h. Vermeiden eines Single-Point-of-Failure).
- Die Umgebung, in der Sie NetWitness Platform ausführen möchten
 - Physische RSA-Hosts (Software, die auf von RSA bereitgestellter Hardware ausgeführt wird)
Detaillierte Anweisungen zur Bereitstellung physischer RSA-Hosts finden Sie im *RSA NetWitness® PlatformHandbuch zur Installation physischer Hosts*.
 - Nur von RSA bereitgestellte Software:
 - Lokale virtuelle Hosts
Detaillierte Anweisungen zur Bereitstellung lokaler virtueller Hosts finden Sie im *RSA NetWitness® PlatformHandbuch zur Installation virtueller Hosts*.
 - VCloud:
 - Amazon Web Services (AWS)
Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in AWS finden Sie im *RSA NetWitness® PlatformAWS-Bereitstellungsleitfaden*.
 - Azure
Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in Azure finden Sie im *RSA NetWitness® PlatformAzure-Bereitstellungsleitfaden*.

Einfache Bereitstellung

Vor der Bereitstellung von NetWitness Platform müssen Sie folgende Voraussetzungen erfüllen:

- Sie haben die Anforderungen Ihres Unternehmens berücksichtigt und verstehen den Bereitstellungsprozess.
- Sie haben einen allgemeinen Überblick über die Komplexität und den Umfang einer NetWitness Platform-Bereitstellung.

Prozess

Die Komponenten und die Topologie eines NetWitness Platform-Netzwerks können bei individuellen Installationen stark abweichen und sollten sorgfältig geplant werden, bevor der Prozess startet. Die anfängliche Planung umfasst Folgendes:

- Berücksichtigung der Standort- und Sicherheitsanforderungen
- Prüfung der Netzwerkarchitektur und Portnutzung
- Unterstützung der Gruppenaggregation auf Archivers und Concentrators und virtuellen Hosts

Wenn Sie bereit sind, mit der Bereitstellung zu beginnen, ist die allgemeine Abfolge wie folgt:

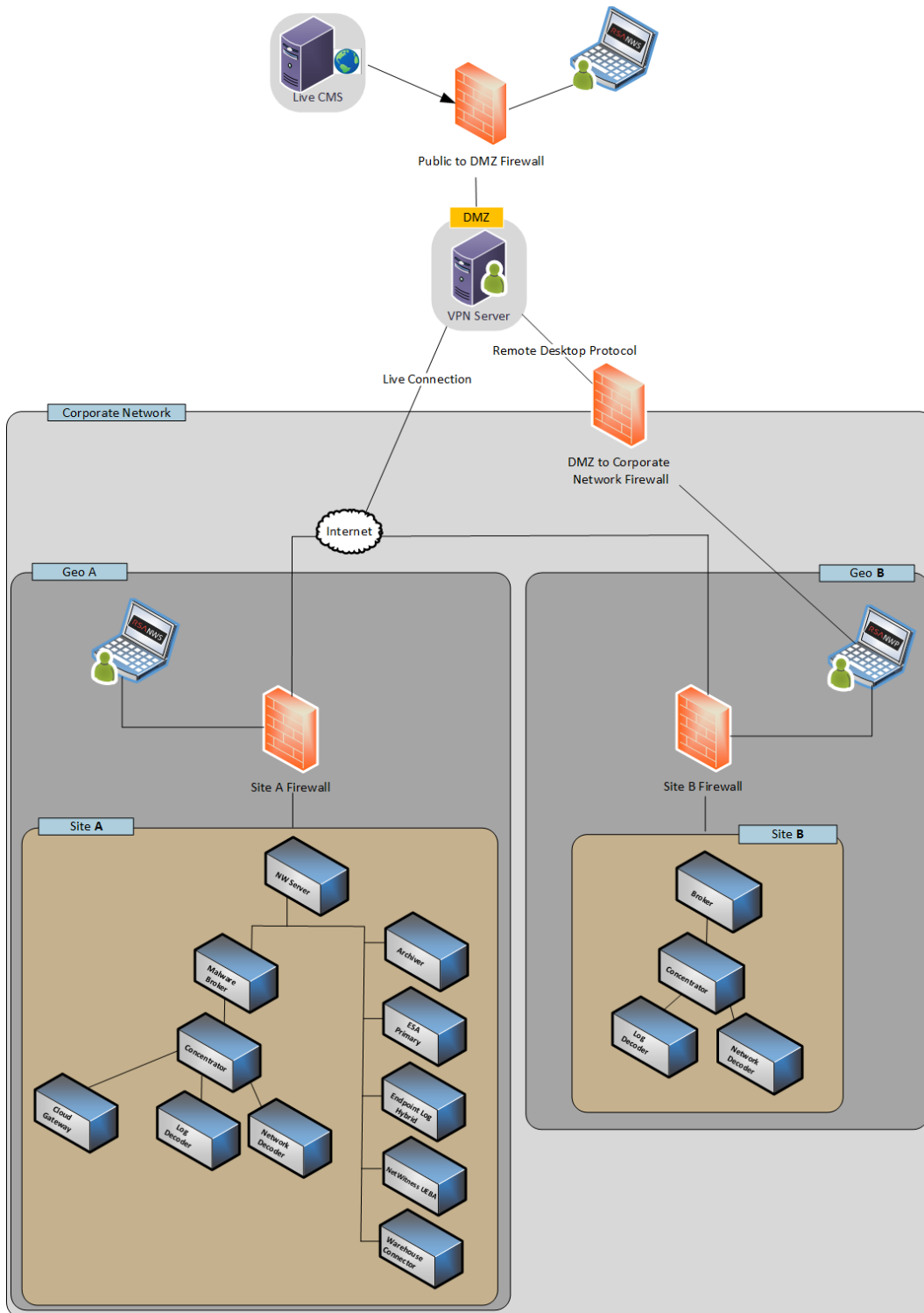
- Für physische RSA-Hosts:
 1. Installieren Sie physische Hosts und stellen Sie eine Verbindung mit dem Netzwerk her, wie im Leitfaden zur Hardwarekonfiguration von RSA NetWitness® Platform und im *RSA NetWitness® Platform Handbuch zur Installation physischer Hosts* beschrieben.
 2. Richten Sie die Lizenzierung für NetWitness Platform ein, wie im *RSA NetWitness® Platform Handbuch zur Lizenzierung* beschrieben.
 3. Konfigurieren Sie einzelne physische Hosts und Services, wie im *RSA NetWitness® Platform Leitfaden für die ersten Schritte mit Hosts und Services* beschrieben. In diesem Leitfaden finden Sie auch Verfahren zur Anwendung von Updates und zur Vorbereitung auf Versionsupgrades.
- Für lokale virtuelle Hosts befolgen Sie die Anweisungen im *RSA NetWitness® Platform Leitfaden zur Einrichtung von virtuellen Hosts*.
- Für AWS befolgen Sie die Anweisungen im *RSA NetWitness® Platform AWS-Bereitstellungsleitfaden*.
- Für Azure befolgen Sie die Anweisungen im *RSA NetWitness® Platform Azure-Bereitstellungsleitfaden*.

Wenn Sie Hosts und Services aktualisieren, befolgen Sie die empfohlenen Richtlinien unter dem Thema „Ausführen im gemischten Modus“ im *RSA NetWitness Platform Leitfaden für die ersten Schritte mit Hosts und Services*.

Außerdem sollten Sie sich mit Hosts, Hosttypen und Services vertraut machen, da sie im Zusammenhang mit NetWitness Platform verwendet werden. Eine Beschreibung finden Sie im *RSA NetWitness Platform Leitfaden für die ersten Schritte mit Hosts und Services*.

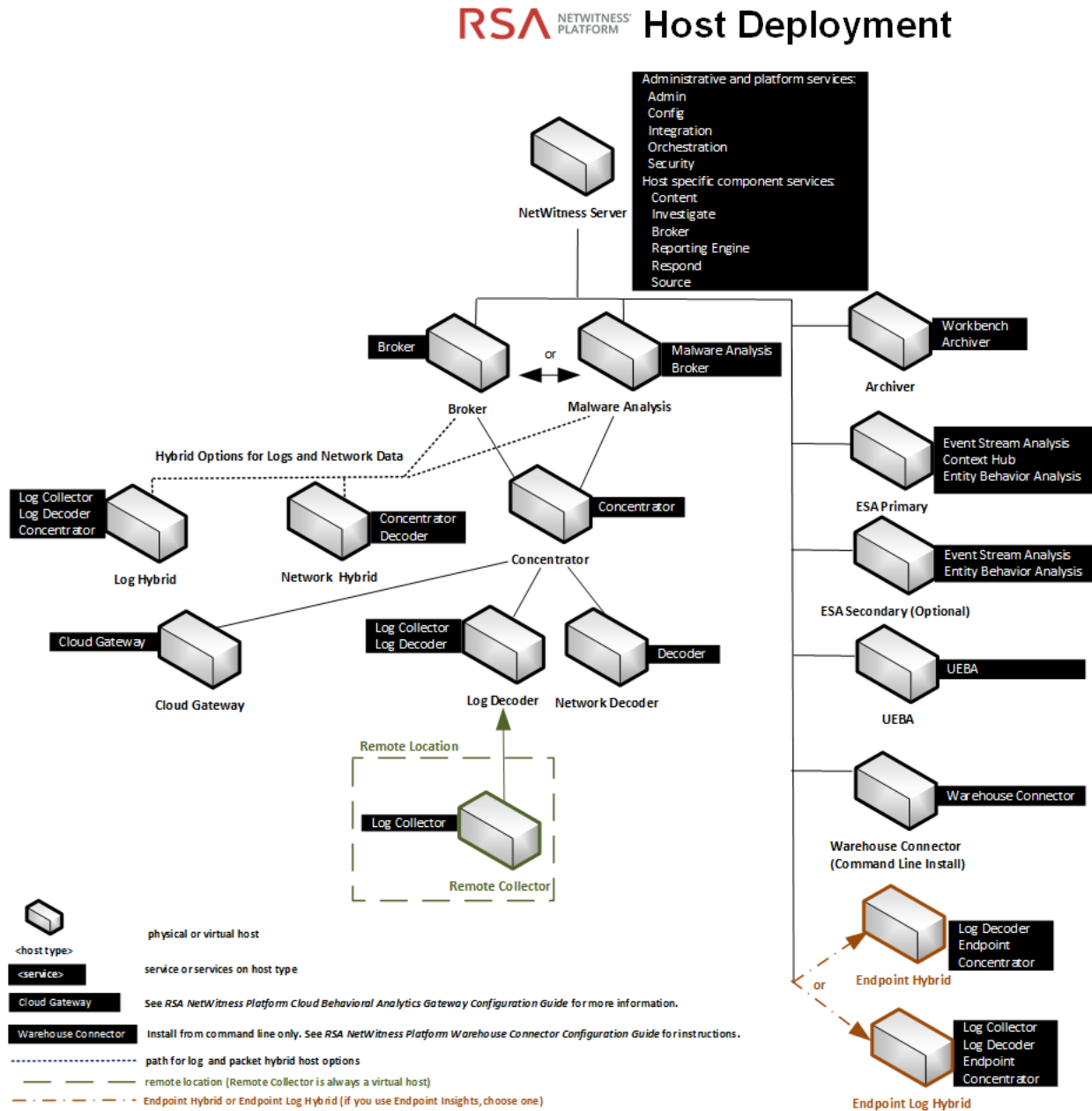
Allgemeines Bereitstellungsdiagramm für NetWitness Platform

Im folgenden Diagramm ist eine einfache NetWitness Platform-Bereitstellung an mehreren Standorten dargestellt.



Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Platform

Das folgende Diagramm zeigt ein Beispiel einer NetWitness Platform-Bereitstellung, die auf physischen oder virtuellen Rechnern gehostet wird. Anweisungen zum Installieren von NetWitness Platform finden Sie im *Installationshandbuch für physische Hosts*, im *Handbuch zur Installation virtueller Hosts*, im *AWS-Bereitstellungsleitfaden* oder im *Azure-Bereitstellungsleitfaden*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.



Netzwerkarchitektur und Ports

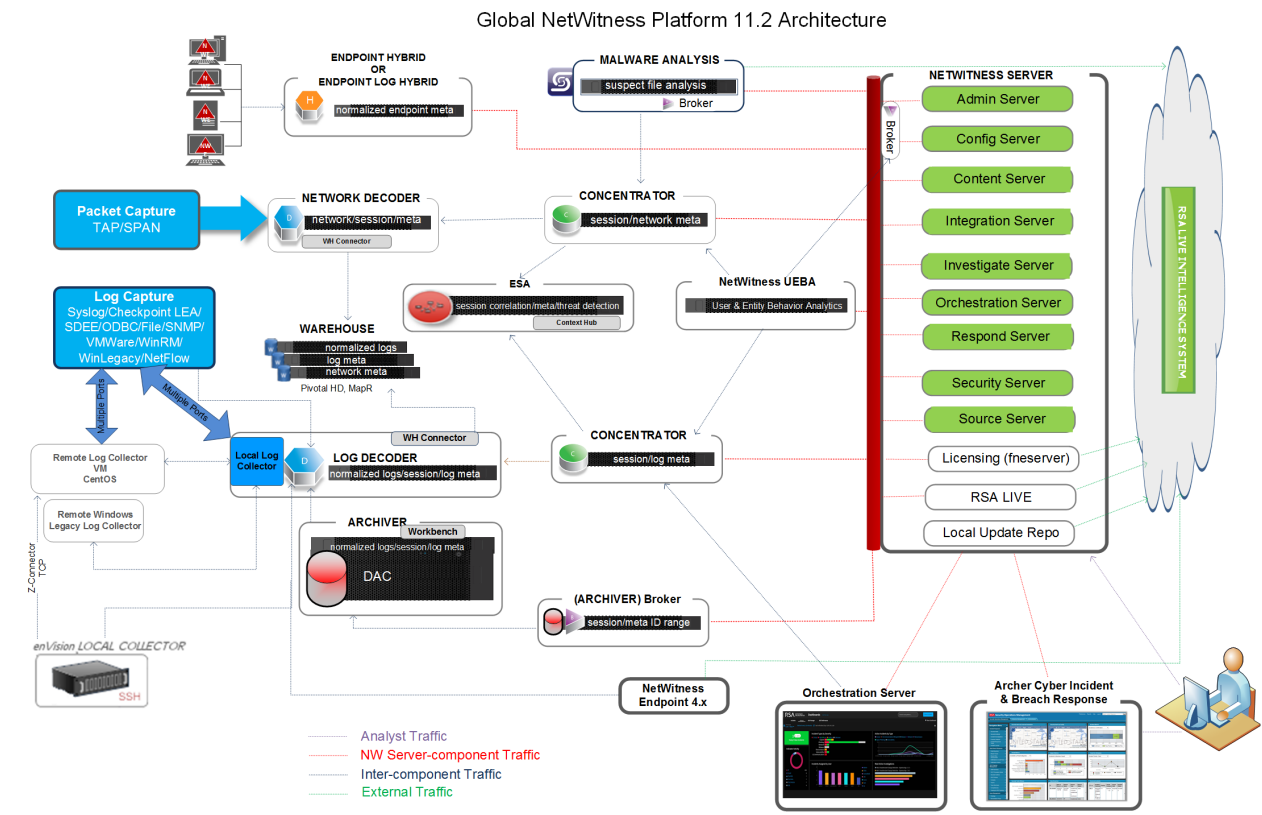
Mit den Informationen im folgenden Diagramm und in der Porttabelle können Sie sicherstellen, dass alle relevanten Ports für Komponenten in Ihrer NetWitness Platform-Bereitstellung geöffnet sind und miteinander kommunizieren können.

Einzelne Endpunkt-Architekturdiagramme finden Sie unter [NetWitness Endpoint Insights-Architektur](#) am Ende dieses Themas.

Diagramm der NetWitness Platform-Netzwerkarchitektur

Das folgende Diagramm veranschaulicht die Netzwerkarchitektur von NetWitness Platform mit allen zugehörigen Produktkomponenten.

Hinweis: NetWitness Platform-Core-Hosts müssen mit dem NetWitness Server (dem primären Server in einer Bereitstellung mit mehreren Servern) über UDP-Port 123 kommunizieren können, um eine NTP-Synchronisation (Network Time Protocol) durchzuführen.



Note:
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, and Security services come online automatically when you deploy the NW Server.
 The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).
 NW Endpoint needs to access <https://cms.netwitness.com> to download Live Feeds.
 RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.
 See [RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide](#) for information on the Cloud Gateway service.



Umfassende Liste der Host- und Serviceports von NetWitness Platform

Hinweis: Informationen zu Ports, die in der Ereignissammlung über die NetWitness Logs verwendet werden, finden Sie unter „Grundlagen“ im *RSA NetWitness Suite Leitfaden zur Bereitstellung der Protokollsammlung*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Dieser Abschnitt enthält die Portspezifikationen für die folgenden Hosts.

NW-Serverhost	Log Collector-Host
Archiver-Host	Log Decoder-Host
Broker-Host	Log Hybrid-Host
Concentrator-Host	Malware-Host
Endpoint Hybrid/Endpoint Log Hybrid Host	Network Decoder-Host
Event Stream Analysis-Host	Network Hybrid-Host
	UEBA-Host

NW-Serverhost

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	NW-Server	TCP 443, 80	NGINX – NetWitness-Benutzeroberfläche
NW-Hosts	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
NW-Hosts	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	NW-Server	TCP 22	SSH
NW-Hosts	NW-Server	TCP 4505, 4506	Salt Master-Ports
NW-Hosts	NW-Server	TCP 5671	RabbitMQ-amqp
NW-Server	NW-Server	UDP 50514	Auditdaten – Remote Syslog
NW-Hosts	NW-Server	UDP 123	NTP
NW-Server	NW-Hosts	UDP 123	NTP
NW-Hosts	NW-Server	TCP 27017	MongoDB
NW-Server	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
NW-Server	NW Endpoint	TCP 443, 9443	Für NW-Endpoint 4.x-Integrationen

Archiver-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Archiver	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Archiver	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Archiver	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Archiver	TCP 22	SSH
NW-Server	Archiver	TCP 56008 (SSL), 50008 (Nicht-SSL), 50108 (REST)	Archiver-Anwendungsports
NW-Server	Archiver	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Archiver	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
NW-Server	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Nicht-SSL), 50107 (REST), UDP 514	Workbench-Anwendungsports
Archiver	Archiver	UDP 50514	Auditdaten – Remote Syslog
Archiver	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Broker-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Broker	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Broker	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Broker	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Broker	TCP 22	SSH
NW-Server	Broker	TCP 56003 (SSL), 50003 (Nicht-SSL), 50103 (REST)	Broker-Anwendungsports
NW-Server	Broker	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Broker	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Broker	Broker	UDP 50514	Auditdaten – Remote Syslog
Broker	NW-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Concentrator-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Concentrator	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Concentrator	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Concentrator	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Concentrator	TCP 22	SSH
NW-Server	Concentrator	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW-Server	Concentrator	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Concentrator	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Concentrator	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
Concentrator	Concentrator	UDP 50514	Auditdaten – Remote Syslog

Endpoint Hybrid oder Endpoint Log Hybrid

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint 11.2 Agent	Endpoint Hybrid oder Endpoint Log Hybrid	TCP 443	NGINX HTTPS
Endpoint 11.2 Agent	Log Decoder oder Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows-Protokollsammlung
Endpunktserver	Log Decoder (extern)	TCP 50102, 56202, 50202	Um Metadaten an einen externen Log Decoder weiterzuleiten
Endpunktserver	NW-Server	TCP 443	RSA Update-Repository
NW-Server	Endpoint Hybrid oder Endpoint Log Hybrid	TCP 7050	Webdatenverkehr über die Benutzeroberfläche
Endpoint Hybrid oder Endpoint Log Hybrid	NW-Server	TCP 5671	Nachrichtenbus
Endpunktserver	NW-Server	TCP 27017	MongoDB

Endpoint Hybrid oder Endpoint Log Hybrid mit NetWitness Endpoint 4.4

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Konsolenserver (ab 4.4.0.2)	Endpoint Hybrid	TCP 443	NGINX HTTPS
Metadatenservice	Log Decoder	TCP 50102, 56202, 50202	NGINX HTTPS Um Metadaten an einen Log Decoder weiterzuleiten Endpoint Hybrid oder Endpoint Log Hybrid mit NWE 4.4

Event Stream Analysis (ESA)-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	ESA	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
ESA Primary und Secondary	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
ESA Primary und 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-Anwendungsport
NW-Server	ESA	TCP 50035 (SSL)	ESA-Anwendungsport
NW-Server	ESA	TCP 50036 (SSL)	ESA-Anwendungsport
NW-Server	ESA	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
ESA Primary und Secondary	cms.netwitness.com	TCP 443	Live
ESA Primary und Secondary	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
ESA Primary und Secondary	Active Directory	636 (SSL)/389 (Nicht-SSL)	
NW-Server	ESA	80 (HTTP)/443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Nicht-SSL)	
ESA Primary	ESA Primary	TCP 7007	Start-Port
ESA Primary	ESA Primary	UDP 50514	Auditdaten – Remote Syslog

Log Collector-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Collector	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Collector	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Collector	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Collector	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu Masterinhaltsverzeichnis , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Protokollsammelungsports
Protokollereignisquellen	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Protokollsammelungs-FTP/S-Ports
NW-Server	Log Collector	TCP 56001 (SSL), 50001 (Nicht-SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Collector	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Log Collector	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Log Collector	Log Collector	UDP 50514	Auditdaten – Remote Syslog

Quellhost	Zielhost	Zielports	Anmerkungen
Log Collector	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
Log Collector	Virtual Log Collector	TCP 5671	Im Pull-Modus
Virtual Log Collector	Log Collector	TCP 5671	Im Push-Modus

Log Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Decoder	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Decoder	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu Masterinhaltsverzeichnis , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammelungsports
Protokollereignisquellen	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammelungs-FTP/S-Ports
NW-Server	Log Decoder	TCP 56001 (SSL), 50001 (Nicht-SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Decoder	TCP 56002 (SSL), 50002 (Nicht-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Decoder	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS)- Nachrichtenbus für alle NW- Hosts.
Log Decoder	Log Decoder	UDP 50514	Auditdaten – Remote Syslog
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Log Hybrid-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Hybrid	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Hybrid	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Hybrid	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu Masterinhaltsverzeichnis , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammelungsports
Protokollereignisquellen	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammelungs-FTP/S-Ports
NW-Server	Log Hybrid	TCP 56001 (SSL), 50001 (Nicht-SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Hybrid	TCP 56002 (SSL), 50002 (Nicht-SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Hybrid	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Server	Log Hybrid	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS)- Nachrichtenbus für alle NW- Hosts
Log Hybrid	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Malware-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Malware	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Malware	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Malware	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Malware	TCP 22	SSH
NW-Server	Malware	TCP 60007	Malware-Anwendungsports
NW-Server	Malware	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Malware	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
NW-Server	Malware	TCP 5432	PostgreSQL
NW-Server	Malware	TCP 56003 (SSL), 50003 (Nicht-SSL), 50103 (REST)	Broker-Anwendungsports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community-Bewertung/Opwat
Malware	Malware	UDP 50514	Auditdaten – Remote Syslog
Malware	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Network Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Network Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Decoder	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Decoder	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Network Decoder	TCP 22	SSH
NW-Server	Network Decoder	TCP 56004 (SSL), 50004 (Nicht-SSL), 50104 (REST)	Network Decoder-Anwendungsports
NW-Server	Network Decoder	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Network Decoder	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Network Decoder	Network Decoder	UDP 50514	Auditdaten – Remote Syslog
Network Decoder	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Network Hybrid-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Network Hybrid	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Hybrid	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Hybrid	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Network Hybrid	TCP 22	SSH
NW-Server	Network Hybrid	TCP 56004 (SSL), 50004 (Nicht-SSL), 50104 (REST)	Network Decoder-Anwendungsports
NW-Server	Network Hybrid	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports
NW-Server	Network Hybrid	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Network Hybrid	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Network Hybrid	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

UEBA-Host

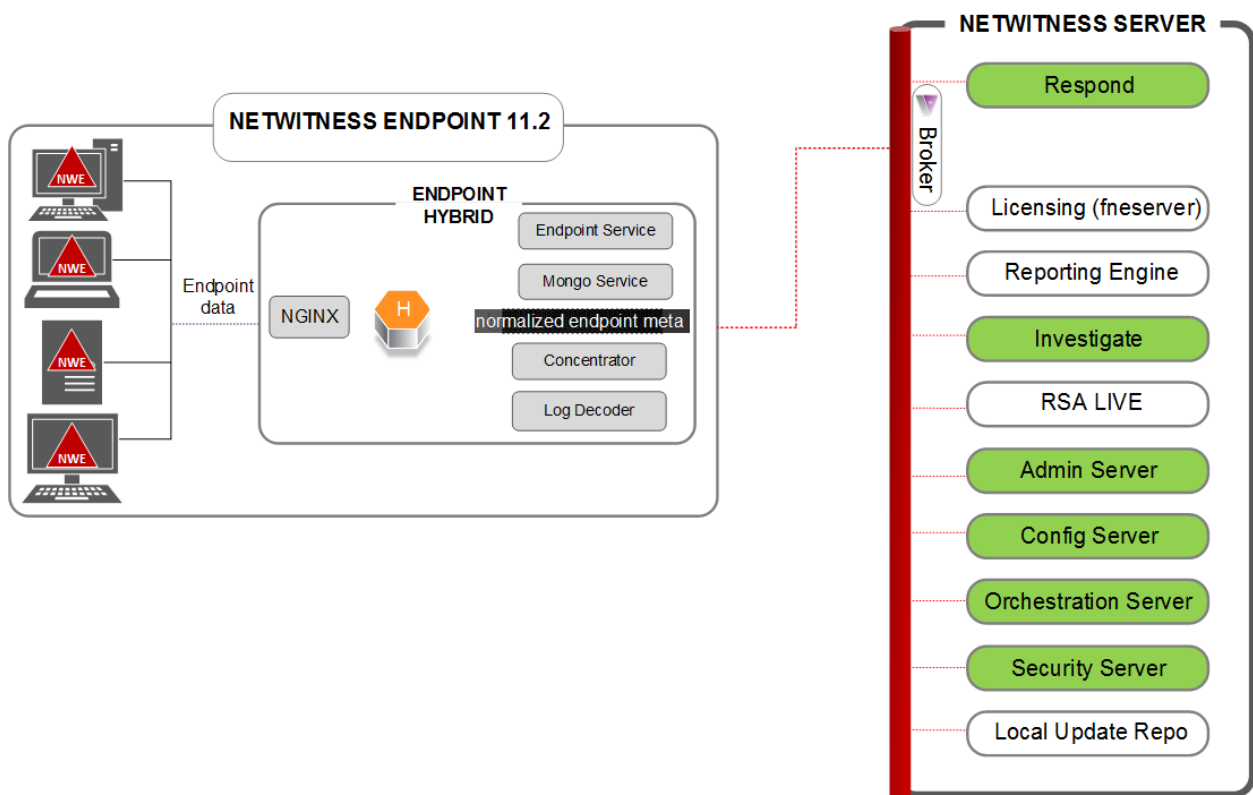
Quellhost	Zielhost	Zielports	Anmerkungen
UEBA-Server	NW-Server	TCP 443	RSA Update-Repository
UEBA-Server	NW-Server	TCP 56003 (SSL), 50003 (Nicht-SSL), 50103 (REST)	Broker-Anwendungsports
UEBA-Server	NW-Server	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports
Admin-Workstation	UEBA-Server	443	UEBA-Monitoring
Admin-Workstation	UEBA-Server	22	SSH
UEBA-Server	NW-Server	15671	UEBA-Warnmeldungen werden an Respond weitergeleitet

NetWitness Endpoint Insights-Architektur

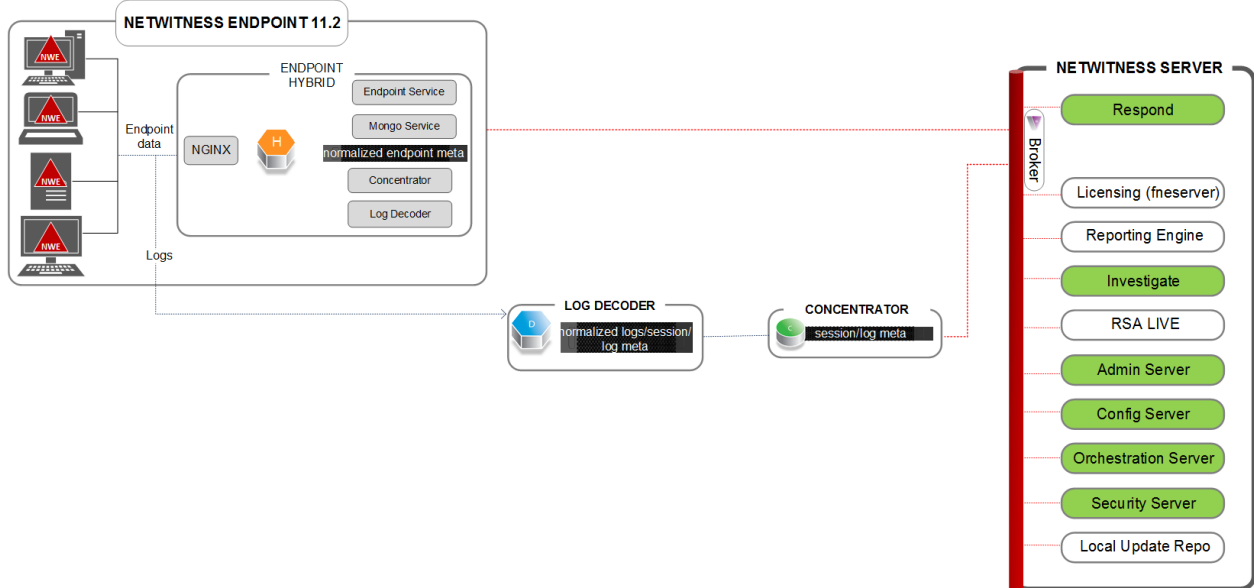
Die folgenden Diagramme zeigen die Netzwerkarchitektur von NetWitness Endpoint Insights.

NetWitness Endpoint Insights 11.2

NetWitness Endpoint Architecture

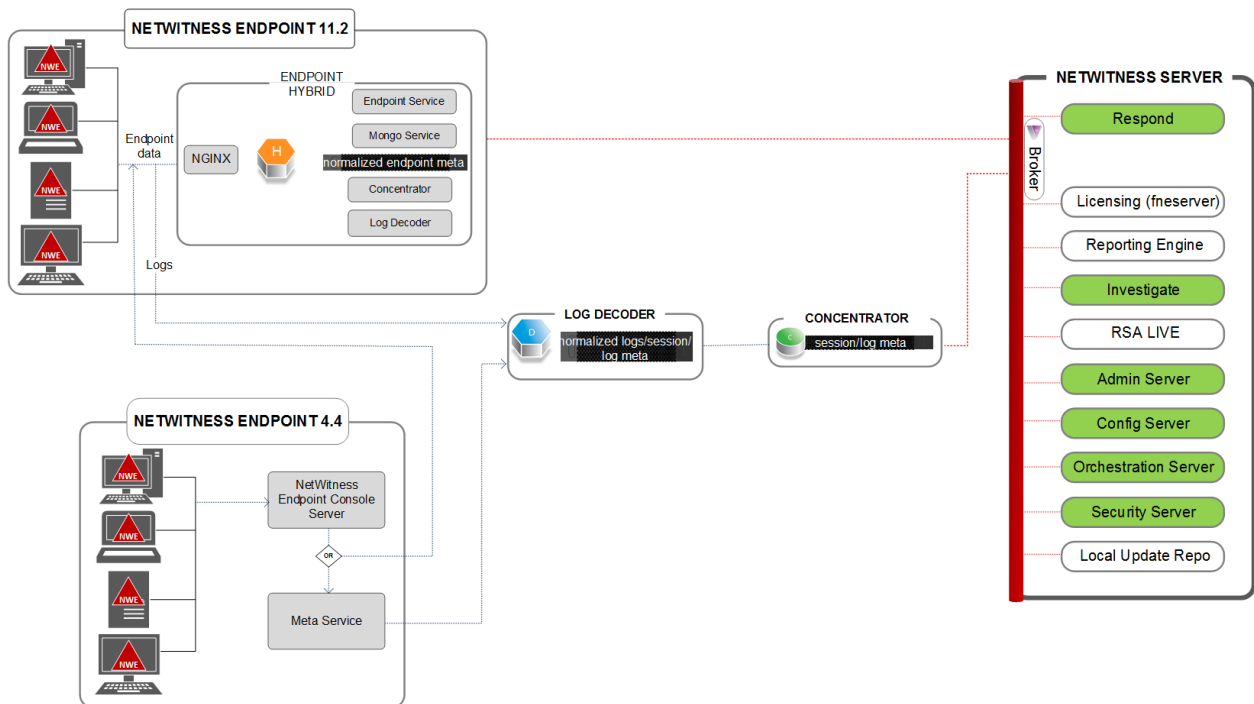


NetWitness Endpoint Insights 11.2 mit Log Decoder



Integration von NetWitness Endpoint 4.4 in NetWitness Endpoint Insights 11.2

NetWitness Endpoint Architecture



Weitere Informationen zu Services, die auf Endpoint Hybrid ausgeführt werden, finden Sie unter *Konfigurationsleitfaden für RSA NetWitness Endpoint Insights*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Anforderungen an den Standort und Sicherheit

Lesen Sie dieses Thema unbedingt sorgfältig durch und beachten Sie alle Warnhinweise und Vorsichtsmaßnahmen vor der Installation oder Wartung Ihrer RSA-Geräte.

Vorgesehene Anwendung

Dieses Produkt ist ein Informationstechnologie-Gerät, das in Büros, Schulen, Computerräumen und ähnlichen gewerblich genutzten Innenräumen installiert werden kann. Das Gerät ist nicht zur Verbindung mit einem Außenkabel geeignet.

Service

Dieses Gerät enthält keine Komponenten, die vom Nutzer gewartet werden können. Im Falle einer Funktionsstörung kontaktieren Sie bitte den Customer Service. Im Falle einer Störung können sich innerhalb des Geräts hohe Temperaturen entwickeln, was ein Alarmsignal auslöst. Ertönt ein solches Alarmsignal, sollten Sie das Gerät umgehend von der Stromquelle trennen und den Customer Service kontaktieren. Eine weitere Verwendung des Geräts würde ein Sicherheitsrisiko darstellen und könnte zu Verletzungen und Sachschäden führen.

Sicherheitsinformationen

Standortauswahl

Das System ist für eine typische Büroumgebung konzipiert. Wählen Sie einen Standort nach den folgenden Kriterien aus:

- Sauber, trocken und ohne Partikel in der Luft (abgesehen von dem normalen Hausstaub).
- Gut belüftet und nicht in der Nähe von Hitzequellen, wie direktes Sonnenlicht oder Heizungen.
- Nicht in der Nähe von Vibrations- oder Erschütterungsquellen.
- Isoliert von starken elektromagnetischen Feldern, die durch elektronische Geräte erzeugt werden.
- In Regionen, die anfällig für Gewitterstürme sind, empfehlen wir, das System an einen Überspannungsschutz anzuschließen.
- Ausgestattet mit ordnungsgemäß geerdeten Wandsteckdosen.
- Ausreichend Platz, um auf Netzkabel zugreifen zu können, da diese die Hauptstromquelle darstellen.

Vorgehensweise zur Handhabung des Geräts

Reduzieren Sie das Risiko von Personen- oder Sachschäden, indem Sie Folgendes beachten:

- Halten Sie die lokalen Vorschriften zu Sicherheit und Gesundheitsschutz am Arbeitsplatz ein, wenn Sie das Gerät anheben oder bewegen.
- Verwenden Sie mechanische oder andere geeignete Hilfsmittel, wenn Sie das Gerät anheben oder bewegen.
- Verringern Sie das Gewicht des Geräts für eine leichtere Handhabung, indem Sie alle leicht lösbaren Komponenten entfernen.

Warnhinweise für Strom und Elektronik

Achtung: Der Hauptschalter, gekennzeichnet durch die Stand-by-Stromversorgungsanzeige, schaltet die Wechselstromversorgung des Systems NICHT komplett aus. Ein Stand-by-Stromverbrauch von 5 W ist immer zu verzeichnen, wenn das System angeschlossen ist. Um die Stromversorgung des Systems zu unterbrechen, müssen Sie die Wechselstromkabel aus der Steckdose ziehen.

- Verwenden und bearbeiten Sie kein Wechselstromkabel, das nicht exakt dem erforderlichen Typ entspricht. Für jede Systemversorgung wird ein separates Netzkabel benötigt.
- Dieses Produkt enthält keine Komponenten, die vom Nutzer gewartet werden können. Öffnen Sie das System nicht.
- Beim Austauschen von Hot-Plug-Netzteilen ziehen Sie das Stromkabel von dem auszutauschenden Netzteil ab, bevor Sie es von dem Server entfernen.

Warnhinweise für Rackmontage

- Befestigen Sie das Rack des Geräts an einem nicht beweglichen Gebäudeteil, um ein Umfallen zu verhindern, wenn ein Server oder Teil des Geräts erweitert wird. Das Rack muss gemäß den Herstelleranweisungen für die Rackmontage installiert werden.
- Die Montage des Geräts in einer Rackhalterung sollte so vorgenommen werden, dass keine gefährliche Situation aufgrund einer ungleichmäßigen mechanischen Belastung entstehen kann.
- Erweitern Sie die Anlage jeweils nur mit einem Teil vom Rack aus.
- Um das Risiko eines möglichen Stromschlags zu vermeiden, muss eine ordnungsgemäße Sicherheitserdung für das Rack und alle darin installierten Anlagenteile eingerichtet sein.

Kühlung und Luftstrom

Die Installation des Geräts sollte so erfolgen, dass die für den sicheren Betrieb der Geräte erforderliche Luftstrommenge nicht beeinträchtigt wird.

Antennenpositionierung

Das Gerät sollte so installiert und betrieben werden, dass eine minimale Distanz von 7 cm zwischen dem Heizkörper und Ihrem Körper besteht. Die Antennen der Sender dürfen nicht am gleichen Ort installiert oder zusammen mit anderen Antennen oder Sendern betrieben werden.

Konfiguration der Gruppenaggregation

Mit der Gruppenaggregation können Sie mehrere Archiver- oder Concentrator-Services als Gruppe konfigurieren und die Aggregationsaufgaben zwischen ihnen aufteilen. Sie können mehrere Archiver-Services oder Concentrator-Services konfigurieren, um eine effiziente Aggregation aus mehreren Log Decoder-Services zu erreichen und so die Abfrageperformance der folgenden Daten zu verbessern:

- Im Archiver gespeicherte Daten
- Über den Concentrator verarbeitete Daten

Empfehlungen zur Bereitstellung der RSA-Gruppenaggregation

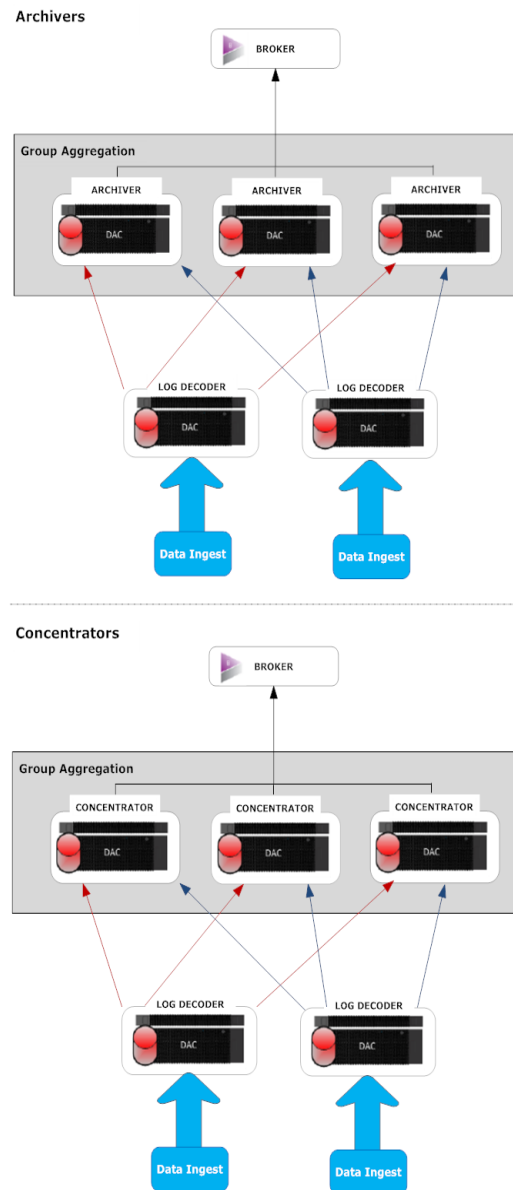
RSA empfiehlt die folgende Bereitstellung für die Gruppenaggregation:

- 1 bis 2 Log Decoder
- 3 bis 5 Archiver oder Concentrators

Vorteile bei Verwendung der Gruppenaggregation

- Erhöht die Geschwindigkeit der RSA NetWitness® Platform-Abfragen.
- Verbessert die Performance von aggregierten Abfragen (Count und Sum) in der Umgebung
- Verbessert die Performance des Investigation-Service
- Daten können für Ermittlungszwecke für einen längeren Zeitraum gespeichert werden.

In der folgenden Abbildung wird die Gruppenaggregation dargestellt.



Sie können beliebig viele Archivers oder Concentrators gruppieren und daraus eine Aggregationsgruppe bilden. Die aggregierten Sitzungen werden auf die Archiver- oder Concentrator-Services in der Gruppe aufgeteilt, wobei die Anzahl der Sitzungen im Parameter „Max. Sitzungen für Aggregation“ festgelegt ist.

Wenn eine Aggregationsgruppe z. B. aus zwei Archiver-Services oder zwei Concentrator-Services besteht und der Parameter „Max. Sitzungen für Aggregation“ auf 10.000 festgelegt wird, werden die Sitzungen wie in der folgenden Tabelle dargestellt auf die Services aufgeteilt.

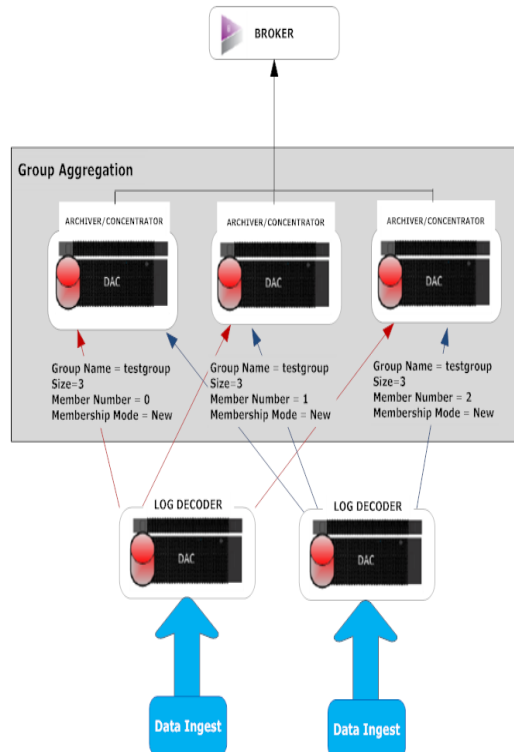
Archiver 0 oder Concentrator 0	Archiver 1 oder Concentrator 1
1 - 9.999	10.000–19.999
20.000–29.999	30.000–39.999
40.000–49.999	50.000–59.999

Konfiguration der Gruppenaggregation

Schließen Sie dieses Verfahren ab, um mehrere Archiver- oder Concentrator-Services als Gruppe zu konfigurieren und die Aggregationsaufgaben zwischen ihnen aufzuteilen.

Voraussetzungen

Planen Sie das Netzwerkdesign für die Gruppenaggregation. In der folgenden Abbildung ist ein Beispiel für eine Konfiguration einer Gruppenaggregation gezeigt.



Stellen Sie sicher, dass Sie die Parameter der Gruppenaggregation in der folgenden Tabelle verstehen, und erstellen Sie einen Gruppenaggregationsplan.

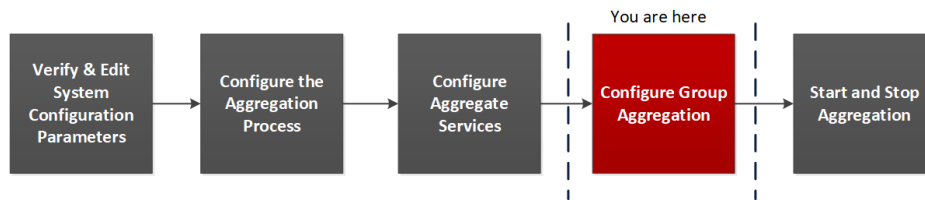
Parameter	Beschreibung
Gruppenname	Bestimmt die Gruppe, zu der der Archiver oder Concentrator gehört. Sie können eine beliebige Anzahl von Gruppen hinzuzufügen, die Daten von einem Log Decoder aggregieren. Der Parameter „Gruppenname“ wird vom Log Decoder verwendet, um zu ermitteln, welche Archiver- oder Concentrator-Services zusammenarbeiten. Alle Archiver- oder Concentrator-Services in der Gruppe sollten denselben Gruppennamen haben.
Größe	Bestimmt die Anzahl der Archiver- oder Concentrator-Services in der Aggregationsgruppe.

Parameter	Beschreibung
Mitgliedsnummer	<p>Bestimmt die Position des Archiver oder Concentrator in der Aggregationsgruppe. Für eine Gruppe der Größe N muss die Mitgliedsnummer von 0 bis N-1 auf jedem Archiver- oder Concentrator-Service in der Aggregationsgruppe definiert sein.</p> <p>Beispiel: Wenn die Größe der Aggregationsgruppe 2 beträgt, sollte die Mitgliedsnummer eines der Archiver- oder Concentrator-Services auf 0 und die Mitgliedsnummer des anderen Archiver oder Concentrator auf 1 festgelegt werden.</p>
Mitgliedschaftsmodus	<p>Es gibt zwei Mitgliedschaftsmodi:</p> <ul style="list-style-type: none">• Neu: Hinzufügen eines neuen Archiver- oder Concentrator-Services als Mitglied zu einer bestehenden Aggregationsgruppe oder Erstellen einer neuen Aggregationsgruppe. Der Archiver- oder Concentrator-Service aggregiert keine bestehenden Sitzungen vom Service, da andere Mitglieder der Gruppe wahrscheinlich bereits alle Sitzungen auf dem Service aggregiert haben. Dieser Archiver- oder Concentrator-Service aggregiert nur neue Sitzungen, die auf dem Service angezeigt werden.• Ersetzen: Ersetzen eines bestehenden Mitglieds einer Aggregationsgruppe. Der Archiver oder Concentrator beginnt die Aggregation bei der ältesten verfügbaren Sitzung auf dem Service, von dem er aggregiert.



Hinweis: Der Mitgliedschaftsmodus-Parameter hat nur Auswirkungen, wenn von dem Service noch keine Sitzungen aggregiert wurden. Nachdem eine Sitzung aggregiert wurde, hat dieser Parameter keine Auswirkungen mehr.

Einrichten der Gruppenaggregation

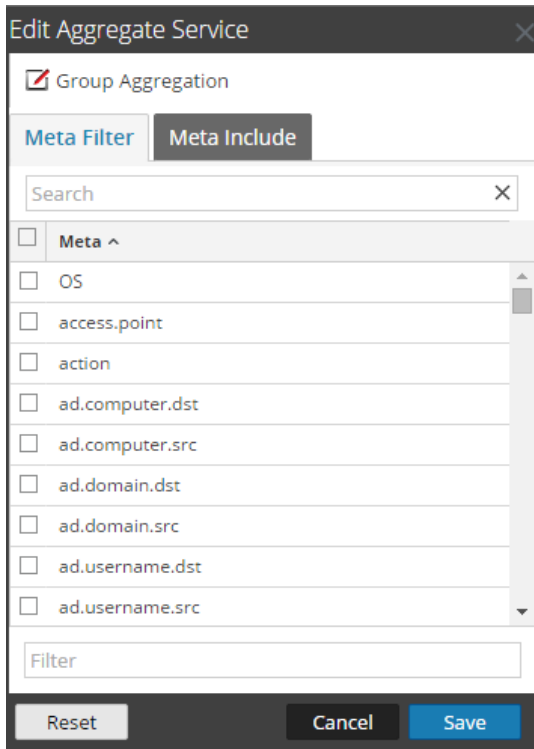
Dieser Workflow zeigt die Schritte, die Sie zur Konfiguration der Gruppenaggregation abschließen müssen.



So richten Sie die Gruppenaggregation ein:

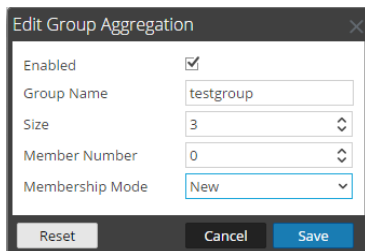
1. Konfigurieren Sie mehrere Archiver- oder Concentrator-Services in Ihrer Umgebung. Vergewissern Sie sich, dass Sie den gleichen Log Decoder als Datenquelle zu allen Services hinzufügen.
2. Führen Sie die folgenden Schritte für alle Archiver- oder Concentrator-Services aus, die zur Aggregationsgruppe gehören sollen:
 - a. Navigieren Sie zu **ADMIN > Services**.
 - b. Wählen Sie den Archiver- oder Concentrator-Service aus und wählen Sie dann in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
Die Ansicht „Servicekonfiguration“ von Archiver oder Concentrator wird angezeigt.
 - c. Wählen Sie im Abschnitt **Services aggregieren** die Option **Log Decoder** aus.
 - d. Klicken Sie auf  **Toggle Service** , um den Status des Log Decoder in „offline“ zu ändern, sofern er „online“ lautet.
 - e. Klicken Sie auf .

Das Dialogfeld **Aggregierten Service bearbeiten** wird angezeigt.



- f. Klicken Sie auf **Group Aggregation**.

Das Dialogfeld **Gruppenaggregation bearbeiten** wird angezeigt.



- g. Aktivieren Sie das Kontrollkästchen **Aktiviert** und legen Sie die folgenden Parameter fest:
- Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein.
 - Wählen Sie im Feld **Größe** die Anzahl der Archiver- oder Concentrator-Services in der Aggregationsgruppe aus.
 - Wählen Sie im Feld **Mitgliedsnummer** die Position des Archiver oder Concentrator in der Aggregationsgruppe aus.
 - Wählen Sie den Modus im Drop-down-Menü **Mitgliedschaftsmodus** aus.
- h. Klicken Sie auf **Speichern**.
- i. Klicken Sie in der Ansicht „Servicekonfiguration“ auf **Anwenden**.
- j. Führen Sie **Schritt b** bis **Schritt i** für alle anderen Archiver- oder Concentrator-Services aus, die Teil der Gruppenaggregation sein sollen.

3. Legen Sie im Abschnitt **Aggregationskonfiguration** den Parameter für **Max. Sitzungen für Aggregation** auf **10.000** fest.

The screenshot displays the RSA NetWitness Suite Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, showing 'HOSTS', 'SERVICES', 'EVENT SOURCES', 'HEALTH & WELLNESS', 'SYSTEM', and 'SECURITY'. The 'SERVICES' section is selected, and the 'Config' tab is active. The 'Appliance Service Configuration' tab is selected, showing the configuration for an aggregation service.

The 'Aggregate Services' table shows the following data:

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
<input type="checkbox"/> 10.31.125.245	50004	0	0	0				no	consuming
<input checked="" type="checkbox"/> 10.31.125.246	50002	0	0	0				yes	offline

The 'System Configuration' table shows the following data:

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input checked="" type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20

The 'Aggregation Configuration' table shows the following data:

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	10000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

An 'Apply' button is located at the bottom center of the configuration page.