RSA NETWITNESS® SUITE

Leitfaden zur Bereitstellung

für Version 11,1

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, 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

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.

Juli 2018

Inhalt

Die Grundlagen 5

Grundlegender Bereitstellungsprozess 7

Prozess 7

Allgemeines Bereitstellungsdiagramm für NetWitness Suite 9

Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Suite 11

Netzwerkarchitektur und Ports 13

Diagramm der NetWitness Suite-Netzwerkarchitektur 13

Umfassende Liste der Host- und Serviceports von NetWitness Suite 14

NW-Serverhost 15

Archiver-Host 17

Broker-Host 18

Concentrator-Host 19

Endpoint Hybrid oder Endpoint Log Hybrid 20

Event Stream Analysis (ESA)-Host 21

Log Collector-Host 23

Log Decoder-Host 25

Log Hybrid-Host 27

Malware-Host 29

Packet Decoder-Host 30

Packet Hybrid-Host 31

NetWitness Endpoint Insights-Architektur 32

NetWitness Endpoint Insights 11.1 32

NetWitness Endpoint Insights 11.1 mit Log Decoder 32

Integration von NetWitness Endpoint 4.4 in NetWitness Endpoint Insights 11.1 33

Anforderungen an den Standort und Sicherheit 34

Vorgesehene Anwendung 34

Service 34

Sicherheitsinformationen 34

Standortauswahl 34

Vorgehensweise zur Handhabung des Geräts 35

Warnhinweise für Strom und Elektronik 35

Warnhinweise für Rackmontage 35
Kühlung und Luftstrom 36
Antennenpositionierung 36

Konfiguration der Gruppenaggregation 37

Empfehlungen zur Bereitstellung der RSA-Gruppenaggregation 37
Vorteile bei Verwendung der Gruppenaggregation 37
Konfiguration der Gruppenaggregation 39
Voraussetzungen 39
Einrichten der Gruppenaggregation 41

Die Grundlagen

In diesem Handbuch werden die grundlegenden Anforderungen einerNetWitness Suite-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 für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Es gibt viele Faktoren, die Sie berücksichtigen müssen, bevor Sie NetWitness Suite 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 Suite verwenden werden)
- Menge der Pakete und Protokolle, die Sie verarbeiten müssen
- Performance, die jede einzelne NetWitness Suite-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 Suite ausführen möchten
  - RSA-Appliances (Software, die auf von RSA bereitgestellter Hardware ausgeführt wird)
    Detaillierte Anweisungen zur Bereitstellung von RSA-Appliances finden Sie im *RSA NetWitness® Suite Handbuch für die Installation physischer Hosts*.
  - Nur von RSA bereitgestellte Software:
    - Lokale virtuelle Hosts
      Detaillierte Anweisungen zur Bereitstellung lokaler virtueller Hosts finden Sie im *RSA NetWitness® SuiteHandbuch zur Installation virtueller Hosts*.
    - VCloud:
      - Amazon Web Services (AWS)
        Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in AWS finden Sie im *RSA NetWitness® SuiteAWS-Bereitstellungsleitfaden*.

- Azure
  Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in Azure finden Sie im *RSA NetWitness® SuiteAzure-Bereitstellungsleitfaden*.

Grundlegender Bereitstellungsprozess

Vor der Bereitstellung von NetWitness Suite 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 Suite-Bereitstellung.

Prozess

Die Komponenten und die Topologie eines NetWitness Suite-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 RSA-Appliances:
  1. Installieren Sie Appliances und verbinden Sie sich mit dem Netzwerk, wie in den RSA NetWitness® Suite Handbüchern zur Hardwarekonfiguration und im *RSA NetWitness® Suite Handbuch für die Installation physischer Hosts* beschrieben.
  2. Richten Sie die Lizenzierung für NetWitness Suite ein, wie im *RSA NetWitness® Suite Handbuch zur Lizenzierung* beschrieben.
  3. Konfigurieren Sie einzelne Appliances und Services, wie im *RSA NetWitness® Suite 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® Suite Leitfaden zur Einrichtung von virtuellen Hosts*.
- Für AWS befolgen Sie die Anweisungen im *RSA NetWitness® Suite AWS-Bereitstellungsleitfaden*.

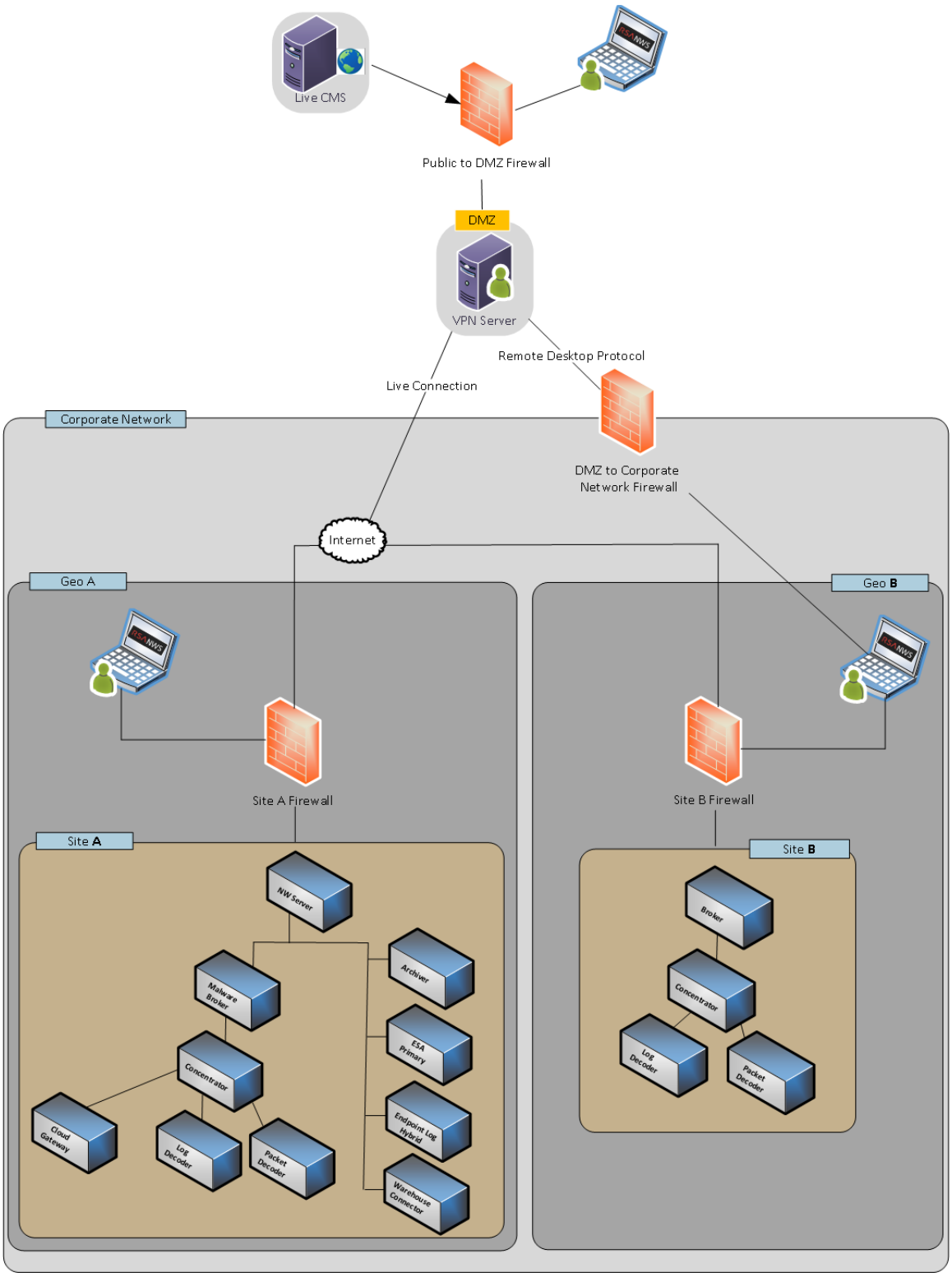
- Für Azure befolgen Sie die Anweisungen im *RSA NetWitness® Suite Azure-Bereitstellungsleitfaden*.

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

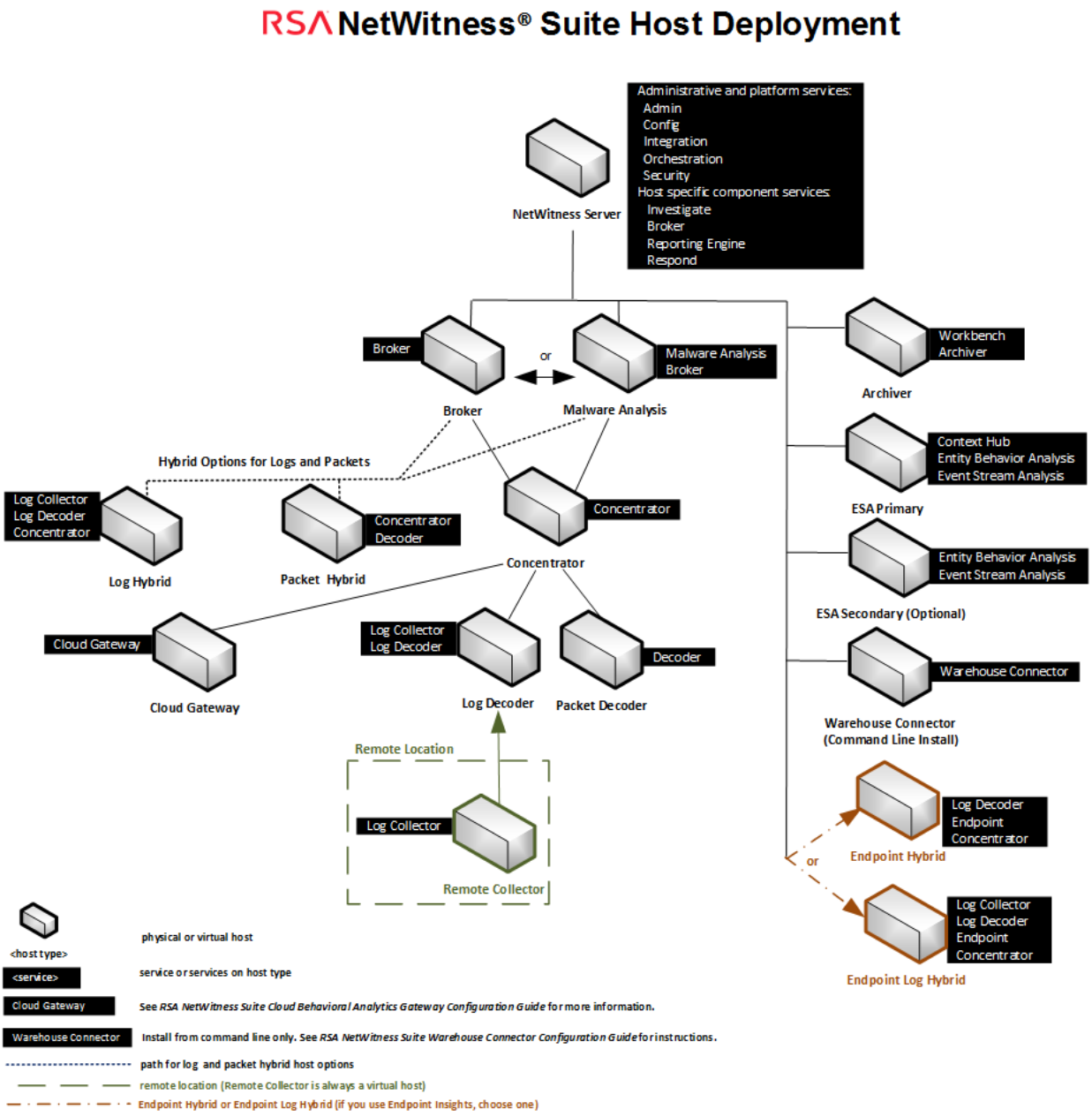
Allgemeines Bereitstellungsdiagramm für NetWitness Suite

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


Live CMS
Public to DMZ Firewall
DMZ
VPN Server
Remote Desktop Protocol
Live Connection
Corporate Network
DMZ to Corporate Network Firewall
Internet
Geo A
Geo B
Site A Firewall
Site B Firewall
Site A
Site B
NW Server
Malware Broker
Archiver
Concentrator
ESA Primary
Cloud Gateway
Log Decoder
Packet Decoder
Endpoint Log Hybrid
Warehouse Connector
Broker
Concentrator
Log Decoder
Packet Decoder

Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Suite

Das folgende Diagramm zeigt ein Beispiel einer NetWitness Suite-Bereitstellung, die auf physischen oder virtuellen Rechnern gehostet wird. Anweisungen zum Installieren von NetWitness Suite finden Sie im *Installationshandbuch für physische Hosts*, im *Handbuch zur Installation virtueller Hosts*, im *AWS-Bereitstellungsleitfaden* oder im *Azure-Bereitstellungsleitfaden*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.



Netzwerkarchitektur und Ports

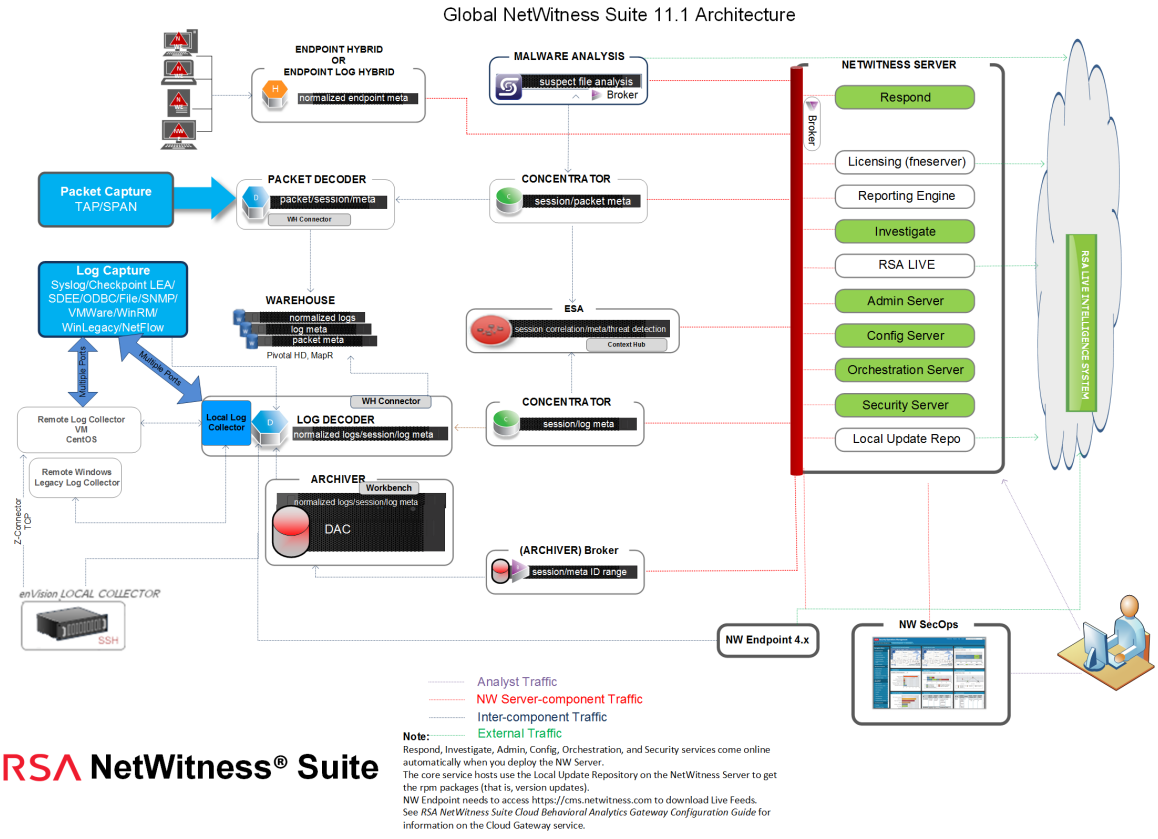
Mit den Informationen im folgenden Diagramm und in der Porttabelle können Sie sicherstellen, dass alle relevanten Ports für Komponenten in Ihrer NetWitness Suite-Bereitstellung geöffnet sind und miteinander kommunizieren können.

Einzelne Endpunkt-Architekturdiagramme finden Sie unter NetWitness Endpoint Insights-Architektur am Ende dieses Themas.

Diagramm der NetWitness Suite-Netzwerkarchitektur

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

Hinweis: NetWitness Suite-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.



Umfassende Liste der Host- und Serviceports von NetWitness Suite

Hinweis: 1.) Informationen zu Ports, die in der Ereignissammlung über die RSA NetWitness Logs verwendet werden, finden Sie unter „Grundlagen“ im *RSA NetWitness Suite Leitfaden zur Bereitstellung der Protokollsammlung*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Dieser Abschnitt enthält die Portspezifikationen für die folgenden Hosts.

NW-Serverhost

Archiver-Host

Broker-Host

Concentrator-Host

Endpoint Hybrid/Endpoint Log Hybrid Host

Event Stream Analysis-Host

Log Collector-Host

Log Decoder-Host

Log Hybrid-Host

Malware-Host

Packet Decoder-Host

Packet Hybrid-Host

NW-Serverhost

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	NW-Server	TCP 443, 80	NGINX – NetWitness-Benutzeroberfläche
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-Server	NW-Server	TCP 50003, 50103, 56003	Broker-Ports
NW-Server	NW-Server	TCP 5671	RabbitMQ-amqp
NW-Server	NW-Server	UDP 50514	Auditports
NW-Server	NW-Server	TCP 7000, 7003, 7009, 7010	Start-Ports
NW-Server	NW-Server	TCP 50006, 50106, 56006	NetWitness-Appliance-Ports
NW-Hosts	NW-Server	UDP 123	NTP

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Hosts	NW-Server	TCP 27017	MongoDB
NW-Server	NW-Server	UDP 123	NTP
NW-Server	NFS-Server	TCP 111 2049 UDP 111 204	iDRAC-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
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
Archiver	Archiver	UDP 123	NTP
Archiver	NFS-Server	TCP 111 2049 UDP 111 204	iDRAC-Installationen

Broker-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Broker	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Broker	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
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
Broker	Broker	UDP 123	NTP
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
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 111 204	iDRAC-Installationen
Concentrator	Concentrator	UDP 50514	Auditdaten
Concentrator	Concentrator	UDP 123	NTP

Endpoint Hybrid oder Endpoint Log Hybrid

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint 11.1 Agent	Endpoint Hybrid oder Endpoint Log Hybrid	TCP 443	NGINX HTTPS
Endpoint 11.1 Agent	Log Decoder oder Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows-Protokollsammlung
Endpoint-Server	Log Decoder (extern)	TCP 50102, 56202, 50202	Um Metadaten an einen externen Log Decoder weiterzuleiten
NW-Server	Endpoint Hybrid oder Endpoint Log Hybrid	TCP 7050	Webdatenverkehr über die Benutzeroberfläche
Endpoint Hybrid oder Endpoint Log Hybrid	NW-Server	TCP 5672	Nachrichtenbus
Endpoint-Server	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	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
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	cms.netwitness.com	TCP 443	Live
ESA	NFS-Server	TCP 111 2049 UDP 111 2049	NTP
ESA	Active Directory	636 (SSL)/389 (Nicht-SSL)	
NW-Server	ESA	80 (HTTP)/443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Nicht-SSL)	

Quellhost	Zielhost	Zielports	Anmerkungen
ESA Primary	ESA Primary	TCP 7007	Start-Port
ESA Primary	ESA Primary	UDP 50514	Auditdaten
ESA Primary	ESA Primary	UDP 123	NTP

Log Collector-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Collector	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Collector	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	Log Collector	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe *Protokollsammlung-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.	
Protokollereignisquellen	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Protokollsammlungsports

Quellhost	Zielhost	Zielports	Anmerkungen
Protokollereignisquellen	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Protokollsammlungs-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
Log Collector	Log Collector	UDP 123	NTP
Log Collector	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

Log Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Decoder	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Protokollereignisquellen	Siehe *Protokollsammlung-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.	
Protokollereignisquellen	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammlungsports

Quellhost	Zielhost	Zielports	Anmerkungen
Protokollereignisquellen	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammlungs-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 (Endpunkt), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Decoder	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts.
Log Decoder	Log Decoder	UDP 50514	Auditdaten
Log Decoder	Log Decoder	UDP 123	NTP
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS-Server	TCP 111 2049 UDP 111 204	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
Admin-Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe *Protokollsammlung-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.	
Protokollereignisquellen	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammlungsports

Quellhost	Zielhost	Zielports	Anmerkungen
Protokollereignisquellen	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammlungs-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 (Endpunkt), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Hybrid	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports
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 111 204	iDRAC-Installationen

Malware-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Malware	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Malware	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
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/Opswat
Malware	Malware	UDP 50514	Auditdaten
Malware	Malware	UDP 123	NTP
Malware	NFS-Server	TCP 111 2049 UDP 111 204	iDRAC-Installationen

Packet Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Packet Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Packet-Decoder	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	Packet Decoder	TCP 22	SSH
NW-Server	Packet Decoder	TCP 56004 (SSL), 50004 (Nicht-SSL), 50104 (REST)	Packet Decoder-Anwendungsports
NW-Server	Packet Decoder	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Packet Decoder	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Packet Decoder	Packet Decoder	UDP 50514	Auditdaten
Packet Decoder	Packet Decoder	UDP 123	NTP
Packet Decoder	NFS-Server	TCP 111 2049 UDP 111 204	iDRAC-Installationen

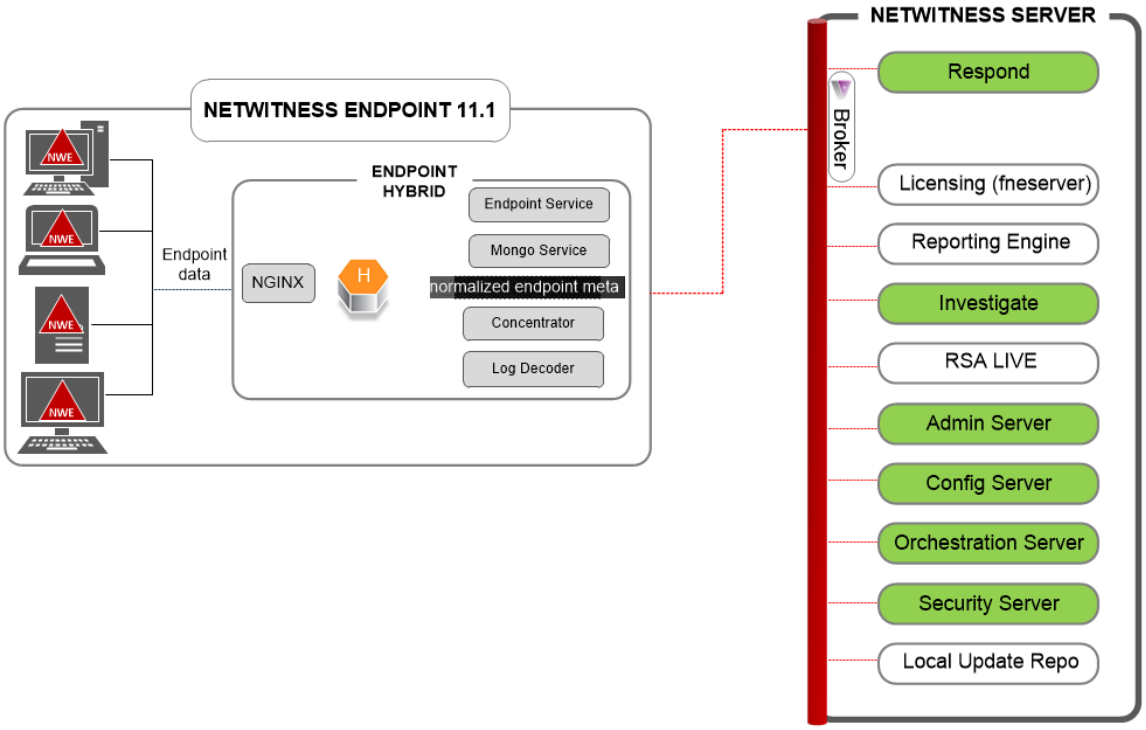
Packet Hybrid-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Packet Hybrid	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Packet Hybrid	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	Packet Hybrid	TCP 22	SSH
NW-Server	Packet Hybrid	TCP 56004 (SSL), 50004 (Nicht-SSL), 50104 (REST)	Packet Decoder-Anwendungsports
NW-Server	Packet Hybrid	TCP 56005 (SSL), 50005 (Nicht-SSL), 50105 (REST)	Concentrator-Anwendungsports
NW-Server	Packet Hybrid	TCP 56006 (SSL), 50006 (Nicht-SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Packet Hybrid	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Packet Hybrid	NFS-Server	TCP 111 2049 UDP 111 204	iDRAC-Installationen

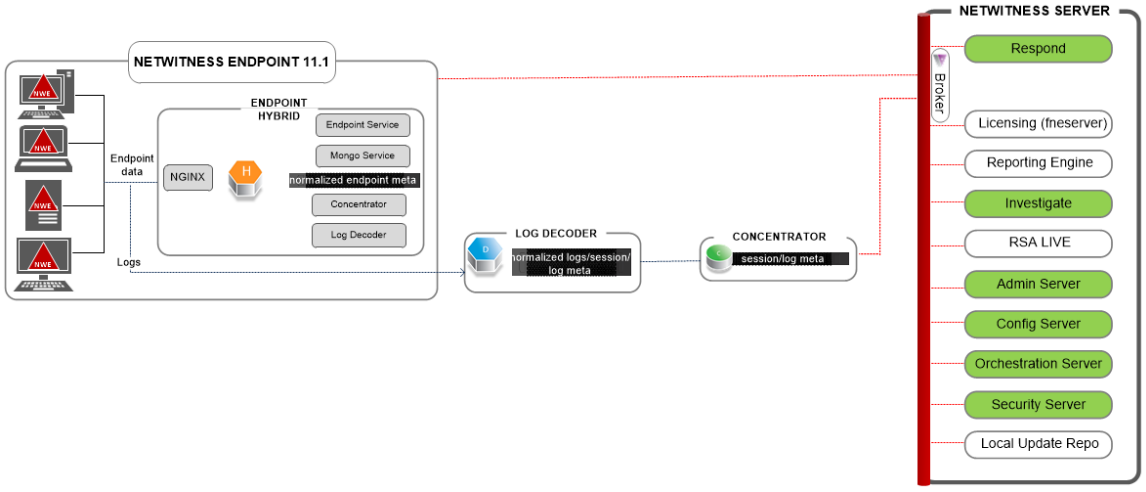
NetWitness Endpoint Insights-Architektur

Die folgenden Diagramme zeigen die Netzwerkarchitektur von NetWitness Endpoint Insights.

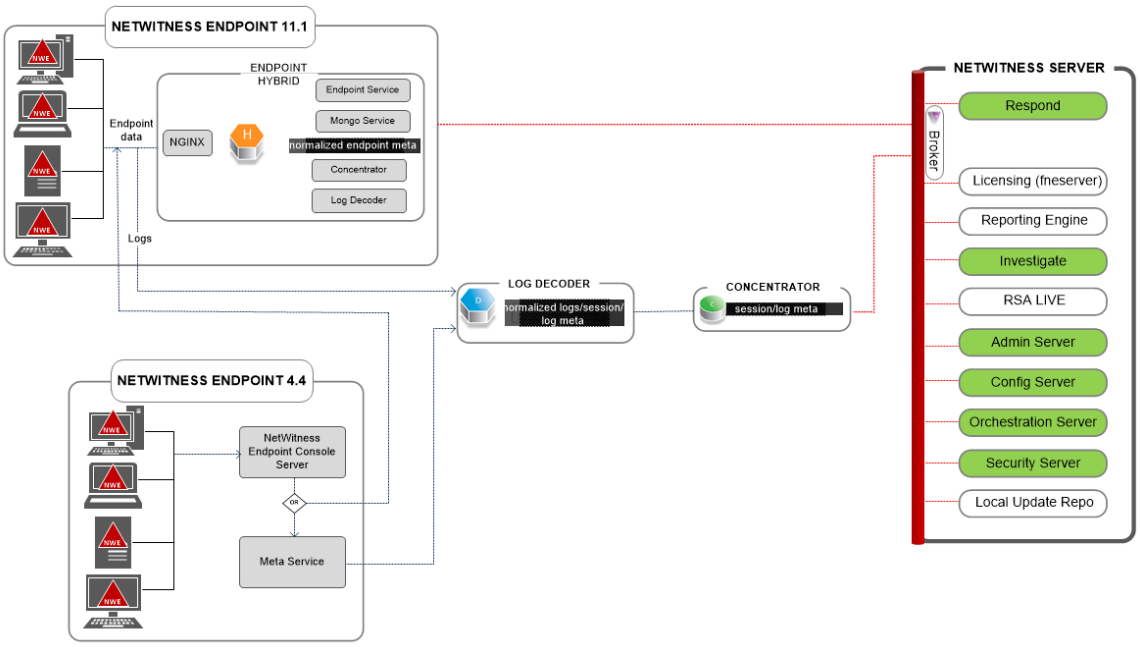
NetWitness Endpoint Insights 11.1



NetWitness Endpoint Insights 11.1 mit Log Decoder



Integration von NetWitness Endpoint 4.4 in NetWitness Endpoint Insights 11.1



Weitere Informationen zu Services, die auf Endpoint Hybrid ausgeführt werden, finden Sie unter *Konfigurationsleitfaden für RSA NetWitness Endpoint Insights*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

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 Benutzer 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 entfernen 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 erzeugte 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 V 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

- Befestigung Sie die das Rack des Gerätes an einem nicht beweglichen Gebäudeteil, um ein Umfallen zu verhindern, wenn ein Server oder Teil des Gerätes erweitert wird. Das Rack muss gemäß den Herstelleranweisungen für die Rackmontage installiert werden.
- Die Montage des Gerätes in einer Rack-Halterung 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.

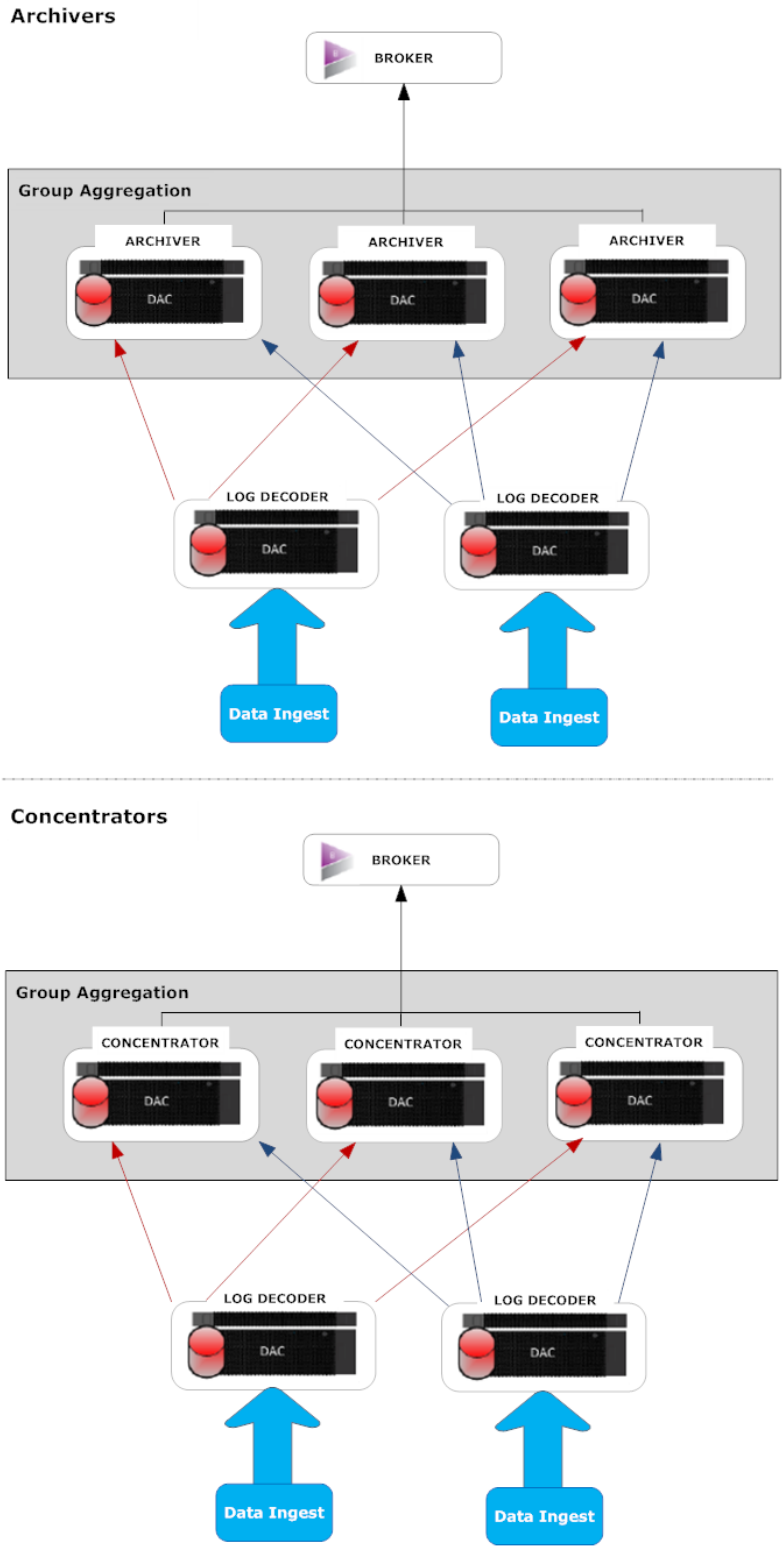
- 1 bis 2 Log Decoder
- 3 bis 5 Archiver oder Concentrators

Vorteile bei Verwendung der Gruppenaggregation

Gruppenaggregation:

- Erhöht die Geschwindigkeit der RSA NetWitness® Suite-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.


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

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 2 Archiver-Services oder 2 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.

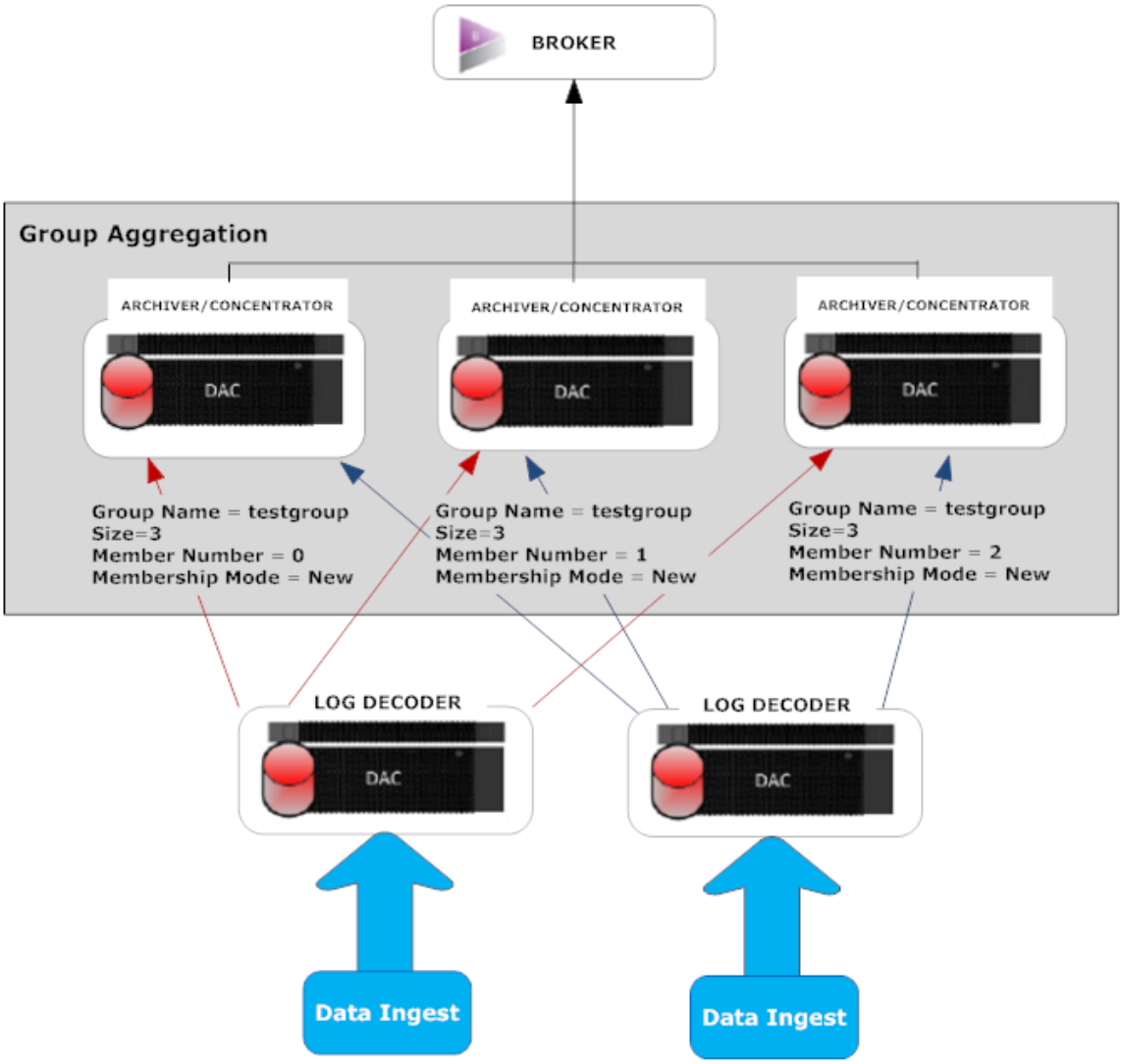
Archiver 0 oder Concentrator 0	Archiver 1 oder Concentrator 1
1–9.999	10.000–19.999
20.000–29.999	30.000–39.999
40.000–49.999	50.000–59.999

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

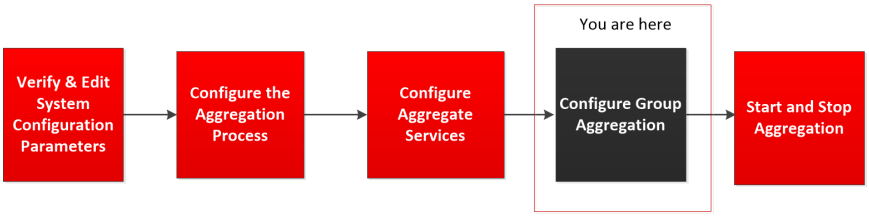
Planen Sie das Netzwerkdesign für die Gruppenaggregation. In der folgenden Abbildung ist ein Beispiel für eine Konfiguration einer Gruppenaggregation gezeigt.



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

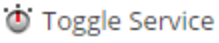
Parameter	Beschreibung
Gruppenname	Bestimmt die Gruppe, zu der der Archiver oder Concentrator gehört. Sie können eine beliebige Anzahl von Gruppen hinzuzufügen, die Daten von einem Log Decoder aggregieren. Der Parameter „Gruppenname“ wird vom Log Decoder verwendet, um zu ermitteln, welche Archiver- oder 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.
Mitgliedsnummer	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. 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.
Mitgliedschaftsmodus	Es gibt zwei Mitgliedschaftsmodi: Neu und Ersetzen. 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:** Dieser Parameter hat nur Auswirkungen, wenn von dem Service noch keine Sitzungen aggregiert wurden. Nachdem eine Sitzung aggregiert wurde, hat dieser Parameter keine Auswirkungen mehr.

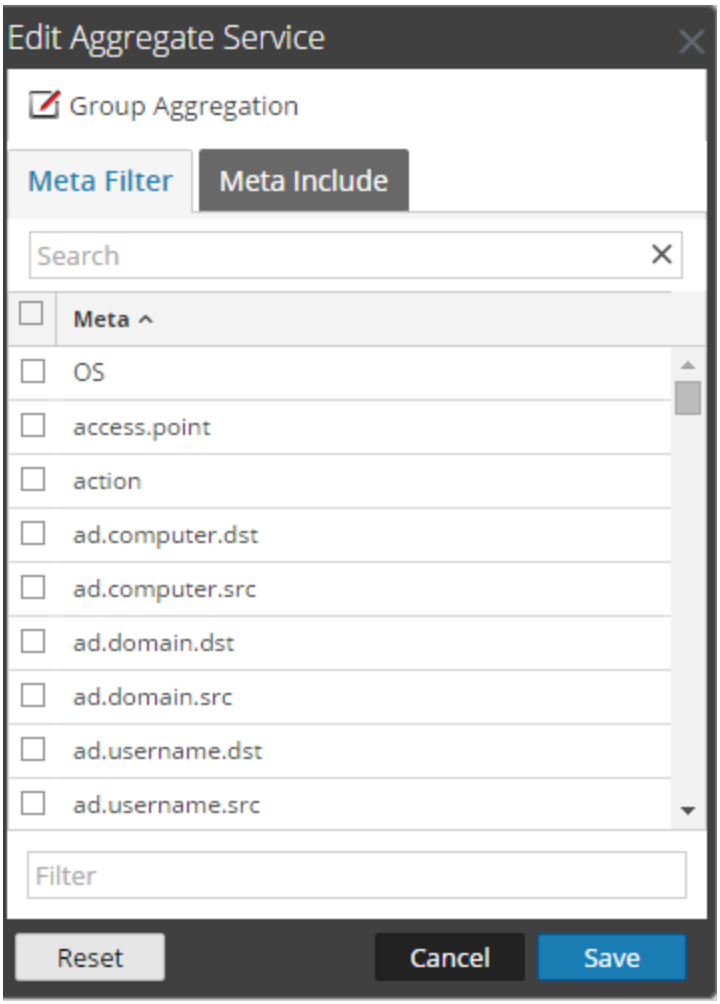


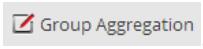
Einrichten der Gruppenaggregation

Schließen Sie das folgende Verfahren ab, um die Gruppenaggregation einzurichten.

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. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
   b. Wählen Sie den Archiver- oder Concentrator-Service aus und wählen Sie dann in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
      Die Ansicht „Gerätekonfiguration“ des Archiver- oder Concentrator-Services wird angezeigt.
   c. Wählen Sie im Abschnitt **Services aggregieren** das Log Decoder-Gerät aus.
   d. Klicken Sie auf 

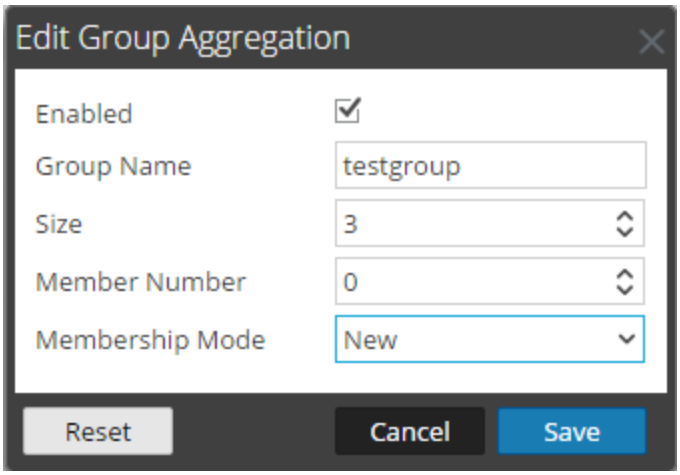
, um den Status des Log Decoder in „offline“ zu ändern, sofern er „online“ lautet.
   e. Klicken Sie auf  .
      Das Dialogfeld **Aggregierten Service bearbeiten** wird angezeigt.



f. Klicken Sie auf 

.

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 auf der Seite Ansicht Gerätekonfiguration 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.