RSA NETWITNESS® PLATFORM

Leitfaden für die ersten Schritte mit Hosts und Services

für Version 11.2

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

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

Hosts und Services – Grundlagen

Dieser Leitfaden bietet Administratoren Informationen zu den Standardverfahren für das Hinzufügen und Konfigurieren von Hosts und Services in NetWitness Platform. Nach der Einführung in den grundlegenden Zweck von Hosts und Services und ihre Funktionsweise im NetWitness Platform-Netzwerk werden in diesem Leitfaden die folgenden Themen behandelt:

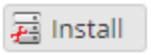
- Die Aufgaben, die Sie zum Konfigurieren von Hosts und Services in Ihrem Netzwerk durchführen müssen
- Zusätzliche Verfahren, die Sie basierend auf den langfristigen und täglichen betrieblichen Anforderungen Ihres Unternehmens abschließen
- Referenzthemen, in denen die Benutzeroberfläche beschrieben wird

Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Was ist ein Host?

Ein Host ist der Computer, auf dem ein Service ausgeführt wird. Hierbei kann es sich um eine physische oder eine virtuelle Maschine handeln. Im „Detaillierten Hostbereitstellungsdiagramm für NetWitness Platform im *NetWitness PlatformBereitstellungshandbuch* wird die Vorgehensweise bei der Bereitstellung von Hosts veranschaulicht.

Was ist ein Hosttyp?

Ein Hosttyp weist einem Host einen oder mehrere Services zu, wenn Sie einen Host über die Ansicht „Hosts“ installieren. Wählen Sie im Dialogfeld **Services installieren** einen **Hosttyp** aus. Das Dialogfeld wird angezeigt, wenn Sie in der Ansicht „Hosts“ einen Host auswählen und auf 

klicken. In der folgenden Tabelle werden die einzelnen Hosttypen und die Services aufgeführt, die installiert werden. Im „Detaillierten Hostbereitstellungsdiagramm für NetWitness Platform im *NetWitness PlatformBereitstellungshandbuch* wird die Vorgehensweise bei der Bereitstellung von Hosts veranschaulicht.

Hosttyp	Installierte Services
Archiver	Workbench und Archiver
Broker	Broker
Cloud Gateway	Cloud Gateway
Concentrator	Concentrator
Endpoint Hybrid	Log Decoder, Endpoint und Concentrator

Hosttyp	Installierte Services
Endpoint Log Hybrid	Log Collector, Log Decoder, Endpoint und Concentrator
ESA Primary	Context Hub, Entity Behavior Analysis und Event Stream Analysis
ESA Secondary	Event Stream Analysis und Entity Behavior Analysis
Log Collector	Log Collector
Log Decoder	Log Collector und Log Decoder
Log Hybrid	Log Collector, Log Decoder und Concentrator
Malware Analysis	Malware Analysis und Broker
Network Decoder	Decoder (Pakete)
Netzwerk-Hybrid	Concentrator und Decoder
UEBA	UEBA
Warehouse Connector	Warehouse Connector

Was ist ein Service?

Ein Service führt eine eindeutige Funktion aus, wie das Sammeln von Protokollen oder Archivieren von Daten. Jeder Service wird auf einem dedizierten Port ausgeführt und ist als Plug-in modelliert, das je nach Funktion des Hosts aktiviert oder deaktiviert wird.

Sie müssen die folgenden Core-Services zuerst konfigurieren:

- Decoder
- Concentrator
- Broker
- Log Decoder

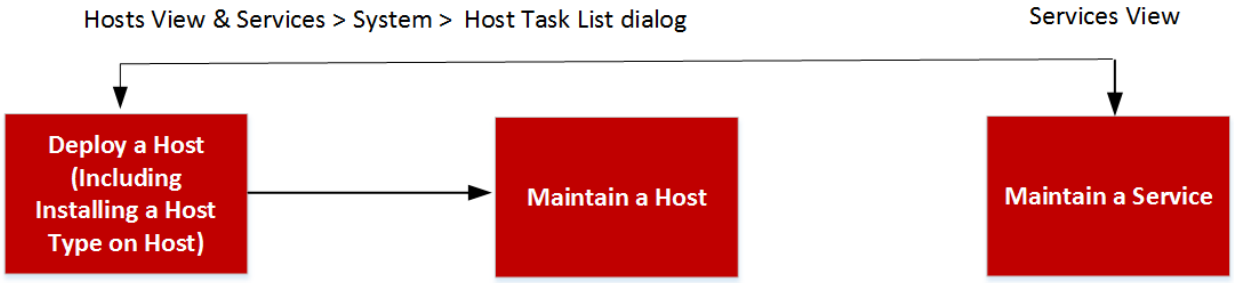
Alle Services sind nachfolgend aufgeführt. Für jeden Service außer den Log Collector sind eigene Leitfäden verfügbar bzw. in den *Leitfäden zur Host- und Servicekonfiguration* enthalten. Für den Log Collector ist ein eigener Satz von Konfigurationsleitfäden vorhanden, um die Konfiguration für alle unterstützten Ereignissammlungsprotokolle zu abzudecken. Informationen zum Log Collector finden Sie unter*Leitfäden zur Protokollsammlung*.

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Admin	-	-	Wird mit dem NW-Server implementiert.
Archiver	50008	56008	

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Broker	50003	56003	Core-Service
Cloud Gateway	–	–	
Concentrator	50005	56005	Core-Service
Konfiguration	–	–	Wird mit dem NW-Server implementiert.
Inhalt	-	-	Wird mit dem NW-Server implementiert.
Context Hub	–	–	
Decoder (Pakete)	50004	56004	Core-Service
Endpoint	-	-	
Entity Behavior Analysis	–	–	
Event Stream Analysis	–	50030	
Integration	–	–	Wird mit dem NW-Server implementiert.
Untersuchen	–	–	Wird mit dem NW-Server implementiert.
Log Collector	50001	56001	
Log Decoder	50002	56002	Core-Service
Malware Analysis	–	60007	
Orchestrierung	–	–	Wird mit dem NW-Server implementiert.
Reporting Engine	-	51113	Wird mit dem NW-Server implementiert.
Respond	–	–	Wird mit dem NW-Server implementiert.
Sicherheit	–	–	Wird mit dem NW-Server implementiert.
Quelle	-	-	Wird mit dem NW-Server implementiert.
UEBA	-	-	

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Sie müssen Hosts und Services für die Kommunikation mit dem Netzwerk und miteinander konfigurieren,damit sie ihre Funktionen wie das Speichern oder Erfassen von Daten durchführen können.



Einrichten eines Hosts

Verwenden Sie die Ansicht „Hosts“, um NetWitness Platform einen Host hinzuzufügen. Siehe Schritt 1. Hinzufügen eines Hosts.

Verwalten von Hosts

Verwenden Sie die Hauptansicht „ADMIN > Hosts“, um Ihrer Bereitstellung Hosts hinzuzufügen, diese zu bearbeiten und zu löschen sowie andere Wartungsaufgaben durchzuführen. Aufgaben im Zusammenhang mit einem Host und dessen Kommunikation mit dem Netzwerk können Sie über das Dialogfeld „Aufgabenliste“ durchführen. Ausführliche Anweisungen finden Sie im Abschnitt zu Verfahren bei Hosts und Services.

Nach der ersten Implementierung von NetWitness Platform ist die Hauptaufgabe, die Sie über die Ansicht „Hosts“ durchführen, das Aktualisieren Ihrer NetWitness Platform-Bereitstellung auf eine neue Version.

Benennungskonvention beim Aktualisieren der Version

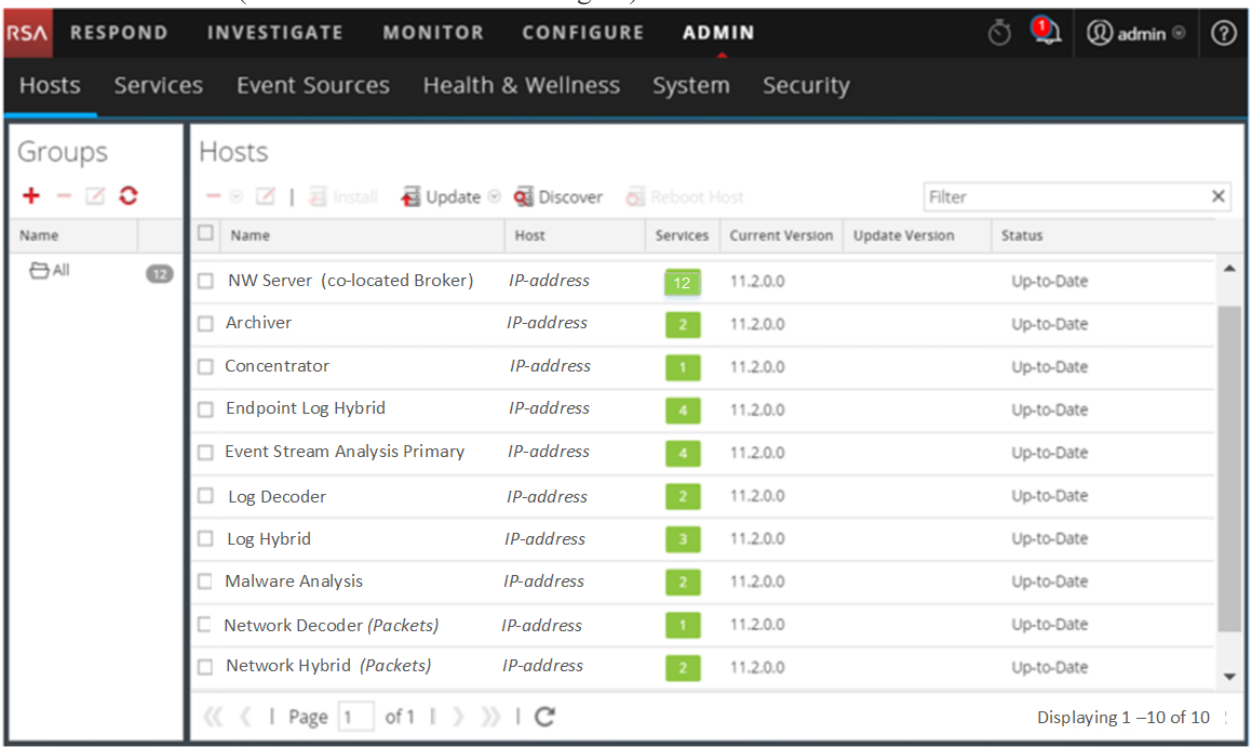
Sie verwenden die Ansicht „Hosts“, um die neuesten Versionsaktualisierungen über Ihr Auffüllen des lokalen Update-Repository anzuwenden. Sie müssen die Benennungskonvention für das Aktualisieren der Version verstehen, um zu entscheiden, welche Version Sie für den Host anwenden möchten. Die Benennungskonvention ist ***Hauptversion.Nebenversion.Service Pack.Patch***. Wenn Sie beispielsweise 11.6.1.2 auswählen, installieren Sie die folgende Version auf dem Host.

- 11 = Hauptversion
- 6 = Nebenversion

- 1 = Service Pack
- 2 = Patch

NetWitness Platform unterstützt mehrere Versionen in Ihrer Bereitstellung. Der NetWitness Server (NW-Serverhost) wird zuerst aktualisiert und alle anderen Hosts müssen dieselbe oder eine frühere Version als der NW Server-Host aufweisen.

Das folgende Beispiel ist eine Bereitstellung als einzelne Version, bei der alle Hosts auf 11.2.0.0 aktualisiert wurden (neueste RSA-Version verfügbar).



Verwalten von Services

Verwenden Sie die Ansicht „ADMIN > Services“, um Ihrer Bereitstellung Services hinzuzufügen, diese zu bearbeiten und zu löschen sowie andere Wartungsaufgaben durchzuführen. Ausführliche Anweisungen finden Sie im Abschnitt zu Verfahren bei Hosts und Services.

Mit dem NetWitness Server implementierte Services

Die Services in der folgenden Tabelle werden implementiert, wenn die Bereitstellung von NW Server Folgendes unterstützt:

- Die Erweiterung von physischen und virtuellen Bereitstellungsplattformen und Verbesserungen an der Host- und Servicewartung
- Content- Investigate- Respond- und Source-Funktionen.

Achtung: Sie müssen diese Services nicht konfigurieren, um NetWitness Platform bereitzustellen. RSA empfiehlt, den Betriebsstatus dieser Services mithilfe der Funktion „Integrität und Zustand“ zu überwachen. Versuchen Sie nicht, die Parameter in der Ansicht „Durchsuchen“ zu ändern, ohne Kontakt zum Kundensupport aufzunehmen (https://community.rsa.com/docs/DOC-1294).

Service	Zweck
Administrator	Der Administration Server (**Adminserver**) ist der Back-end-Service für administrative Aufgaben auf der Benutzeroberfläche (UI) von NetWitness Platform. Er abstrahiert die Authentifizierung, das Management von globalen Einstellungen und die Autorisierungsunterstützung für die Benutzeroberfläche. Der **Adminserver** benötigt den **Konfigurationsserver** und den **Sicherheitsserver**, um online sein und seine Aufgaben ausführen zu können.
Konfig	Der Configuration Server (**Konfigurationsserver**) speichert und verwaltet Konfigurationssätze. Ein Konfigurationssatz ist eine Gruppe beliebiger logischer Konfigurationen, die unabhängig verwaltet wird. Der **Konfigurationsserver** ermöglicht die gemeinsame Nutzung von Eigenschaften durch Services, bietet Möglichkeiten zur Sicherung und Wiederherstellung von Konfigurationen und erfasst Änderungen an den Eigenschaften.
Content	Der Content-Server verwaltet die von RSA bereitgestellten und die vom Nutzer erstellten Parser-Regeln. Falls Sie weitere Informationen zum Parser-Management benötigen, suchen Sie in RSA-Link nach "Parser".
Integration	Der Integrationsserver verwaltet Interaktionen mit externen Systemen. Der Service verarbeitet die folgenden aus- oder eingehenden Kanäle. • REST-API-Gateway: Gateway für externe Rest-Clients, das Aufrufe der NetWitness-API (Application Programming Interface) zuweist • Notifications Dispatcher: zentraler Dispatcher für alle ausgehenden Benachrichtigungen aus der NetWitness-Bereitstellung.
Investigate	Der Investigate-Server unterstützt die Funktionen „Ermittlung und Malware-Analyse“. Weitere Informationen finden Sie im *NetWitness PlatformErmittlung und Malware-Analyse – Benutzerhandbuch*.
Orchestrierung	Der Orchestrierungsserver stellt alle Services in Ihrer NetWitness Platform-Bereitstellung bereit und installiert und konfiguriert diese.
Respond	Der Respond-Server unterstützt Respond-Funktionen. Weitere Informationen finden Sie im *NetWitness PlatformKonfigurationsleitfaden für Respond*.

Service	Zweck
Security	Der NetWitness Platform Security Server (**Sicherheitsserver**) verwaltet die Sicherheitsinfrastruktur einer NetWitness Platform-Bereitstellung. Er ist für die folgenden sicherheitsbezogenen Bereiche verantwortlich. • Benutzer- und Authentifizierungskonten • Rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) • Bereitstellung der PKI (Public Key Infrastructure) Eine NetWitness Platform-Bereitstellung weist Benutzer mit Authentifizierungskonten auf. Unabhängig davon, wie die Identität des Analysten (z. B. Active Directory) überprüft wird, muss NetWitness Platform den Benutzerstatus speichern, was nicht bei allen Authentifizierungsanbietern möglich ist (z. B. Zeitpunkt der letzten Anmeldung, fehlgeschlagene Anmeldeversuche und Rollen). Es wird zwischen dem Konzept eines Nutzers und der ihm zugewiesenen Identität unterschieden. Der **Sicherheitsserver** verwaltet diese als separate Nutzer- und Kontoentitäten. Der Server unterstützt zusätzlich zu den verfügbaren lokalen NetWitness-Konten, die in allen NetWitness-Bereistellungen verfügbar sind, auch externe Authentifizierungsanbieter. Der **Sicherheitsserver** implementiert durch die Verwaltung von Rollen- und Berechtigungsentitäten außerdem RBAC. Berechtigungen können Rollen und Rollen wiederum Benutzern zugewiesen werden. Zusammen ermöglichen sie eine flexible Autorisierungs-Policy für die Bereitstellung. Der Server unterstützt zudem die Generierung von kryptografisch sicheren Token, die die entsprechende Autorisierung für einen Benutzer codieren. Diese Token bilden die Grundlage für eine bereitstellungsweite Autorisierung.
Source	Der Source-Server ist für die zukünftige Nutzung reserviert und stellt einen zentralen Speicherort zum Konfigurieren von Quellen (z. B. Endpunkt- und Protokollquellen) bereit.

Ausführen im gemischten Modus

Der gemischte Modus ist aktiv, wenn einige Services auf eine neue Version aktualisiert werden und andere in älteren Versionen beibehalten werden. Dieser Zustand tritt ein, wenn Sie die Hosts in Ihrer Bereitstellung phasenweise auf eine neue Version aktualisieren oder die Aktualisierung gestaffelt vornehmen.

Funktionslücken bei einer gestaffelten Aktualisierung

Wenn Sie die Aktualisierung gestaffelt vornehmen, kann Folgendes auftreten:

- Möglicherweise sind nicht alle Funktionen einsatzfähig, bis Sie die gesamte Bereitstellung aktualisiert haben.
- Ihnen stehen keine administrativen Funktionen in Services zur Verfügung, bis alle Hosts in Ihrer

Bereitstellung aktualisiert sind.

- Die Datenerfassung ist möglicherweise eine Zeit lang nicht verfügbar.

Beispiele für gestaffelte Aktualisierungen

In den folgenden Beispielen nehmen wir an, dass alle Hosts die Version 11.2.0.x haben und Sie die Hostaktualisierungen auf Version 11.2.1.0 gestaffelt vornehmen möchten.

Beispiel 1. Mehrere Decoder und Concentrator, Alternative 1

In diesem Beispiel umfasst die 11.2.0.x-Bereitstellung Folgendes: einen NW-Serverhost, zwei Decoder-Hosts, zwei Concentrator-Hosts, einen Archiver-Host, einen Broker-Host, einen Event Stream Analysis-Host und einen Malware Analysis-Host.

Sie müssen zunächst Phase 1 abschließen und die Hosts in der für Phase 1 angegebenen Reihenfolge aktualisieren.

RSA empfiehlt, die Hosts in Phase 2 in der für Phase 1 angegebenen Reihenfolge zu aktualisieren.

Phase 1 – Sitzung 1

1. Aktualisieren Sie den NetWitness-Serverhost.
2. Aktualisieren Sie den Event Stream Analysis-Host.
3. Aktualisieren Sie den Malware Analysis-Host.
4. Aktualisieren Sie den Broker- oder Concentrator-Host.

Phase 2 – Sitzung 2

1. Aktualisieren Sie die 2 Decoder-Hosts.
2. Aktualisieren Sie die 2 Concentrator-Hosts und den Archiver-Host.

Phase 2 – Sitzung 3

1. Aktualisieren aller anderen Hosts

Beispiel 2. Mehrere Decoder und Concentrator, Alternative 2

In diesem Beispiel umfasst die 11.2.0.x-Bereitstellung Folgendes: einen NW-Serverhost, zwei Decoder-Hosts, zwei Concentrator-Hosts, einen Broker-Host, einen Event Stream Analysis-Host und einen Malware Analysis-Host. RSA empfiehlt, die Hosts in Phase 2 in der folgenden Reihenfolge zu aktualisieren. Beachten Sie, dass Sie zuerst Phase 1 abschließen und die Hosts in der aufgeführten Reihenfolge aktualisieren müssen.

Phase 1 – Sitzung 1

1. Aktualisieren Sie den NetWitness-Serverhost.
2. Aktualisieren Sie den Event Stream Analysis-Host.
3. Aktualisieren Sie den Malware Analysis-Host.
4. Aktualisieren Sie den Broker-Host.

Phase 2 – Sitzung 2

1. Aktualisieren Sie einen Decoder- und einen Concentrator-Host.
   Es dauert eine Weile, bis NetWitness Platform den Großteil der Daten verarbeitet hat.

Phase 2 – Sitzung 3

1. Aktualisieren Sie einen Decoder-Host, einen Concentrator-Host und den Broker-Host.
2. Aktualisieren Sie alle Log Decoder-Hosts, bevor Sie die Virtual Log Collectors aktualisieren.
3. Aktualisieren aller anderen Hosts

Beispiel 3. Mehrere Bereiche

In diesem Beispiel umfasst die 11.2.0.x-Bereitstellung Folgendes: einen NW-Serverhost, einen Event Stream Analysis-Host, einen Malware Analysis-Host, vier Decoder-Hosts, vier Concentrator-Hosts, zwei Broker-Hosts (zwei Standorte mit jeweils zwei Decoders, zwei Concentrators und einem Broker).

Phase 1 – Standort 1 aktualisieren

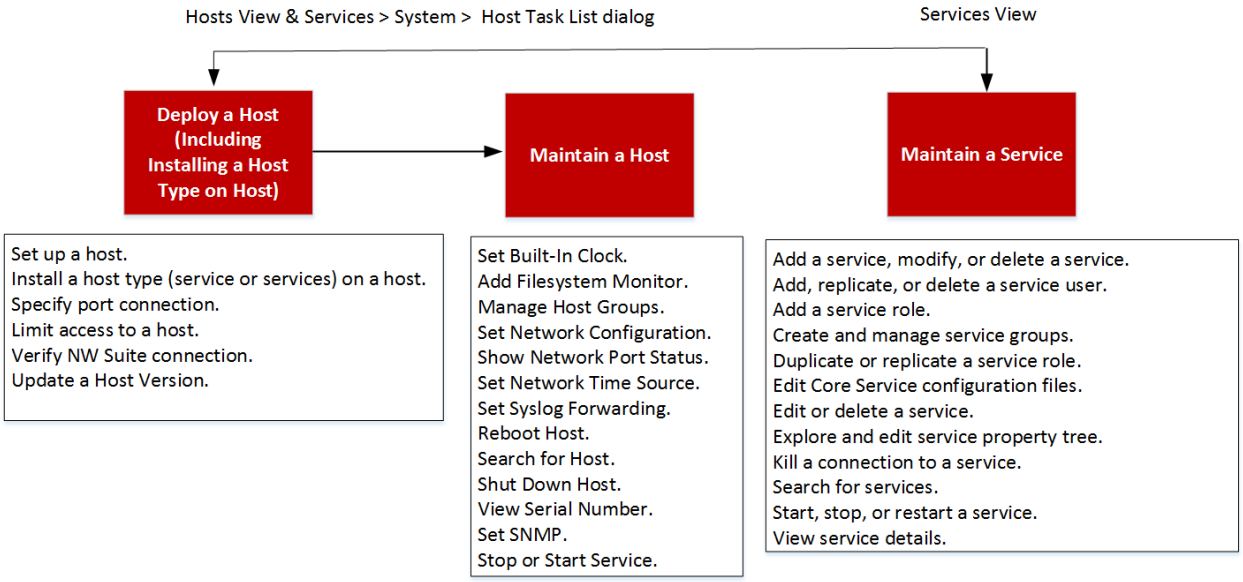
1. Aktualisieren Sie den NW-Serverhost.
2. Aktualisieren Sie den Event Stream Analysis-Host.
3. Aktualisieren Sie den Malware Analysis-Host.
4. Aktualisieren Sie einen Broker-Host, zwei Decoder-Hosts und zwei Concentrator-Hosts.
5. Aktualisieren Sie alle anderen Hosts.

Phase 2 – Standort 2 aktualisieren

1. Aktualisieren Sie die Broker-Hosts.
2. Aktualisieren Sie zwei Decoder-Hosts.
3. Aktualisieren Sie zwei Concentrator-Hosts.
4. Aktualisieren Sie alle anderen Hosts.

Hosts und Services – Verfahren

Jeder Service erfordert einen Host. Nach dem Einrichten eines Hosts können Sie diesem Host und von diesem Host aus anderen Hosts in der NetWitness Platform-Bereitstellung Services zuweisen.



Allgemeine Aufgaben	Beschreibung
Einrichten eines Hosts	Führen Sie die folgenden Schritte aus, um einen Host einzurichten. Schritt 1. Bereitstellen eines Hosts Schritt 2. Installieren eines Service auf einem Host Schritt 3. Überprüfen von SSL-Ports auf vertrauenswürdige Verbindungen Schritt 4. Verwalten des Zugriffs auf einen Service

Allgemeine Aufgaben	Beschreibung

Warten eines Hosts – Grundlagen	Die folgenden Wartungsaufgaben werden in alphabetischer Reihenfolge angezeigt.
	• Anwenden von Versionsaktualisierungen auf einen Host
	  • Auffüllen des lokalen Aktualisierungs-Repository
	  • Einrichten eines externen Repository mit RSA und Betriebssystemupdates
	• Erstellen und Managen von Hostgruppen
	• Suchen nach Hosts
	• Festlegen der Netzwerkkonfiguration
	• Festlegen der Quelle für die Netzwerkzeit
	• Anzeigen des Netzwerkportstatus
	• Anzeigen der Seriennummer
	• Herunterfahren eines Hosts
	• Beenden und Starten eines Service auf einem Host

Warten eines Hosts über das Dialogfeld „Hostaufgabenliste“	Sie können das Dialogfeld Hostaufgabenliste verwenden, um Aufgaben zu managen, die im Zusammenhang mit einem Host und dessen Kommunikation mit dem Netzwerk stehen. Für Core-Hosts sind mehrere Service- und Hostkonfigurationsoptionen verfügbar. • Ausführen einer Aufgabe aus der Hostaufgabenliste • Hinzufügen und Löschen einer Dateisystemüberwachung • Neustarten eines Hosts • Einstellen der internen Uhr des Hosts • Festlegen der Netzwerkkonfiguration • Festlegen der Quelle für die Netzwerkzeit • SNMP festlegen • Einrichten der Syslog-Weiterleitung • Anzeigen des Netzwerkportstatus • Anzeigen der Seriennummer • Herunterfahren eines Hosts • Beenden und Starten eines Service auf einem Host

Allgemeine Aufgaben	Beschreibung
Verwalten eines Service	Anhand der folgenden Abläufe wird beschrieben, wie Services verwaltet werden. • Hinzufügen, Replizieren oder Löschen eines Servicebenutzers • Hinzufügen einer Servicebenutzerrolle • Ändern eines Servicebenutzerpassworts • Erstellen und Managen von Servicegruppen • Duplizieren oder Replizieren einer Servicerolle • Bearbeiten von Core-Servicekonfigurationsdateien • Bearbeiten oder Löschen eines Service • Durchsuchen und Bearbeiten der Service-Eigenschaftenstruktur • Beenden der Verbindung zu einem Service • Suchen nach Services • Starten, Beenden oder Neustarten eines Service • Anzeigen von Servicedetails

Schritt 1. Bereitstellen eines Hosts

Achtung: Wenn Sie „.“ in einen Hostnamen einfügen, muss dieser auch einen gültigen Domainnamen enthalten.

1. Stellen Sie einen Host bereit.

   Sie können einen physischen Host (RSA Appliance), einen virtuellen Host lokal, einen virtuellen Host in AWS oder einen virtuellen Host in Azure bereitstellen. In den folgenden Leitfäden finden Sie Anweisungen zur Bereitstellung von Hosts.

   - *RSA NetWitness® Platform – Leitfaden zur Bereitstellung eines physischen Hosts*
   - *RSA NetWitness® Platform – Leitfaden zur Bereitstellung eines virtuellen Hosts*
   - *RSA NetWitness® Platform – Leitfaden zur Bereitstellung in AWS*
   - *RSA NetWitness® Platform – Leitfaden zur Bereitstellung in Azure*

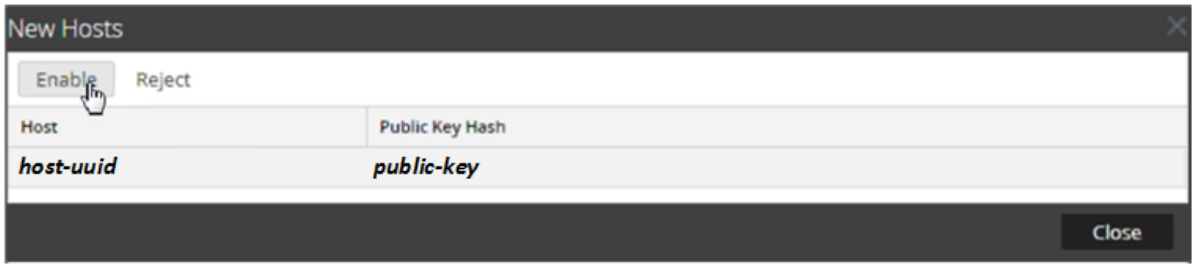
2. Navigieren Sie zu **Administration** > **Hosts**.

   Das Dialogfeld **Neue Hosts** mit den bereitgestellten Hosts wird angezeigt.

3. Wählen Sie die Hosts aus, die Sie aktivieren möchten.

   Die Menüoption **Aktivieren** wird aktiv.

4. Klicken Sie auf **Aktivieren**.



5. Wählen Sie den Host aus, den Sie aktiviert haben.

   Der Host wird in der Ansicht „Hosts“ angezeigt. An diesem Punkt können Sie einen Service auf dem Host installieren.

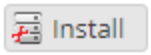
Schritt 2. Installieren eines Service auf einem Host

Führen Sie die folgenden Schritte aus, um einen Service auf einem Host zu installieren.

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Hosts**.

   Die Ansicht **Hosts** wird angezeigt.

2. Wählen Sie den Host aus, auf dem Sie den Service installieren möchten (z. B **Event Stream Analysis**).

3. Klicken Sie in der Symbolleiste auf 

.

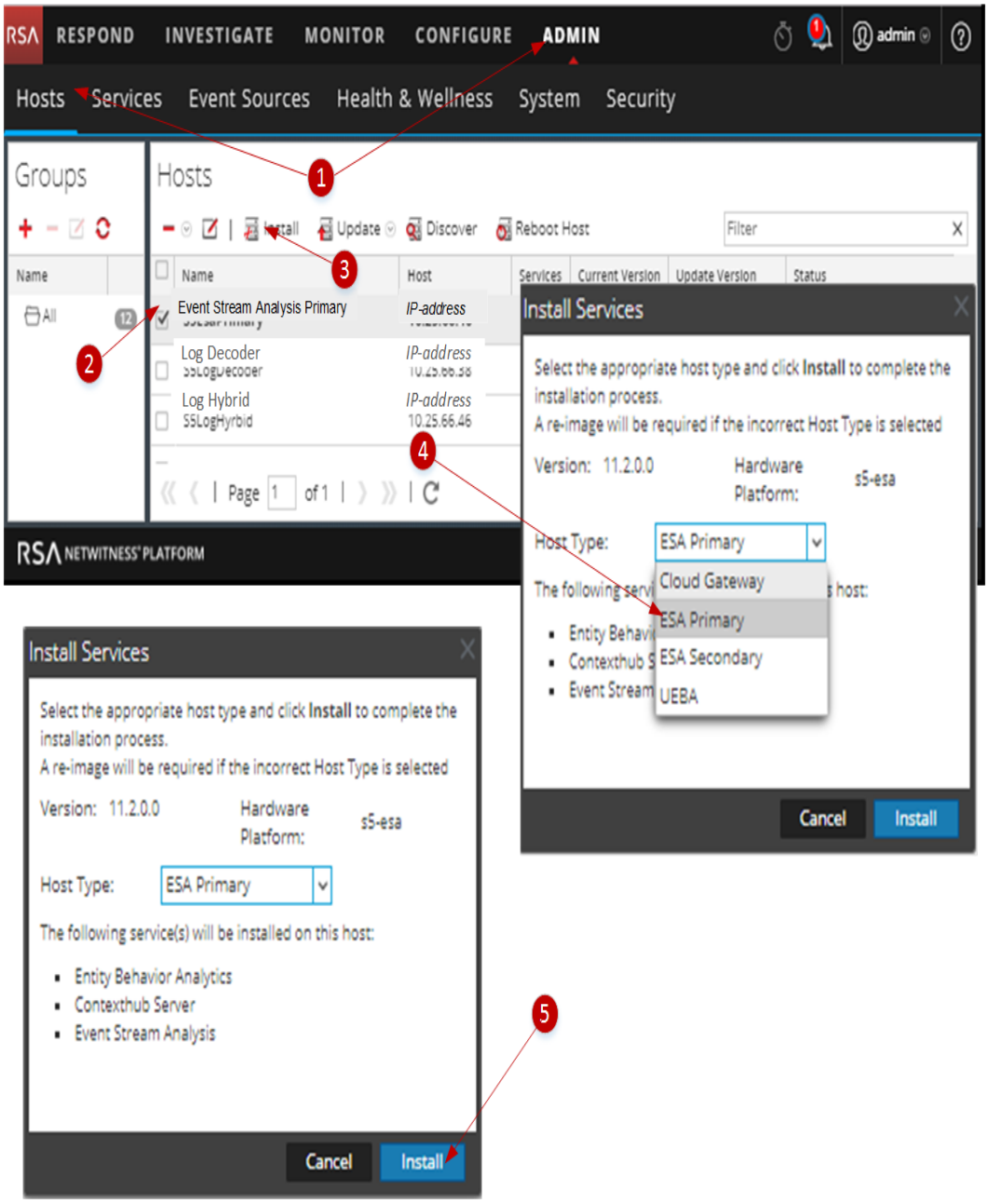
   Das Dialogfeld **Services installieren** wird angezeigt.

4. Wählen Sie in der Drop-down-Liste **Hosttyp** einen Service aus (**ESA Primary**).

wird im Dialogfeld **Services installieren** aktiv.

5. Klicken Sie auf Install.



Schritt 3. Überprüfen von SSL-Ports auf vertrauenswürdige Verbindungen

Um vertrauenswürdige Verbindungen zu unterstützen, besitzt jeder Core-Service zwei Ports: einen unverschlüsselten Nicht-SSL-Port und einen verschlüsselten SSL-Port. Vertrauenswürdige Verbindungen setzen einen verschlüsselten SSL-Port voraus.

Verschlüsselte SSL-Ports

Wenn Sie die Version 10.4 oder höher installieren oder ein Upgrade auf diese Version durchführen, werden vertrauenswürdige Verbindungen standardmäßig mit zwei Einstellungen hergestellt:

- SSL ist aktiviert.
- Der Core-Service ist mit einem verschlüsselten SSL-Port verbunden.

Jeder NetWitness Platform Core-Service verfügt über zwei Ports:

- Unverschlüsselter **Nicht-SSL-Port**
  Beispiel: Archiver 50008
- Verschlüsselter **SSL-Port**
  Beispiel: Archiver 56008

Der SSL-Port ist der Nicht-SSL-Port + 6000.

In der folgenden Tabelle werden alle NetWitness Platform-Servicesmit den entsprechenden Ports aufgelistet und es wird gezeigt, dass jeder Core-Service über zwei Ports verfügt. Alle aufgelisteten Portnummern sind TCPs.

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Admin	-	-	Wird mit dem NW-Server implementiert.
Archiver	50008	56008	
Broker	50003	56003	Core-Service
Cloud Gateway	–	–	
Concentrator	50005	56005	Core-Service
Konfiguration	–	–	Wird mit dem NW-Server implementiert.
Inhalt	-	-	Wird mit dem NW-Server implementiert.
Context Hub	–	–	
Decoder (Pakete)	50004	56004	Core-Service
Endpoint	-	-	
Entity Behavior Analysis	–	–	
Event Stream Analysis	–	50030	

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Integration	–	–	Wird mit dem NW-Server implementiert.
Untersuchen	–	–	Wird mit dem NW-Server implementiert.
Log Collector	50001	56001	
Log Decoder	50002	56002	Core-Service
Malware Analysis	–	60007	
Orchestrierung	–	–	Wird mit dem NW-Server implementiert.
Reporting Engine	-	51113	Wird mit dem NW-Server implementiert.
Respond	–	–	Wird mit dem NW-Server implementiert.
Sicherheit	–	–	Wird mit dem NW-Server implementiert.
Quelle	-	-	Wird mit dem NW-Server implementiert.
UEBA	-	-	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Schritt 4. Managen des Zugriffs auf einen Service

In einer vertrauenswürdigen Verbindung überlässt ein Service explizit NW Server das Managen und Authentifizieren von Benutzern. Mit dieser vertrauenswürdigen Verbindung können Services in **ADMINISTRATION >Services** ohne Anmeldedaten für alle NetWitness Platform Core-Services definiert werden. Stattdessen können Benutzer, die vom Server authentifiziert wurden, auf den Service zugreifen, ohne ein anderes Passwort eingeben zu müssen.

Testen einer vertrauenswürdigen Verbindung

Voraussetzungen

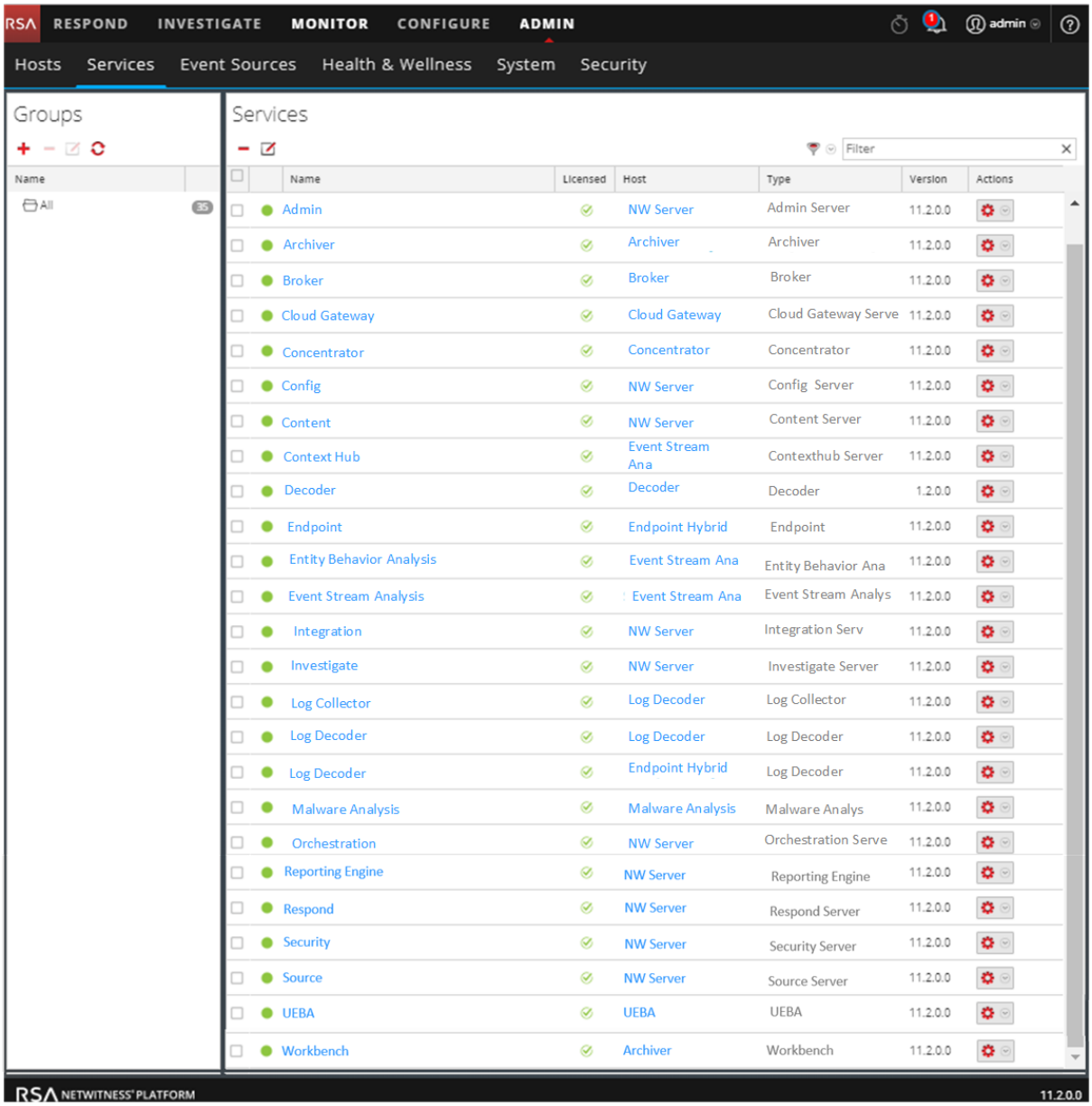
1. Dem Benutzer muss ein Rolle zugewiesen sein.
   Weitere Informationen finden Sie im Thema **Hinzufügen eines Nutzers und einer Rolle** im

Handbuch „Systemsicherheit und Benutzerverwaltung“.

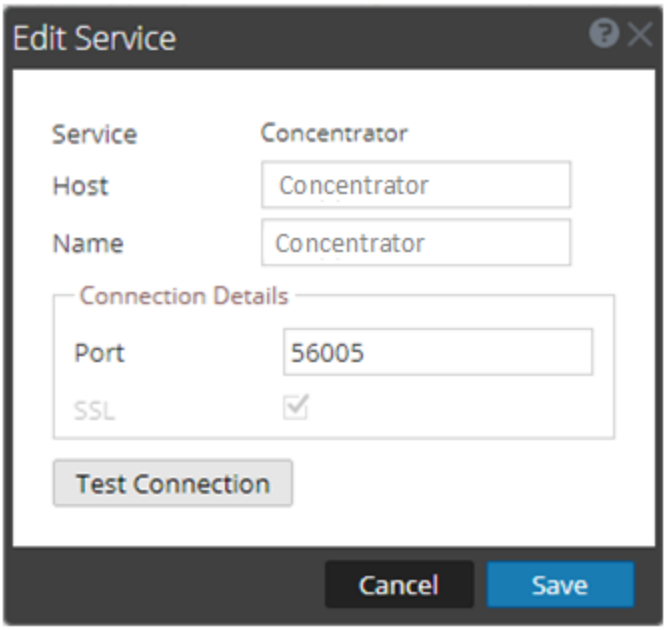
2. Der Benutzer muss:
   - Melden Sie sich bei NetWitness Platform an, damit der Server den Nutzer authentifizieren kann.
   - Zugriff auf den Service haben.

Verfahren

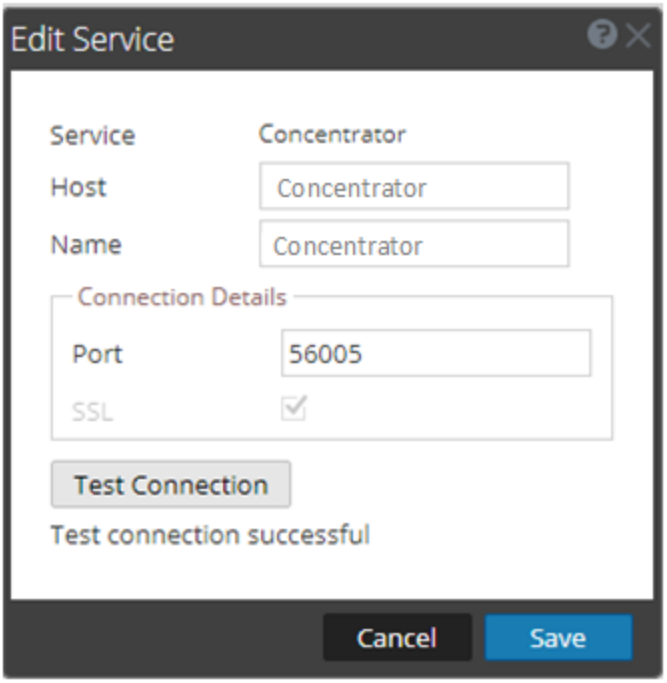
1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
   Die Ansicht -Services wird angezeigt.



2. Wählen Sie den zu testenden Service (z. B. einen Concentrator) aus und klicken Sie auf .
   Das Dialogfeld**Service bearbeiten** wird angezeigt.



3. Entfernen Sie den **Benutzernamen**, um die Verbindung ohne Anmeldedaten zu testen.
4. Klicken Sie auf **Verbindung testen**.



   Die Meldung **Verbindungstest erfolgreich** bestätigt, dass die vertrauenswürdige Verbindung hergestellt wurde.
   Ein zuvor authentifizierter Benutzer kann auf den Service zugreifen, ohne beim Service einen Benutzernamen und ein Passwort einzugeben.

5. Klicken Sie auf **Speichern**.

Anwenden von Versionsaktualisierungen auf einen Host

Führen Sie die folgenden Aufgaben aus, um einen Host auf eine neue Version zu aktualisieren.

Es gibt zwei Methoden, Versionsaktualisierungen auf einen Host anzuwenden.

Hinweis: Wenn Sie das Verzeichnis für das Repository geändert haben, finden Sie weitere Anweisungen unter Einrichten eines externen Repository mit RSA und Betriebssystemupdates.

- Anwenden von Aktualisierungen über die Ansicht „Hosts“ (Webzugriff)
- Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)

Anwenden von Aktualisierungen über die Ansicht „Hosts“ (Webzugriff)

Aufgabe 1. Auffüllen des lokalen Repository oder Einrichten eines externen Repository

Wenn Sie Ihren NW-Server einrichten, wählen Sie das lokale Repository oder ein externes Repository aus. Die Ansicht „Hosts“ ruft Versionsaktualisierungen aus dem ausgewählten Repository ab.

Wenn Sie das lokale Repository ausgewählen, müssen Sie dieses nicht einrichten, aber Sie müssen sicherstellen, dass es die neuesten Aktualisierungen enthält. Anweisungen zum Auffüllen des Repository mit einer Versionsaktualisierung finden Sie unter Auffüllen des lokalen Update-Repository.

Hinweis: Wenn Sie ein externes Repository ausgewählt haben, müssen Sie es einrichten. Weitere Informationen dazu, wie es mit einer Versionsaktualisierung aufgefüllt wird, finden Sie unter Einrichten eines externen Repository mit RSA und Betriebssystemupdates.

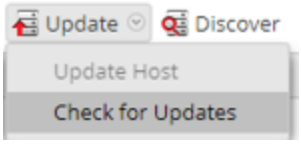
Aufgabe 2. Anwenden von Aktualisierungen über die Ansicht „Hosts“ auf einzelne Hosts

In der Ansicht „Hosts“ werden die in Ihrem lokalen Update-Repository verfügbaren Softwareversionsaktualisierungen angezeigt und Sie wählen die gewünschten Aktualisierungen über die Ansicht „Hosts“ aus und wenden diese an.

In diesem Verfahren erfahren Sie, wie Sie einen Host auf eine neue Version von NetWitness Platform aktualisieren.

Hinweis: In diesem Thema wird die Aktualisierung von NetWitness Platform 11.0.x.x auf 11.1.0.0 als Beispiel verwendet.

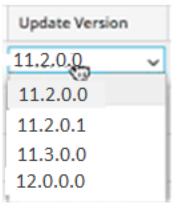
1. Melden Sie sich bei NetWitness Platform an.
2. Navigieren Sie zu **ADMIN > Hosts**.
3. (Bedingungsabhängig) Überprüfen Sie die neuesten Aktualisierungen.



4. Wählen Sie einen Host oder Hosts aus.

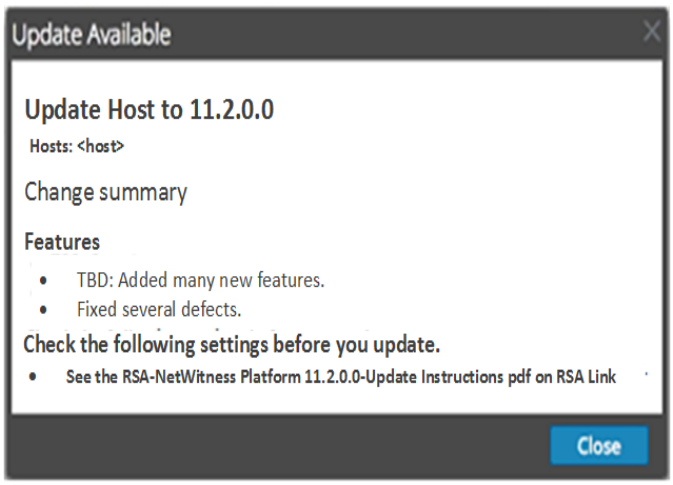
   Sie müssen zunächst den NW-Server auf die neueste Version aktualisieren. Sie können die anderen Hosts in beliebiger Reihenfolge aktualisieren, aber RSA empfiehlt, dass Sie die Richtlinien unter Ausführen im gemischten Modus befolgen.
   Aktualisierung verfügbar wird in der Spalte **Status** angezeigt, wenn Sie eine Versionsaktualisierung in Ihrem lokalen Update-Repository für die ausgewählten Hosts haben.

5. Wählen Sie die Version, die Sie anwenden möchten, aus der Spalte **Update-Version** aus.



   Gehen Sie in folgenden Fällen wie folgt vor:

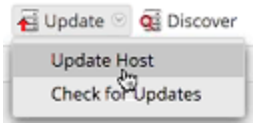
   - Wenn Sie mehr als einen Host auf diese Version aktualisieren möchten, dann aktivieren Sie nach der Aktualisierung des NW-Serverhosts das Kontrollkästchen links neben den Hosts. Es sind nur Versionen von Aktualisierungen aufgelistet, die derzeit unterstützt werden.
   - Wenn Sie ein Dialogfeld mit den wichtigsten Funktionen der Aktualisierung anzeigen möchten, klicken Sie auf das Symbol ⓘ rechts neben der Versionsnummer der Aktualisierung. Nachfolgend finden Sie ein Beispiel für das Dialogfeld.



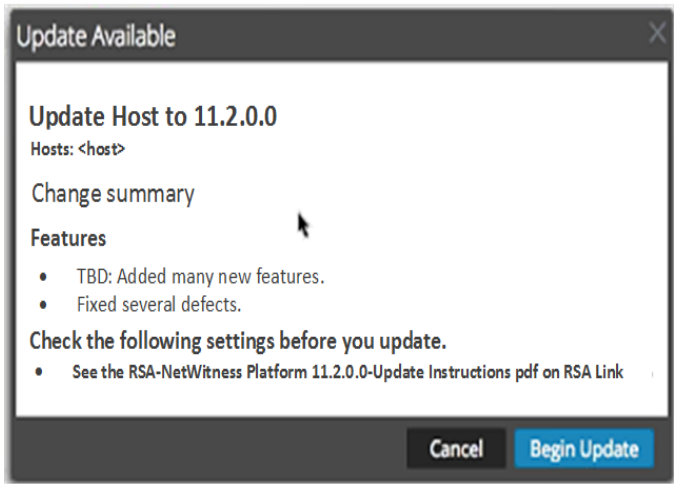
   - Wenn Sie die gewünschte Version nicht finden können, wählen Sie **Aktualisieren > Nach Updates suchen** aus, um das Repository auf alle verfügbaren Aktualisierungen zu prüfen. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Es sind neue Hostaktualisierungen verfügbar“ angezeigt, und die Spalte **Status** wird automatisch aktualisiert und zeigt

Aktualisierung verfügbar an. Standardmäßig werden nur die unterstützten Aktualisierungen für den ausgewählten Host angezeigt.

6. Klicken Sie in der Symbolleiste auf **Aktualisieren > Host aktualisieren**.



Ein Dialogfeld wird mit Informationen über die ausgewählte Aktualisierung wird angezeigt. Klicken Sie auf **Update beginnen**.



Die Spalte **Status** informiert Sie darüber, was in jeder der folgenden Phasen der Aktualisierung geschieht:

- Phase 1: **Aktualisierungspakete werden heruntergeladen** – lädt die Repository-Artefakte auf den NW-Server für die Services auf dem ausgewählten Host herunter.
- Phase 2: **Aktualisierungspakete werden konfiguriert** – konfiguriert die Aktualisierungsdateien im richtigen Format.
- Phase 3: **Aktualisierung wird durchgeführt** – aktualisiert den Host auf die neue Version.

7. Wenn **Aktualisierung wird durchgeführt** angezeigt wird, aktualisieren Sie den Browser.

   Daraufhin wird möglicherweise der Anmeldebildschirm von NetWitness angezeigt, über den Sie sich erneut anmelden und zurück zur Host-Ansicht navigieren.

   Nachdem der Host aktualisiert wurde, zeigt NetWitness Platform die Aufforderung **Host neu starten** an.

8. Klicken Sie auf **Host neu starten** in der Symbolleiste.

   NetWitness Platform zeigt den Status **Wird neu gestartet...** an, bis der Host wieder online ist und der **Status Auf dem neuesten Stand** angezeigt wird. Wenden Sie sich an die Kundenbetreuung, wenn der Host nicht wieder online geschaltet wird.

Hinweis: Wenn der Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) aktiviert ist, kann das Öffnen der Kerndienste etwa 5 bis 10 Minuten dauern. Grund für diese Verzögerung ist das Erstellen neuer Zertifikate.

Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)

Wenn Ihre Bereitstellung von NetWitness Platform keinen Webzugriff hat, schließen Sie das folgende Verfahren ab, um eine Versionsaktualisierung anzuwenden.

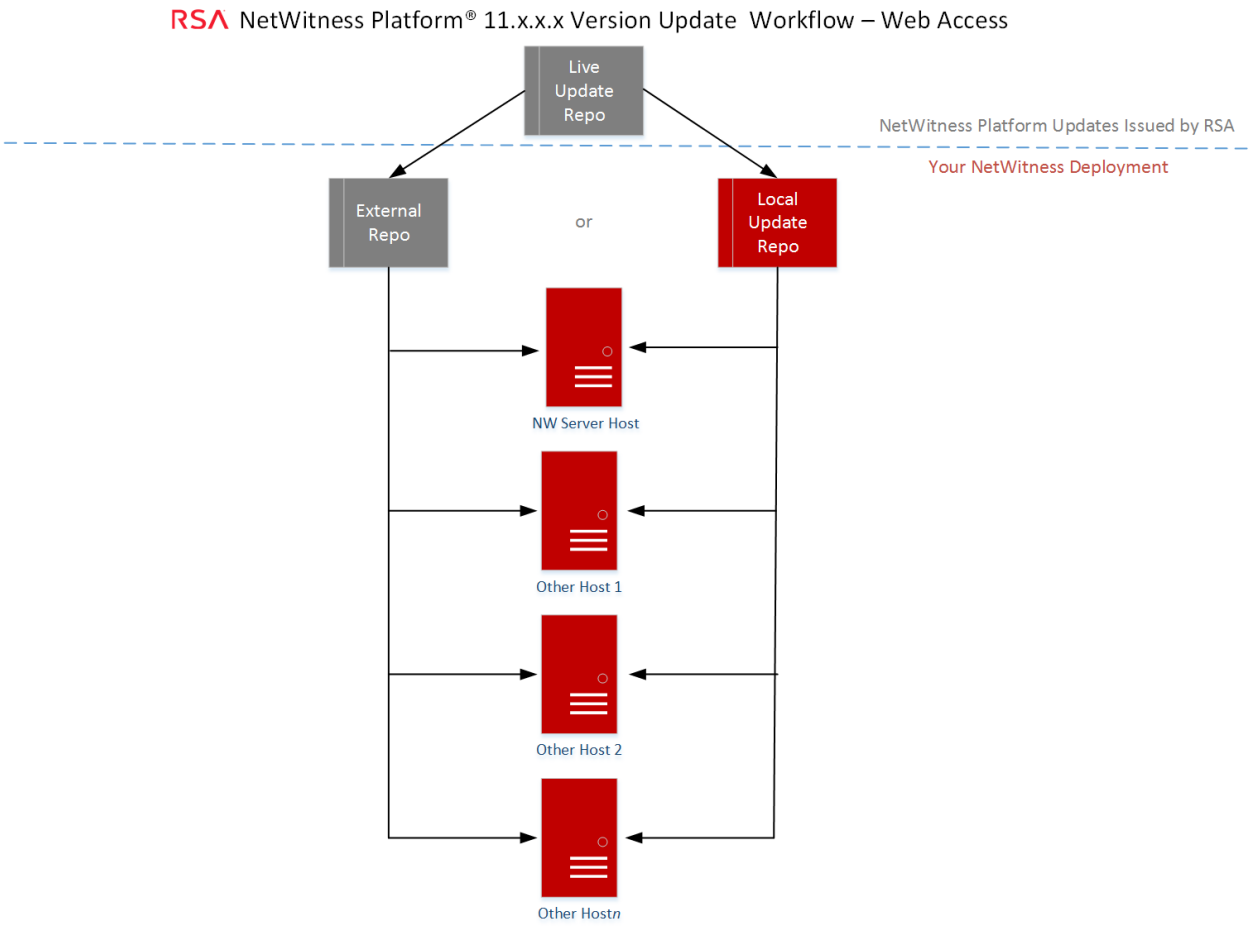
Hinweis: Im folgenden Verfahren ist 11.1.0.0 die Versionsaktualisierung, die als Beispiel in den Codezeichenfolgen verwendet wird.

1. Laden Sie das Aktualisierungspaket `.zip` für die gewünschte Version (z. B. `netwitness-11.1.0.0.zip`) von RSA Link in ein lokales Verzeichnis herunter.
2. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
3. Erstellen Sie ein Bereitstellungsverzeichnis `/tmp/upgrade/<version>` für die gewünschte Version (z. B. `tmp/upgrade/11.1.0.0`).
   `mkdir -p /tmp/upgrade/11.1.0.0`
4. Kopieren Sie das `.zip`-Updatepaket in ein anderes Verzeichnis als das Stagingverzeichnis auf dem NW-Server (z. B. das `/tmp`-Verzeichnis).
5. Entpacken Sie das Paket in das Staging-Verzeichnis, das Sie erstellt haben (z. B. `/tmp/upgrade/11.1.0.0`).
   `unzip /<download-location>/netwitness-11.1.0.0.zip -d /tmp/upgrade/11.1.0.0`
6. Initialisieren Sie die Aktualisierung auf dem NW-Server.
   `upgrade-cli-client --init --version 11.1.0.0 --stage-dir /tmp/upgrade/`
7. Wenden Sie die Aktualisierung auf den NW-Server an.
   `upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.1.0.0`
8. Melden Sie sich bei NetWitness Platform an und starten Sie den NW-Serverhost in der Ansicht „Host“.
9. Wenden Sie die Aktualisierung auf jeden Nicht-NW-Serverhost an.
   `upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.1.0.0`
   Die Aktualisierung ist abgeschlossen, wenn der Abruf abgeschlossen ist.
10. Melden Sie sich bei NetWitness Platform an und starten Sie den Host in der Ansicht „Host“ neu.
    Sie können mit dem folgenden Befehl überprüfen, welche Version auf den Host angewendet wurde:
    `upgrade-cli-client --list`

Auffüllen des lokalen Update-Repository

NetWitness Platform sendet Versionsaktualisierungen aus dem Live-Update-Repository in das lokale Update-Repository. Für den Zugriff auf das Live-Update-Repository ist die Eingabe der Anmeldedaten des Live-Kontos erforderlich, die unter **ADMIN >SYSTEM > Live** konfiguriert werden. Darüber hinaus müssen Sie das Kontrollkästchen `Automatically download information about new updates every day` unter **ADMIN > SYSTEM > Aktualisierungen** aktivieren, um das lokale Repository täglich aufzufüllen.

Das folgende Diagramm zeigt, wie Sie Versionsaktualisierungen erhalten, wenn Ihre NetWitness Platform-Bereitstellung über Webzugriff verfügt.



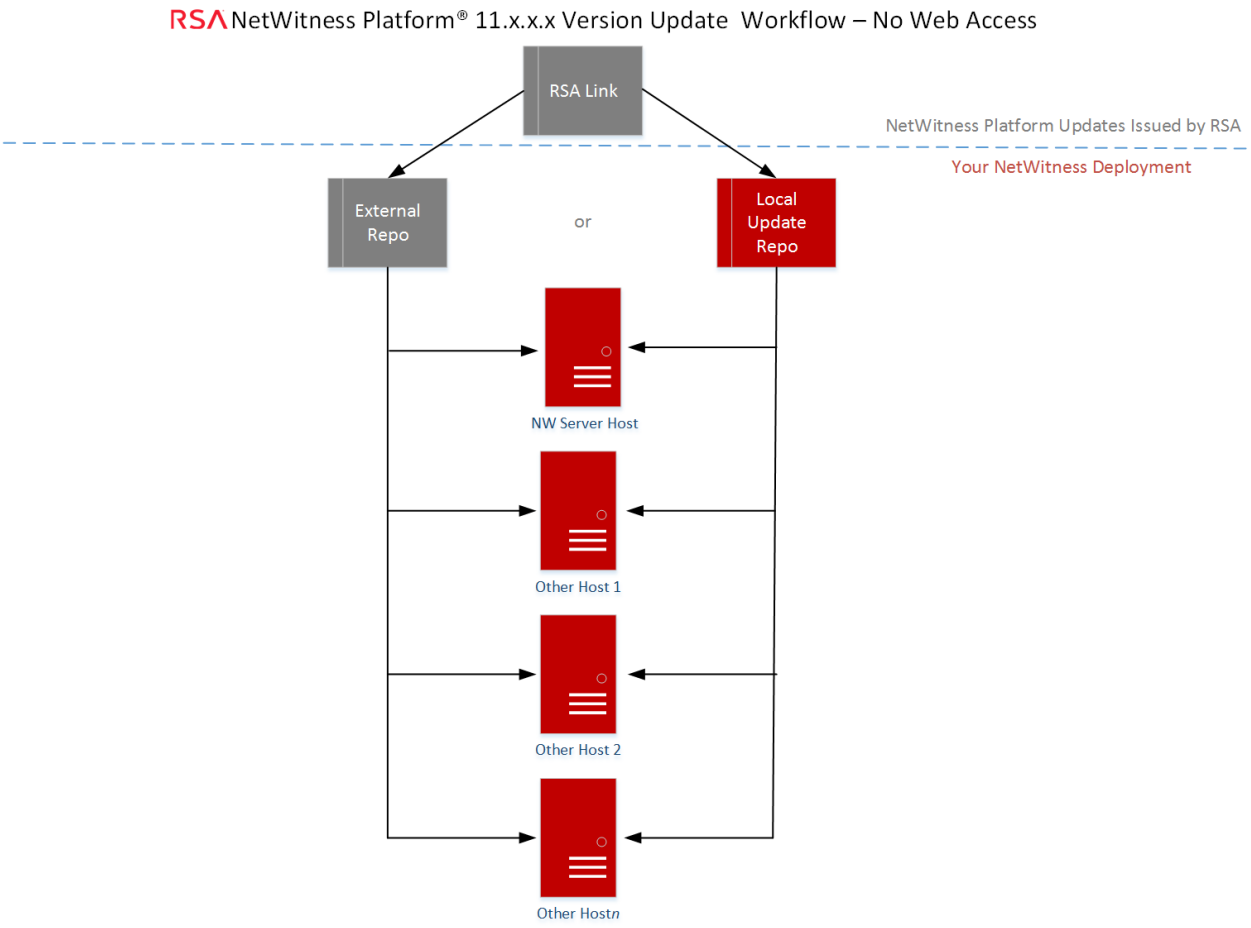
Hinweis: Wenn Sie erstmalig eine Verbindung mit dem Live-Update-Repository herstellen, können Sie auf alle CentOS 7-Systempakete und die RSA-Produktionspakete zugreifen. Je nach Internetverbindung Ihres NW-Servers und Datenverkehr des RSA-Repository kann der Download dieser Daten von mehr als 2,5 GB längere Zeit in Anspruch nehmen. Es ist nicht obligatorisch, das Live-Update-Repository zu verwenden. Alternativ können Sie ein externes Repository verwenden, wie beschrieben unter Einrichten eines externen Repository mit RSA und Betriebssystemupdates.

Zur Verbindung mit dem Live-Update-Repository navigieren Sie zu der Ansicht „ADMIN“ > „System“, wählen Sie im Optionsbereich **Live-Services** aus und vergewissern Sie sich, dass die Anmeldedaten konfiguriert sind (**Verbindung** sollte grün markiert sein). Wenn es nicht grün ist, klicken Sie auf **Anmelden** und stellen Sie eine Verbindung her.

Hinweis: Wenn Sie Proxys zum Kommunizieren mit dem Live-Update-Repository benötigen, können Sie den Proxy-Host, den Proxybenutzernamen und das Proxypasswort konfigurieren. Weitere Informationen finden Sie unter „Konfigurieren des Proxy fürNetWitness Platform“ im *Systemkonfigurationsleitfaden für NetWitness Platform 1.1*.

Wenn Ihre NetWitness Platform-Bereitstellung keinen Webzugriff hat, siehe Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff).

Das folgende Diagramm zeigt, wie Sie Versionsaktualisierungen erhalten, wenn Ihre NetWitness Platform-Bereitstellung nicht über Webzugriff verfügt.



Einrichten eines externen Repository mit RSA und Betriebssystemupdates

Hinweis: Im folgenden Verfahren ist 11.1.0.0 die Versionsaktualisierung, die als Beispiel in den Codezeichenfolgen verwendet wird.

Führen Sie das folgende Verfahren aus, um ein externes Repository (Repo) einzurichten.

Hinweis: 1.) Auf dem Host muss ein Dienstprogramm zum Entpacken installiert sein, damit Sie dieses Verfahren abschließen können. 2.) Sie müssen wissen, wie Sie einen Webserver erstellen, bevor Sie das folgende Verfahren durchführen.

1. (Bedingungsabhängig) Führen Sie diesen Schritt durch, wenn Sie ein externes Repository haben und Sie dieses außer Kraft setzen möchten.
   - 1. Fall: Sie haben den Host von einem externen Repository aus per Bootstrap neu gestartet und Sie möchten ein Upgrade durchführen mithilfe eines lokalen Repository auf dem Adminserver.
     a. Erstellen Sie die Datei `/etc/netwitness/platform/repobase`.
     ```
     vi /etc/netwitness/platform/netwitness/repobase
     ```

b. Bearbeiten Sie die Datei `repobase`, sodass die einzige Information in der Datei die folgende URL ist.
`https://nw-node-zero/nwrpmrepo`

c. Führen Sie die Anweisungen zum Ausführen des Upgrade mithilfe des Tools `upgrade-cli-client` aus.

- 2. Fall: Sie haben den Host von eines lokalen Repository auf dem Adminserver (NW-Serverhost) per Bootstrap neu gestartet und Sie möchten ein externes Repository für das Upgrade verwenden.

a. Erstellen Sie die Datei `/etc/netwitness/platform/repobase`.
`vi /etc/netwitness/platform/netwitness/repobase`

b. Bearbeiten Sie die Datei `repobase`, sodass die einzige Information in der Datei die folgende URL ist.
`https://<webserver-ip>/<alias-for-repo>`

c. Führen Sie die Anweisungen zum Ausführen des Upgrade mithilfe des Tools `upgrade-cli-client` aus.
Die Anweisungen finden Sie unter Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff).

2. Richten Sie das externe Repository ein.

a. Melden Sie sich bei dem Webserverhost an.

b. Erstellen Sie ein Verzeichnis, um das NW-Repository (`netwitness-11.2.0.0.zip`) zu hosten, z. B. `ziprepo` unter `web-root` des Webservers. Beispiel: Wenn /var/netwitness das „web-root“-Verzeichnis ist, senden Sie die folgende Befehlszeichenfolge.
`mkdir -p /var/netwitness/<your-zip-file-repo>`

c. Erstellen Sie das Verzeichnis 11.2.0.0 unter `/var/netwitness/<your-zip-file-repo>`.
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`

d. Erstellen Sie die Verzeichnisse `OS` und `RSA` unter `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

e. Entpacken Sie die Datei `netwitness-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
`unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0`
Durch das Entpacken von `netwitness-11.2.0.0.zip` entstehen zwei Zip-Dateien (`OS-11.2.0.0.zip` und `RSA-11.2.0.0.zip`) und einige andere Dateien.

f. Entpacken Sie die Datei:

i. `OS-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`.
`unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -`

`d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`

Das folgende Beispiel zeigt, wie die Dateistruktur des Betriebssystems (OS) aussieht, nachdem Sie die Datei entpackt haben.

Parent Directory		-
GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49	1.1M
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07	4.6M
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05	1.5M
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	502K
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	15K
PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30	160K
SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39	204K
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04	81K
adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10	706K
alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52	421K
at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	51K
atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53	258K
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04	66K

ii. `RSA-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`.

`unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`

Das folgende Beispiel zeigt, wie die Dateistruktur der RSA Versionsaktualisierung aussieht, nachdem Sie die Datei entpackt haben.

Parent Directory		-
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K
fneserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K

Der externe URL für das Repository ist `http://<web server IP address>/<your-zip-file-repo>`.

g. (Bedingungsabhängig – für Azure) Befolgen Sie diese Schritte, um Azure zu aktualisieren.

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`

ii. `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`

iv. `createrepo .`

h. Verwenden Sie die `http://<web server IP address>/<your-zip-file-repo>` als Antwort auf die Eingabeaufforderung **Geben Sie den Basis-URL des externen Update-Repository ein** des NW 11.2.0.0 Setup-Programms (`nwsetup-tui`).

Erstellen und Managen von Hostgruppen

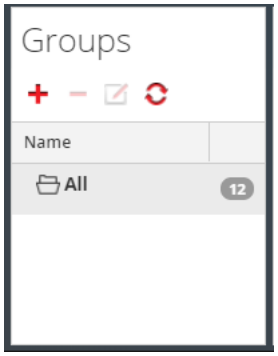
Die Ansicht „Hosts“ enthält Optionen zum Erstellen und Verwalten von Hostgruppen. Die Symbolleiste des Bereichs „Gruppen“ umfasst Optionen zum Erstellen, Bearbeiten und Löschen von Hostgruppen. Nachdem Gruppen erstellt wurden, können Sie einzelne Hosts aus dem Bereich Hosts in eine Gruppe ziehen.

Gruppen können funktionale, geografische, projektorientierte oder beliebige andere hilfreiche Unternehmensprinzipien widerspiegeln. Ein Host kann zu mehreren Gruppen gehören. Im Folgenden sind einige Beispiele für mögliche Gruppierungen aufgeführt:

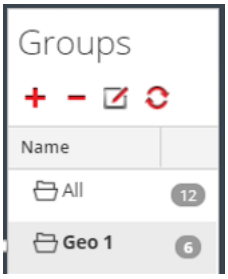
- Gruppieren Sie unterschiedliche Hosttypen, um alle Broker, Decoder oder Concentrators leichter konfigurieren und überwachen zu können.
- Gruppieren Sie Hosts, die Teil des gleichen Datenflusses sind, z. B. einen Broker und alle zugehörigen Concentrators und Decoder.
- Gruppieren Sie Hosts entsprechend ihrer geographischen Region und dem Standort in der Region. Wenn an einem Standort ein größerer Stromausfall auftritt, sind dann alle potenziell betroffenen Hosts leicht zu identifizieren.

Erstellen einer Gruppe

1. Wählen Sie **ADMIN** > **Hosts** aus.
   Die Ansicht „Hosts“ wird angezeigt.
2. Klicken Sie im Bereich **Gruppen** auf der Symbolleiste auf +.
   Ein Feld für die neue Gruppe wird mit blinkendem Cursor darin geöffnet.



3. Geben Sie den Namen der neuen Gruppe in das Feld ein (z. B. **Geo 1**) und drücken Sie die **Eingabetaste**.
   Die Gruppe wird als Ordner in der Struktur erstellt. Die Zahl neben der Gruppe gibt die Anzahl der Hosts in dieser Gruppe an.



Ändern des Namens einer Gruppe

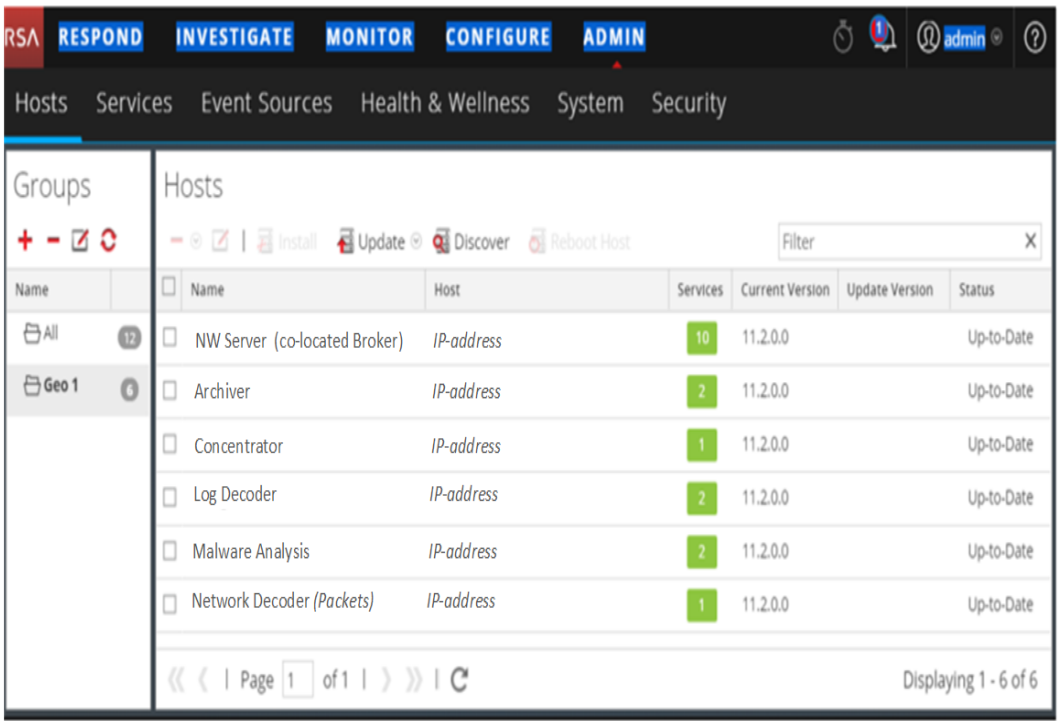
1. Klicken Sie in der Ansicht „Hosts“ im Bereich **Gruppen** doppelt auf den Gruppennamen oder wählen Sie die Gruppe aus und klicken Sie auf .
   Das Namensfeld wird mit blinkendem Cursor darin geöffnet.
2. Geben Sie den neuen Namen der Gruppe ein und drücken Sie die **Eingabetaste**.
   Das Namensfeld wird geschlossen und der neue Gruppenname wird in der Struktur angezeigt.

Hinzufügen eines Hosts zu einer Gruppe

Wählen Sie in der Ansicht „Hosts“ im Bereich **Hosts** einen Host aus und ziehen Sie den Host in einen Gruppenordner im Bereich „Gruppen“.
Der Host wird der Gruppe hinzugefügt.

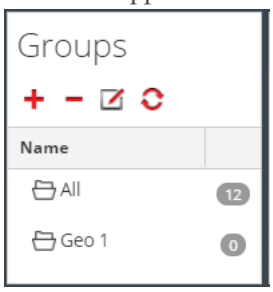
Anzeigen der Hosts in einer Gruppe

Klicken Sie zum Aufrufen der Hosts in einer Gruppe im Bereich **Gruppen** auf die Gruppe.
Im Bereich **Hosts** werden die Hosts in dieser Gruppe aufgelistet.



Entfernen eines Hosts aus einer Gruppe

1. Wählen Sie in der Ansicht „Hosts“ im Bereich **Gruppen** die Gruppe aus, die den zu entfernenden Host enthält. Die Hosts in dieser Gruppe werden im Bereich „Hosts“ angezeigt.
2. Wählen Sie im Bereich **Hosts** einen oder mehrere Hosts aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie dann auf der Symbolleiste > **Aus Gruppe entfernen** aus.
   Die ausgewählten Hosts werden aus der Gruppe entfernt, aber nicht von der NetWitness Platform-Benutzeroberfläche. Die Anzahl der Hosts in der Gruppe, die neben dem Gruppennamen angezeigt wird, verringert sich um die Anzahl der aus der Gruppe entfernten Hosts. Die Gruppe **Alle** enthält die Hosts, die aus der Gruppe entfernt wurden.
   Im folgenden Beispiel sind in der Hostgruppe namens **Geo 1** keine Hosts enthalten, da alle Hosts in dieser Gruppe entfernt wurden.



Löschen von Gruppen

1. Wählen Sie in der Ansicht „Hosts“ im Bereich **Gruppen** die Gruppe aus, die Sie löschen möchten.
2. Klicken Sie auf .
   Die ausgewählte Gruppe wird aus dem Bereich „Gruppen“ entfernt. Die Hosts, die sich in der Gruppe befanden, werden nicht von der NetWitness Platform-Benutzeroberfläche entfernt. Die Gruppe **Alle** enthält die Hosts der gelöschten Gruppe.

Suchen nach Hosts

Sie können über eine Liste mit Hosts in der Ansicht „Hosts“ nach Hosts suchen. Mithilfe der Ansicht „Hosts“ können Sie die Hostliste schnell nach Name und Host filtern. Sie können mehrere NetWitness Platform-Hosts für verschiedene Zwecke verwenden. Anstatt durch die Hostliste zu scrollen, können Sie diese einfach filtern, um die Hosts zu suchen, die Sie verwalten möchten.

In der Ansicht „Services“ können Sie nach einem Service suchen und den Host, der diesen Service ausführt, schnell finden.

Suchen eines Hosts

1. Wählen Sie **ADMIN** > **Hosts** aus.
2. Geben Sie in der Symbolleiste im **Bereich Hosts** im Feld **Filtern** einen **Namen** für den Host oder einen Hostnamen ein.

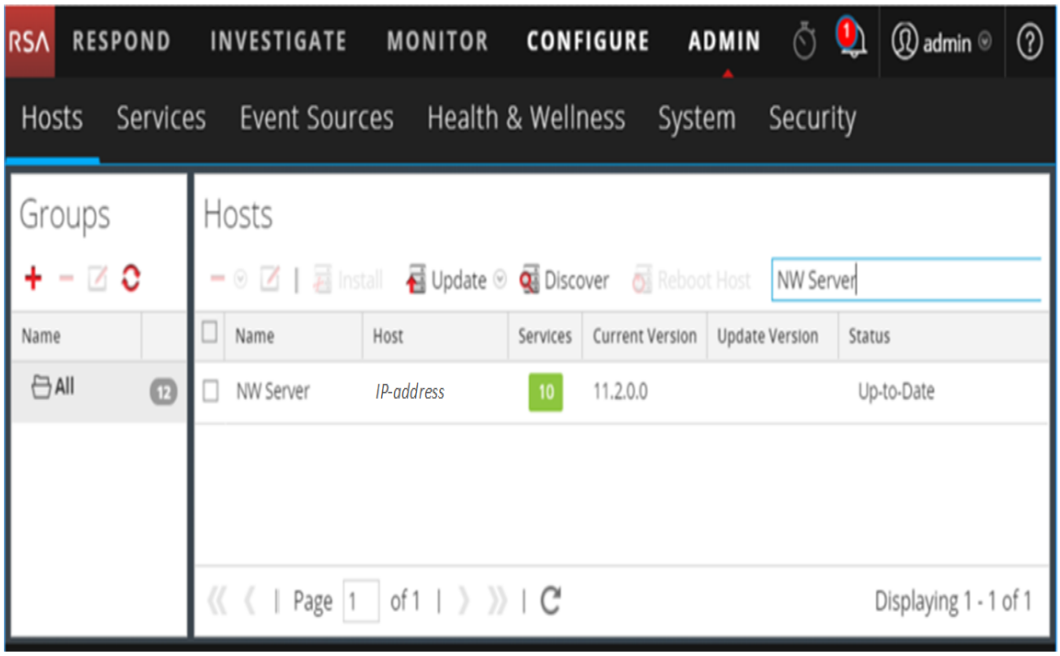
   

   Im Bereich „Hosts“ werden die Hosts aufgelistet, die mit den ins Feld „Filter“ eingegebenen Namen übereinstimmen.

Suchen des Hosts, der einen Service ausführt

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie in der Ansicht „Services“ einen Service aus. Der zugeordnete Host wird in der Spalte **Host** für diesen Service aufgelistet.
3. Klicken Sie zum Verwalten des Hosts in der Ansicht „Hosts“ auf den Link in der Spalte **Host** zu diesen Service. Der dem ausgewählten Service zugeordnete Host wird in der Ansicht „Hosts“

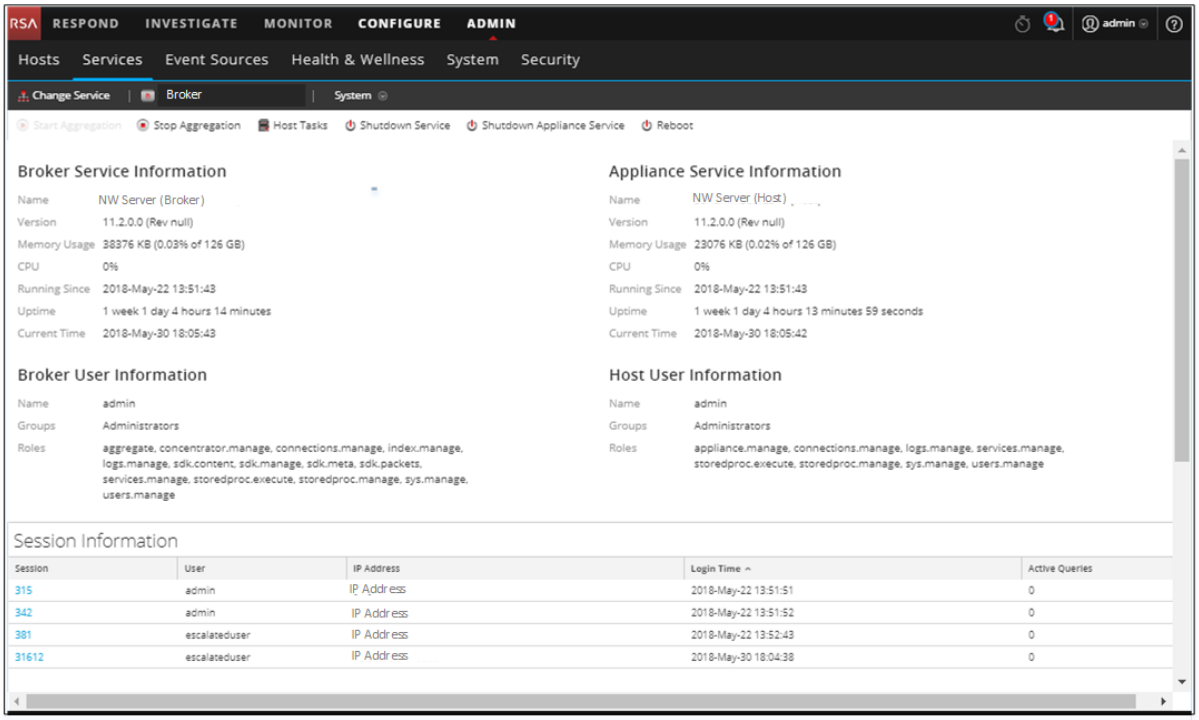
angezeigt.



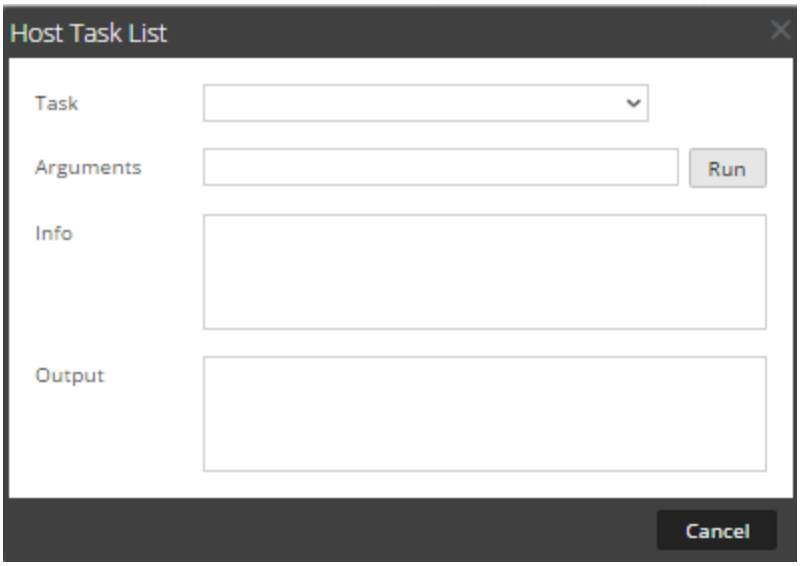
Ausführen einer Aufgabe aus der Hostaufgabenliste

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht > System**.

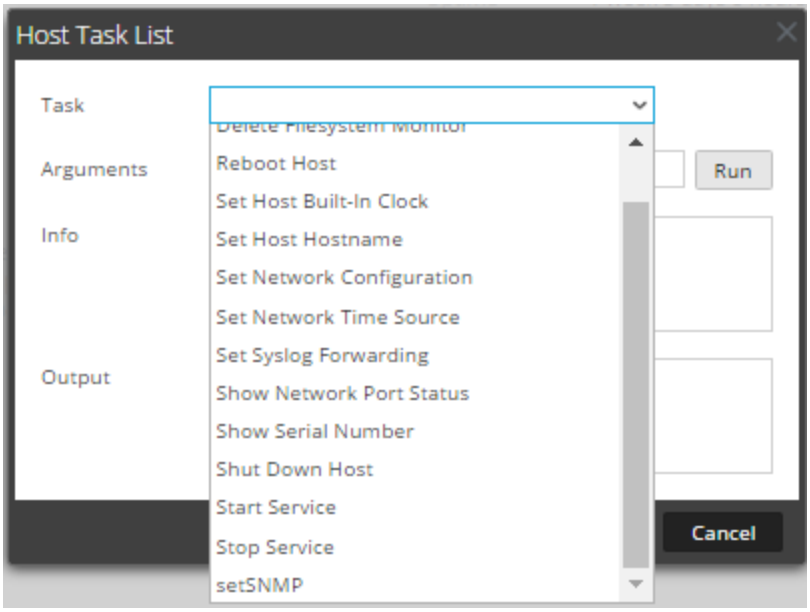
Hinweis: Die Services „Admin“, Konfigurieren“, „Orchestrieren“, „Sicherheit“, „Untersuchen“ und „Reagieren“ haben Zugriff auf die Ansicht „System“. Sie haben nur Zugriff auf die Ansicht „Durchsuchen“.
Die Ansicht System für den Service wird angezeigt.



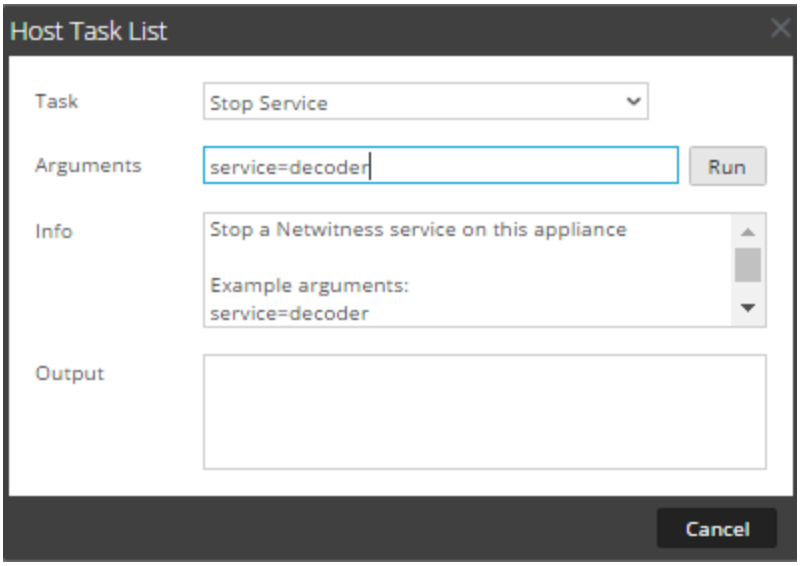
3. Klicken Sie in der Symbolleiste der Ansicht **Services-System** auf Host Tasks .



4. Klicken Sie in der **Hostaufgabenliste** auf das Feld **Aufgabe**, um eine Drop-down-Liste der auf dem Host ausgeführten Aufgaben anzuzeigen.



5. Wählen Sie eine Aufgabe aus und klicken Sie zum Beispiel auf **Service anhalten**.
   Die Aufgabe wird im Feld **Aufgabe** angezeigt und die Aufgabenbeschreibung, Beispielargumente, Sicherheitsrollen und Parameter werden im Bereich **Info** angezeigt.



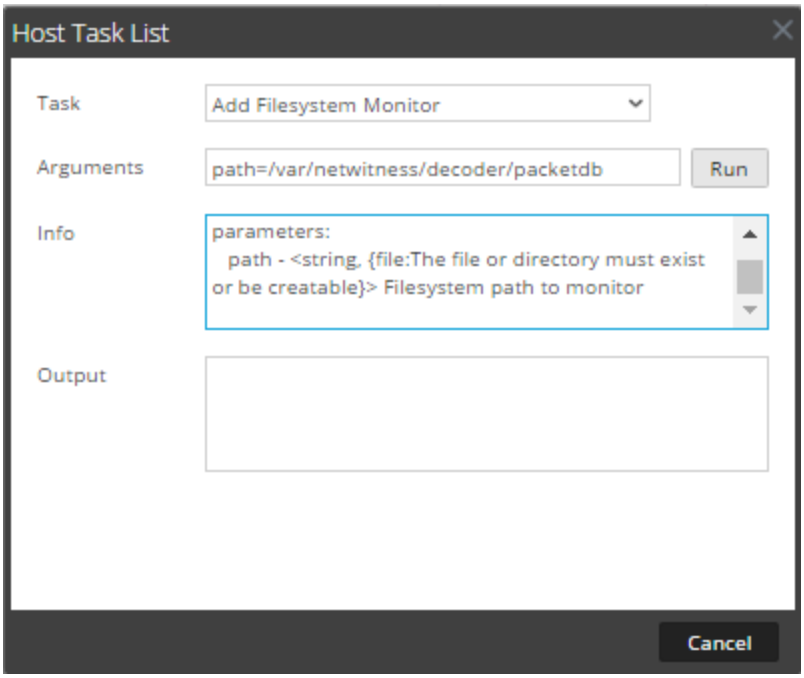
6. Geben Sie, falls erforderlich, Argumente ein und klicken Sie auf **Ausführen**.
   Der Befehl wird ausgeführt und das Ergebnis wird im Abschnitt **Ausgabe** angezeigt.

Hinzufügen und Löschen einer Dateisystemüberwachung

Wenn ein Service Datenverkehr für ein bestimmtes Dateisystem überwachen soll, können Sie den Service auswählen und anschließend den Pfad angeben. NetWitness Platform fügt eine Dateisystemüberwachung hinzu. Sobald einem Service eine Dateisystemüberwachung hinzugefügt wurde, setzt der Service die Überwachung des Datenverkehrs für diesen Pfad solang fort, bis die Dateisystemüberwachung gelöscht wird.

Konfigurieren der Dateisystemüberwachung

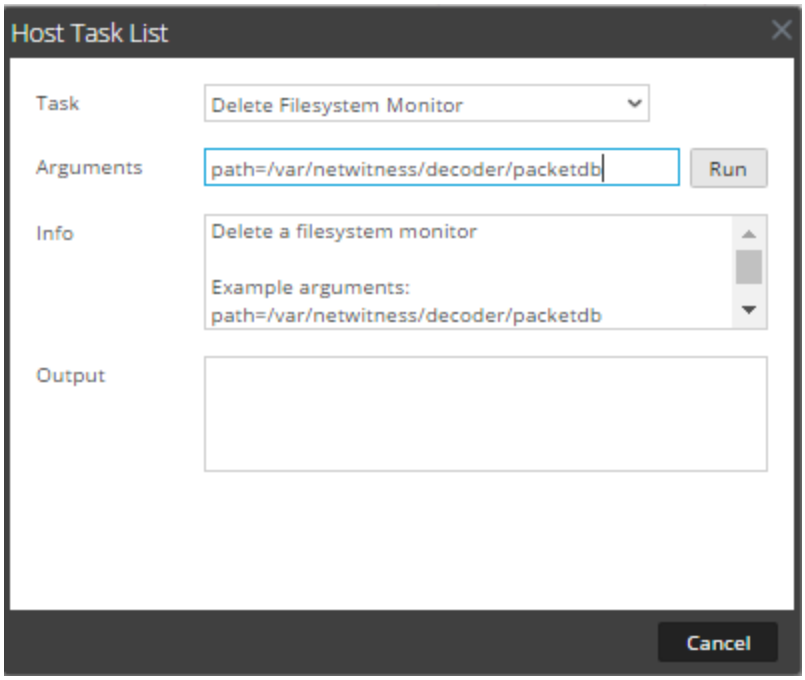
1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht > System**. Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste** die Option **Dateisystemüberwachung hinzufügen** aus. Im Bereich **Info** wird eine kurze Erläuterung der Aufgabe und der Aufgabenargumente angezeigt.
5. Geben Sie im Feld **Argumente** den Pfad ein, um das zu überwachende Dateisystem zu identifizieren. Beispiel:
   path=/var/netwitness/decoder/packetdb



6. Klicken Sie auf **Run**.
   Das Ergebnis wird im Bereich **Ausgabe** angezeigt. Der Service beginnt mit der Überwachung des Dateisystems und setzt diese Überwachung solange fort, bis Sie die Dateisystemüberwachung löschen.

Löschen einer Dateisystemüberwachung

1. Navigieren Sie zum Dialogfeld **Hostaufgabenliste**.
2. Wählen Sie in der **Hostaufgabenliste** die Option **Dateisystemüberwachung löschen** aus.
   Im Bereich **Info** wird eine kurze Erläuterung der Aufgabe und der Aufgabenargumente angezeigt.
3. Geben Sie im Feld **Argumente** den Pfad ein, um das Dateisystem zu identifizieren, dessen Überwachung angehalten werden soll. Beispiel:
   path=/var/netwitness/decoder/packetdb



4. Klicken Sie auf **Run**.
   Das Ergebnis wird im Bereich **Ausgabe** angezeigt. Der Service beendet die Überwachung des Dateisystems.

Neustarten eines Hosts

Unter bestimmten Bedingungen ist ein Neustart des Hosts notwendig, zum Beispiel nach der Installation eines Softwareupgrades. Bei diesem Vorgang wird eine Meldung in der Hostaufgabenliste angezeigt, bei der Sie aufgefordert werden, den Host herunterzufahren und neu zu starten.

NetWitness Platform bietet auch andere Optionen zum Herunterfahren eines Hosts:

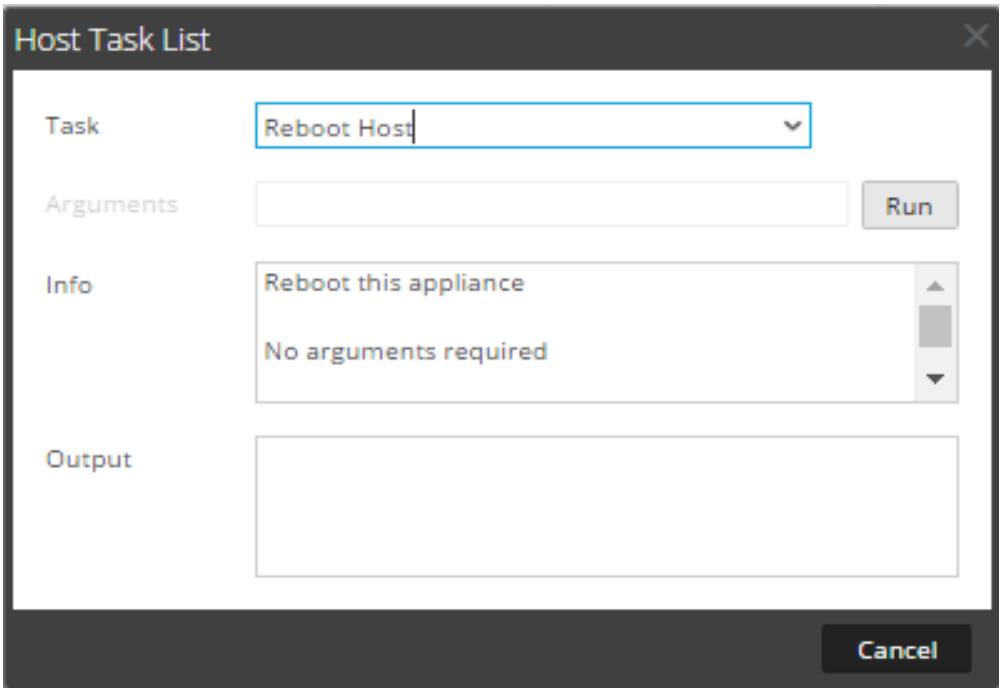
- Zum Herunterfahren und erneuten Starten eines Hosts über einen verknüpften Service gehen Sie zur Ansicht „Hosts“ von einem Service in der Ansicht „Services“ aus (siehe Suchen nach Hosts) und befolgen Sie dann das unten angegebene Verfahren *Herunterfahren und Neustart eines Hosts über die Ansicht „Hosts“*.
- Weitere Informationen zum Herunterfahren des physischen Hosts, ohne diesen neu zu starten, finden Sie unter Herunterfahren des Hosts.

Fahren Sie einen Host über die Ansicht Hosts herunter und starten Sie diesen neu.

1. Wählen Sie **ADMIN > Hosts** aus.
2. Wählen Sie im Bereich **Hosts** einen Host aus.
3. Wählen Sie in der Symbolleiste Reboot Host aus.

Herunterfahren und Neustart eines Hosts aus der Hostaufgabenliste

1. Wählen Sie **ADMINISTRATION** > **Services** aus.
2. Wählen Sie im Bereich **Services** einen Service aus und klicken Sie auf > **Ansicht > System**.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste** die Option **Host neu starten** im Feld **Aufgabe** aus.
   Es sind keine Argumente erforderlich.



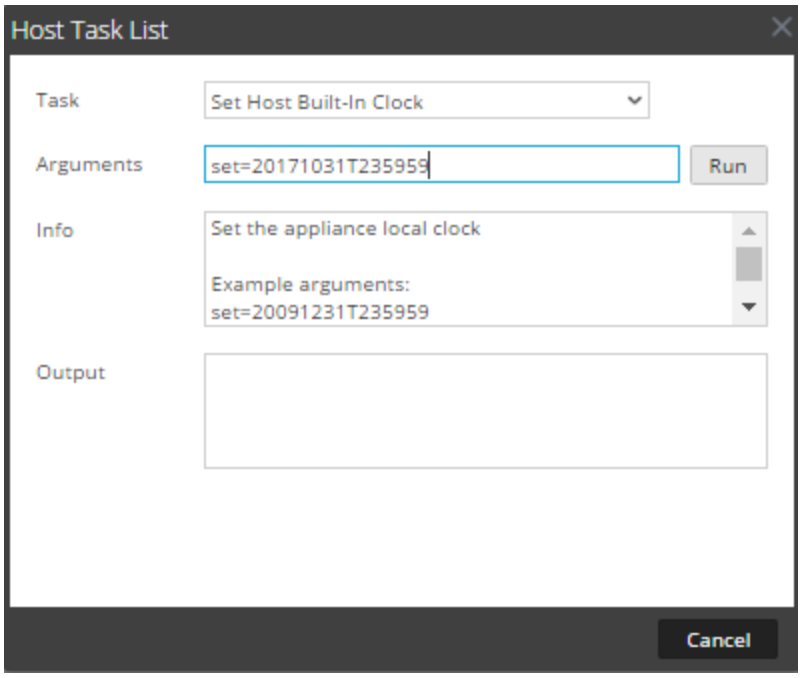
5. Klicken Sie auf **Run**.
   Der Host wird neu gestartet und das Ergebnis wird im Bereich **Ausgabe** angezeigt.

Einstellen der internen Uhr des Hosts

Nach einer Abschaltung oder einem Batterieausfall müssen Sie möglicherweise die lokale Uhr eines Hosts neu stellen. Mit der Aufgabe „Interne Uhr des Hosts einstellen“ wird die Uhrzeit zurückgesetzt.

Einstellen der Zeit der lokalen Uhr

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service und anschließend > **Ansicht > System** aus.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste** die Option **Interne Uhr des Hosts einstellen** aus. Hilfe zur Aufgabe wird im Bereich **Info** angezeigt.
5. Geben Sie die Argumente für Datum und Uhrzeit im Feld **Argumente** ein. Geben Sie beispielsweise für das Datum 31. Oktober 2017 und die Uhrzeit 23:59:59 Folgendes ein:
   set=20171031T235959



6. Klicken Sie auf **Run**.
   Die Uhrzeit wird auf die angegebene Zeit eingestellt und im Bereich **Ausgabe** eine Meldung angezeigt.

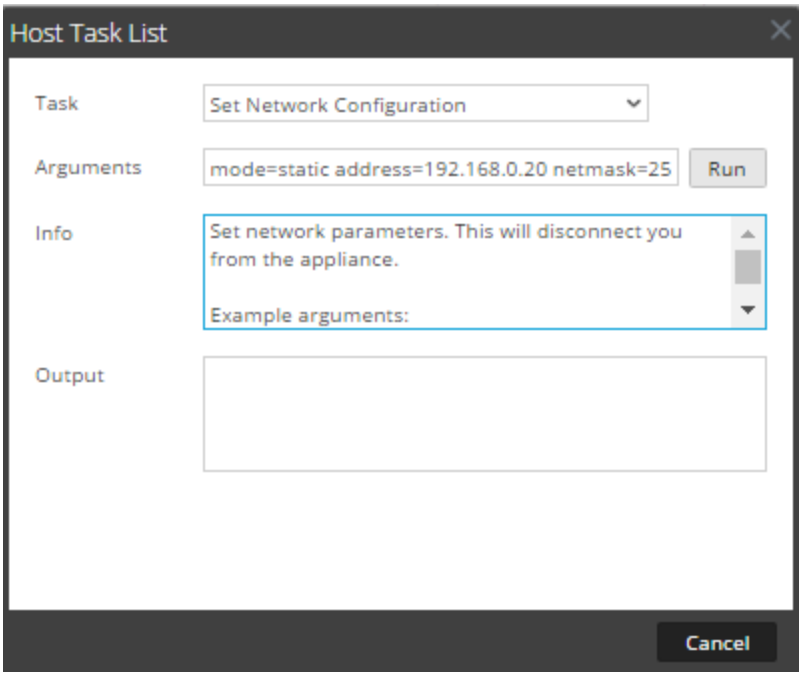
Festlegen der Netzwerkkonfiguration

Wenn bei einem konfigurierten Core-Host die Adresse geändert werden muss, können Sie über die Meldung **Netzwerkkonfiguration festlegen** in der **Hostaufgabenliste** Host eine neue Netzwerkadresse, eine neue Subnetzmaske und ein neues Gateway für den Host festlegen.

Achtung: Die Änderung tritt sofort in Kraft und der Host wird von NetWitness Platform getrennt. Fügen Sie den Host dann mit der neuen Netzwerkadresse NetWitness Platform wieder hinzufügen.

Angeben der Netzwerkadresse für einen Host

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht** > **System**.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Klicken Sie in der **Hostaufgabenliste** auf die Option **Netzwerkkonfiguration festlegen**.
   Die Aufgabe wird im Feld **Aufgabe** angezeigt und die Hilfe im Bereich **Info**.
5. Geben Sie die Argumente in das Feld **Argumente** ein. Beispiel:
   mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1



6. Klicken Sie auf **Ausführen**.
   Die Aufgabe wird ausgeführt und das Ergebnis im Bereich **Ausgabe** angezeigt. Der Host ist von NetWitness Platform getrennt. Fügen Sie den Host dann mit der neuen Adresse wieder hinzu.

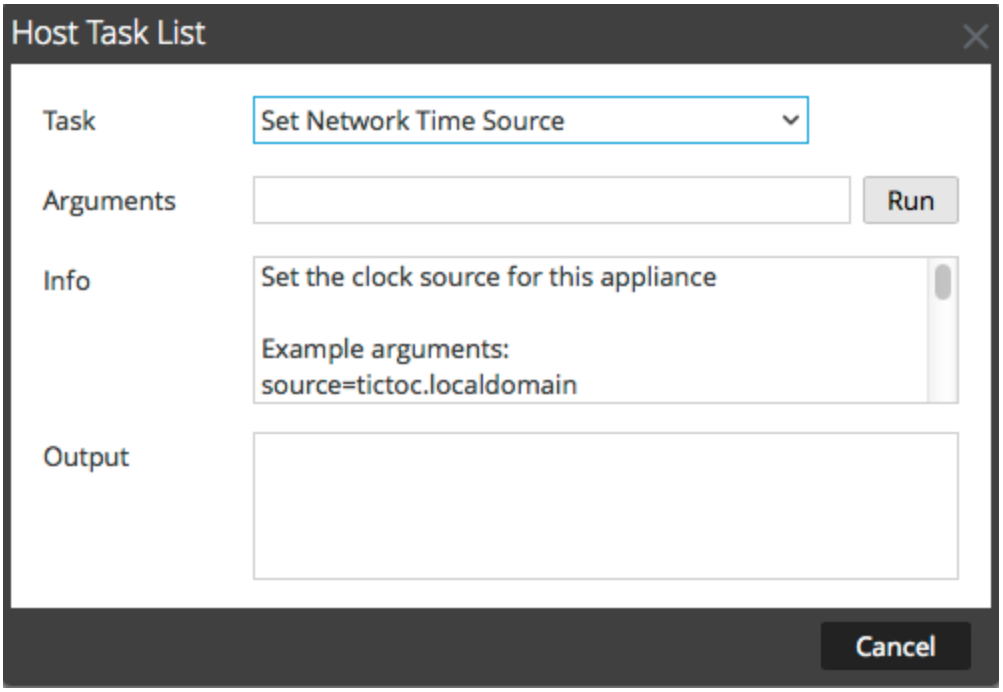
Hinweis: Wenn es sich beim Modus um DHCP handelt, ist es möglicherweise nicht möglich, die neue Adresse zu bestimmen. Um die neue Adresse zu ermitteln, müssen Sie möglicherweise eine direkte Verbindung zum Host herstellen.

Festlegen der Quelle für die Netzwerkzeit

Beim Einrichten der Uhrzeitquelle für einen Host geben Sie den Hostnamen oder die Adresse eines NTP-Servers an, der als Netzwerkuhrzeitquelle für den Host dienen soll. Verwendet der Host eine lokale Uhrzeitquelle, müssen Sie hier **Lokal** angeben, damit **Lokale Zeitquelle einrichten** aktiviert wird.

Angeben der Netzwerkzeitquelle

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht > System**.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste** die Option **Quelle für die Netzwerkzeit festlegen** aus.



5. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie den Hostnamen oder die Adresse des NTP-Servers an, der als Uhrzeitquelle für diesen Host dienen soll, z. B. **source=tictoc.localdomain.**
   - Wenn Sie die Hostzeit als Uhrzeitquelle verwenden möchten, geben Sie Folgendes ein: **source=local**
6. Klicken Sie auf **Run**.
   Die Uhrzeitquelle wird festgelegt und eine Meldung wird im Bereich **Ausgabe** angezeigt.

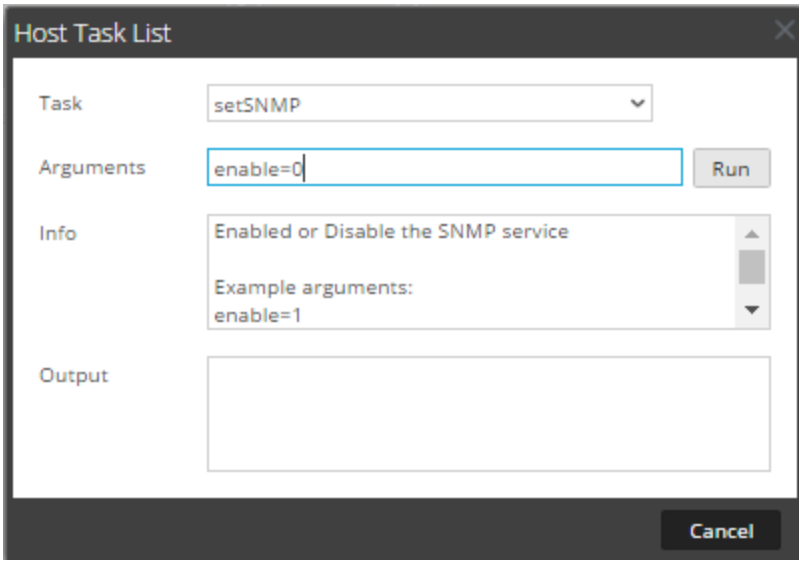
Hinweis: Wenn Sie als NTP-Uhrzeitquelle **Lokal** angegeben haben, dient die Hostzeit als Uhrzeitquelle und die Zeit wird unter Interne Uhr des Hosts einstellen konfiguriert.

Festlegen des SNMP

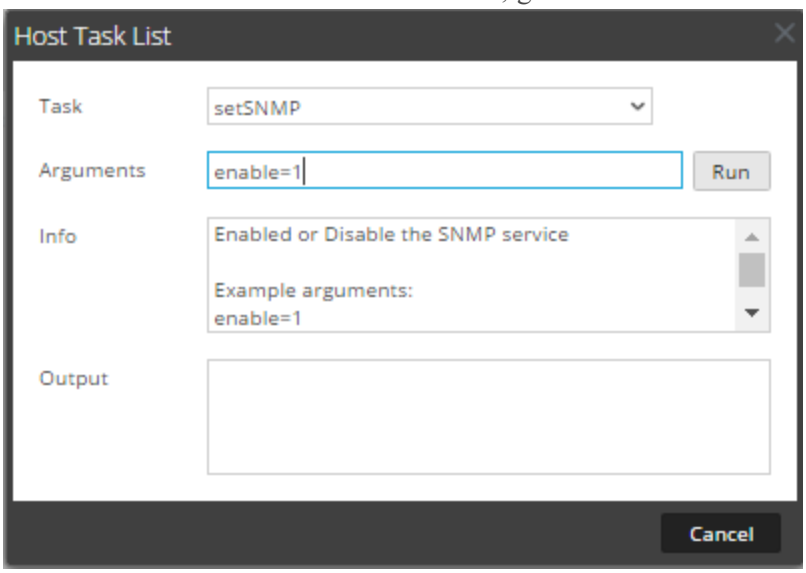
Mit „SNMP festlegen“ in der Hostaufgabenliste wird der SNMP-Service auf einem Host aktiviert oder deaktiviert. Der SNMP-Service muss aktiviert werden, damit ein Host SNMP-Benachrichtigungen erhalten kann. Wenn Sie SNMP nicht für NetWitness Platform-Benachrichtigungen verwenden, ist es nicht erforderlich, diesen Service zu aktivieren.

Wechseln des SNMP-Services auf dem Host

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht > System**.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste** die Option **setSNMP** aus.
   Im Bereich **Info** wird eine kurze Erläuterung der Aufgabe und der Aufgabenargumente angezeigt.
5. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den Service deaktivieren möchten, geben Sie **enable=0** im Feld **Argumente** ein.



- Wenn Sie den Service aktivieren möchten, geben Sie **enable=1** im Feld **Argumente** ein.



6. Klicken Sie auf **Run**.
   Das Ergebnis wird im Bereich **Ausgabe** angezeigt.

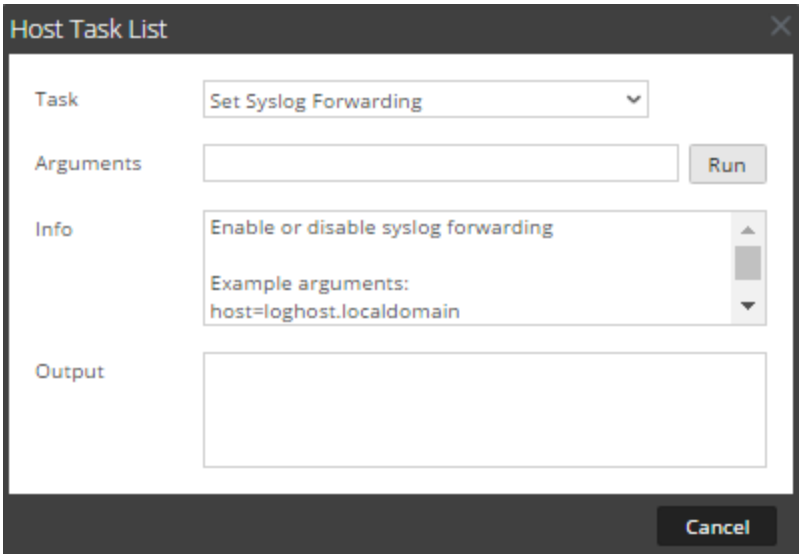
Einrichten der Syslog-Weiterleitung

Sie können die Syslog-Weiterleitung so konfigurieren, dass die Betriebssystemprotokolle Ihrer NetWitness Platform-Hosts an einen Remote-Syslog-Server weitergeleitet werden. Sie können die Aufgabe „Syslog-Weiterleitung einrichten“ in der Hostaufgabenliste verwenden, um die Syslog-Weiterleitung zu aktivieren oder zu deaktivieren.

Einrichten und Starten der Syslog-Weiterleitung

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf  **> Ansicht > System**.
   Die Ansicht „System“ für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.

4. Wählen Sie in der **Hostaufgabenliste** die Option **Syslog-Weiterleitung einrichten** aus.
   Im Bereich **Info** wird eine kurze Erläuterung der Aufgabe und der Aufgabenargumente angezeigt.



5. Führen Sie im Feld **Argumente** einen der folgenden Schritte aus:
   - Geben Sie eines der folgenden Formate an, um die Syslog-Weiterleitung zu aktivieren:
     - **host=<loghost>.<localdomain>** (for example, host=syslogserver.local).
     - **host=<loghost>.<localdomain>:<port>** (for example, host=syslogserver.local:514).
     - **host=<IP>** (for example, host=10.31.244.244).
     - **host=<IP>:<port>** (for example, host=10.31.244.244:514).
       In der folgenden Tabelle sind die Parameter zum Aktivieren der Syslog-Weiterleitung aufgeführt.

Parameter	Beschreibung
loghost	Der Hostname des Remote-Syslog-Servers.
localdomain	Die Domain des Remote-Syslog-Servers.
port	IP-Adresse des Remote-Syslog-Servers.
IP	Die Nummer des Ports, auf dem der Remote-Syslog-Server Syslog-Nachrichten erhält.

   - Geben Sie **host=disable** ein, um die Syslog-Weiterleitung zu deaktivieren.

6. Klicken Sie auf **Ausführen**.
   Das Ergebnis wird im Bereich **Ausgabe** angezeigt.

Sobald die Syslog-Weiterleitung aktiviert oder deaktiviert ist, wird die Datei `/etc/rsyslog.conf` automatisch aktualisiert, sodass die Syslog-Weiterleitung auf das Remote-Syslog-Ziel aktiviert oder deaktiviert wird und der Syslog-Service erneut gestartet wird.

Wenn Sie die Syslog-Weiterleitung aktivieren, werden die Protokolle aus dem konfigurierten Service solange an den definierten Syslog-Server weitergeleitet, bis die Weiterleitung deaktiviert wird.

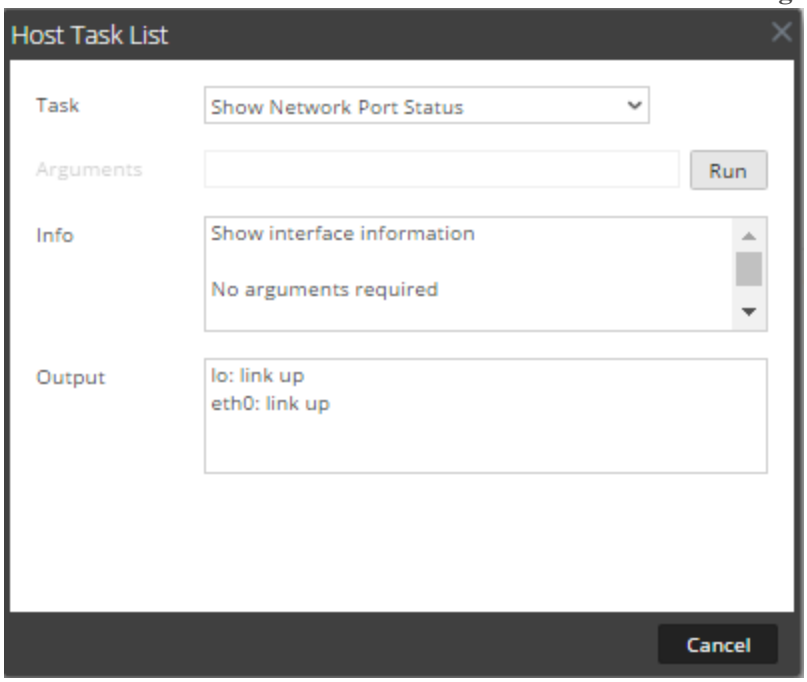
Hinweis: Sie können sich jetzt beim Remote-Syslog-Server anmelden und überprüfen, ob die Nachrichten von den NetWitness Platform-Services empfangen werden, die für die Syslog-Weiterleitung konfiguriert sind.

Anzeigen des Netzwerkportstatus

Die Aufgabe „Netzwerkportstatus anzeigen“ in der Hostaufgabenliste gibt den Status aller in dem Host konfigurierten Ports zurück.

Anzeigen des Netzwerkportstatus

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service und > **Ansicht > System** aus.
   Die Ansicht „System“ für den ausgewählten Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Klicken Sie in der **Hostaufgabenliste auf** Netzwerkportstatus anzeigen.
   Die Aufgabe wird im Feld **Aufgabe** und Informationen über die Aufgabe werden im Bereich **Info** angezeigt.
5. Um die Aufgabe auszuführen, klicken Sie auf **Ausführen**.
   Der Status der einzelnen Ports in dem Host wird im Bereich **Ausgabe** angezeigt.

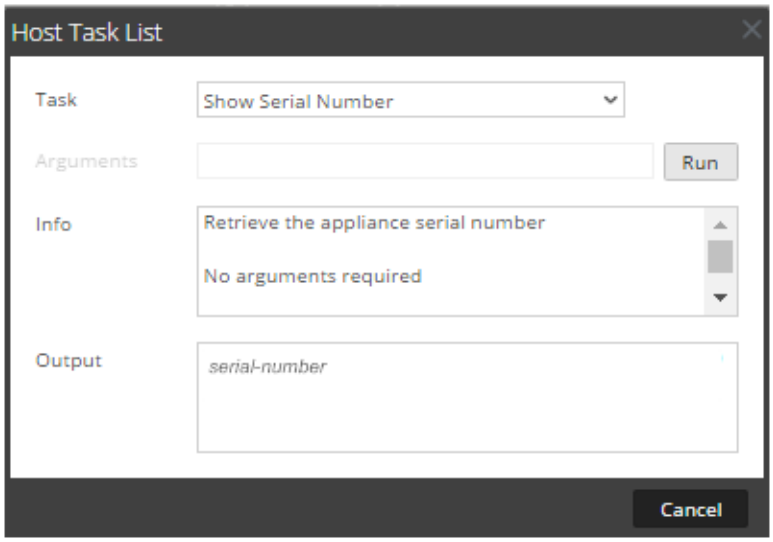


Anzeigen der Seriennummer

Die Aufgabe Seriennummer anzeigen in der Hostaufgabenliste zeigt die Seriennummer eines Hosts an.

Anzeigen der Seriennummer

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht > System**. Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Wählen Sie in der **Hostaufgabenliste die Option** Seriennummer anzeigen aus.Im Bereich **Info** wird eine kurze Erläuterung der Aufgabe und der Aufgabenargumente angezeigt.
5. Für diese Aufgabe sind keine Argumente erforderlich. Klicken Sie auf **Run**. Die Seriennummer des ausgewählten Hosts wird im Bereich **Ausgabe** angezeigt.



Herunterfahren des Hosts

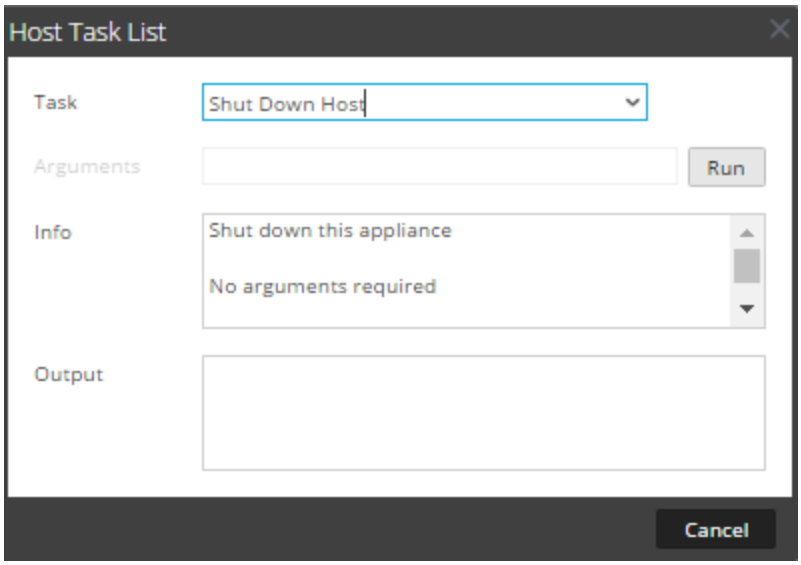
Unter bestimmten Bedingungen, z. B. bei einem Hardwareupgrade oder einem längeren Stromausfall, der die Reservestromkapazität übersteigt, kann es notwendig werden, einen physischen Host herunterzufahren. Beim Herunterfahren eines Hosts werden alle darauf ausgeführten Services beendet und der physische Host wird abgeschaltet.

Der physische Host wird nicht automatisch gestartet. Verwenden Sie den Netzschalter, um den Host neu zu starten. Nachdem der physische Host neu gestartet wurde, werden der Host und die Services so konfiguriert, dass sie automatisch neu gestartet werden.

Starten Sie einen Host neu, um einen Host anzuhalten und zu starten, ohne den Host herunterzufahren.

Herunterfahren des Hosts

1. Wählen Sie im Dialogfeld „Hostaufgabenliste“ im Feld **Aufgabe** die Option **Host herunterfahren** aus.



2. Um die Aufgabe auszuführen, klicken Sie auf **Ausführen**.
   Der Host wird heruntergefahren und ausgeschaltet.

Beenden und Starten eines Services auf einem Host

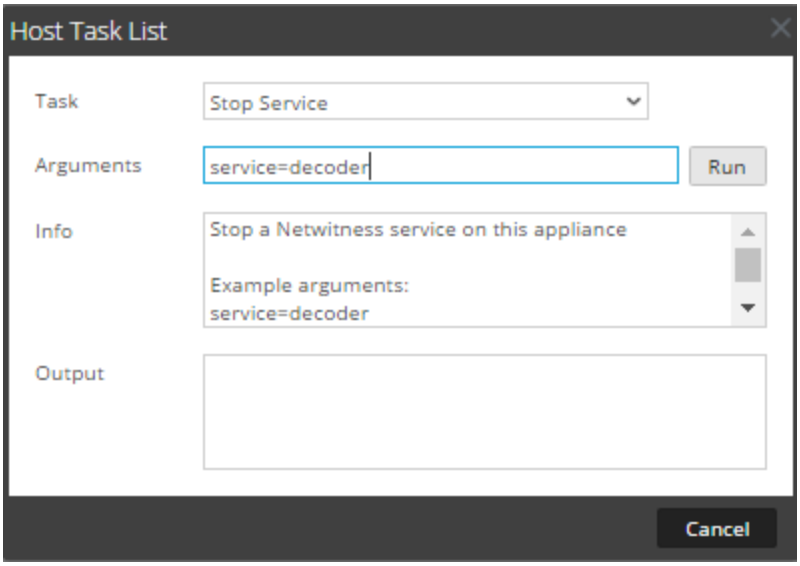
Die Hostaufgabenliste umfasst zwei Optionen zum Beenden und Starten eines Services auf einem Host. Wenn Sie einen Service mithilfe der Aufgabe **Service anhalten** beenden, werden alle Prozesse des Services beendet und mit diesem Service verbundene Benutzer werden getrennt. Wenn es kein Problem mit dem Service gibt, startet er automatisch neu. Dies entspricht der Option **Service herunterfahren** in der Ansicht „Services-System“.

Wenn ein Service nach dem Beenden nicht automatisch neu gestartet wird, können Sie ihn mithilfe der Aufgabe **Service starten** manuell neu starten.

Beenden eines Services auf einem Host

1. Wählen Sie **ADMINISTRATION** > **Services** aus.
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf > **Ansicht** > **System**.
   Die Ansicht System für den Service wird angezeigt.
3. Klicken Sie in der Symbolleiste der Ansicht **Services > System** auf **Hostaufgaben**.
4. Klicken Sie in der **Hostaufgabenliste** auf **Service anhalten**.
   Die Aufgabe wird im Feld **Aufgabe** und Informationen über die Aufgabe werden im Bereich **Info** angezeigt.

5. Geben Sie den Service (`decoder`, `concentrator broker`, `logdecoder`, `logcollector`) an, der im Feld **Argumente** beendet werden soll, z. B. **service=decoder**.

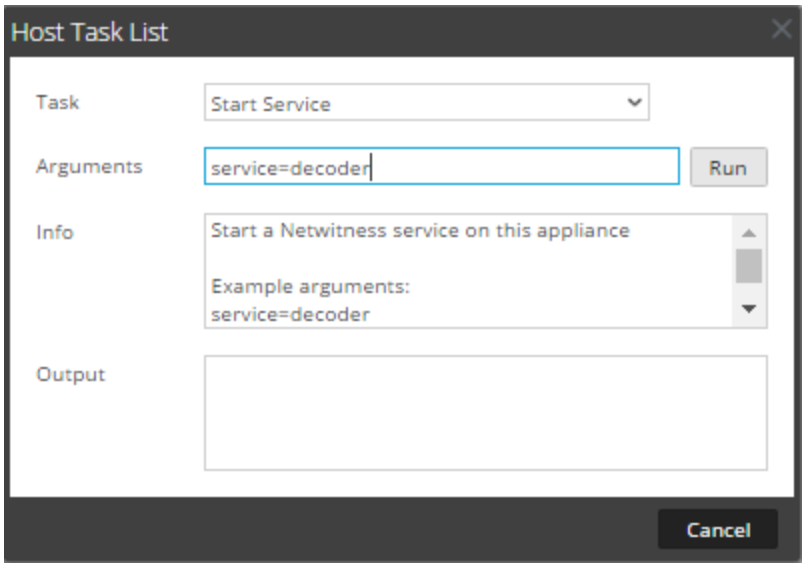


6. Um die Aufgabe auszuführen, klicken Sie auf **Ausführen**.
   Der Service wird beendet und der Status wird im Bereich **Ausgabe** angezeigt. Alle Prozesse des Services werden beendet und mit dem Service verbundene Benutzer werden getrennt. Wenn es kein Problem mit dem Service gibt, startet er automatisch neu.

Starten eines Services auf einem Host

1. Wählen Sie in der **Hostaufgabenliste** im Drop-down-Menü „Aufgabe“ die Option **Service starten** aus.
   Die Aufgabe wird im Feld **Aufgabe** und Informationen über die Aufgabe werden im Bereich **Info** angezeigt.
2. Geben Sie den zu startenden Service (decoder, concentrator, broker, logdecoder, logcollector) im Feld **Argumente** an, z. B.

service=decoder.



3. Um die Aufgabe auszuführen, klicken Sie auf **Ausführen**.
   Der Service wird gestartet und der Status wird im Bereich **Ausgabe** angezeigt.

Hinzufügen, Replizieren oder Löschen eines Servicenutzers

Für folgende Aufgaben müssen Sie einem Service einen Benutzer hinzufügen:

- Aggregation
- Zugriff auf den Service mit dem:
  - Thick-Client
  - REST-API

Hinweis: Dieses Thema gilt nicht für Benutzer, die über die Benutzeroberfläche auf NetWitness Server auf Services zugreifen. Diese Benutzer müssen Sie dem System hinzufügen, nicht einem Service. Weitere Informationen finden Sie im Thema **Einrichten eines Benutzers** unter *Systemsicherheit und Benutzerverwaltung*.

Für jeden Servicebenutzer können Sie:

- die Benutzerauthentifizierung und die Abfrageverarbeitungseigenschaften für den Service konfigurieren
- den Benutzer als Mitglied einer Rolle festlegen, die über einen Satz an Berechtigungen verfügt, die der Benutzer erhält
- das Benutzerkonto auf anderen Services replizieren
- das Servicebenutzerpasswort auf ausgewählten Services ändern

Ändern eines Servicebenutzerpassworts bietet Anweisungen für das Ändern von Servicebenutzerpasswörtern über Services hinweg.

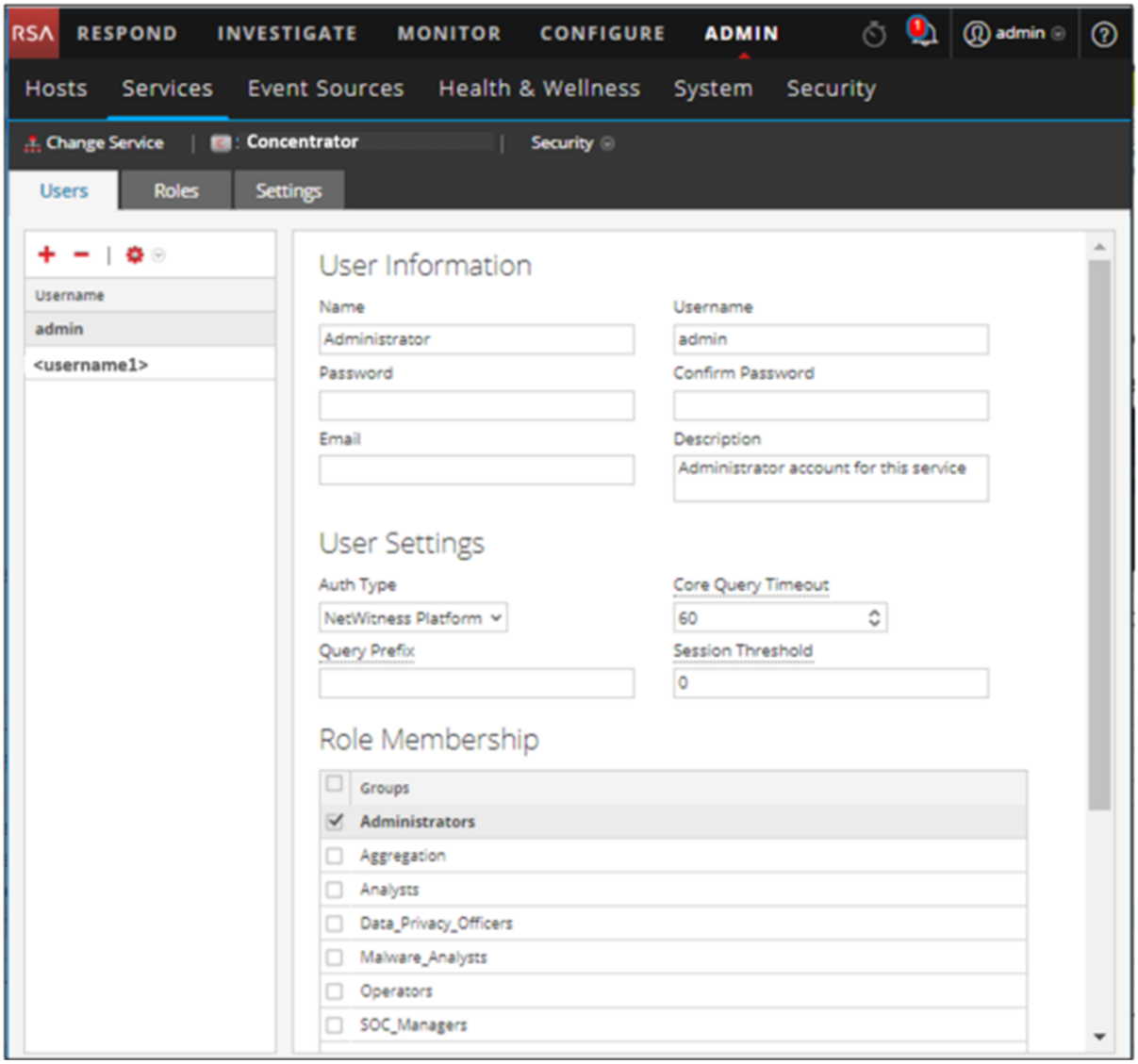
Methoden

ZUGREIFEN AUF DIE ANSICHT „SICHERHEIT“

Jedes der folgenden Verfahren startet in der Ansicht Services-Sicherheit.

So navigieren Sie zur Ansicht Services-Sicherheit:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie einen Service und anschließend  **> Ansicht > Sicherheit** aus.
   Die Ansicht „Sicherheit“ für den ausgewählten Service wird mit geöffneter Registerkarte „Benutzer“ angezeigt.



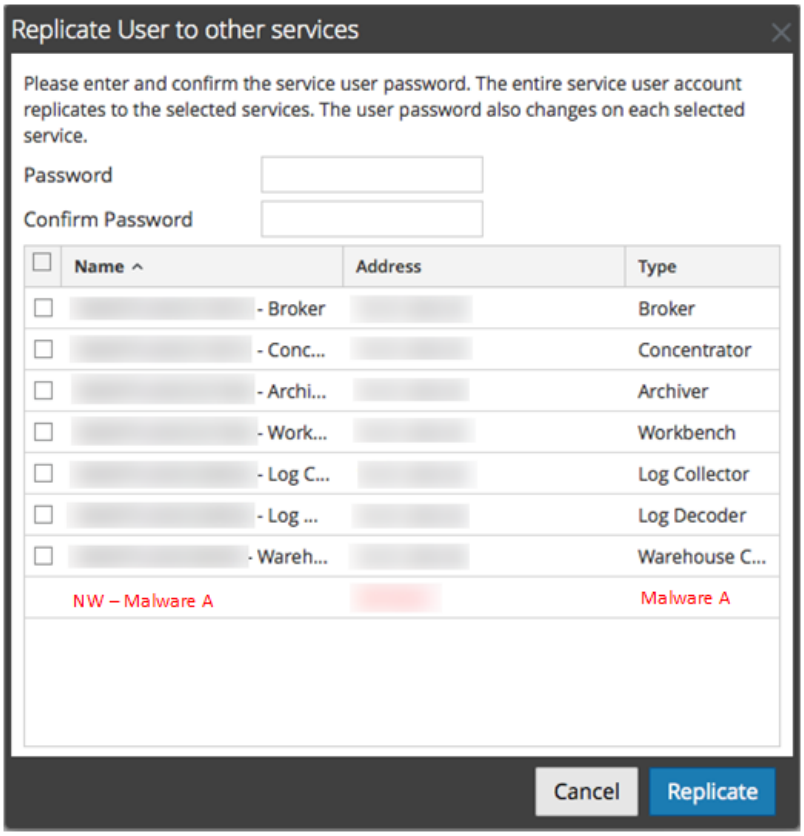
Hinweis: Für NetWitness Platform 10.4 und frühere Serviceversionen wird im Abschnitt „Benutzereinstellungen“ das Feld **Abfrageebene** anstatt **Core-Abfragetimeout** angezeigt.

HINZUFÜGEN EINES SERVICEBENUTZERS

1. Klicken Sie auf der Registerkarte **Nutzer** auf +.
2. Geben Sie den Nutzernamen für den Zugriff auf den Service an und drücken Sie dann die **Eingabetaste**.
   Im Abschnitt „Nutzerinformationen“ wird der Nutzername angezeigt, und die übrigen Felder sind zur Bearbeitung verfügbar.
3. Geben Sie das Passwort zur Anmeldung beim Service in den Feldern **Passwort** und **Passwort bestätigen** an.
4. (Optional) Geben Sie zusätzliche Informationen an:
   - **Name** für die Anmeldung bei NetWitness Platform
   - **E-Mail**-Adresse
   - **Beschreibung** des Benutzers
5. Wählen Sie im Abschnitt „Benutzereinstellungen“ die folgenden Informationen aus:
   - **Authentifizierungstyp**
     - Wenn NetWitness Platform den Nutzer authentifiziert, wählen Sie „NetWitness“ aus.
     - Wenn Active Directory oder PAM auf NetWitness Server zur Authentifizierung des Benutzers konfiguriert ist, wählen Sie „Extern“ aus.
   - **Core-Abfragetimeout für Abfrage** ist die maximale Anzahl Minuten, die ein Nutzer eine Abfrage auf dem Service ausführen kann. Dieses Feld gilt für NetWitness Platform 10.5 und spätere Serviceversionen und wird nicht in 10.4 und früheren Versionen angezeigt.
6. (Optional) Geben Sie zusätzliche Abfragekriterien an:
   - **Abfragepräfix** filtert Abfragen. Geben Sie ein Präfix ein, um die Ergebnisse zu beschränken, die der Benutzer sieht.
   - **Sitzungsschwellenwert** steuert, wie der Service Metawerte scannt, um die Sitzungsanzahl festzustellen. Ein Metawert mit einer Sitzungsanzahl über dem Schwellenwert stoppt die Feststellung der wirklichen Sitzungsanzahl.
7. Wählen Sie im Abschnitt **Rollenmitgliedschaft** nacheinander alle Rollen aus, die Sie dem Benutzer zuweisen möchten. Wenn ein Benutzer ein Mitglied einer Rolle bei einem Service ist, hat der Benutzer die Berechtigungen, die der Rolle zugewiesen wurden.
8. Klicken Sie zum Aktivieren des neuen Servicebenutzers auf **Anwenden**.

REPLIZIEREN EINES BENUTZERS NACH ANDEREN SERVICES

1. Wählen Sie in der Registerkarte „Benutzer“ einen Benutzer aus und klicken Sie auf ⚙ > **Replizieren**.
   Das Dialogfeld „Benutzer nach anderen Services replizieren“ wird angezeigt.



2. Geben Sie das Passwort ein, und bestätigen Sie es.
3. Wählen Sie nacheinander alle Services aus, nach denen Sie den Benutzer replizieren.
4. Klicken Sie auf **Replizieren**.

LÖSCHEN EINES SERVICEBENUTZERS

1. Wählen Sie in der Registerkarte **Benutzer** den **Benutzernamen** aus und klicken Sie auf −. NetWitness Platform fordert Sie auf, zu bestätigen, dass Sie die ausgewählten Benutzer löschen möchten..
2. Klicken Sie zur Bestätigung auf **Ja**.

Hinzufügen einer Servicebenutzerrolle

In NetWitness Platform gibt es vorkonfigurierte Rollen, die auf dem Server und jedem Service installiert werden. Sie können auch benutzerdefinierte Rollen hinzufügen. In der folgenden Tabelle sind die vorkonfigurierten Systemrollen und ihre Berechtigungen aufgelistet.

Rolle	Berechtigung
Administratoren	Voller Systemzugriff
Operatoren	Zugriff auf die Konfigurationen, aber nicht auf Meta- und Sitzungsinhalte

Rolle	Berechtigung
Analysten	Zugriff auf Meta- und Sitzungsinhalte, aber nicht auf Konfigurationen
SOC_Managers	Gleicher Zugriff wie Analysten und zusätzliche Berechtigungen für das Verarbeiten von Incidents
Malware_ Analysts	Zugriff auf Schadsoftwareereignisse und Meta- sowie Sitzungsinhalt
Data_Privacy_ Officers	Zugriff auf Metadaten und Sitzungsinhalte sowie auf Konfigurationsoptionen für das Management der Verschleierung und die Anzeige sensibler Daten innerhalb des Systems (siehe „Datenschutzmanagement“)

Sie müssen eine Servicerolle hinzufügen, wenn Sie Folgendes hinzugefügt haben:

- Einen oder mehrere **Service**-Benutzer, die einen neuen Satz an Berechtigungen benötigen.
- Eine **benutzerdefinierte Rolle auf dem NetWitness Server-Server**, da es für vertrauenswürdige Verbindungen notwendig ist, dass die gleiche benutzerdefinierte Rolle auf dem Server und jedem Service vorhanden ist, auf den die benutzerdefinierte Rolle zugreift. Die Namen müssen identisch sein. Beispiel: Wenn Sie die Rolle „Junior Analysts“ auf dem Server hinzufügen, müssen Sie auf jedem Service, auf den die Rolle zugreift, eine Rolle „Junior Analysts“ hinzufügen. Weitere Informationen finden Sie im Thema **Hinzufügen einer Rolle und Zuweisen von Berechtigungen** unter *Systemsicherheit und Benutzerverwaltung*.

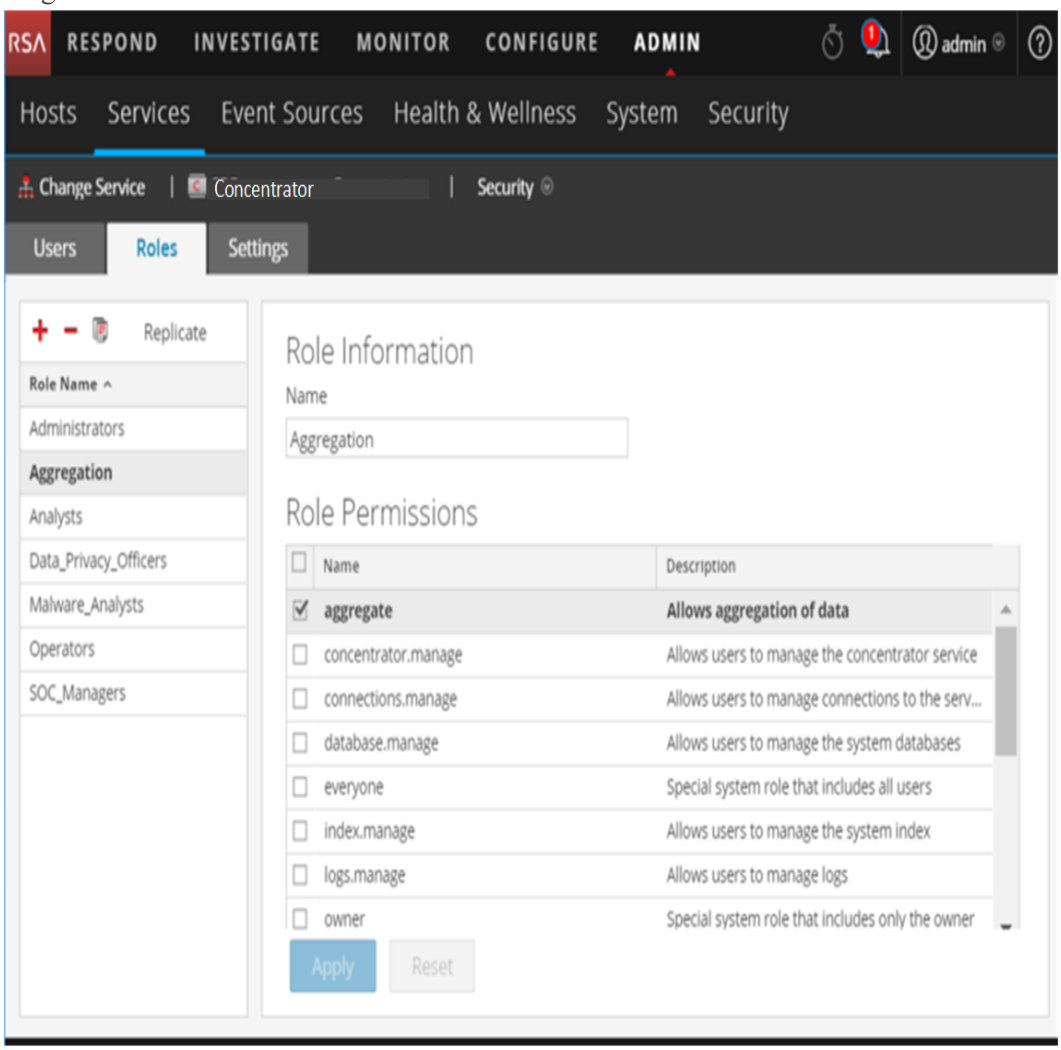
Es ist auch eine vorkonfigurierte Servicerolle **Aggregation** vorhanden. Weitere Informationen erhalten Sie unter Rolle "Aggregation" und Servicebenutzerrollen und -berechtigungen.

Verfahren

So fügen Sie eine Servicebenutzerrolle hinzu und weisen ihr Berechtigungen zu:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie einen Service und anschließend  **> Ansicht > Sicherheit** aus.
   Die Ansicht „Sicherheit“ für den ausgewählten Service wird mit geöffneter Registerkarte „Benutzer“ angezeigt.
3. Wählen Sie die Registerkarte **Rollen** aus und klicken Sie auf  .
   Die Ansicht „Services-Sicherheit“ wird angezeigt und fünf vorkonfigurierte Rollen sind bereits

aufgelistet.



4. Klicken Sie auf +, geben Sie den **Rollennamen** ein und drücken Sie die **Eingabetaste**. Die Rollen-ID wird über einer Liste von **Rollenberechtigungen** angezeigt.
5. Wählen Sie die Berechtigungen, die die Rolle im Service haben soll, nacheinander aus.
6. Klicken Sie auf **Anwenden**.

Auf der Registerkarte **Benutzer** können Sie ihr Benutzer hinzufügen.

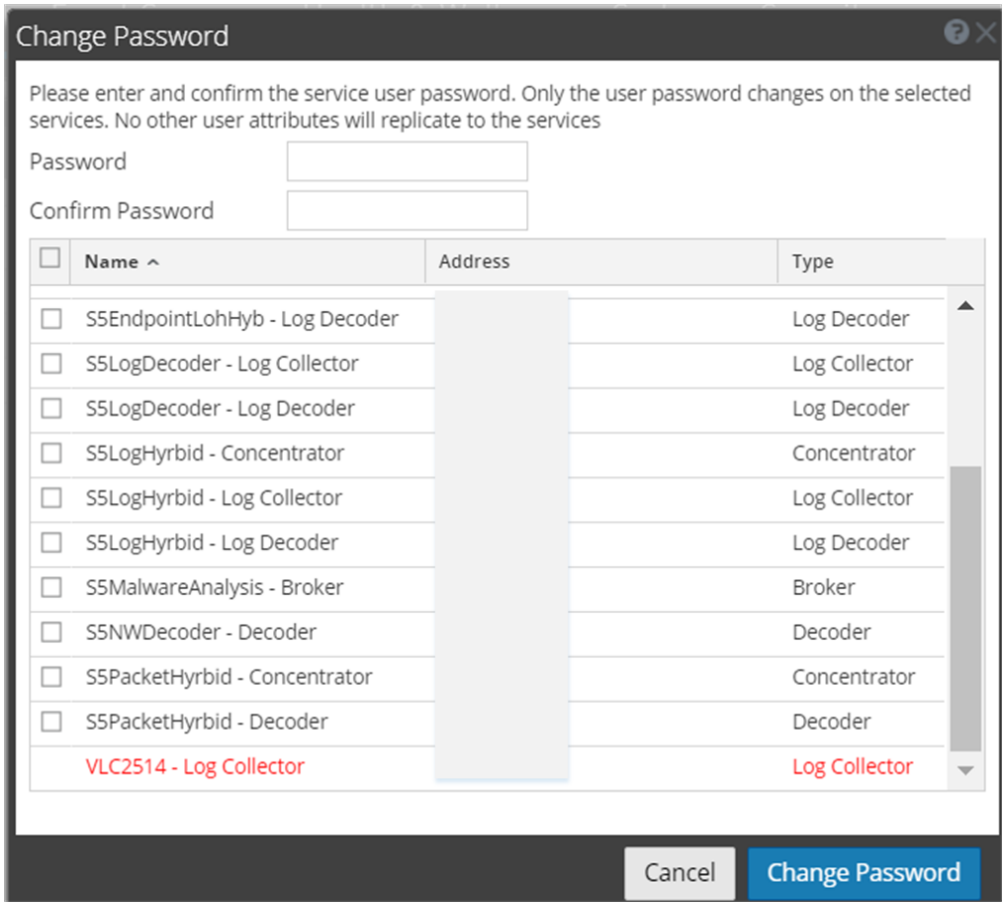
Ändern eines Servicebenutzerpassworts

Mit diesem Verfahren können Administratoren das Passwort eines Servicenutzers ändern und das neue Passwort in allen Core-Services replizieren, in denen dieses Nutzerkonto definiert ist. Dabei wird nur die Passwortänderung und nicht das gesamte Benutzerkonto in den ausgewählten Core-Services repliziert. Die Administratoren können auch das Passwort des **admin**-Kontos in den Core-Services ändern.

Hinweis: Die Option „Passwort ändern“ gilt nicht für externe Benutzer.

So ändern Sie das Passwort eines Servicebenutzers

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
   Die Ansicht „Administration“ > „Services“ wird angezeigt.
2. Wählen Sie einen Service aus und klicken Sie anschließend auf  **> Ansicht > Sicherheit**.
   Die Ansicht „Sicherheit“ für die ausgewählten Services wird angezeigt.
3. Wählen Sie in der Registerkarte **Benutzer** einen Benutzer und dann über das Aktionssymbol **Passwort ändern** aus.
   Das Dialogfeld **Passwort ändern** wird angezeigt.



4. Geben Sie ein neues Passwort für den Benutzer ein und bestätigen Sie es.
5. Wählen Sie die Services aus, in denen Sie das Benutzerpasswort ändern möchten.
6. Klicken Sie auf **Passwort ändern**.
   Der Status der Passwortänderung in den ausgewählten Services wird angezeigt.

Erstellen und Managen von Servicegruppen

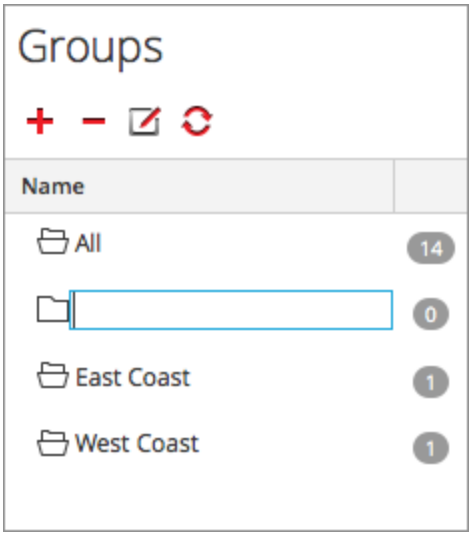
Die Ansicht „Administration > Services“ enthält Optionen zum Erstellen und Managen von Servicegruppen. Die Symbolleiste des Bereichs „Services“ umfasst Optionen für das Erstellen, Bearbeiten und Löschen von Servicegruppen. Sobald Gruppen erstellt wurden, können Sie einzelne Services aus dem Bereich Services in eine Gruppe ziehen.

Gruppen können funktionale, geografische, projektorientierte oder beliebige andere hilfreiche Unternehmensprinzipien widerspiegeln. Ein Service kann zu mehreren Gruppen gehören. Im Folgenden werden einige Beispiele für Gruppierungen genannt.

- Gruppieren Sie unterschiedliche Servicetypen, um alle Broker, Decoder oder Concentrators leichter konfigurieren und überwachen zu können.
- Gruppieren Sie Services, die Teil des gleichen Datenflusses sind, z. B. einen Broker und alle zugehörigen Concentrators und Decoder.
- Gruppieren Sie Services entsprechend ihrer geographischen Region und dem Standort in der Region. Wenn an einem Standort ein größerer Stromausfall auftritt, sind dann alle potenziell betroffenen Services leicht zu identifizieren.

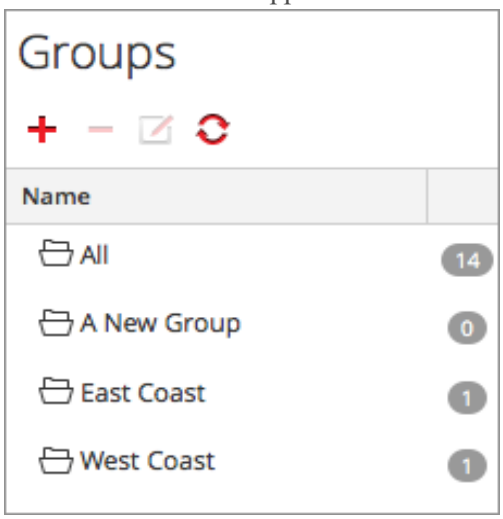
Erstellen einer Gruppe

1. Navigieren Sie in NetWitness Platform zu **ADMIN** > **Services**.
   Die Ansicht „Administration“ > „Services“ wird angezeigt.
2. Klicken Sie im Bereich **Gruppen** auf der Symbolleiste auf +.
   Ein Feld für die neue Gruppe wird mit blinkendem Cursor darin geöffnet.



3. Geben Sie den Namen der neuen Gruppe in das Feld ein (z. B. **Eine neue Gruppe**) und drücken Sie die **Eingabetaste**.
   Die Gruppe wird als Ordner in der Struktur erstellt. Die Zahl neben der Gruppe gibt die Anzahl der

Services in dieser Gruppe an.



Ändern des Namens einer Gruppe

1. Doppelklicken Sie in der Ansicht **Services** im Bereich **Gruppen** auf den Gruppennamen oder wählen Sie die Gruppe aus und klicken Sie auf . Das Namensfeld wird mit blinkendem Cursor darin geöffnet.
2. Geben Sie den neuen Namen der Gruppe ein und drücken Sie die **Eingabetaste**.
   Das Namensfeld wird geschlossen und der neue Gruppenname wird in der Struktur angezeigt.

Hinzufügen eines Services zu einer Gruppe

Wählen Sie in der Ansicht „Services“ im Bereich **Services** einen Service aus und ziehen Sie ihn in einen Gruppenordner im Bereich „Gruppen“, z. B. in den Ordner **Log Collectors**.
Der Service wird der Gruppe hinzugefügt.

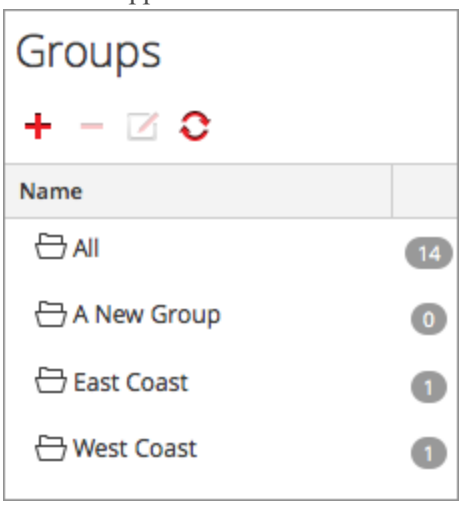
Anzeigen der Services in einer Gruppe

Um die Services in einer Gruppe anzuzeigen, klicken Sie im Bereich **Gruppen** auf die Gruppe.

Im Bereich **Services** werden die Services in dieser Gruppe aufgelistet.

Entfernen eines Services aus einer Gruppe

1. Wählen Sie in der Ansicht „Services“ im Bereich **Gruppen** die Gruppe aus, die den zu entfernenden Service enthält. Die Services in dieser Gruppe werden im Bereich „Services“ angezeigt.
2. Wählen Sie im Bereich **Services** einen oder mehrere Services aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie in der Symbolleiste > **Aus Gruppe entfernen** aus.
   Die ausgewählten Services werden aus der Gruppe entfernt, aber nicht aus der NetWitness Platform-Benutzeroberfläche. Die Anzahl der Services in der Gruppe, die neben dem Gruppennamen angezeigt wird, verringert sich um die Anzahl der aus der Gruppe entfernten Services. Die Gruppe **Alle** enthält die Services, die aus der Gruppe entfernt wurden.
   Im folgenden Beispiel enthält die Servicegruppe **Neue Gruppe** keine Services, da der Service in dieser Gruppe entfernt wurde.



Löschen von Gruppen

1. Wählen Sie in der Ansicht „Services“ im Bereich **Gruppen** die Gruppe aus, die Sie löschen möchten.
2. Klicken Sie auf .
   Die ausgewählte Gruppe wird aus dem Bereich „Gruppen“ entfernt. Die Services, die sich in der Gruppe befanden, werden nicht aus der NetWitness Platform-Benutzeroberfläche entfernt. Die Gruppe **Alle** enthält die Services der gelöschten Gruppe.

Duplizieren oder Replizieren einer Servicerolle

Eine effiziente Möglichkeit, eine neue Servicerolle hinzuzufügen, besteht darin, eine ähnliche Rolle zu duplizieren, sie unter einem neuen Namen zu speichern und die bereits zugewiesenen Berechtigungen zu bearbeiten. Sie können zum Beispiel die Rolle Analysten duplizieren. Speichern Sie diese dann als **JuniorAnalysts** und ändern Sie die Berechtigungen.

Eine schnelle Möglichkeit, eine existierende Rolle zu anderen Services hinzuzufügen, besteht darin, die Rolle zu replizieren. Sie können zum Beispiel die Rolle **JuniorAnalysts**, die auf einem Broker existiert, auf einem Concentrator oder einem Log Decoder replizieren.

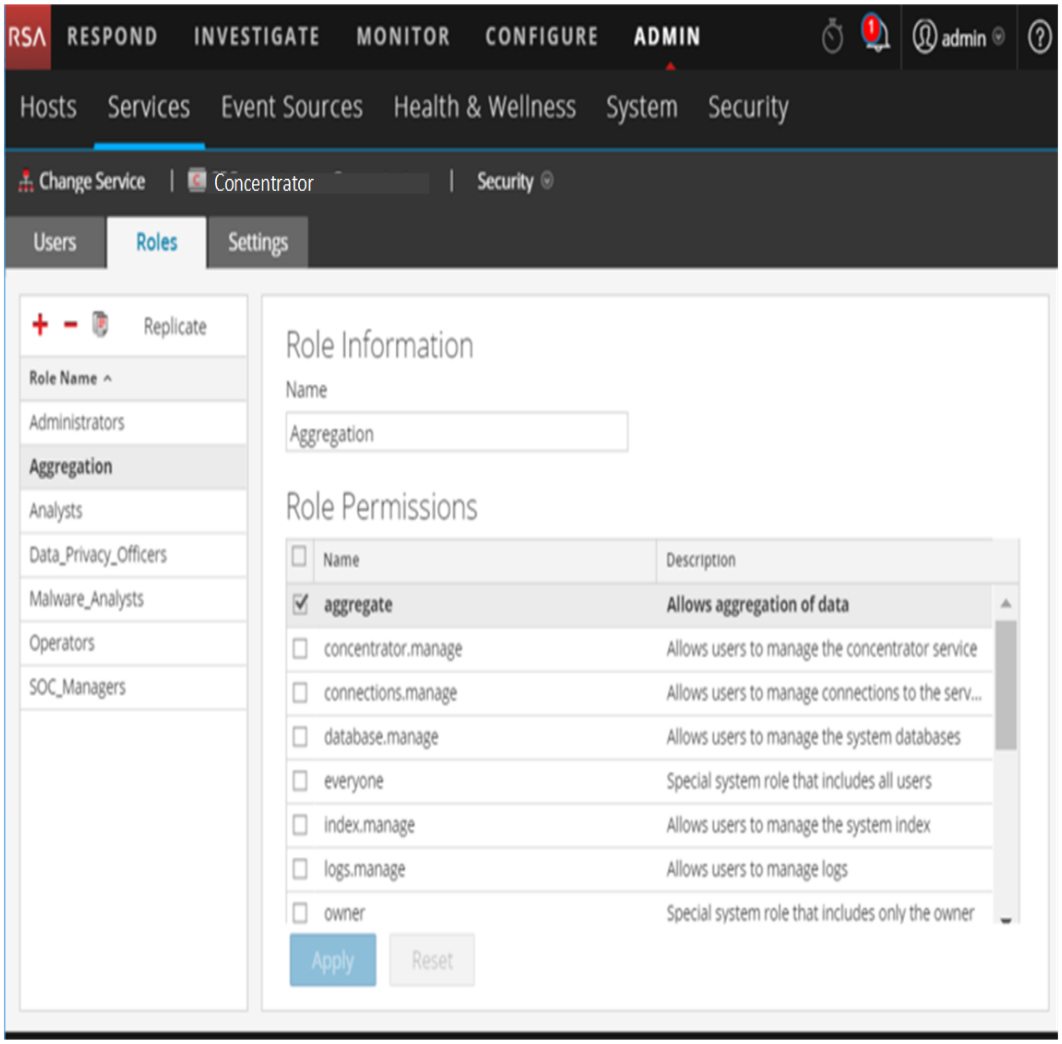
Jedes der folgenden Verfahren startet in der Ansicht Services-Sicherheit.

So navigieren Sie zur Ansicht Services-Sicherheit:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie einen Service und anschließend  **> Ansicht > Sicherheit** aus.
   Die Ansicht „Sicherheit“ für den ausgewählten Service wird mit geöffneter Registerkarte „Benutzer“ angezeigt.
3. Wählen Sie die Registerkarte **Rollen** aus.

Duplizieren einer Servicerolle

1. Wählen Sie in der Registerkarte „Rollen“ die Rolle aus, die Sie duplizieren möchten.



2. Klicken Sie auf **Rolle duplizieren**.

3. Geben Sie einen neuen Namen ein und klicken Sie auf **Anwenden**.
4. Wählen Sie die neue Rolle aus.
5. Aktivieren oder deaktivieren Sie im Abschnitt **Rollenberechtigungen** die Berechtigungen, um die Berechtigungen einer Rolle zu ändern.

Replizieren einer Rolle

1. Wählen Sie in der Registerkarte **Rollen** die Rolle aus, die Sie replizieren möchten, und klicken Sie auf **Replizieren**.
2. Wählen Sie im Dialogfeld **Rolle nach anderen Services replizieren** alle Services aus, zu denen Sie die Rolle hinzufügen möchten.
3. Klicken Sie auf **Replizieren**.

Bearbeiten von Core-Servicekonfigurationsdateien

Die Servicekonfigurationsdateien für Decoder, Log Decoder, Broker, Concentrator, Archiver und Workbench-Services können als Textdateien bearbeitet werden. Auf der Registerkarte „Servicekonfigurationsansicht > Dateien“ können Sie die folgenden Schritte ausführen:

- Eine Servicekonfigurationsdatei, die das NetWitness Platform-System gerade verwendet, anzeigen und bearbeiten
- Das aktuelle Backup der Datei, die Sie gerade bearbeiten, abrufen und wiederherstellen
- Die geöffnete Datei an andere Services übertragen
- An einer Datei vorgenommene Änderungen speichern

Die für die Bearbeitung verfügbaren Dateien sind abhängig von dem Servicetyp, der konfiguriert wird. Die für alle Core-Services verfügbaren Dateien lauten wie folgt:

- Serviceindexdatei
- NetWitness-Datei
- Crash Reporter-Datei
- Planerdatei

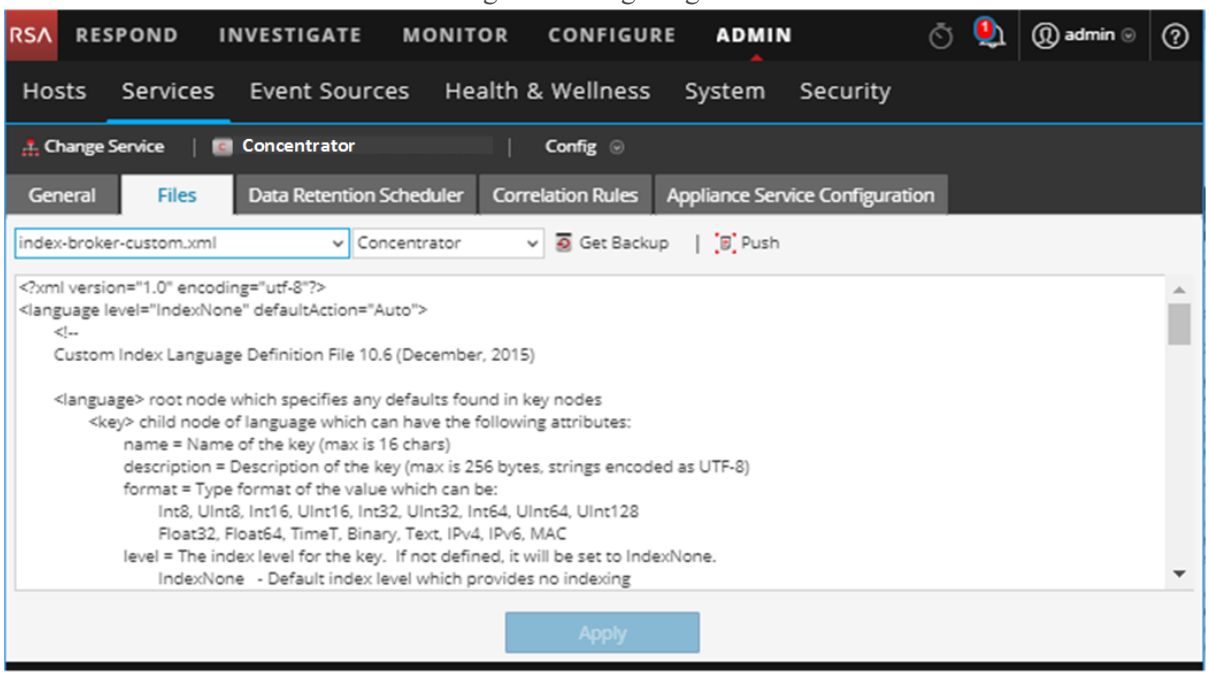
Darüber hinaus hat der Decoder Dateien, die Parser, Feeddefinitionen und einen Wireless-LAN-Adapter konfigurieren.

Hinweis: Die Standardwerte in diesen Konfigurationsdateien sind für die gängigsten Situationen gut geeignet. Eine Bearbeitung ist jedoch bei optionalen Services wie dem Crash Reporter oder dem Scheduler erforderlich. Nur Administratoren mit guten Kenntnissen der Netzwerke und der Einflussfaktoren auf die Art und Weise, wie Services Daten erfassen und analysieren, sollten Änderungen an diesen Dateien in der Registerkarte „Dateien“ vornehmen.

Bearbeiten einer Servicekonfigurationsdatei

So bearbeiten Sie eine Datei:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ einen Service aus.
3. Wählen Sie  **> Ansicht > Konfiguration** aus.
   Die Servicekonfigurationsansicht wird mit geöffneter Registerkarte „Allgemei“n angezeigt.
4. Klicken Sie auf die Registerkarte **Dateien**.
   Der ausgewählte Service, wie etwa Concentrator, wird in der Drop-down-Liste auf der rechten Seite angezeigt.
5. (Optional) Wählen Sie zur Bearbeitung einer Datei für den Host anstatt für den Service in der Drop-down-Liste die Option **Host** aus.
6. Wählen Sie aus der Drop-down-Liste **Wählen Sie eine Datei zur Bearbeitung aus** eine Datei aus.
   Der Inhalt der Datei wird im Bearbeitungsmodus angezeigt.



7. Bearbeiten Sie die Datei und klicken Sie auf **Anwenden**.

Die aktuelle Datei wird überschrieben und eine Backupdatei wird erstellt. Die Änderungen werden nach dem Neustart des Services wirksam.

Wiederherstellen einer Backupversion einer Servicekonfigurationsdatei

Nachdem Sie an einer Konfigurationsdatei Änderungen vorgenommen, die Datei gespeichert und den Service neu gestartet haben, steht eine Backupdatei zur Verfügung. So stellen Sie ein Backup einer Konfigurationsdatei wieder her:

1. Wählen Sie eine Konfigurationsdatei aus, indem Sie die Schritte 1 bis 6 des Verfahrens am Anfang dieses Themas abschließen.

2. Klicken Sie auf Get Backup.
   Die Backupdatei wird im Texteditor geöffnet.
3. Klicken Sie zur Wiederherstellung der Backupversion auf **Speichern**.

Die Änderungen werden nach dem Neustart des Services wirksam.

Übertragen einer Konfigurationsdatei an andere Services

Nachdem Sie eine Servicekonfigurationsdatei bearbeitet haben, können Sie die gleiche Konfiguration auf andere Services des gleichen Typs übertragen.

1. Wählen Sie eine Konfigurationsdatei aus, indem Sie die Schritte 1–6 des Verfahrens Bearbeiten von Servicekonfigurationsdateien am Anfang dieses Themas ausführen.
2. Klicken Sie auf Push. Das Dialogfeld „Services auswählen“ wird angezeigt.
3. Wählen Sie jeden Service aus, um die Konfigurationsdatei auf ihn zu übertragen.
   Jeder Service muss vom gleichen Typ sein wie derjenige, den Sie in der Ansicht Services ausgewählt haben.

   Achtung: Wenn Sie sich dagegen entscheiden, die Konfigurationsdatei zu übertragen, klicken Sie auf **Abbrechen**.
4. Klicken Sie zur Übertragung der Konfigurationsdatei auf alle ausgewählten Services auf **OK**.

Die Konfigurationsdatei wird auf alle ausgewählten Services übertragen.

Konfigurieren des Aufgabenplaners

Planerdatei

Sie können die **Planerdatei** in der Registerkarte „Dateien“ in der Servicekonfigurationsansicht bearbeiten. Diese Datei konfiguriert den integrierten Aufgabenplaner für einen Service. Der Aufgabenplaner kann automatisch in vordefinierten Intervallen oder zu bestimmten Tageszeiten Nachrichten versenden.

Syntax des Aufgabenplaners

Eine Aufgabenzeile in der Planerdatei enthält die folgende Syntax, wenn **<Value>** keine Leerzeichen enthält:

```
<ParamName>=<Value>
```

Enthält **<Value>** Leerzeichen, gilt folgende Syntax:

```
<ParamName>="<Value>"
```

In jeder Aufgabenzeile gelten folgende Guidelines:

- Der Parameter **time** (Zeit) oder einer der Intervallparameter (**seconds** (Sekunden), **minutes** (Minuten) oder **hours** (Stunden)) ist erforderlich.
- Stellen Sie Sonderzeichen einen umgekehrten Schrägstrich \ voran.

Aufgabenzeilenparameter

Die folgenden Aufgabenzeilenparameter werden vom Planer akzeptiert.

Syntax	Beschreibung
daysOfWeek: <string, optional, {enum-any:sun|mon|tue|wed|thu|fri|sat|all}>	Die Wochentage, an denen die Aufgabe ausgeführt werden soll. Der Standardwert ist alle.
deleteOnFinish: <bool, optional>	Aufgabe nach erfolgreicher Durchführung löschen
hours: <uint32, optional, {range:1 to 8760}>	Die Anzahl von Stunden zwischen den Ausführungen.
logOutput: <string, optional>	Die Ausgabe unter Verwendung des angegebenen Modulnamens protokollieren
minutes: <uint32, optional, {range:1 to 525948}>	Die Anzahl von Minuten zwischen den Ausführungen.
msg: <string>	Die Nachricht, die an den Node gesendet werden soll
params: <string, optional>	Die Parameter für die Nachricht
pathname: <string>	Der Pfad des Node, der die Nachricht erhalten soll
seconds: <uint32, optional, {range:1 to 31556926}>	Die Anzahl der Sekunden zwischen den Ausführungen
time: <string>	Die Zeit der Ausführung im Format HH::MM::SS (Ortszeit des Servers)
timesToRun: <uint32, optional>	Häufigkeit der Ausführung aufgrund des Servicestarts, **0** bedeutet unbegrenzt (Standardeinstellung).

Nachrichten

Die folgenden Nachrichtenzeichenfolgen können im Aufgabenplaner als **msg**-Parameter verwendet werden.

Meldung	Beschreibung
addInter	Damit fügen Sie eine Aufgabe hinzu, die in einem definierten Intervall ausgeführt wird. Mit der folgenden Nachricht wird beispielsweise der Befehl **/index save** alle 6 Stunden ausgeführt: addInter hours=6 pathname=/index msg=save
addMil	Damit fügen Sie eine Aufgabe hinzu, die an einem oder mehreren Tagen zu einer bestimmten Uhrzeit ausgeführt wird. Mit der folgenden Nachricht wird beispielsweise der Befehl **/index save** um 1:00 Uhr an jedem Werktag ausgeführt: addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri
delSched	Damit löschen Sie eine bestehende geplante Aufgabe. Der Parameter **id** der Aufgabe muss von der print-Nachricht abgerufen werden.
print	Damit drucken Sie alle geplanten Aufgaben.
replace	Damit weisen Sie alle geplanten Aufgaben in einer Nachricht zu und löschen alle bestehenden Aufgaben.

Meldung	Beschreibung
save	Speicher-Nodes

Beispielaufgabenzeile

Die folgende Beispielaufgabenzeile in der Planerdatei lädt die gepackte Feedsdatei (**feeds.zip**) alle 120 Minuten vom Hostserver des Feeds herunter.

```
minutes=120 pathname=/parsers msg=feed params="type\=wget
file\=http://feedshost/nwlive/feeds.zip"
```

Bearbeiten einer Serviceindexdatei

Dieses Thema enthält wichtige Informationen und Richtlinien zur Konfiguration benutzerdefinierten Serviceindexdateien, die in der Ansicht Services > Konfiguration > Registerkarte Dateien bearbeitet werden können.

Zusammen mit anderen Konfigurationsdateien steuert die Indexdatei die Vorgänge des jeweiligen Core-Services. Durch Zugreifen auf die Indexdatei über die Servicekonfigurationsansicht in NetWitness Platform wird die Datei in einem Text-Editor geöffnet, in dem Sie sie bearbeiten können.

Hinweis: Nur Administratoren mit fundierten und umfassenden Kenntnissen der Core-Servicekonfiguration sind qualifiziert, Änderungen an einer Indexdatei vorzunehmen, die eine der zentralen Konfigurationsdateien für den Appliance-Service darstellt. Die vorgenommenen Änderungen müssen auf allen Core-Services konsistent sein. Ungültige Einträge oder falsch konfigurierte Dateien können einen Start des Systems verhindern und ein Eingreifen des RSA-Supports erfordern, um den Funktionsfähigkeit des Systems wiederherzustellen.

Dies sind die Indexdateien:

- `index-broker.xml` und `index-brokercustom.xml`
- `index-concentrator.xml` und `index-concentrator-custom.xml`
- `index-decoder.xml` und `index-decodercustom.xml`
- `index-logdecoder.xml` und `index-logdecodercustom.xml`
- `index-archiver.xml` und `index-archiver-custom.xml`
- `index-workbench.xml` und `index-workbench-custom.xml`

Indexdateien und benutzerdefinierte Indexdateien

Alle kundenspezifischen Indexänderungen werden in **`index-<service>-custom.xml`** vorgenommen. Diese Datei überschreibt alle Einstellungen in `index-<service>.xml`, die ausschließlich durch RSA gesteuert wird.

Mit der benutzerdefinierten Indexdatei **`index-<service>-custom.xml`** können kundenspezifische Definitionen erstellt oder Ihre eigenen Sprachschlüssel überschrieben werden, die während des Upgradeprozesses nicht überschrieben werden.

- Schlüssel, die in der Datei `index-<service>-custom.xml` definiert sind, ersetzen die Definitionen in der Datei `index-<service>.xml`.
- Schlüssel, die zur Datei `index-<service>custom.xml` hinzugefügt werden und nicht in der Datei `index <service>.xml` vorhanden sind, werden als neuer Schlüssel zur Sprache hinzugefügt.

Einige häufige Anwendungsbeispiele für das Bearbeiten der Indexdatei sind:

- Hinzufügen neuer benutzerdefinierter Metaschlüssel, um neue Felder zur NetWitness Platform-Benutzeroberfläche hinzuzufügen
- Konfiguration geschützter Metaschlüssel als Teil einer Datenschutzlösung wie im Leitfaden *Datenschutzmanagement* beschrieben
- Anpassen der Abfrageperformance der NetWitness Platform Core-Datenbanken wie im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden* beschrieben

Achtung: Setzen Sie die Indexebene auf einem Decoder niemals auf `IndexKeys` oder `IndexValues`, wenn ein Concentrator oder Archiver von dem Decoder aggregiert. Die Größe der Indexpartition ist zu klein, um die Indexierung über den standardmäßigen Metaschlüssel `time` hinaus zu unterstützen.

Aktivieren des Crash Reporter-Service

Der Crash Reporter ist ein optionaler Service für NetWitness Platform-Services. Ist der Crash Reporter für einen der Core-Services aktiviert, generiert dieser automatisch ein Informationspaket, das zur Diagnose und Lösung des Problems, das zum Servicefehler geführt hat, verwendet wird. Das Paket wird automatisch an RSA zur Analyse gesendet. Die Ergebnisse werden an den RSA-Support zur weiteren Bearbeitung gesendet.

Das an RSA gesendete Informationspaket enthält keine erfassten Daten. Dieses Informationspaket enthält die folgenden Informationen:

- Stapelüberwachung
- Protokolle
- Konfigurationseinstellungen
- Softwareversion
- CPU-Informationen
- Installierte RPMs
- Festplattengeometrie

Die Absturzanalyse des Crash Reporter kann für jedes Core-Produkt aktiviert werden.

Die Datei crashreporter.cfg

Eine der zur Bearbeitung verfügbaren Dateien in der in der Registerkarte „Dateien“ in der Ansicht „Servicekonfiguration“ ist **crashreporter.cfg**, die Serverkonfigurationsdatei des Crash Reporter-Clients.

Diese Datei wird von dem Skript verwendet, das Absturzreporte in des Hosts überprüft, aktualisiert und erstellt. Zu überwachende Produkte können Decoder, Concentrators, Hosts und Brokers umfassen.

In dieser Tabelle werden die Einstellungen für die Datei **crashreporter.cfg** aufgelistet.

Einstellung	Beschreibung
applicationlist=decoder, concentrator, host	Definieren Sie die Liste der zu überwachenden Produkte.
sitedir=/var/crashreporter	Speicherort des Seitenverzeichnisses für den Bericht.

Einstellung	Beschreibung
webdir=/usr/share/crashreporter/Web	Speicherort des Web-Verzeichnisses.
devdir=/var/crashreporter/Dev	Speicherort des Entwicklungs-Verzeichnisses.
datadir=/var/crashreporter/data	Speicherort des Verzeichnisses, das Datendateien speichert.
perldir=/usr/share/crashreporter/perl	Speicherort der Perl-Dateien.
bindir=/usr/share/crashreporter/bin	Speicherort der binären ausführbaren Dateien.
libdir=/usr/share/crashreporter/lib	Speicherort der binären Bibliotheken.
cfgdir=/etc/crashreporter	Speicherort der Konfigurationsdateien.
logdir=/var/log/crashreporter	Speicherort der Protokolldateien.
scriptdir=/usr/share/crashreporter/scripts	Speicherort des Verzeichnisses, das Skripts enthält.
workdir=/var/crashreporter/work	Speicherort des Produktionsprozess-Verzeichnisses.
sqldir=/var/crashreporter/sql	Speicherort erstellter sql-Dateien.
reportdir=/var/crashreporter/reports	Erstellungsort temporärer Berichte.
packagedir=/var/crashreporter/packages	Speicherort der erstellten Paket-Dateien.
gdbconfig=/etc/crashreporter/crashreporter.gdb	Speicherort der gdb-Konfigurationsdatei.
corewaittime=30	Definieren Sie die Anzahl der Sekunden, die Sie nach dem Auffinden eines Cores warten, um zu überprüfen, ob sich der Core noch im Erstellungsprozess befindet.
cyclewaittime=10	Definieren Sie die Anzahl an Minuten, die zwischen einzelnen Suchzyklen liegen.

Einstellung	Beschreibung
deletecores=1	Legen Sie fest, ob Core-Dateien nach dem Bericht gelöscht werden sollen. 0 = Nein 1 = Ja **HINWEIS**: Bis zu dem Zeitpunkt, zu dem die Core-Datei gelöscht ist, wird diese Meldung jedes Mal angezeigt, wenn „crashreporter“ neu gestartet wird.
deletereportdir=1	Legen Sie fest, ob das Berichtsverzeichnis nach dem Bericht gelöscht werden soll. Dies eignet sich zur Ansicht von Core-Berichten in einem Dialogfeld. 0 = Nein 1 = Ja **NOTE**: Wird das Verzeichnis nicht gelöscht, wird dieses jedem nachfolgenden Paket hinzugefügt.
debug=1	Legen Sie fest, ob Debugging-Meldungen in der **crashreporter**-Protokollausgabe aktiviert oder deaktiviert werden. 0 = Nein 1 = Ja
posturl=https://www.netwitnesslive.com/crash...ter/submit.php	Definieren Sie die Post-URL des Webservers.
postpackages=0	Legen Sie fest, ob die Pakete an den Webserver gesendet werden oder nicht. 0 = Nein 1 = Ja
deletepackages=1	Legen Sie fest, ob Pakete gelöscht werden sollen, wenn Sie an den Webserver gesendet wurden. 0 = Nein 1 = Ja

Konfigurieren des Crash Reporter-Services

So konfigurieren Sie den Crash Reporter-Service:

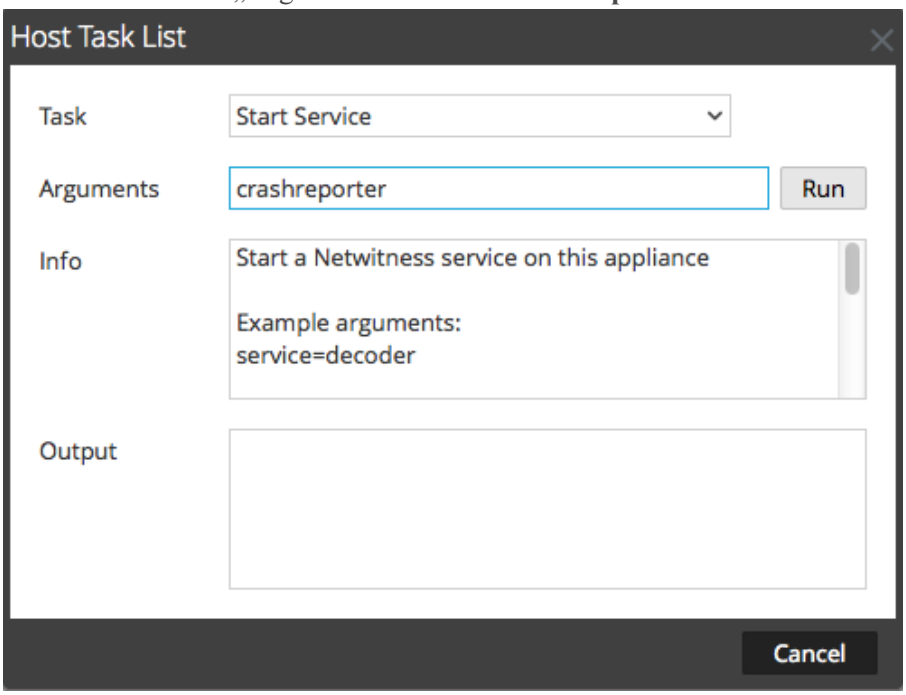
1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie einen Service aus und klicken Sie auf  **> Ansicht > Konfiguration**.
3. Wählen Sie die Registerkarte **Dateien** aus.

4. Bearbeiten Sie die Datei **crashreporter.cfg**.
5. Klicken Sie auf **Speichern**.
6. Um die Ansicht „Service-System“ anzuzeigen, wählen Sie **Konfiguration > System** aus.
7. Um den Service neu zu starten, klicken Sie auf Shutdown Service.
   Der Service fährt herunter und wird neu gestartet.

Starten und Beenden des Crash Reporter-Services

So starten Sie den Crash Reporter-Service:

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie einen Service aus und klicken Sie auf > **Ansicht > System**.
3. Klicken Sie in der Symbolleiste auf Host Tasks.
   Die Hostaufgabenliste wird angezeigt.
4. Wählen Sie in der Drop-down-Liste der Aufgaben **Service starten**.
5. Geben Sie im Feld „Argumente“ den Text **crashreporter** ein und klicken Sie auf **Ausführen**.



Der Crash Reporter-Service ist aktiviert und bleibt so lange aktiv, bis Sie ihn beenden.

Um den Crash Reporter-Service zu beenden, klicken Sie in der Drop-down-Liste „Aufgaben“ auf **Service anhalten**.

Pflegen der Tabellenzuordnungsdateien

Die von RSA bereitgestellte Tabellenzuordnungsdatei `table-map.xml` ist ein sehr wichtiger Teil des Log Decoder. Es handelt sich dabei um eine Definitionsdatei, in der auch die in einem Protokollparser verwendeten Schlüssel den Schlüsseln in der Meta-DB zugeordnet werden.

Hinweis: Bearbeiten Sie nicht die Datei `table-map.xml`. Wenn Sie Änderungen an der Tabellenzuordnung vornehmen möchten, tun Sie dies in der Datei `table-map-custom.xml`. Die neueste Version der Datei `table-map.xml` ist auf Live verfügbar. Sie wird bei Bedarf von RSA aktualisiert. Wenn Sie Änderungen an der Datei `table-map.xml` vornehmen, können diese während eines Service- oder Inhaltsupgrades überschrieben werden.

In der Datei `table-map.xml` sind einige Metaschlüssel auf `Transient` festgelegt und einige auf `None`. Um einen bestimmten Metaschlüssel speichern und indexieren zu können, muss der Schlüssel auf `None` festgelegt sein. Um Änderungen an der Zuordnung vornehmen zu können, müssen Sie eine Kopie der Datei `table-map-custom.xml` auf dem Log Decoder erstellen und die Metaschlüssel auf `None` festlegen.

Zur Metaschlüsselindexierung:

- Wenn ein Schlüssel in der Datei `table-map.xml` im Log Decoder mit `None` markiert ist, ist er indexiert.
- Wenn ein Schlüssel in der Datei **`table-map.xml`** im Log Decoder als `Transient` markiert ist, ist er nicht indexiert. Kopieren Sie zur Indexierung des Schlüssels den Eintrag in die Datei `table-map-custom.xml` und ändern Sie das Schlüsselwort von `flags="Transient"` in `flags="None"`.
- Wenn ein Schlüssel in der Datei `table-map.xml` nicht vorhanden ist, fügen Sie der Datei `table-map-custom.xml` im Log Decoder einen Eintrag hinzu.

Achtung: Aktualisieren Sie die Datei `table-map.xml` nicht, da sie bei einem Upgrade überschrieben werden kann. Nehmen Sie alle Änderungen an der Datei **`table-map-custom.xml`** vor.

Voraussetzungen

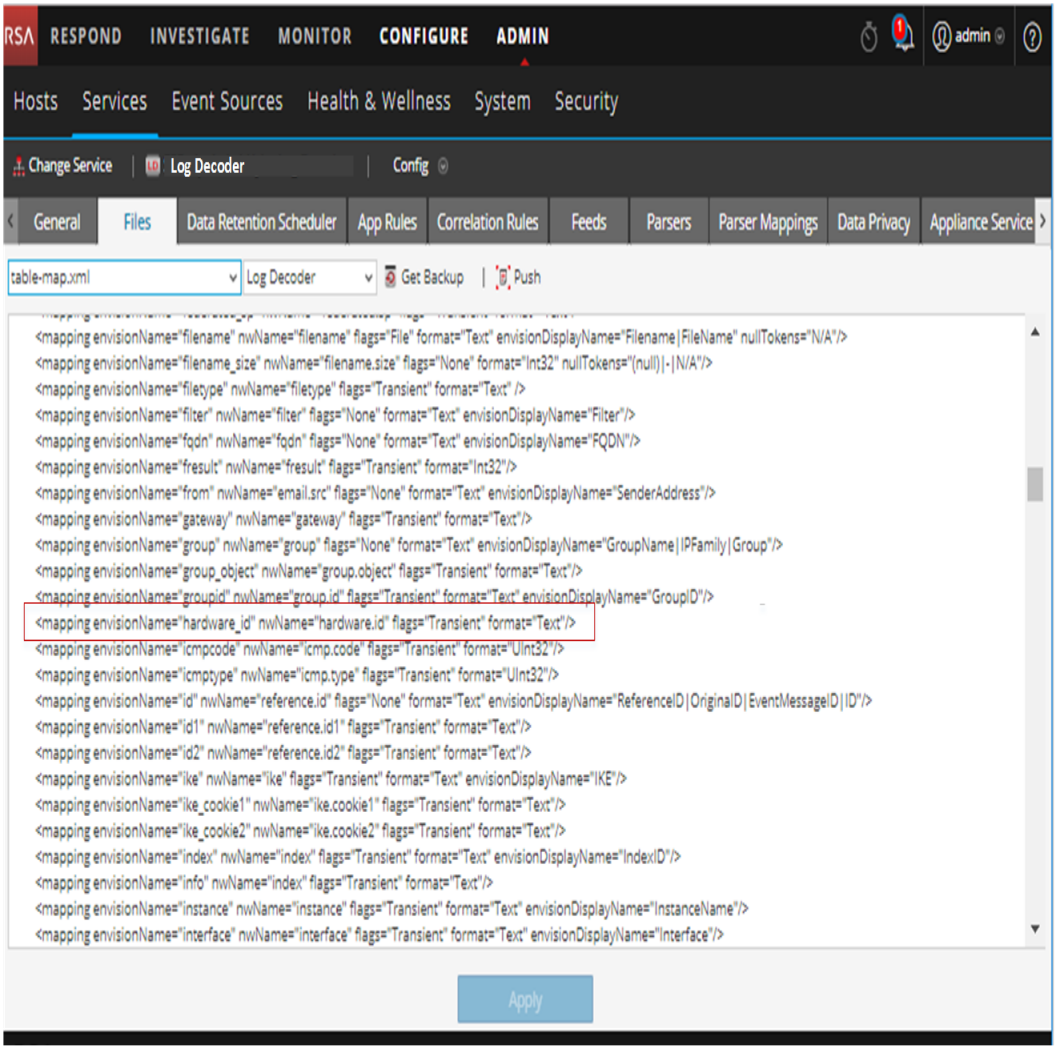
Wenn auf dem Log Decoder keine Datei `table-map-custom.xml` vorhanden ist, erstellen Sie eine Kopie von `table-map.xml` und benennen Sie sie um in `table-map-custom.xml`.

Verfahren

So überprüfen und aktualisieren Sie die Tabellenzuordnungsdatei:

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Wählen Sie im Raster „Services“ einen Log Decoder aus und klicken Sie auf  > **Ansicht** > **Konfiguration**.

3. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie die Datei **`table-map.xml`** aus.



4. Vergewissern Sie sich, dass die Flag-Schlüsselwörter korrekt auf `Transient` oder `None` festgelegt sind.

5. Wenn Sie einen Eintrag ändern müssen, ändern Sie nicht die Datei `table-map.xml` . Kopieren Sie stattdessen den Eintrag, wählen Sie die Datei `table-map-custom.xml` aus, suchen Sie den Eintrag in der Datei `table-map-custom.xml` und ändern Sie das Flag-Schlüsselwort von `Transient` in `None`.
   Der folgende Eintrag für den Metaschlüssel `hardware.id` in der Datei `table-map.xml` ist beispielsweise nicht indexiert und das Flag-Schlüsselwort wird als `Transient` angezeigt:
   `<mapping envisionName="hardware_id" nwName="hardware.id"`
   `flags="Transient"``/>`
   Um den Metaschlüssel `hardware.id` zu indexieren, ändern Sie das Flag-Schlüsselwort von `Transient` in `None` in der Datei `table-map-custom.xml`:
   `<mapping envisionName="hardware_id" nwName="hardware.id"` **`flags="None"`**`/>`

6. Wenn ein Eintrag in der Datei `table-map.xml` nicht vorhanden ist, fügen Sie der Datei `table-map-custom.xml` einen Eintrag hinzu.
7. Klicken Sie nach dem Vornehmen Ihrer Änderungen an der Datei `table-map-custom.xml` auf **Anwenden**.

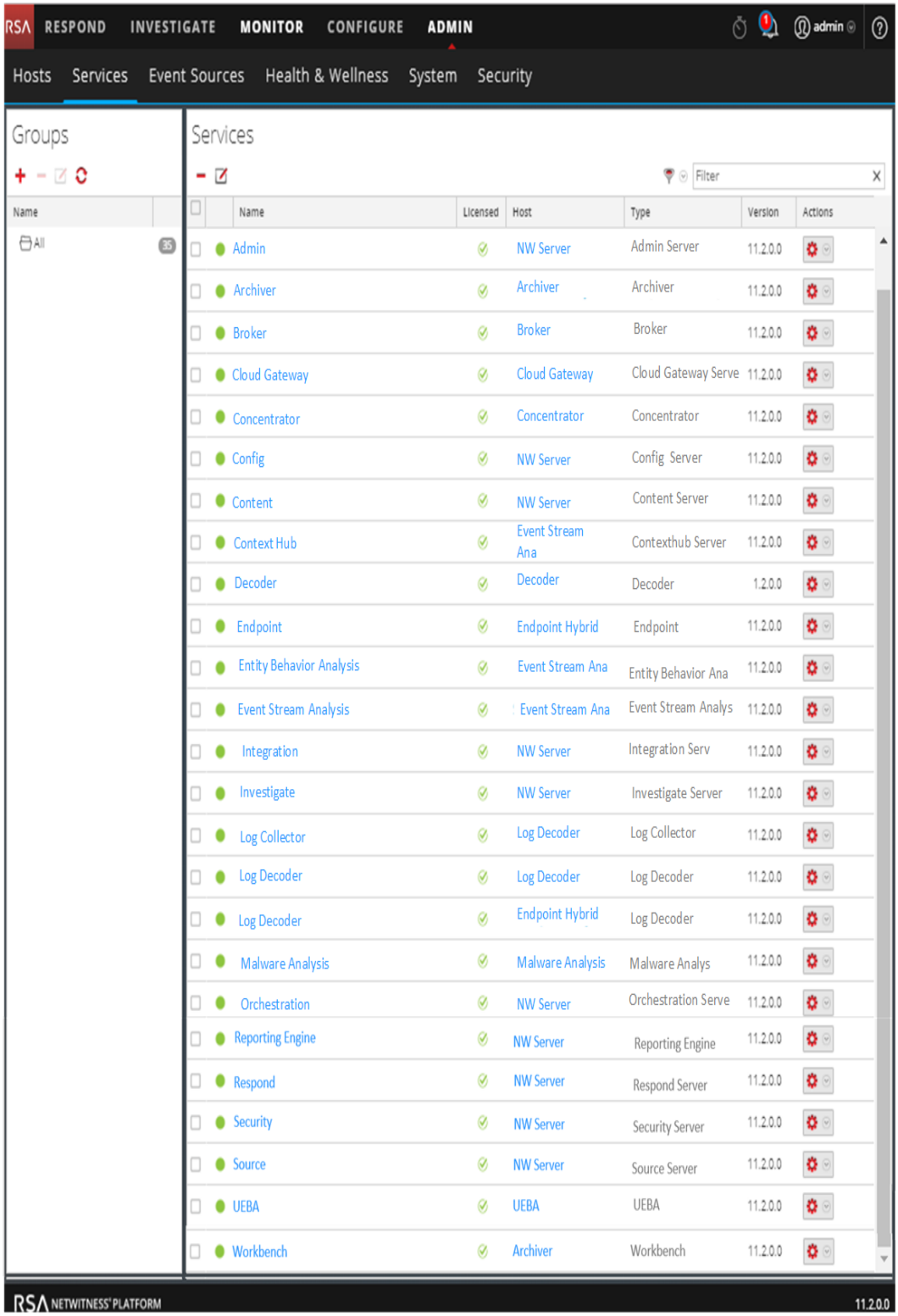
Achtung: Bedenken Sie vor dem Ändern der Tabellenzuordnungsdateien sorgfältig die Folgen der Änderung des Indexes von `Transient` in `None`, da dies Auswirkungen auf den verfügbaren Speicher und die Performance des Log Decoder haben kann. Aus diesem Grund sind nur bestimme Metaschlüssel als indexiert vorkonfiguriert. Verwenden Sie die Datei `table-map-custom.xml` für verschiedene Anwendungsbeispiele.

Bearbeiten oder Löschen eines Services

Sie können Serviceeinstellungen bearbeiten, z. B. den Hostnamen oder die Portnummer ändern oder einen nicht mehr benötigten Service löschen.

Jedes der folgenden Verfahren beginnt in der Services-Ansicht.

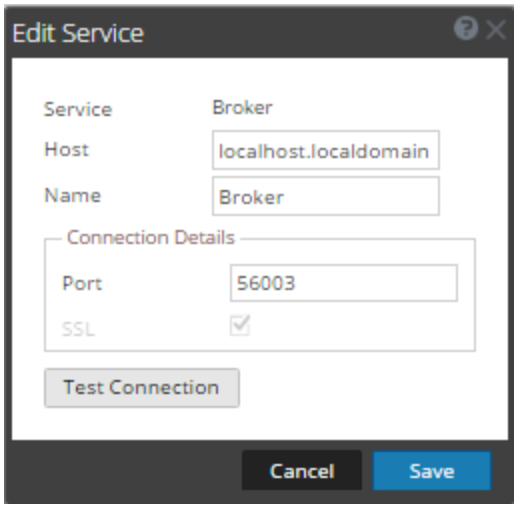
Um die Ansicht „Services“ aufzurufen, navigieren Sie in NetWitness Platformzu **ADMIN > Services**.


RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN
admin
Hosts Services Event Sources Health & Wellness System Security
Groups
Name
All 35
Services
Filter
Name Licensed Host Type Version Actions
Admin NW Server Admin Server 11.2.0.0
Archiver Archiver Archiver 11.2.0.0
Broker Broker Broker 11.2.0.0
Cloud Gateway Cloud Gateway Cloud Gateway Serve 11.2.0.0
Concentrator Concentrator Concentrator 11.2.0.0
Config NW Server Config Server 11.2.0.0
Content NW Server Content Server 11.2.0.0
Context Hub Event Stream Ana Contexthub Server 11.2.0.0
Decoder Decoder Decoder 1.2.0.0
Endpoint Endpoint Hybrid Endpoint 11.2.0.0
Entity Behavior Analysis Event Stream Ana Entity Behavior Ana 11.2.0.0
Event Stream Analysis Event Stream Ana Event Stream Analys 11.2.0.0
Integration NW Server Integration Serv 11.2.0.0
Investigate NW Server Investigate Server 11.2.0.0
Log Collector Log Decoder Log Collector 11.2.0.0
Log Decoder Log Decoder Log Decoder 11.2.0.0
Log Decoder Endpoint Hybrid Log Decoder 11.2.0.0
Malware Analysis Malware Analysis Malware Analys 11.2.0.0
Orchestration NW Server Orchestration Serve 11.2.0.0
Reporting Engine NW Server Reporting Engine 11.2.0.0
Respond NW Server Respond Server 11.2.0.0
Security NW Server Security Server 11.2.0.0
Source NW Server Source Server 11.2.0.0
UEBA UEBA UEBA 11.2.0.0
Workbench Archiver Workbench 11.2.0.0
RSA NETWITNESS PLATFORM
11.2.0.0

Methoden

Bearbeiten eines Services

1. Wählen Sie in der Ansicht „Services“ einen Service aus und klicken Sie auf oder > **Bearbeiten**.
   Das Dialogfeld **Service bearbeiten** wird angezeigt. Es enthält nur die Felder, die auf den ausgewählten Service zutreffen.



2. Bearbeiten Sie die Servicedetails durch Ändern folgender Felder:
   - **Name**
   - **Port**: Jeder Core-Service hat zwei Ports: SSL und Nicht-SSL. Sichere Verbindungen werden mit dem SSL-Port gewährleistet.
   - **SSL**: Für sichere Verbindungen müssen Sie SSL verwenden.
   - **Benutzername** und **Passwort**: Verwenden Sie diese Anmeldedaten zum Testen der Verbindung mit einem Service.
     a. Wenn Sie eine sichere Verbindung verwenden, können Sie den Benutzernamen löschen. Wenn Sie keine sichere Verbindung verwenden, geben Sie einen Benutzernamen und ein Passwort ein.
     b. Klicken Sie auf **Verbindung testen**.
3. Klicken Sie auf **Speichern**.

Löschen eines Services

1. Wählen Sie in der Ansicht „Services“ einen oder mehrere Services aus und klicken Sie auf oder > **Löschen**.
2. In einem Dialogfeld werden Sie zur Bestätigung aufgefordert. Um den Service zu löschen, klicken Sie auf **Ja**.

Der gelöschte Service steht nicht mehr in den NetWitness Platform-Modulen zur Verfügung.

Durchsuchen und Bearbeiten der Service-Eigenschaftenstruktur

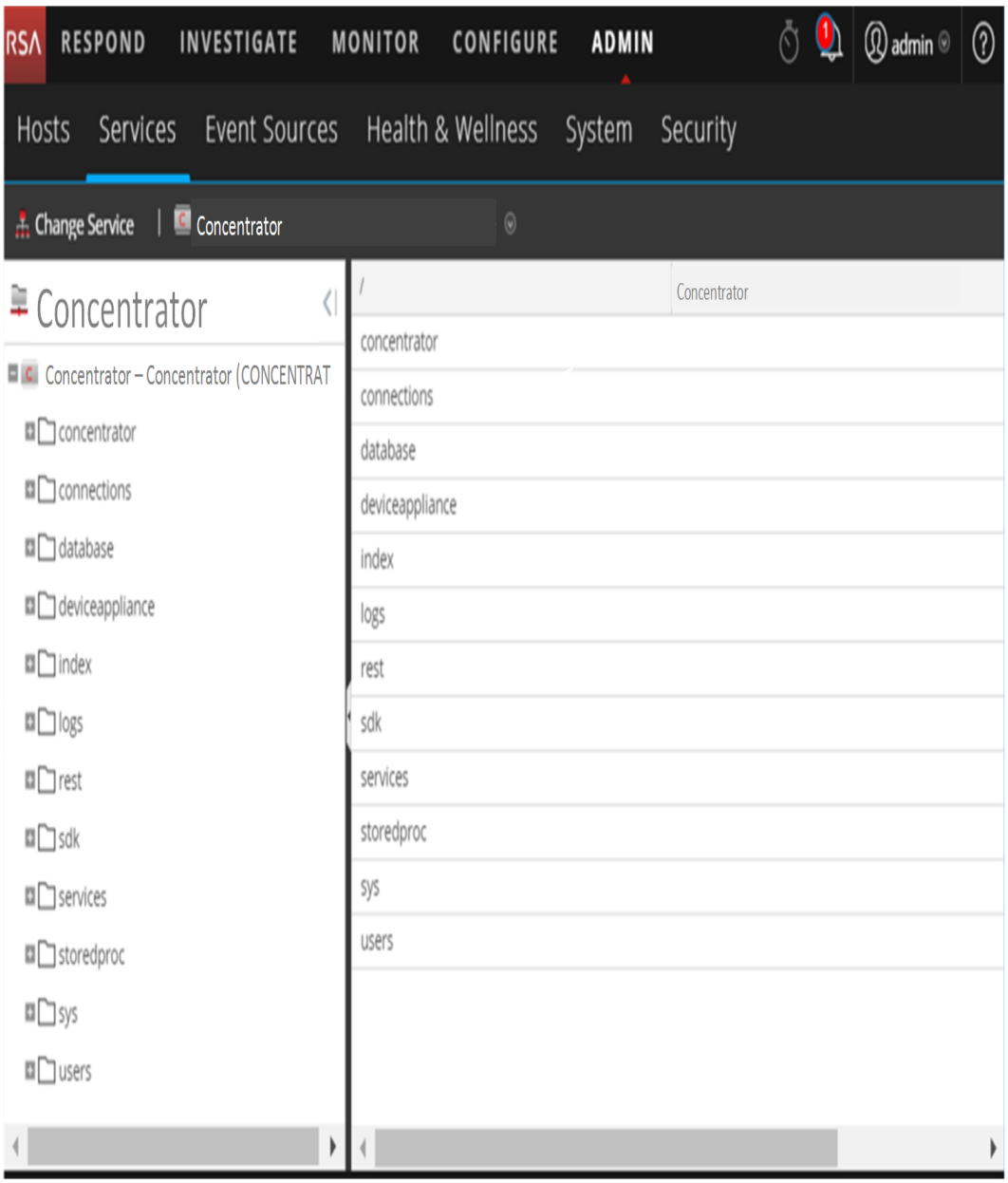
Die Ansicht Durchsuchen zu einem Service ist in zwei Teile unterteilt und bietet Ihnen erweiterten Zugriff auf und Kontrolle über die Servicefunktion. Die Liste „Node“ zeigt die Servicefunktion in einer Baumstruktur der Ordner an. Der Bereich „Monitor“ zeigt die Eigenschaften des Ordners oder der Datei an, der bzw. die in der Liste „Node“ ausgewählt ist.

Jedes der folgenden Verfahren beginnt in der Ansicht „Durchsuchen“.

So navigieren Sie zur Ansicht „Durchsuchen“:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie einen Service und anschließend  **> Ansicht > Durchsuchen** aus.
   Die Ansicht Durchsuchen wird angezeigt. Die Liste „Node“ ist auf der linken Seite und der Bereich

„Monitor“ ist auf der rechten Seite.



ANZEIGEN ODER BEARBEITEN EINER SERVICEEIGENSCHAFT

So zeigen Sie eine Serviceeigenschaft an:

1. Klicken Sie mit der rechten Maustaste auf eine Datei in der Liste Node oder im Bereich Monitor.
2. Klicken Sie auf **Eigenschaften**.

So bearbeiten Sie den Wert einer Serviceeigenschaft:

1. Wählen Sie im Bereich **Monitor** einen bearbeitbaren Eigenschaftswert.
2. Geben Sie einen neuen Wert ein.

SENDEN EINER MELDUNG AN EINEN NODE

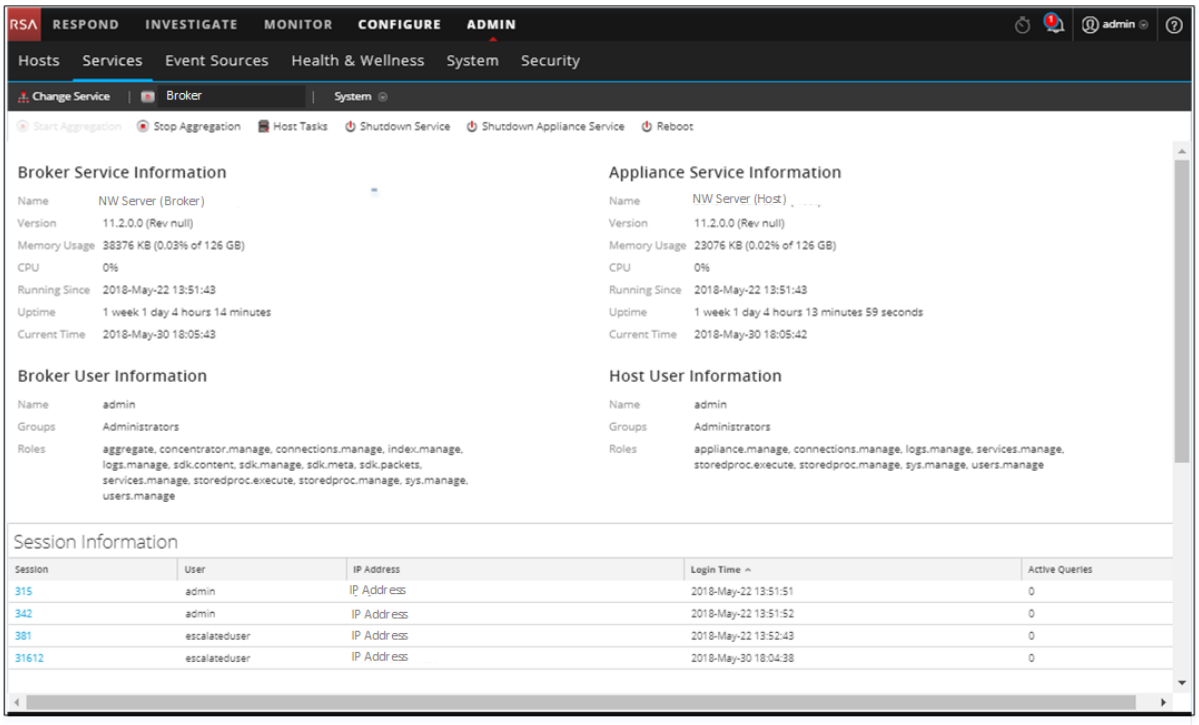
1. Wählen Sie im Dialogfeld „Eigenschaften“ einen **Meldungstyp** aus. Welche Optionen verfügbar sind, hängt von der in der Liste „Node“ ausgewählten Datei ab.
   Im Feld **Hilfe zu Meldungen** wird eine Beschreibung des ausgewählten Meldungstyps angezeigt.
2. (Optional) Geben Sie die **Parameter** ein, falls sie von der Meldung benötigt werden.
3. Klicken Sie auf **Senden**.
   Im Feld **Antwortausgabe** wird der Wert oder das Format angezeigt.

Beenden der Verbindung zu einem Service

Sie können Sitzungen, die in einem Service ausgeführt werden, in der Ansicht „Service-System“ anzeigen. Sie können von der Liste der Sitzungen aus die Sitzungen sowie aktive Abfragen innerhalb einer Sitzung beenden.

Beenden einer Sitzung über einen Service

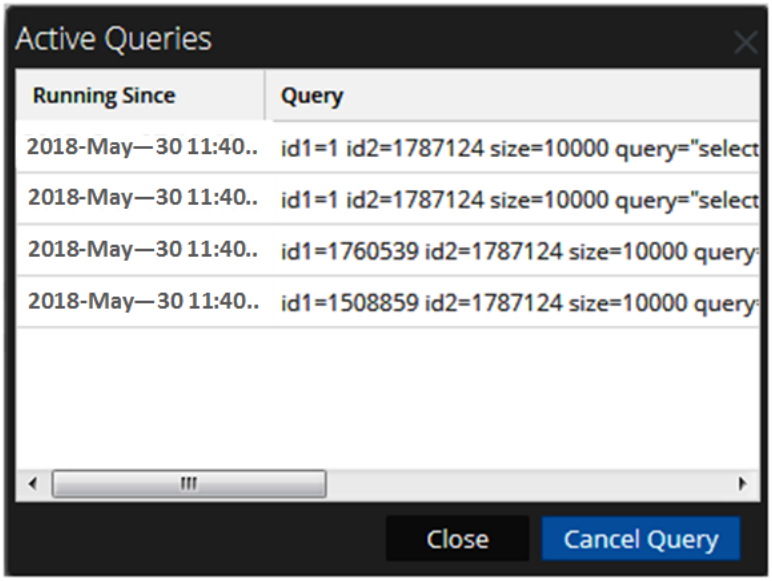
1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
   Die Ansicht „Admin-Services“ wird angezeigt.
2. Wählen Sie einen Service und anschließend  **> Ansicht > System** aus.
   Die Ansicht „Service-System“ wird angezeigt.



3. Klicken Sie im Raster **Sitzungsinformationen** unten auf eine ***Sitzungsnummer***.
   Das Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.

Beenden einer aktiven Abfrage in einer Sitzung

1. Scrollen Sie zu dem Raster **Sitzungen** herunter.
2. Klicken Sie in der Spalte **Aktive Abfragen** auf eine Anzahl aktiver Abfragen einer Sitzung, die größer als null ist. Sie können nicht darauf klicken, wenn es 0 aktive Abfragen gibt.
   Das Dialogfeld „Aktive Abfragen“ wird angezeigt.



3. Wählen Sie eine Abfrage aus und klicken Sie auf **Abfrage abbrechen**.
   Die Abfrage wird abgebrochen und die Spalte Aktive Abfragen wird aktualisiert.

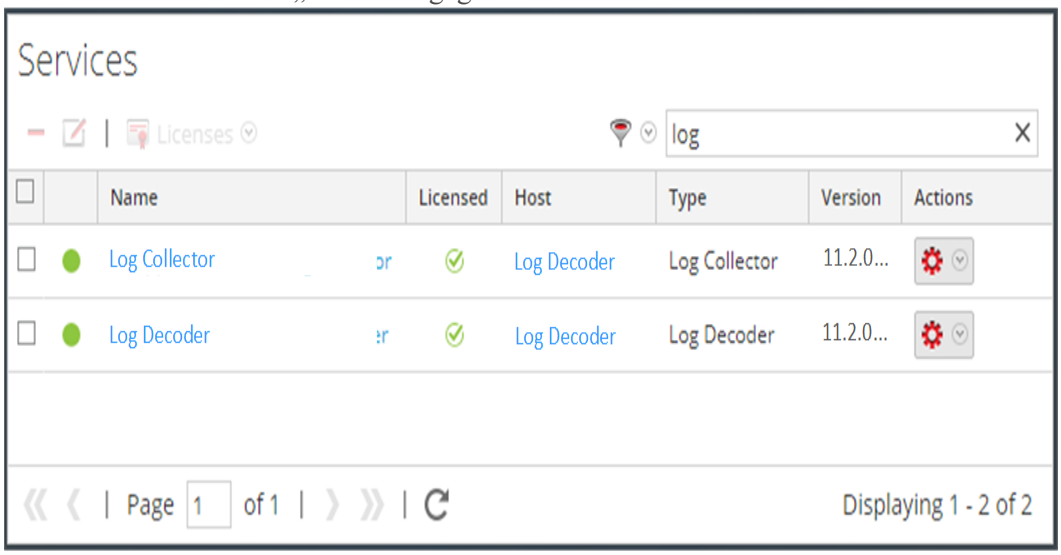
Suchen nach Services

Sie können in der Ansicht „Services“ in der Serviceliste nach den gewünschten Services suchen. Die Ansicht „Services“ ermöglicht es Ihnen, die Liste der Services schnell nach Name, Host und Servicetyp zu filtern. Sie können das Drop-down-Menü „Filtern“ und das Feld „Filtern“ separat oder gleichzeitig verwenden, um die Ansicht „Services“ zu filtern.

Suchen nach einem Service

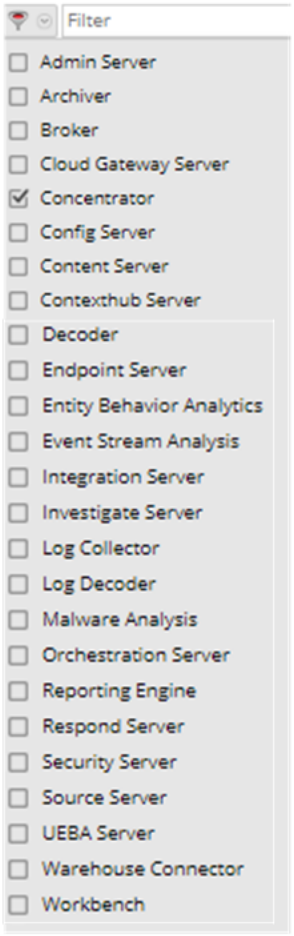
1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Geben Sie in der Symbolleiste des Bereichs **Services** den **Namen** eines Services oder einen **Host** im Feld **Filter** ein.

Im Bereich „Services“ werden die Services aufgelistet, die mit den ins Feld „Filter“ eingegebenen Namen übereinstimmen. Im folgenden Beispiel sind die Suchergebnisse aufgeführt, nachdem das Wort **Protokoll** im Feld „Filter“ eingegeben wurde.

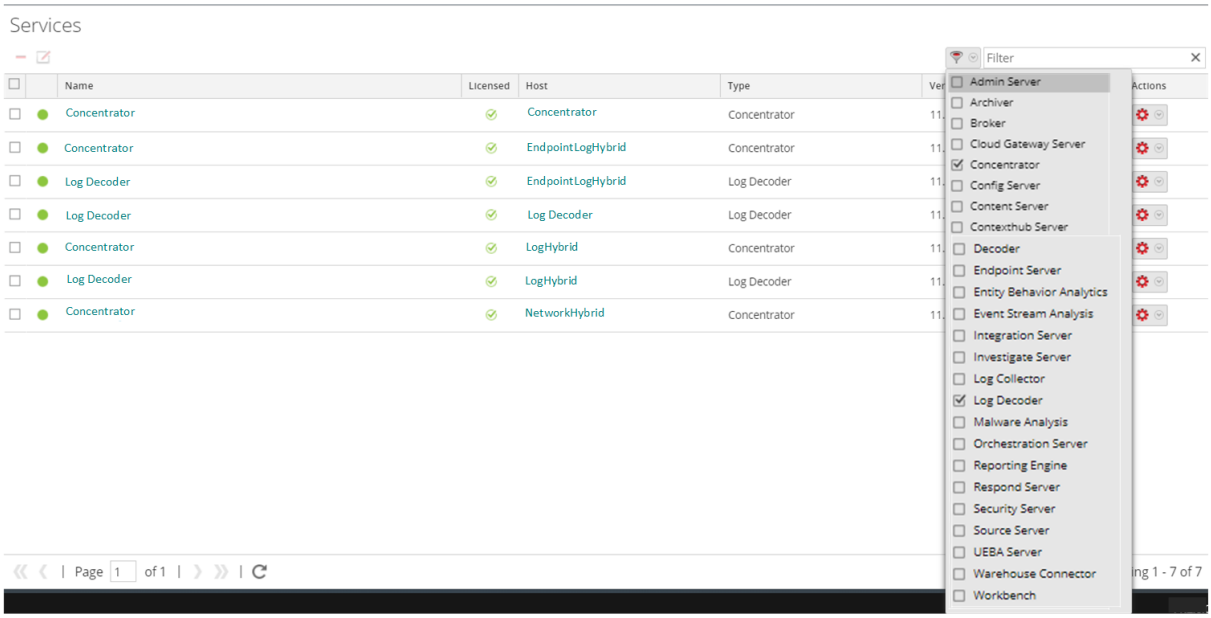


Filtern von Services nach Typ

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Klicken Sie in der Ansicht „Services“ auf und wählen Sie die Servicetypen aus, die in der Ansicht „Services“ angezeigt werden sollen.



Die ausgewählten Servicetypen werden in der Ansicht „Services“ angezeigt. Im folgenden Beispiel ist die Ansicht „Services“ dargestellt, die nach einem Concentrator und einem Log Decoder gefiltert wurde.

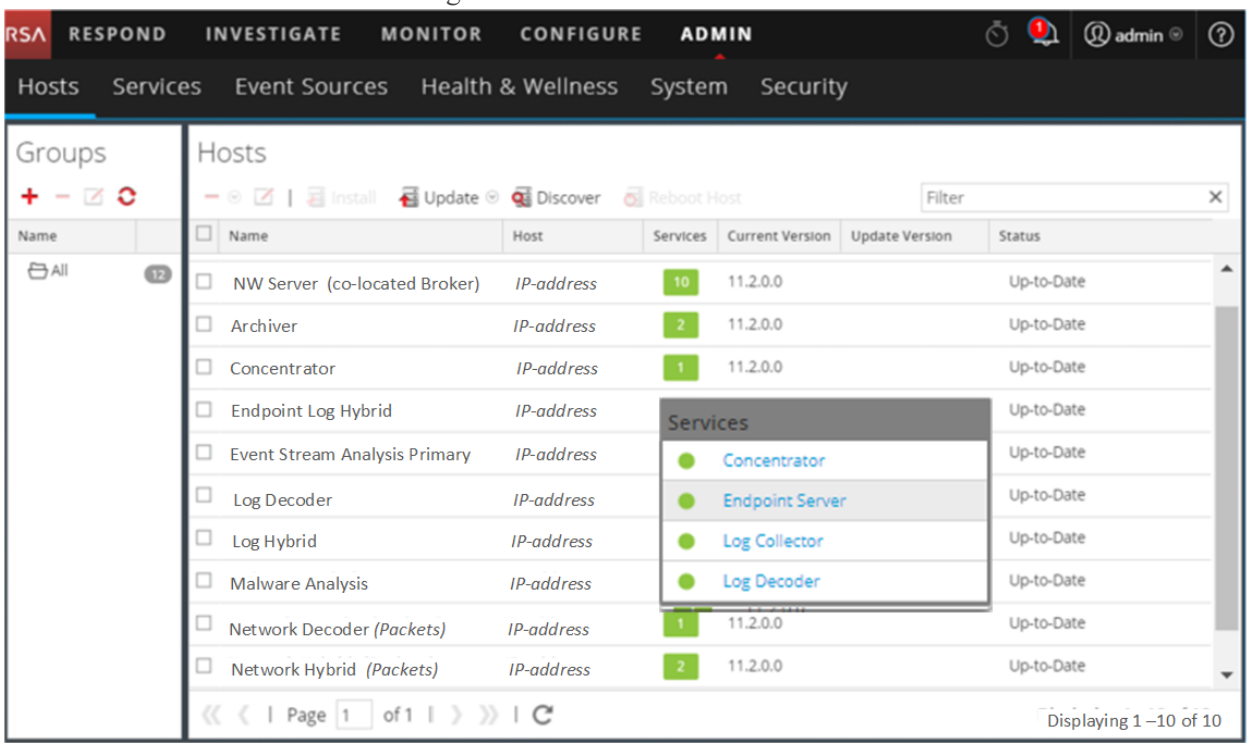


Suchen der Services auf einem Host

Sie können die Services für einen Host nicht nur in der Ansicht Services finden, sondern auch die Services, die auf einem Host ausgeführt werden, schnell in der Ansicht Hostssuchen.

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Hosts**.
2. Wählen Sie in der Ansicht „Hosts“ einen Host aus und klicken Sie in der Spalte **Services** auf das Feld, das eine Zahl enthält (die Anzahl der Services).
   Eine Liste der Services auf dem ausgewählten Host wird angezeigt.

Im folgenden Beispiel wird eine Liste mit vier Services auf dem ausgewählten Host angegeben, nachdem auf das Feld mit der Zahl 4 geklickt wurde.



3. Sie können auf die Servicelinks klicken, um die Services in der Ansicht „Services“ anzuzeigen.

Starten, Beenden oder Neustarten eines Service

Diese Verfahren gelten nur für Core-Services.

Jedes der folgenden Verfahren beginnt in der Services-Ansicht. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.

Starten, Beenden oder Neustarten eines Services

Wählen Sie einen Service aus und klicken Sie auf  **>Starten**.

Beenden eines Services

Wenn Sie einen Service beenden, werden auch alle zugehörigen Prozesse beendet und alle aktiven Benutzer werden vom Service getrennt.

So beenden Sie einen Service:

1. Wählen Sie einen Service aus und klicken Sie auf  > **Beenden**.
2. In einem Dialogfeld werden Sie zur Bestätigung aufgefordert. Um den Service zu beenden, klicken Sie auf **Ja**.

Neustarten eines Services

Gelegentlich müssen Sie einen Service von Neuem starten, damit Änderungen wirksam werden. Wenn Sie einen Parameter ändern, für den ein Neustart erforderlich ist, wird in NetWitness Platform eine Meldung angezeigt.

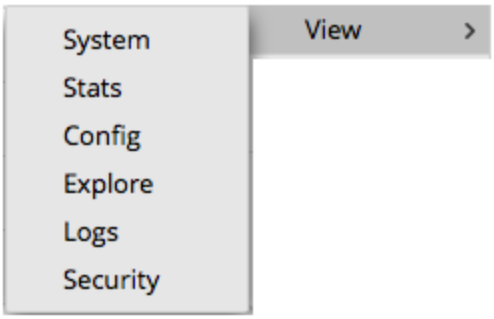
So starten Sie einen Service von Neuem:

1. Wählen Sie einen Service aus und klicken Sie auf  > **Neustart**.
2. In einem Dialogfeld werden Sie zur Bestätigung aufgefordert. Um den Service zu beenden, klicken Sie auf **Ja**.

Der Service wird beendet und startet dann automatisch von Neuem.

Anzeigen von Servicedetails

Sie können Informationen über Services anzeigen und bearbeiten, indem Sie das Menü „Ansicht“ für einen Service aufrufen.



Zweck der einzelnen Serviceansichten

Jede Ansicht zeigt einen funktionalen Bereich eines Services an. Die Ansichten werden in einem eigenen Abschnitt im Detail beschrieben:

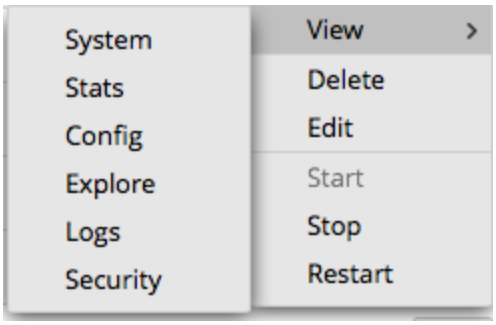
- Die Ansicht „System“ zeigt eine Übersicht der Informationen für Services, Applianceservices, Hostnutzer und Sitzungen an.
- Die Ansicht „Statistik“ bietet die Möglichkeit, Status und Operationen des Services zu überwachen.

- Die Ansicht „Konfiguration“ dient der Konfiguration aller Aspekte eines Services.
- Die Ansicht „Durchsuchen“ dient der Anzeige und Bearbeitung der Host- und Servicekonfigurationen.
- Der Bereich „Systemprotokollierung“ zeigt die Serviceprotokolle an, die Sie durchsuchen können.
- Die Ansicht „Sicherheit“ ermöglicht es, NetWitness Platform Core-Nutzerkonten für Nutzer von Aggregation, Thick-Client und REST-API hinzuzufügen.

Ansicht Zugriff auf einen Service

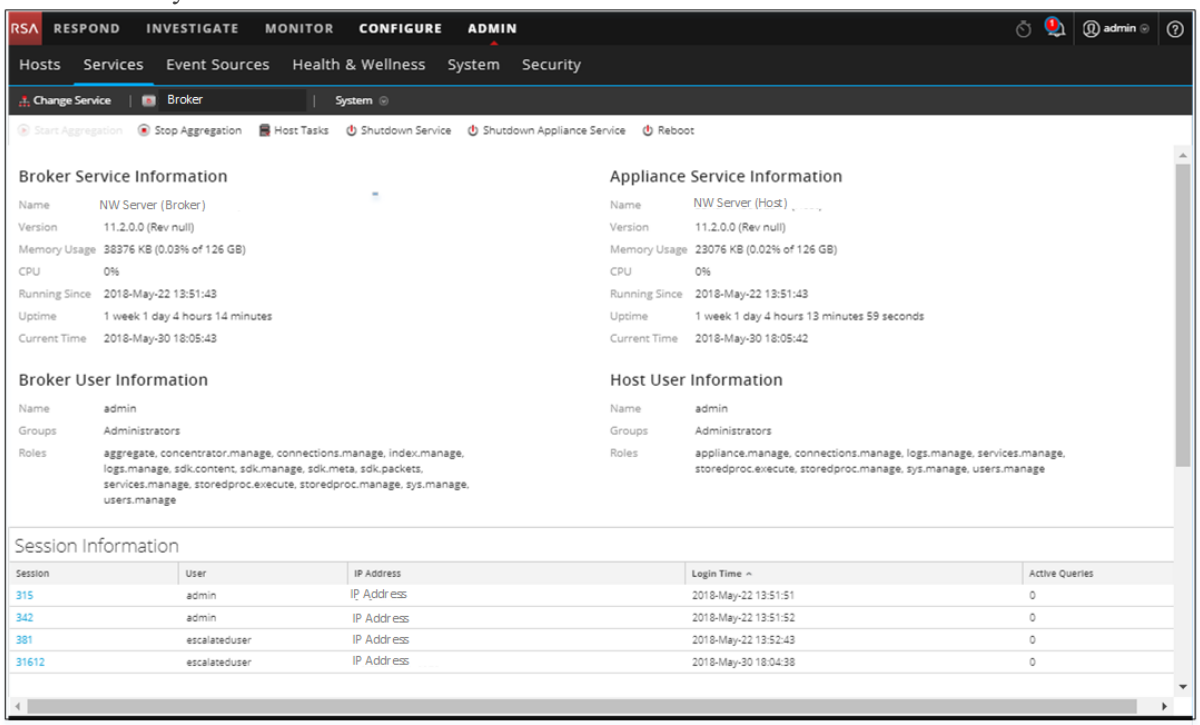
So greifen Sie auf eine Ansicht für einen Service zu:

1. Navigieren Sie in NetWitness Platform zu **ADMIN > Services**.
2. Wählen Sie einen Service aus und klicken Sie auf  **> Ansicht**.
   Das Menü „Ansicht“ wird angezeigt.

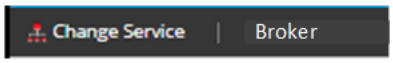


3. Wählen Sie in den Optionen auf der linken Seite eine Ansicht aus.

Dies ist eine Systemansicht für einen Broker.



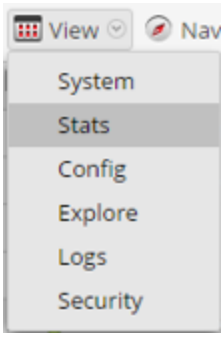
4. Navigieren Sie mithilfe der Symbolleiste:



   a. Klicken Sie auf **Service ändern**, um einen anderen Service auszuwählen.
   Das Dialogfeld **Service verwalten** wird angezeigt.

   b. Aktivieren Sie das Kontrollkästchen links neben dem gewünschten Service.

   c. Wählen Sie die gewünschte Ansicht für den Service aus, den Sie im Drop-down-Menü „Ansicht“ ausgewählt haben.



   Die neue Ansicht (z. B. „Statistik“) für den ausgewählten Service wird angezeigt.

Ansichten für Hosts und Services – Referenzen

Dieses Thema dient als Referenz für Funktionen auf der NetWitness Platform-Benutzeroberfläche für Administratoren.

Im Thema werden die Funktionen beschrieben, die auf der NetWitness Platform-Benutzeroberfläche für Administratoren verfügbar sind. Das Administratormodul zeigt NetWitness Platform-Administrationsaktivitäten in einer zentralen Ansicht an, in der Hosts (Appliances), Services, Aufgaben und die Sicherheit überwacht und verwaltet werden können.

Themen

Ansicht „Hosts“

Die Ansicht **Hosts** ist für die Einrichtung und Wartung der physischen Computer oder virtuellen Maschinen gedacht, auf denen NetWitness Platform-Services ausgeführt werden.

WICHTIG: Hilfe bei der Behebung von Fehlern, die Sie während der Installation und Aktualisierung von Versionen erhalten, finden Sie unter Troubleshooting von Versionsinstallationen und -aktualisierungen.

Ein Service führt eine eindeutige Funktion aus, wie das Sammeln von Protokollen oder Archivieren von Daten. Jeder Service wird auf einem dedizierten Port ausgeführt und ist als Plug-in modelliert, das je nach Funktion des Hosts aktiviert oder deaktiviert wird. Sie müssen die Core-Services zuerst konfigurieren.

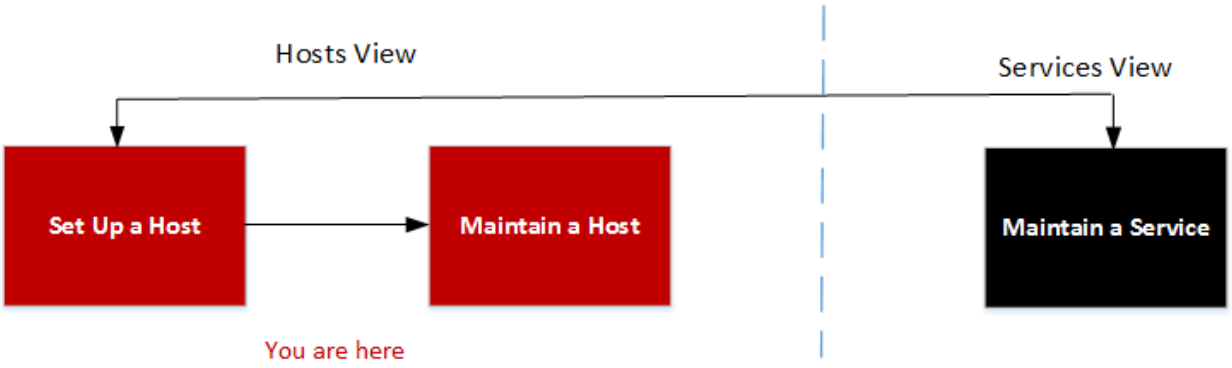
Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Admin	-	-	Wird mit dem NW-Server implementiert.
Archiver	50008	56008	
Broker	50003	56003	Core-Service
Cloud Gateway	–	–	
Concentrator	50005	56005	Core-Service
Konfiguration	–	–	Wird mit dem NW-Server implementiert.
Inhalt	-	-	Wird mit dem NW-Server implementiert.
Context Hub	–	–	
Decoder (Pakete)	50004	56004	Core-Service
Endpoint	-	-	
Entity Behavior Analysis	–	–	
Event Stream Analysis	–	50030	
Integration	–	–	Wird mit dem NW-Server implementiert.
Untersuchen	–	–	Wird mit dem NW-Server implementiert.
Log Collector	50001	56001	

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Log Decoder	50002	56002	Core-Service
Malware Analysis	–	60007	
Orchestrierung	–	–	Wird mit dem NW-Server implementiert.
Reporting Engine	-	51113	Wird mit dem NW-Server implementiert.
Respond	–	–	Wird mit dem NW-Server implementiert.
Sicherheit	–	–	Wird mit dem NW-Server implementiert.
Quelle	-	-	Wird mit dem NW-Server implementiert.
UEBA	-	-	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Sie müssen Hosts und Services für die Kommunikation mit dem Netzwerk und miteinander konfigurieren,damit sie ihre Funktionen wie das Speichern oder Erfassen von Daten durchführen können.

Workflow

Dieser Workflow veranschaulicht die Verfahren zur Einrichtung und Wartung eines Hosts sowie zur Aktualisierung eines Hosts auf neue NetWitness Platform-Versionen. Die Einrichtung eines Hosts ist die erste Aufgabe in diesem Workflow. Die Hosts mit Core-Services sind bereits bei Lieferung eingerichtet. Daneben können Sie zusätzliche Hosts einrichten, um Ihre NetWitness Platform-Bereitstellung zu erweitern. Die anderen beiden Aufgaben (Wartung des Hosts und Aktualisierung des Hosts mit einer neuen Version) werden nach Bedarf ausgeführt. Sie müssen nicht in einer bestimmten Reihenfolge ausgeführt werden.



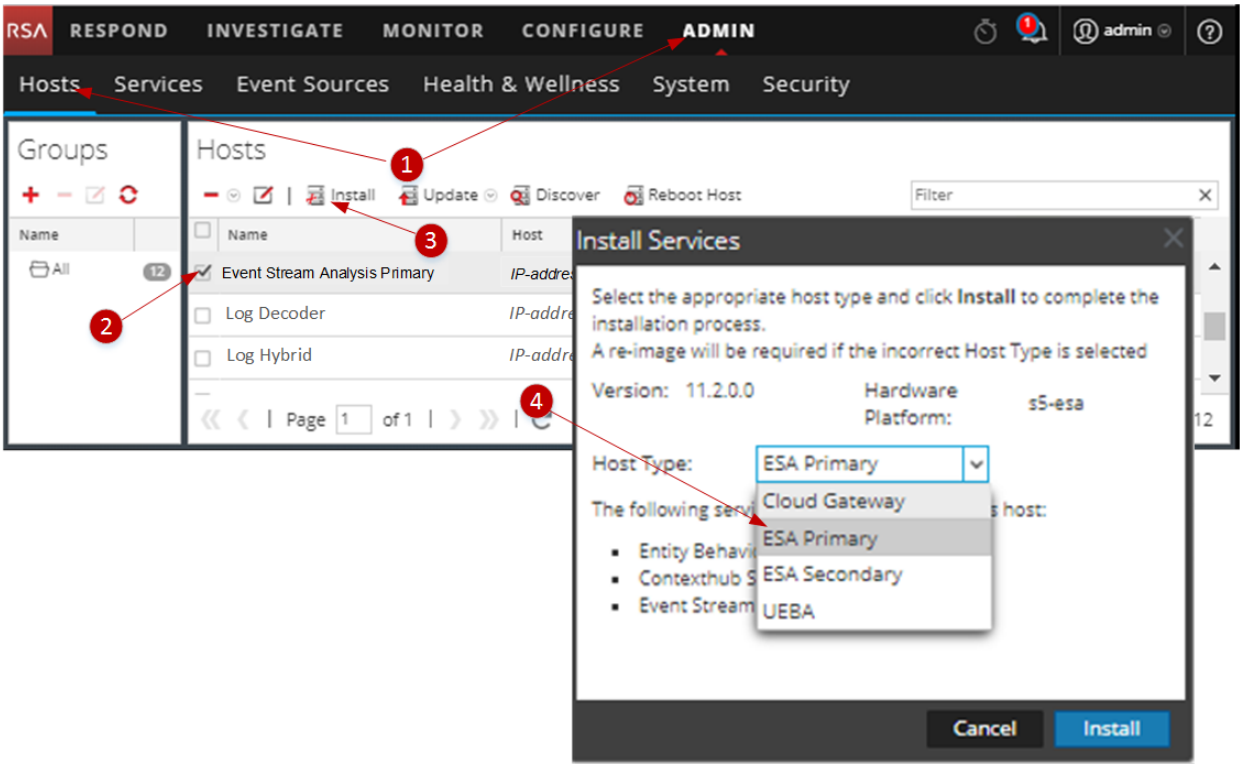
Was möchten Sie tun?

Ausführliche Anweisungen zu den nachfolgend aufgeführten Aufgaben finden Sie im Abschnitt Hosts und Services – Verfahren.

Rolle	Ziel
Administrator	Host einrichten
Administrator	Host warten
Administrator	Anwenden von Versionsaktualisierungen auf einen Host.

*Sie können diese Aufgaben in der aktuellen Ansicht durchführen.

Überblick



Im folgenden Beispiel wird beschrieben, wie Sie einen Host einrichten.

1. Klicken Sie auf „ADMIN“ > „Hosts“.
2. Wählen Sie den Host aus, den Sie bereitgestellt haben (z. B. **Event Stream Analysis Primary**).
3. Klicken Sie auf Install (Installationssymbol).
4. Wählen Sie im Dialogfeld **Services installieren** den Hosttyp aus, den Sie installieren möchten (z. B. **ESA Primary**). Dieser Hosttyp installiert die Services „Entitätsverhaltensanalysen“, „Context Hub“ und „Event Stream Analysis“ auf diesem Host.

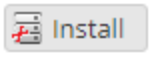
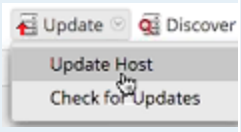
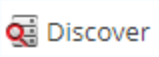
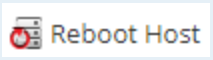
Symbolleiste des Bereichs „Hosts“

Die Symbolleiste der Ansicht „Hosts“ enthält Tools, mit denen Sie die Hosts in Ihrer NetWitness Platform-Bereitstellung verwalten können.

Wählen Sie in NetWitness Platform die Option **Admin** > **Hosts**, um auf die Ansicht „Hosts“ zuzugreifen. Die Symbolleiste des Bereichs „Hosts“ befindet sich oben im Raster „Hosts“ in der Ansicht „Hosts“.

Funktionen

In der folgenden Tabelle sind die Funktionen der Symbolleiste im Bereich „Hosts“ beschrieben.

Funktionen	Beschreibung
	**Aus Gruppe entfernen**: Wenn der Host Teil einer Hostgruppe ist, können Sie den Host aus der Gruppe entfernen.
	Öffnen Sie das Dialogfeld „Host bearbeiten“, in dem Sie eine Host- oder Serviceidentifikation und grundlegende Kommunikationseinstellungen bearbeiten. Dieses Dialogfeld verfügt über dieselben Funktionen wie das Dialogfeld „Host hinzufügen“. Zugehöriges Verfahren: Schritt 1. Bereitstellen eines Hosts
	Es wird das Dialogfeld **Services installieren** geöffnet, über das Sie einen Service auf einem bereitgestellten Host installieren können. Zugehörige Verfahren: Schritt 2. Installieren eines Service auf einem Host
	• **Update**: Aktualisiert den Host bzw. die Hosts, die Sie ausgewählt haben, mit der Version, die Sie in der Spalte **Update-Version** auswählen. • **Nach Updates suchen**: Überprüft das lokale Repository für Aktualisierungen auf die neuesten Updates von RSA. Zugehöriges Verfahren: Anwenden von Versionsaktualisierungen auf einen Host
	In den meisten Fällen wird die Erkennungsfunktion automatisch ausgeführt, ohne dass Sie hierfür auf die Schaltfläche **Erkennen** klicken müssen. Klicken Sie bei einer Neuinstallation auf **Erkennen**, um das Dialogfeld „Bereitstellung“ anzuzeigen und die Bereitstellungsphase abzuschließen. Nach der Bereitstellungsphase wird die Erkennung von auf dem Host ausgeführten Services in NetWitness Platform automatisch durchgeführt und Sie müssen nicht mehr auf diese Schaltfläche klicken. Klicken Sie bei einer Neuinstallation auf **Erkennen**, um das Dialogfeld „Bereitstellung“ anzuzeigen und die Bereitstellungsphase abzuschließen. Nach der Bereitstellungsphase wird die Erkennung von auf dem Host ausgeführten Services in NetWitness Platform automatisch durchgeführt.
	Starten Sie den Host neu.
Filter	Filtert Hosts nach Name oder Host.

Symbolleiste „Gruppenbereich“

Die Symbolleiste des Bereichs Gruppen enthält Optionen zum Managen von Hostgruppen. Verwenden Sie die Symbolleiste, um Gruppen zu erstellen, zu bearbeiten und zu löschen. Nach dem Erstellen einer Gruppe können Sie einzelne Hosts aus dem Bereich „Hosts“ in die Gruppe ziehen.

Verwenden Sie Gruppen, um Hosts nach Funktion, geografischem Standort, Projekt oder einem beliebigen anderen nützlichen Organisationsprinzip zu ordnen. Ein Host kann zu mehreren Gruppen gehören.

Navigieren Sie in NetWitness Platform zu **ADMIN > Hosts**. Die Symbolleiste des Bereichs „Gruppen“ befindet sich in der Ansicht „Hosts“ oben im Raster „Gruppen“.

Im Gruppenbereich können Sie Hosts zu logischen Gruppen zusammenfassen. Durch die Zusammenfassung von Hosts in Gruppen ist es einfacher, Vorgänge auf mehrere Hosts gleichzeitig anzuwenden, da alle Hosts in einer Gruppe gleichzeitig bearbeitet werden. Sie müssen also nicht alle Hosts einer nicht gruppierten Liste einzeln bearbeiten.

Hinweis: In NetWitness Live können Gruppen Ressourcen abonnieren. Einzelne Hosts haben diese Möglichkeit nicht.

Der Bereich „Gruppen“ enthält ein Raster mit der Liste aller definierten Hostgruppen sowie eine eigene Symbolleiste.

Spalte	Beschreibung
	Zeigt eine neue Zeile im Raster „Gruppen“ an, in die Sie den Namen einer neuen Gruppe eingeben können.
	Fordert Sie auf, zu bestätigen, dass Sie die Gruppe oder den Host wirklich löschen möchten. Sie können den Löschvorgang bestätigen oder abbrechen.
	Öffnet das Namensfeld in einer Zeile des Rasters „Gruppen“, sodass Sie einen neuen Namen für eine vorhandene Gruppe eingeben können.
	Aktualisiert die ausgewählte Gruppe.
Name	Der Name der Hostgruppe. Klicken Sie auf den Gruppennamen, um die Hosts in dieser Gruppe im Bereich „Hosts“ anzuzeigen.
<Blank>	Zeigt die Anzahl der Hosts in der Gruppe an. Wenn Sie auf die angegebene Hostanzahl für eine Gruppe klicken, wird im Bereich „Hosts“ eine Liste der Hosts in dieser Gruppe angezeigt.

Ansicht „Services“

NetWitness PlatformServices werden in der Ansicht **Services** verwaltet. In der Ansicht Services können Sie folgende Aufgaben ausführen:

- Schnelle Suche nach einem bestimmten Service oder Servicetyp, z. B. einem Log Decoder oder Warehouse Connector
- Schnelles Aufrufen von Verwaltungsaufgaben über Verknüpfungen
- Hinzufügen, Bearbeiten und Entfernen von Services
- Sortieren der Services nach Name und Host
- Filtern von Services nach Typ und nach Name und Host
- Starten, Beenden oder Neustarten von Services

Ein Service führt eine eindeutige Funktion aus, wie das Sammeln von Protokollen oder Archivieren von Daten. Jeder Service wird auf einem dedizierten Port ausgeführt und ist als Plug-in modelliert, das je nach Funktion des Hosts aktiviert oder deaktiviert wird. Sie müssen die folgenden Core-Services zuerst konfigurieren:

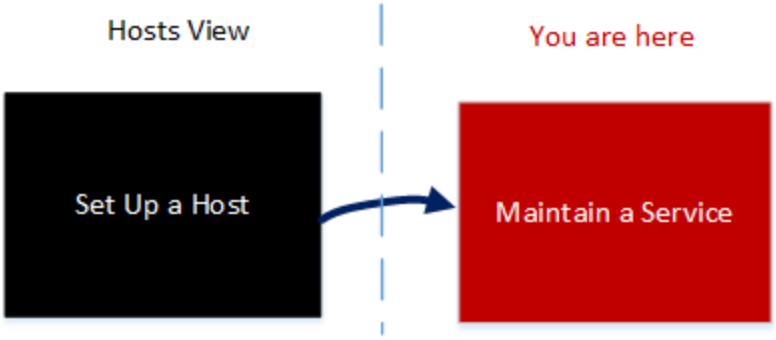
Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Admin	-	-	Wird mit dem NW-Server implementiert.
Archiver	50008	56008	
Broker	50003	56003	Core-Service
Cloud Gateway	–	–	
Concentrator	50005	56005	Core-Service
Konfiguration	–	–	Wird mit dem NW-Server implementiert.
Inhalt	-	-	Wird mit dem NW-Server implementiert.
Context Hub	–	–	
Decoder (Pakete)	50004	56004	Core-Service
Endpoint	-	-	
Entity Behavior Analysis	–	–	
Event Stream Analysis	–	50030	

Service	Unverschlüsselter Nicht-SSL-Port	Verschlüsselter SSL-Port	Anmerkungen
Integration	–	–	Wird mit dem NW-Server implementiert.
Untersuchen	–	–	Wird mit dem NW-Server implementiert.
Log Collector	50001	56001	
Log Decoder	50002	56002	Core-Service
Malware Analysis	–	60007	
Orchestrierung	–	–	Wird mit dem NW-Server implementiert.
Reporting Engine	-	51113	Wird mit dem NW-Server implementiert.
Respond	–	–	Wird mit dem NW-Server implementiert.
Sicherheit	–	–	Wird mit dem NW-Server implementiert.
Quelle	-	-	Wird mit dem NW-Server implementiert.
UEBA	-	-	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Sie müssen Hosts und Services für die Kommunikation mit dem Netzwerk und miteinander konfigurieren,damit sie ihre Funktionen wie das Speichern oder Erfassen von Daten durchführen können.

Workflow

Dieser Workflow zeigt die Verfahren zum Einrichten und Verwalten von einem Service. Hinzufügen eines Services zu einem Host ist die erste Aufgabe bei diesem Workflow. Die Hosts mit Core-Services sind bereits bei Lieferung eingerichtet. Daneben können Sie zusätzliche Services auf Hosts einrichten, um Ihre NetWitness Platform-Bereitstellung zu erweitern.



Was möchten Sie tun?

Ausführliche Anweisungen zu den nachfolgend aufgeführten Aufgaben finden Sie im Abschnitt Hosts und Services – Verfahren.

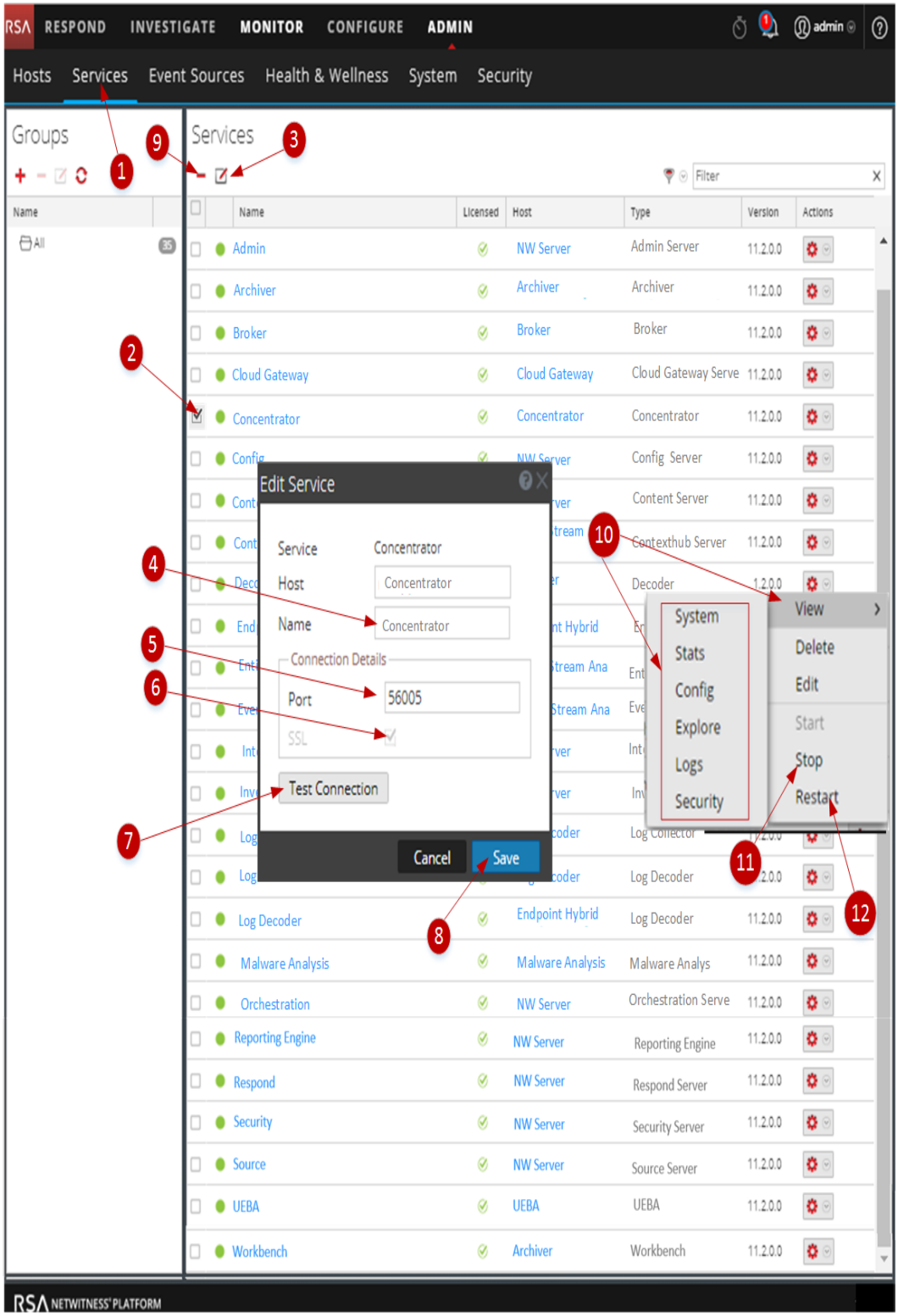
Rolle	Ziel
Administrator	Verwalten eines Service
Administrator	Einrichten eines Hosts

Verwandtes Thema

- Troubleshooting von Versionsinstallationen und -aktualisierungen

Überblick

Im folgenden Beispiel wird beschrieben, wie Sie einen Host verwalten.



Wählen Sie einen Service.

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Klicken Sie auf das Kontrollkästchen links neben dem Service, den Sie auswählen möchten.

Bearbeiten Sie den Namen und die Verbindung des Service.

3. Klicken Sie auf (oder wählen Sie alternativ „Bearbeiten“ unter  (Drop-down-Menü „Aktion“) aus.
4. Bearbeiten Sie den **Hostnamen** .
5. Bearbeiten Sie die **Portnummer**.
6. Aktivieren oder deaktivieren Sie die SSL-Kommunikationsverbindung.
7. Klicken Sie auf **Verbindung testen**.
8. Klicken Sie auf „Speichern“.

Löschen eines Services.

9. **Wählen Sie einen Service** aus und klicken Sie auf das Löschsymbol.

Servicestatistiken anzeigen und Parameter konfigurieren

10. Führen Sie die folgenden Schritte aus, um Servicestatistiken anzeigen und einen Serviceparameter zu konfigurieren.
    a. **Wählen Sie einen Service** aus und klicken Sie auf das Löschsymbol.
    b. Klicken Sie auf **Ansicht** und wählen Sie:
    - **System**, um:
      - Aktuelle allgemeine Informationen über den Service und den Host anzuzeigen.
      - Auf die Symbolleiste der Ansicht „System“ zuzugreifen.
    - **Statistik** zum Anzeigen von detaillierten Servicestatistiken aufzurufen.
    - **Konfigurieren** zum Anzeigen und Konfigurieren von Serviceparametern aufzurufen.
    - **Durchsuchen** zum Anzeigen und Konfigurieren von Serviceparametern in der NetWitness Platform Ansicht Durchsuchen aufzurufen.
    - **Protokolle** zum Anzeigen von Protokollmeldungen des Service aufzurufen.
11. **Wählen Sie einen Service**, klicken Sie auf das Symbol „Aktionen“ und klicken Sie auf **Beenden** eines gerade ausgeführten Service.
12. **Wählen Sie einen Service**, klicken Sie auf das Symbol „Aktionen“ und klicken Sie auf **Neu starten**, um einen beendeten Service neu zu starten.

Themen

Finden Sie in den folgenden RSA NetWitness Platform-Leitfäden detaillierte Informationen zu einzelnen Services. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Konfigurationsleitfaden Archiver

Konfigurationsleitfaden für Broker und Concentrator

Cloud Behavioral Analytics Gateway – Konfigurationsleitfaden

Context-Hub-Konfigurationsleitfaden

Konfigurationsleitfaden für Decoder und Log Decoder

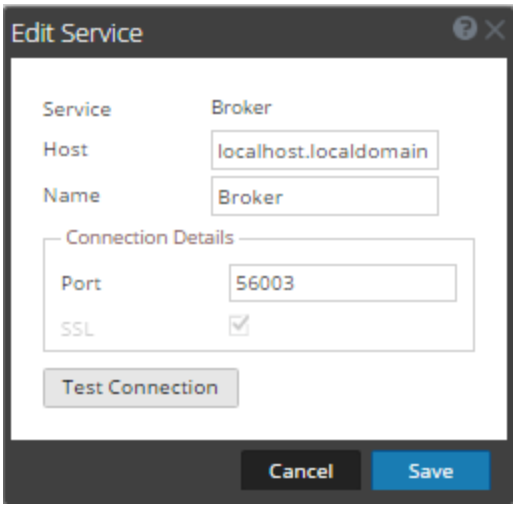
Endpoint Insights – Konfigurationsleitfaden
Konfigurationsleitfaden für Event Stream Analysis (ESA)
Ermittlung und Malware-Analyse – Benutzerhandbuch
Protokollsammlung-Konfigurationsleitfaden
Konfigurationsleitfaden Malware Analysis
Reporting Engine – Benutzerhandbuch
Respond – Konfigurationsleitfaden
RSA NetWitness UEBA – Benutzerhandbuch
Konfigurationsleitfaden Workbench
Warehouse Connector – Konfigurationsleitfaden

Dialogfeld „Service bearbeiten“

In diesem Thema wird das Dialogfeld „Service bearbeiten“ beschrieben, auf das über die Ansicht „Administrationsservices“ („Administration > Services“) zugegriffen werden kann.

NetWitness Platform-Services werden in NetWitness Platform automatisch erkannt.

Sie können das Dialogfeld „Service bearbeiten“ verwenden, um Services zu ändern. Um auf das Dialogfeld „Service bearbeiten“ zuzugreifen, navigieren Sie zu **Administration > Services** und klicken Sie auf in der Symbolleiste des Bereichs **Services**.



Verfahren im Zusammenhang mit Services sind unter Hosts und Services – Verfahren beschrieben.

Funktionen

In dieser Tabelle werden die Funktionen des Dialogfelds Service hinzufügen bzw. Service bearbeiten beschrieben.

Feld oder Option	Beschreibung
Service	Zeigt den Servicetyp an. Sie können die folgenden Services hinzufügen: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector und Workbench.
Host	Gibt den Host an, auf dem sich der Service befindet.
Name	Gibt den Namen an, mit dem der Service identifiziert wird; z. B. **Broker**. Eine verständliche Benennungskonvention kann administrative Aufgaben vereinfachen. Einige Administratoren finden es praktisch, den Hostnamen oder die IP-Adresse (angegeben im Feld **Host**) auch für das Feld **Name** zu verwenden.

Feld oder Option	Beschreibung
Port	Gibt den Port an, der zur Kommunikation mit diesem Service verwendet wird. Hier ist automatisch der Standardport für den im Feld **Service** ausgefüllten Servicetyp eingetragen. Wenn Sie darunter **SSL** aktivieren, wird dieser Port zu einem SSL-Port. Wenn Sie **SSL** deaktivieren, ist der Port kein SSL-Port. Sie können diesen Port anpassen, indem Sie eine Firewall für den Port öffnen, den Sie hinzufügen. Weitere Informationen über Ports finden Sie unter **Netzwerkarchitektur und Ports** im *Leitfaden zur Bereitstellung*.
SSL	Gibt an, dass NetWitness Platformzur Kommunikation mit diesem Service SSL verwendet.
Nutzername	Gibt den Nutzernamen zur Anmeldung bei diesem Service an. Der Standardbenutzername lautet **admin**.
Password	Gibt das Passwort zur Anmeldung bei diesem Service an. Das Standardpasswort ist **netwitness**.
Verbindung testen	Testet die Verbindung eines Service, den Sie hinzufügen.
Abbrechen	Schließt das Dialogfeld „Service hinzufügen“ oder „Service bearbeiten“. Wenn Sie den Service vor dem Schließen des Dialogfelds nicht speichern, wird er nicht hinzugefügt oder bearbeitet.
Speichern	Speichert den neuen Service.

Symbolleiste „Gruppenbereich“

In diesem Thema werden die Funktionen und Optionen unter **Administration > Services** > Symbolleiste im Bereich **Gruppen** beschrieben.

Die Symbolleiste des Bereichs „Gruppen“ enthält Optionen zum Managen von Servicegruppen. Die Symbolleiste umfasst Optionen für das Erstellen, Bearbeiten und Löschen von Gruppen. Sobald Gruppen erstellt wurden, können Sie einzelne Services aus dem Bereich „Services“ in eine Gruppe ziehen.

Gruppen können funktionale, geografische, projektorientierte oder beliebige andere hilfreiche Unternehmensprinzipien widerspiegeln. Ein Service kann zu mehreren Gruppen gehören.

Gehen Sie zum Zugreifen auf die Ansicht „Services“ in **NetWitness Platform** zu **Administration > Services**. Die Symbolleiste des Bereichs „Gruppen“ befindet sich oben im Raster „Gruppen“ in der Ansicht „Services“.

Funktionen

In dieser Tabelle werden Symbolleistenfunktionen beschrieben.

Option	Beschreibung
	Zeigt eine neue Zeile im Gruppenraster an, in die Sie den Namen einer neuen Gruppe eingeben können.
	Zeigt eine Bestätigungsmeldung zum Löschen der Gruppe oder des Services an. Sie können den Löschvorgang bestätigen oder abbrechen.
	Öffnet das Namensfeld in einer Zeile des Rasters „Gruppen“, sodass Sie einen neuen Namen für eine vorhandene Gruppe eingeben können.
	Aktualisiert die ausgewählte Gruppe.

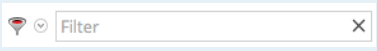
Symbolleiste „Servicebereich“

In diesem Thema werden die Optionen in der Symbolleiste des Bereichs „Services“ zum Hinzufügen, Entfernen, Bearbeiten und Lizenzieren von Services erläutert. Sie können die im Servicebereich aufgeführten Services auch filtern.

Navigieren Sie zum Zugreifen auf die Ansicht „Services“ in **NetWitness Platform** zu **Administration > Services**. Die Symbolleiste des Bereichs „Services“ befindet sich oben im Raster „Services“ in der Ansicht „Services“.

Funktionen

In der Tabelle werden die Funktionen der Symbolleiste des Servicebereichs beschrieben.

Funktion	Beschreibung
	Fügt einen Service für diese zu managende RSA NetWitness Platform-Instanz hinzu (siehe Schritt 2. Installieren eines Service auf einem Host).
	Löscht einen Service aus dieser NetWitness Platform-Instanz (siehe Bearbeiten oder Löschen eines Services).
	Bearbeitet die Serviceidentifikation und grundlegende Kommunikationseinstellungen.
	Filtert die in der Ansicht „Services“ aufgelisteten Services. Im Drop-down-Menü Filtern können Sie die Services nach einem oder mehreren ausgewählten Servicetypen filtern. Wenn Sie in diesem Beispiel Concentrator und Decoder auswählen, werden in der Serviceansicht nur die Concentrator- und Decoder-Services angezeigt. Im Feld Filtern können Sie die Services nach Name und Host filtern. Das Drop-down-Menü Filtern und das Feld Filtern können gleichzeitig verwendet werden, um die in der Serviceansicht aufgelisteten Services zu filtern.

Ansicht „Servicekonfiguration“

Dieses Thema enthält eine Einführung in die Funktionen der Ansicht „Service-Konfiguration“.

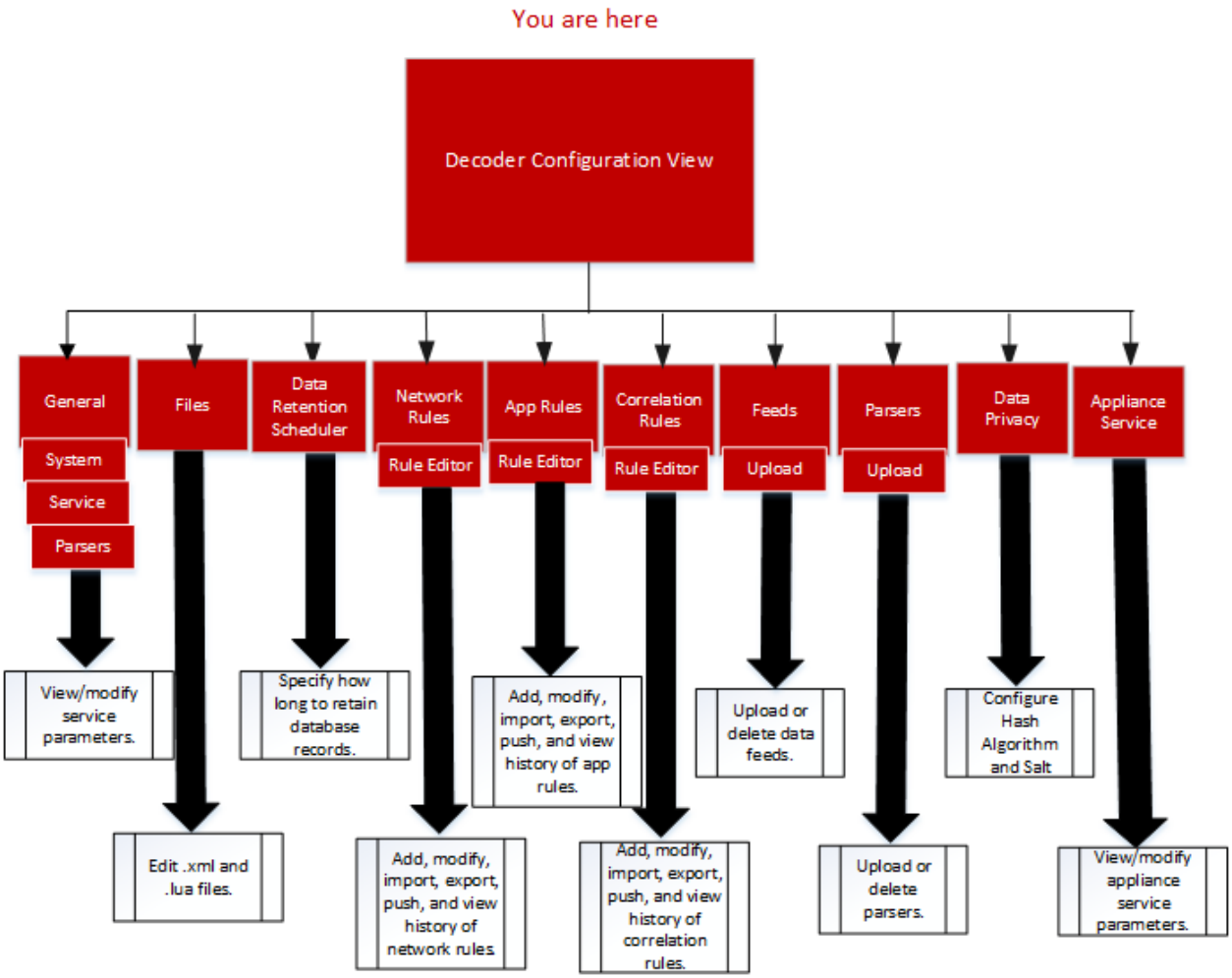
Die Ansicht „Services > Konfiguration“ ist eine der Ansichten, die in der Ansicht **Services** über das Menü „Aktionen“ () verfügbar ist. Sie bietet eine Benutzeroberfläche für die Konfiguration aller Aspekte eines Core-Service oder eines NetWitness Platform-Service.

Die Konfigurationsoptionen in der Ansicht „Service-Konfiguration“ sind in Registerkarten organisiert. Jede Registerkarte enthält eine Ansicht verschiedener zusammenhängender Parameter. Anders als die Ansicht Durchsuchen zu einem Service, in der Sie direkten Zugriff auf alle Konfigurationsdateien für einen Service haben, enthalten diese Registerkarten die am häufigsten geänderten Parameter der Servicekonfiguration in einer benutzerfreundlichen Darstellung.

Aufgrund der Konfigurationsanforderungen der unterschiedlichen Services, unterscheiden sich die verfügbaren Registerkarten und Konfigurationsparameter in dieser Ansicht je nach Servicetyp. Einzelne Themen beschreiben die hostspezifischen (Broker und Concentrators, Decoder und Log Decoder) oder servicespezifischen (z. B. Reporting Engine, IPDB Extractor, Log Collector und Warehouse Connector) Konfigurationsparameter.

Workflows

Der folgende Workflow zeigt die Konfigurationsaufgaben für den Decoder-Service als Beispiel. Weitere Informationen zu den Ansichten **Administration > Services > Konfiguration** der Services finden Sie in den Konfigurationsleitfäden der einzelnen Services (z. B. *RSA NetWitness® PlatformBroker- und Concentrator-Konfigurationsleitfaden*).



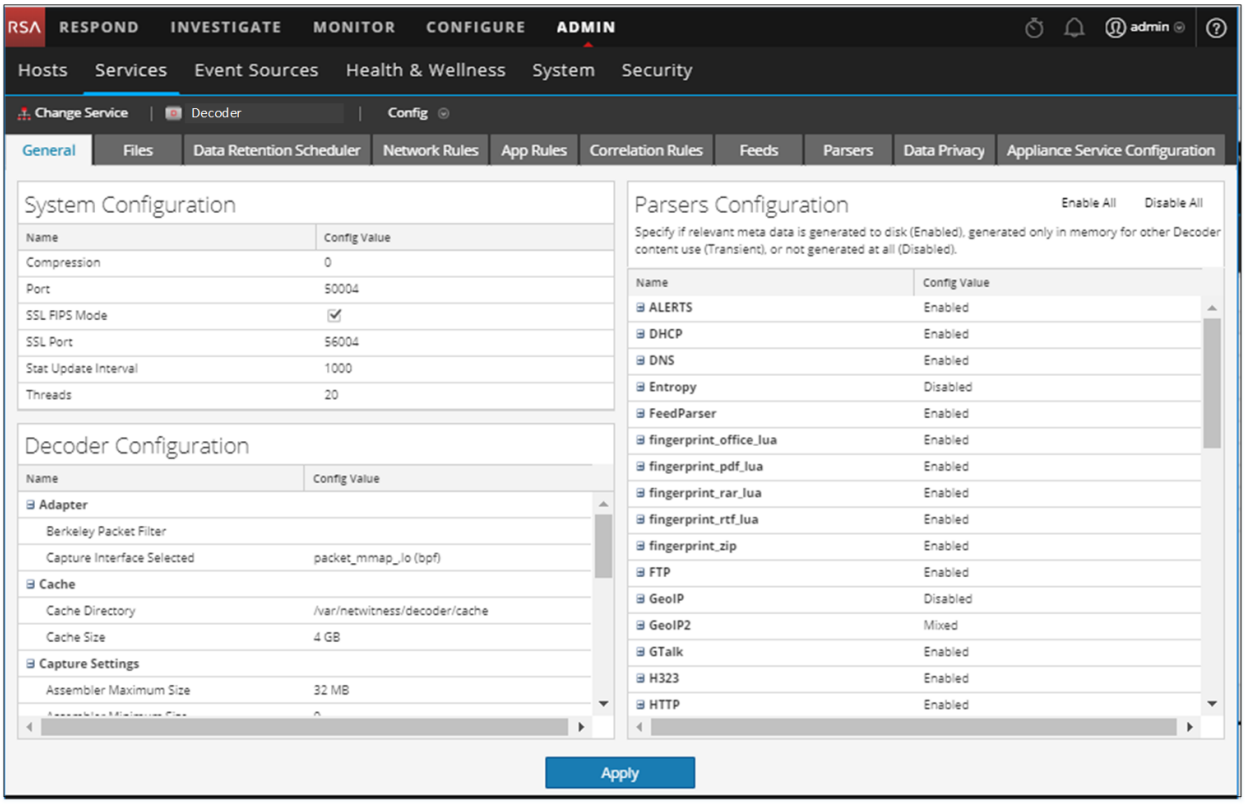
So greifen Sie auf die Ansicht „Service-Konfiguration“ zu:

1. Navigieren Sie zu **NetWitness Platform**ADMINISTRATION > Services.
   Die Ansicht „Administration > Services“ wird angezeigt.

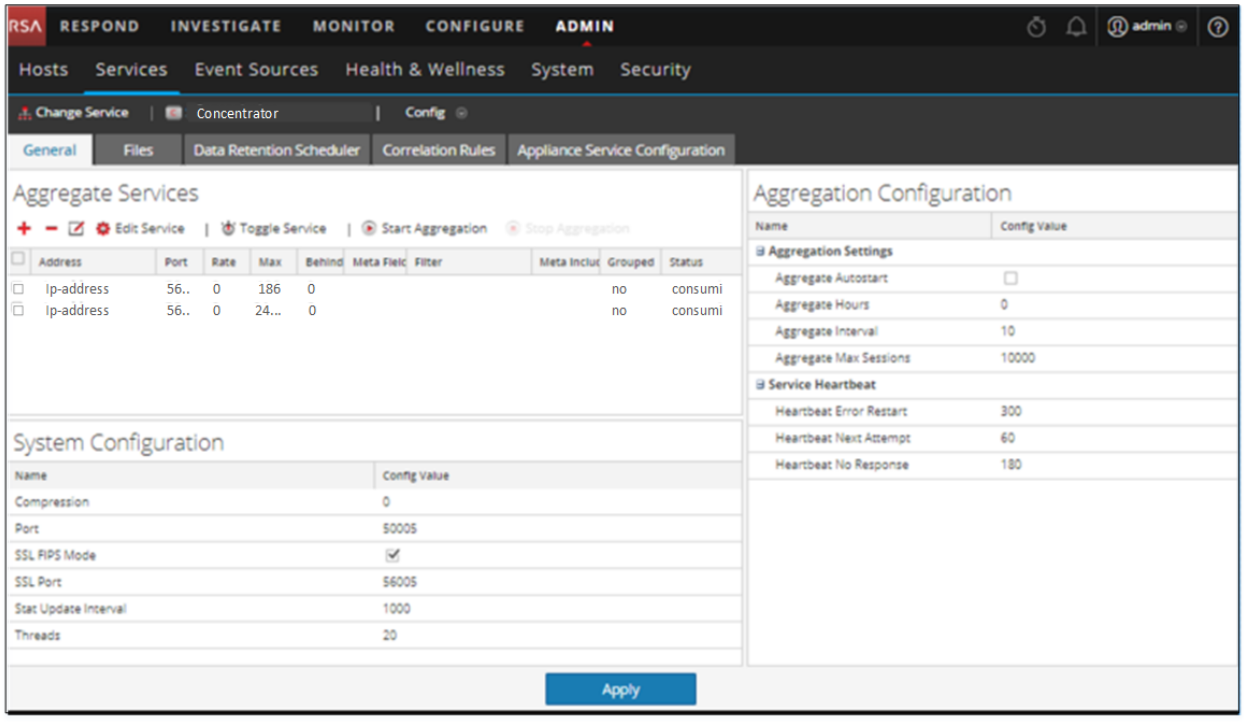
2. Wählen Sie einen Service und dann  **>Ansicht > Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ für den ausgewählten Service wird angezeigt.

Überblick

Hier ein Beispiel für die Ansicht „Service-Konfiguration“ für einen Decoder.



Dieses Beispiel zeigt die Ansicht „Service-Konfiguration“ für einen Concentrator.



Themen

Registerkarte „Appliance-Servicekonfiguration“

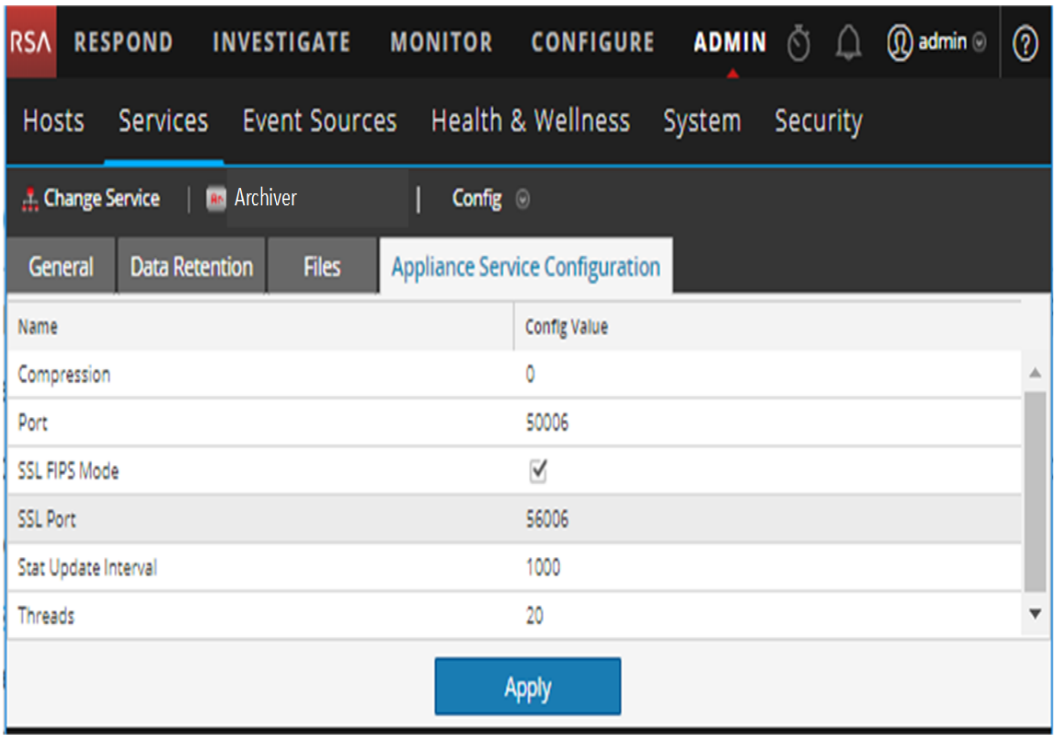
In diesem Thema werden die verfügbaren Konfigurationsparameter für den NetWitness Platform Core Appliance-Service aufgelistet und beschrieben. Der NetWitness Platform Core Appliance-Service bietet Hardwareüberwachung auf Legacy-NetWitness-Hardware.

Die Ansicht Konfiguration für Archiver, Broker, Concentrator, IPDB Extractor, Decoder, Log Collector- oder Log Decoder-Service verfügt über eine Registerkarte „Appliance-Servicekonfiguration“.

Wählen Sie die Registerkarte „Appliance-Servicekonfiguration“ aus.

1. Navigieren Sie zu **NetWitness Platform**ADMINISTRATION > Services.
   Die Ansicht „Administration > Services“ wird angezeigt.
2. Wählen Sie einen Service und dann  **>Ansicht > Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ für den Archiver-Service wird angezeigt.
3. Klicken Sie auf die Registerkarte **Appliance-Servicekonfiguration**.

Im folgenden Beispiel ist die Registerkarte „Appliance-Servicekonfiguration“ für einen Archiver gezeigt.



Name	Beschreibung des Konfigurationswerts	Wann die Änderungen wirksam werden
Komprimierung	Komprimiert eine Meldung, wenn die positive Zahl (in Byte), die Sie angegeben haben, erreicht wird.	Das nächste Mal, wenn Sie sich bei diesem Service anmelden.
Port	Unverschlüsselter Überwachungsport. **0** gibt an, dass der Port deaktiviert ist.	Nach dem Neustart des Services.
SSL FIPS-Modus	Einer der Parameter, die Sie aktivieren oder deaktivieren müssen, ist Federal Information Processing Standards (FIPS). Detaillierte Anweisungen finden Sie unter „Aktivieren oder Deaktivieren von FIPS“ im *RSA NetWitness® Platform Leitfaden Systemwartung*.	Nach dem Neustart des Services.
SSL-Port	Überwachungsport SSL (Secure Sockets Layer). **0** gibt an, dass der Port deaktiviert ist. SSL ist die Standard-Sicherheitstechnologie für den Aufbau eines verschlüsselten Links zwischen einem Webserver und einem Browser. Dieser Link gewährleistet, dass zwischen dem Webserver und dem Browser ausgetauschten Daten geschützt und unangetastet bleiben.	Nach dem Neustart des Services.
Statistikaktualisierungsintervall	Wie oft (in Millisekunden) aktualisiert das System die Statistik-Nodes zum Überwachen von Integrität und Zustand.	Sofort.
Threads	Threads im Thread-Pool, die verwendet werden, um Anforderungen zu verarbeiten. Der **Threads**-Parameter arbeitet mit dem **Polling-Intervall**-Parameter für Ereignis- und Protokoll-Threads.	Sofort.

Thema

Appliance-Servicekonfiguration

Registerkarte „Datenaufbewahrungsplaner“

In diesem Thema werden die konfigurierbaren Optionen auf der Registerkarte „Datenaufbewahrungsplaner“ für Decoder, Log Decoder und Concentrator beschrieben.

Auf der Registerkarte „Datenaufbewahrungsplaner“ können Sie die Kriterien für das Entfernen von Datenbankdatensätzen aus dem primären Speicher für die Services Decoder, Log Decoder und Concentrator festlegen sowie die Zeitpunkte für die Überprüfung des Schwellenwerts planen.

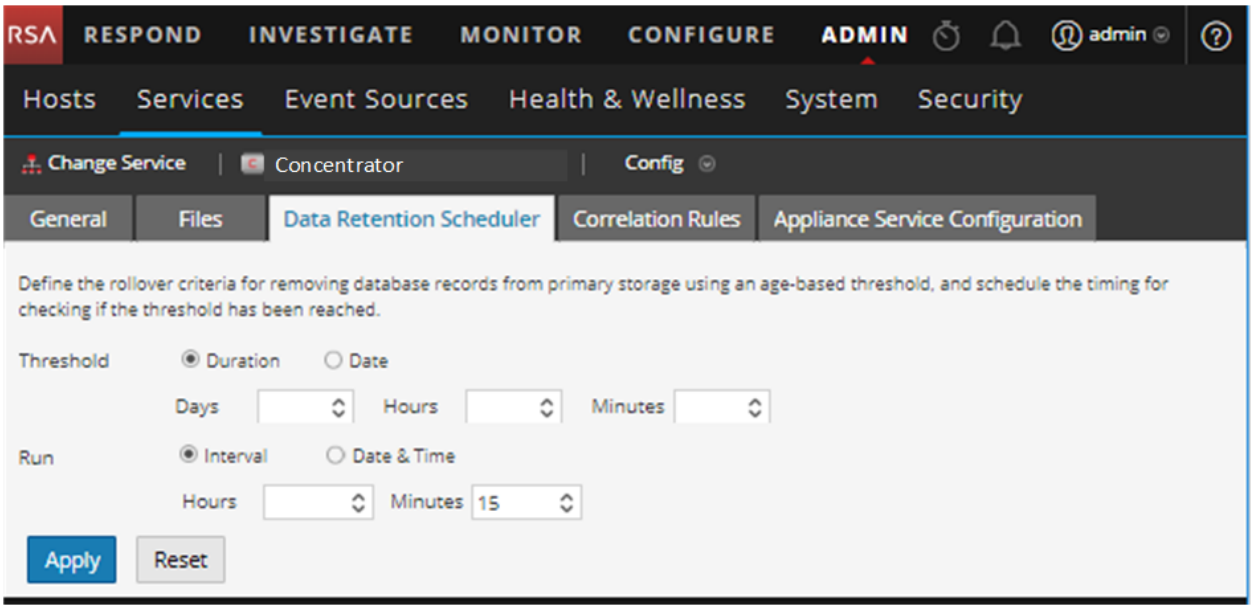
Informationen zur Registerkarte „Datenaufbewahrung“ für Archiver finden Sie unter **Registerkarte „Datenaufbewahrung“ – Archiver** im *Konfigurationsleitfaden Archiver*.

Hinweis: Sollte eine weitere Anpassung erforderlich sein, verwenden Sie den Planer in der Registerkarte „Dateien“ in der Ansicht „Service-Konfiguration“. Wenn zum Beispiel für die Speicherung der RAW-Daten Speicher zur Verfügung steht, für die Metadaten jedoch nicht, verwenden Sie als Schwellenwert die Kapazität und legen Sie für jede Datenbank (Meta- versus Paketdatenbank) unterschiedliche Schwellenwerte fest.

So greifen Sie auf die Registerkarte „Datenaufbewahrungsplaner“ zu:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Decoder, Log Decoder oder Concentrator und dann  Ansicht **Konfiguration** aus.
3. Klicken Sie in der Ansicht **Services > Konfiguration** des Services auf die Registerkarte **Datenaufbewahrungsplaner**.

In der folgenden Abbildung sind die Parameter der Registerkarte „Datenaufbewahrungsplaner“ für einen Concentrator dargestellt.



Funktionen

Die Registerkarte „Datenaufbewahrungsplaner“ enthält Abschnitte für die Angabe der Einstellungen für den Schwellenwert und die Ausführung. In der folgenden Tabelle sind die für die Konfiguration der Datenaufbewahrung unterstützten Parameter aufgeführt.

Parameter	Beschreibung
Schwellenwert	Der Schwellenwert basiert auf dem Alter, der Speicherdauer oder dem Speicherdatum der Daten. Die Daten stammen nicht aus der aktuellen Sitzungszeit, sondern aus der Datenbankdatei. • **Dauer**: Die Zeitdauer, für die Daten vor dem Entfernen gespeichert werden können. Gibt die Anzahl von Tagen (maximal 365), Stunden (maximal 24) und Minuten (maximal 60) an, die seit dem Zeitstempel der Daten vergangen sind. • **Datum**: Das Entfernen der Daten auf der Grundlage des Zeitstempels Gibt Kalendertag und Uhrzeit in den Feldern **Kalender** und **Zeit** an.
Ausführen	Der Ausführungsplan für die Überprüfung der Rollover-Kriterien • **Intervall**: Hier können Sie ein bestimmtes Intervall für die Datenbankprüfung angeben. Gibt die **Stunden** und **Minuten** zwischen den geplanten Prüfvorgängen an. • **Datum und Uhrzeit**: Hier können Sie einen bestimmten Tag und eine bestimmte Uhrzeit für die Ausführung der Datenbankprüfung angeben. Gibt den Tag aus der Drop-down-Liste und die Systemzeit im Format `hh:mm:ss` an. Mögliche Werte für „Tag“ sind **Täglich**, **Wochentags**, **Wochenenden** und **Nutzerdefiniert**, wobei unter **Nutzerdefiniert** ein oder mehrere Wochentage ausgewählt werden können.
Anwenden	Überschreibt etwaige vorhandene Pläne für diesen Service und wendet die neuen Einstellungen sofort an. **Achtung:** Nachdem Sie diese Einstellungen angewendet haben, löscht das System nach Erreichen des Schwellenwerts die alten Daten aus der Datenbank und Sie können nicht mehr darauf zugreifen.
Zurücksetzen	Setzt den Planer auf den zuletzt angewendeten Status zurück.

Registerkarte Dateien

In diesem Thema werden die Servicekonfigurationsdateien beschrieben, die in der Ansicht „Service-Konfiguration“ auf der Registerkarte „Dateien“ angezeigt werden.

Verwenden Sie die Registerkarte „Dateien“ in der Ansicht „Service-Konfiguration“, um Servicekonfigurationsdateien für Decoder, Log Decoder, Broker, Archiver und Concentrators als Textdateien zu bearbeiten.

Die bearbeitbaren Dateien sind abhängig vom Servicetyp, den Sie konfigurieren. Die folgenden Dateien sind für alle Core-Services verfügbar:

- Serviceindexdatei
- NetWitness-Datei
- Crash Reporter-Datei

- Planerdatei
- Feeddefinitionsdatei

Darüber hinaus hat der Decoder Dateien, die Parser, Feeddefinitionen und einen Wireless-LAN-Adapter konfigurieren.

Hinweis: Die Standardwerte in den Konfigurationsdateien decken die häufigsten Situationen ab. Möglicherweise müssen Sie Konfigurationsparameter und -werte für optionale Services wie den Crash Reporter oder den Scheduler bearbeiten. Ändern Sie diese Werte auf der Registerkarte „Dateien“ nicht, sofern Sie nicht über gute Kenntnisse der Netzwerke und der Einflussfaktoren auf die Art und Weise verfügen, wie Services Daten erfassen und analysieren.

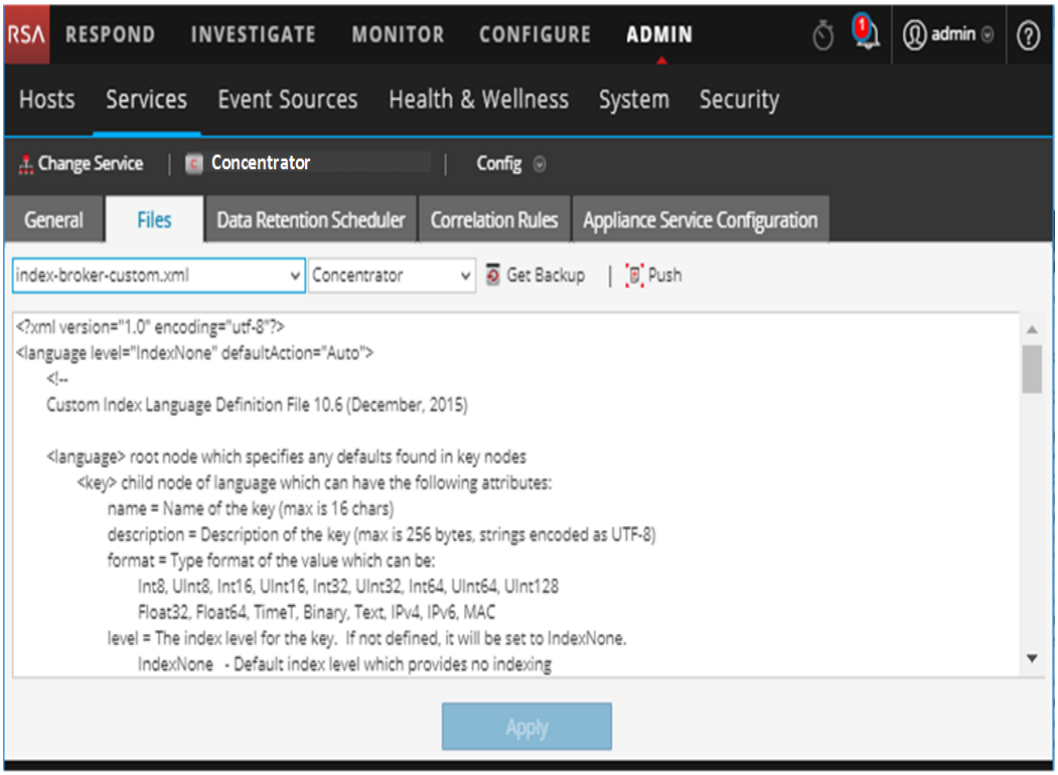
Weitere Informationen über die Servicekonfigurationsparameter erhalten Sie unter Servicekonfigurationseinstellungen.

So greifen Sie auf die Registerkarte Dateien zu:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service und  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ wird mit geöffneter Registerkarte **Allgemein** angezeigt.
3. Klicken Sie auf die Registerkarte **Dateien**.

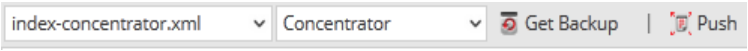
Bearbeiten einer Servicekonfigurationsdatei

Dies ist ein Beispiel für die Registerkarte Dateien.



Symbolleiste auf der Registerkarte „Dateien“

Die Registerkarte Dateien enthält eine Symbolleiste und ein Bearbeitungsfenster. Dies ist ein Beispiel für die Symbolleiste.



Die Symbolleiste der Registerkarte „Dateien“ umfasst die folgenden Funktionen.

Funktion	Beschreibung
Drop-down-Liste **Datei**	Zeigt eine Liste mit zurzeit vom System verwendeten Dateien an. Wenn Sie eine Datei auswählen, wird deren Text im Textbearbeitungsfenster angezeigt. Im Textfenster können Sie die Datei bearbeiten und die Änderungen speichern oder andere Dateien zur Verwendung erstellen.
Drop-down-Liste **Service/Host**	Zeigt den Servicetyp und den Host an. Sie können eine Datei entweder über den Service oder über den Host zur Bearbeitung öffnen.
Get Backup	Mit dieser Option rufen Sie das letzte Backup der aktuellen Datei ab. Dies kann nützlich sein, wenn Sie die Datei geändert haben und zur vorherigen Dateiversion zurückkehren möchten. Erst wenn Sie auf **Speichern** klicken, wird die aktuelle Datei durch das Backup ersetzt.
Push	Mit dieser Option wird ein Dialog angezeigt, in dem Sie Services vom selben Typ auswählen können und die derzeit angezeigte Datei per Push an die Services senden können.
Anwenden	Überschreibt die aktuelle Datei und erstellt eine Backupdatei.

Ansicht „Durchsuchen“

Mit der Ansicht „Durchsuchen“ der NetWitness Platform-Services können Sie Host- und Servicekonfigurationen anzeigen und bearbeiten.

Die Ansicht Services > Durchsuchen zu einem Service bietet erweiterten Zugriff und Steuerung aller NetWitness Platform-Hosts und -Services. Die Funktionen aller Services sind einsehbar über eine Serie von Nodes in einer Verzeichnisstruktur ähnlich der Ansicht im Windows Explorer Ihres Dateisystems. Hier können Sie:

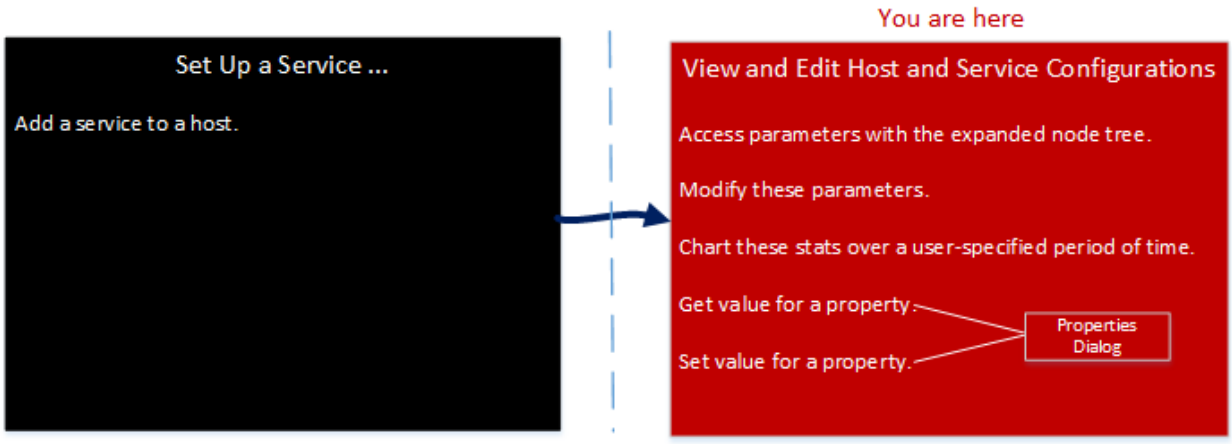
- Eine Verzeichnisstruktur anzeigen, die für alle ausgewählten Services gemeinsame Dateien anzeigt
- Durch das Verzeichnis zu einer Datei navigieren
- Dieselbe Datei für jeden Service öffnen und die Inhalte nebeneinander anzeigen
- Einen Eintrag in der Datei auswählen und den Wert bearbeiten
- Einen Eigenschaftswert von einem Service auf andere Services anwenden.

  Wie in der Abbildung unten dargestellt, kann in der Ansicht Services > Durchsuchen auch ein Dialogfeld „Eigenschaften“ angezeigt werden, eine einfache Benutzeroberfläche zur Anzeige der Eigenschaften jedes Node im System und zum Versenden von Nachrichten an den Node.

Achtung: Ein gutes Verständnis der Nodes und Parameter ist für die Bearbeitung in dieser Ansicht erforderlich. Falsche Einstellungen können Performanceprobleme verursachen.

Workflow

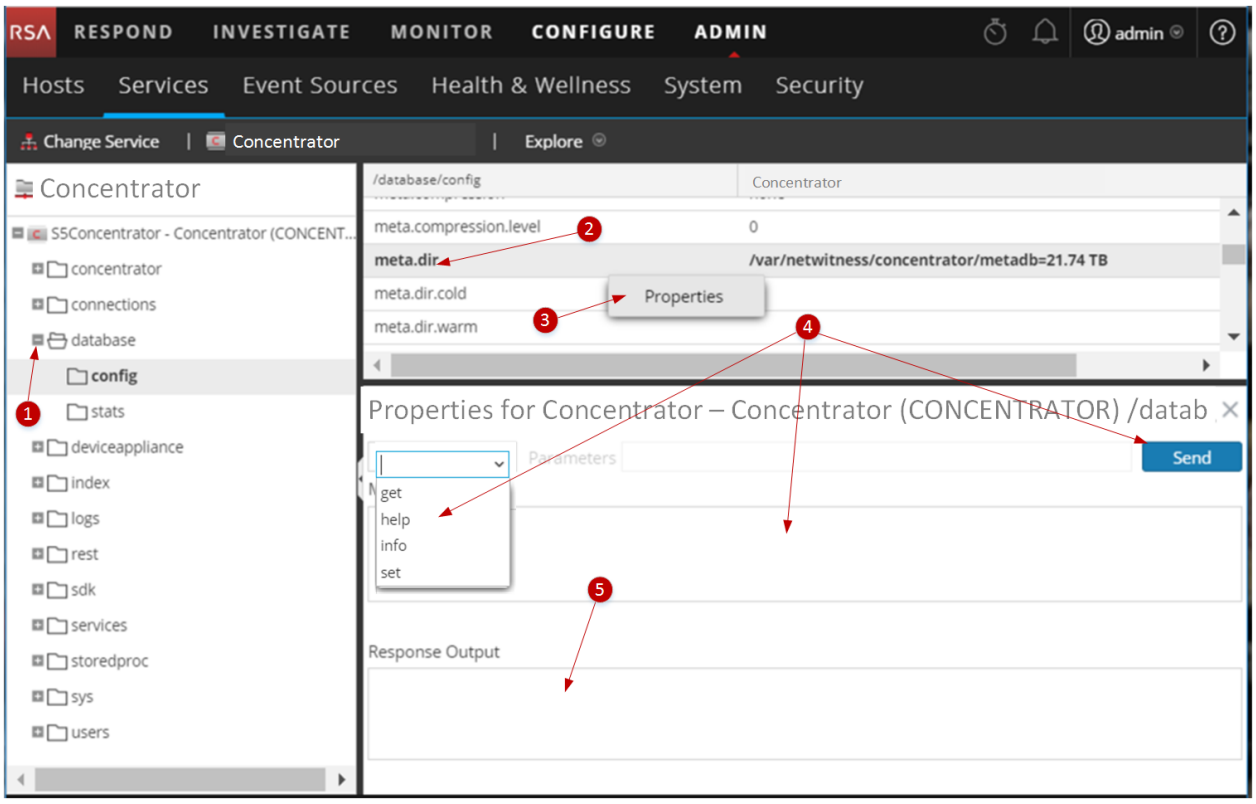
Dieser Workflow zeigt die Aufgaben, die Sie aus der Ansicht „Durchsuchen“ ausführen.



Überblick

So greifen Sie auf die Ansicht Durchsuchen zu einem Service zu:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service aus und wählen Sie  **> Ansicht > Durchsuchen** .



1	Erweitern Sie den Knoten, um seine Parameterkategorien anzuzeigen.
2	Klicken Sie auf eine Eigenschaft (z. B. **meta.dir**), um sie auszuwählen.
3	Klicken Sie auf einen Node oder eine Kategorie und klicken Sie auf **Eigenschaften**, um das Dialogfeld „Eigenschaften“ anzuzeigen.
4	Führen Sie einen Vorgang an einem Node oder einer Kategorie durch: a. Wählen Sie aus der Drop-down-Liste einen Befehl aus. b. Geben Sie eine Befehlszeichenfolge ein (falls erforderlich). c. Klicken Sie auf **Senden**.
5	Überprüfen Sie die Ausgabe.

Funktionen

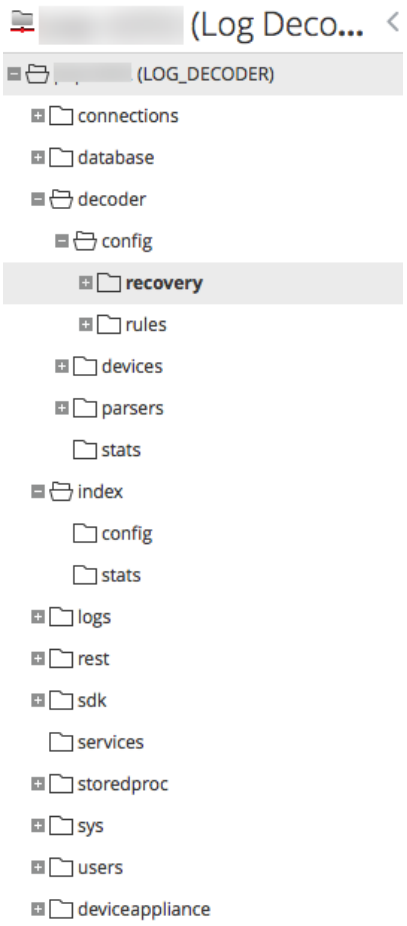
Die Ansicht **Durchsuchen zu einem Service** hat zwei Hauptbereiche:

- Die Node-Liste
- Der Überwachungsbereich

Klicken Sie mit der rechten Maustaste auf eine Datei und wählen Sie „Eigenschaften“ aus, um darauf zuzugreifen.

Die Node-Liste

Die Node-Liste zeigt die Services als Serie von Nodes und Ordnern in einer Verzeichnisstruktur an. Die Level in der Node-Liste können eingeblendet und ausgeblendet werden, um die gesamte Hierarchie anzuzeigen.



Jeder Stammordner ist nach der Funktion benannt, die er zeigt. Zum Beispiel zeigt der Ordner **/connections** alle verbundenen IP-Adressen an. Unterhalb von jedem **IP/Port** sind zwei Ordner, **sessions** und **stats**.

- Der Ordner **sessions** zeigt alle authentifizierten Nutzersitzungen an, die von dem IP/Port ausgehen.
- Der Ordner **stats** zeigt vom Service eingestellte Werte an, wie etwa die Anzahl der gesendeten/empfangenen Nachrichten, gesendeten/empfangenen Byte und andere. Diese können nicht bearbeitet werden.

Wenn ein Ordner in der Verzeichnisansicht ausgewählt wird, werden seine Unterordner im Bereich **Überwachung** angezeigt. Jeder Node in der Verzeichnisstruktur wird aktiv überwacht. Wenn sich also der Wert einer Statistik oder eines Konfigurations-Node ändert, spiegelt sich diese Änderung sofort in der Verzeichnisstruktur und im Überwachungsbereich wieder.

Der Überwachungsbereich

Der Bereich **Überwachung** zeigt Eigenschaften und Werte für einen ausgewählten Node (wie etwa **index**) und einen untergeordneten Ordner (wie etwa **config**) an. Werte können auf zwei Weisen bearbeitet werden:

- Durch Klicken auf den Wert und Eingeben eines neuen Werts
- Durch Senden einer **set**-Nachricht im Dialogfeld „Eigenschaften“

/Index/Config	(Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

Themen

- Funktionen
- Log Decoder-Servicekonfigurationsparameter

Dialogfeld „Eigenschaften“

Verwenden Sie in der Ansicht „Durchsuchen zu einem Service“ das Dialogfeld „Eigenschaften“, um eine der folgenden Aufgaben auszuführen:

- Nachrichten an einen System-Node senden
- Werte für eine Eigenschaft für mehrere Services abrufen
- Werte für eine Eigenschaft für mehrere Services festlegen

Das Dialogfeld „Eigenschaften“ wird unter dem Bereich „Überwachen“ geöffnet, wenn Sie im Kontextmenü die Option „Eigenschaften“ auswählen.

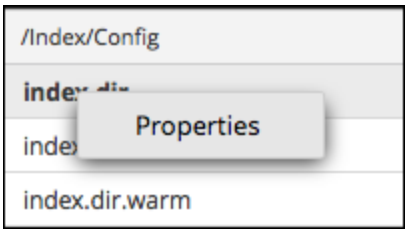
Alle Nodes verfügen über eine Hilfe, die folgende Informationen enthält:

- eine Beschreibung des Node
- die Liste der unterstützten Meldungen mit einer entsprechenden Beschreibung
- die für den Zugriff auf die Meldungen erforderlichen Sicherheitsrollen

Die verfügbaren Meldungen variieren je nach Service und Stammordner. Viele dieser Meldungen sind auch über ein NetWitness Platform-Dashboard oder eine Ansicht als Optionen zugänglich.

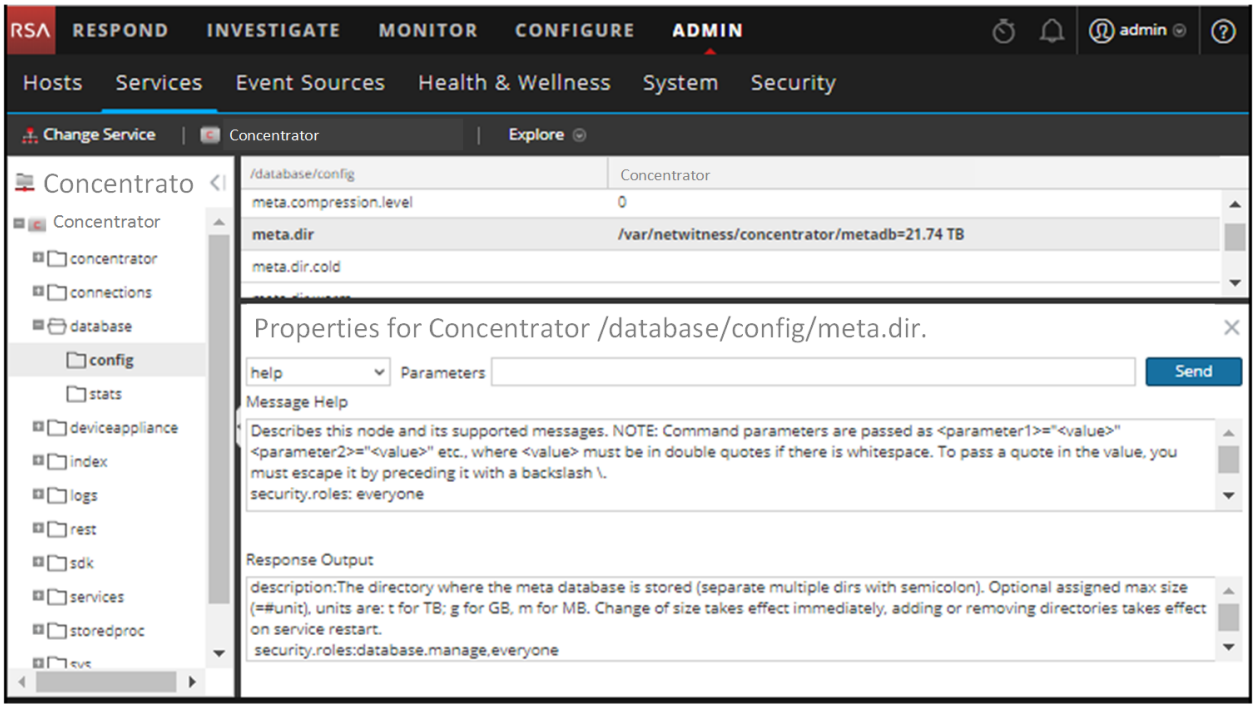
So greifen Sie auf das Dialogfeld „Eigenschaften“ zu:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service aus und wählen Sie  **> Ansicht > Durchsuchen** aus.
3. Wählen Sie in der Liste **Node** eine Datei aus.
4. Klicken Sie im Bereich **Monitor** mit der rechten Maustaste auf eine Eigenschaft und wählen Sie **Eigenschaften** aus.



Das Dialogfeld „Eigenschaften“ wird angezeigt. Sie können auch mit der rechten Maustaste auf eine beliebige Datei in der Liste „Node“ klicken, um das Dialogfeld „Eigenschaften“ anzuzeigen.

Im folgenden Beispiel ist das Dialogfeld „Eigenschaften“ dargestellt, in dem die Hilfe zu einer Meldung (**info**) angezeigt wird.



Funktionen

Das Dialogfeld „Eigenschaften“ bietet die folgenden Funktionen.

Funktion	Beschreibung
Drop-down-Liste **Meldung**	Listet alle verfügbaren Meldungen für den aktuellen Node auf. Wählen Sie eine Meldung aus, die an den Node gesendet werden soll.
Eingabefeld **Parameter**	Geben Sie in diesem Feld die Meldungsparameter ein.
Schaltfläche **Senden**	Sendet die Meldung an den Node.
Hilfe zu Meldungen	Zeigt den Hilfetext für die aktuelle Meldung an.

Funktion	Beschreibung
Antwortausgabe	Zeigt die Antwort auf eine Meldung oder Ausgabe einer Meldung an.

Ansicht „Serviceprotokolle“

In diesem Thema wird die Ansicht Serviceprotokolle beschrieben.

In der Ansicht Serviceprotokolle können Sie die Protokolle für einen bestimmten Service anzeigen und suchen. Die Ansicht Serviceprotokolle entspricht dem Bereich Systemprotokollierung mit Ausnahme von zwei Punkten:

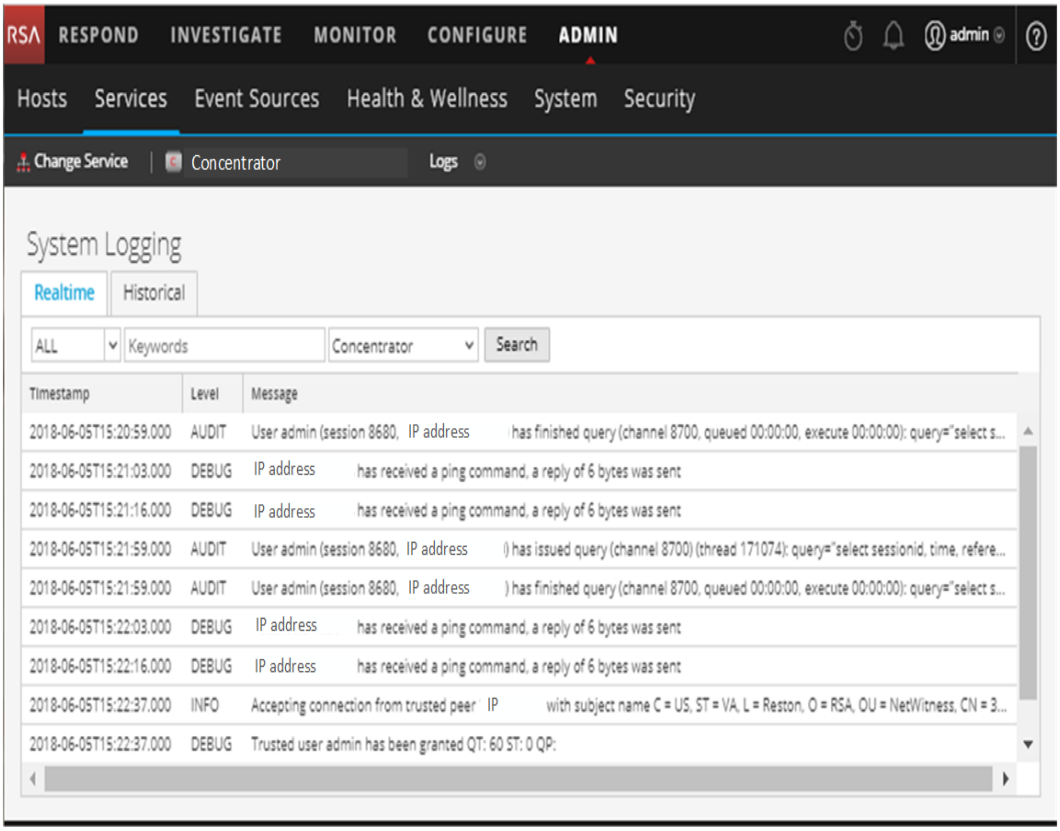
- Die Ansicht Serviceprotokolle hat einen zusätzlichen Filter, um Meldungen für den Service oder den Host auszuwählen.
- Der Bereich Systemprotokollierung hat eine zusätzliche Registerkarte für Einstellungen.

Eine vollständige Beschreibung der NetWitness Platform-Protokollierungsfunktionen finden Sie im Bereich **Administration** > **System** > **Systemprotokollierung**.

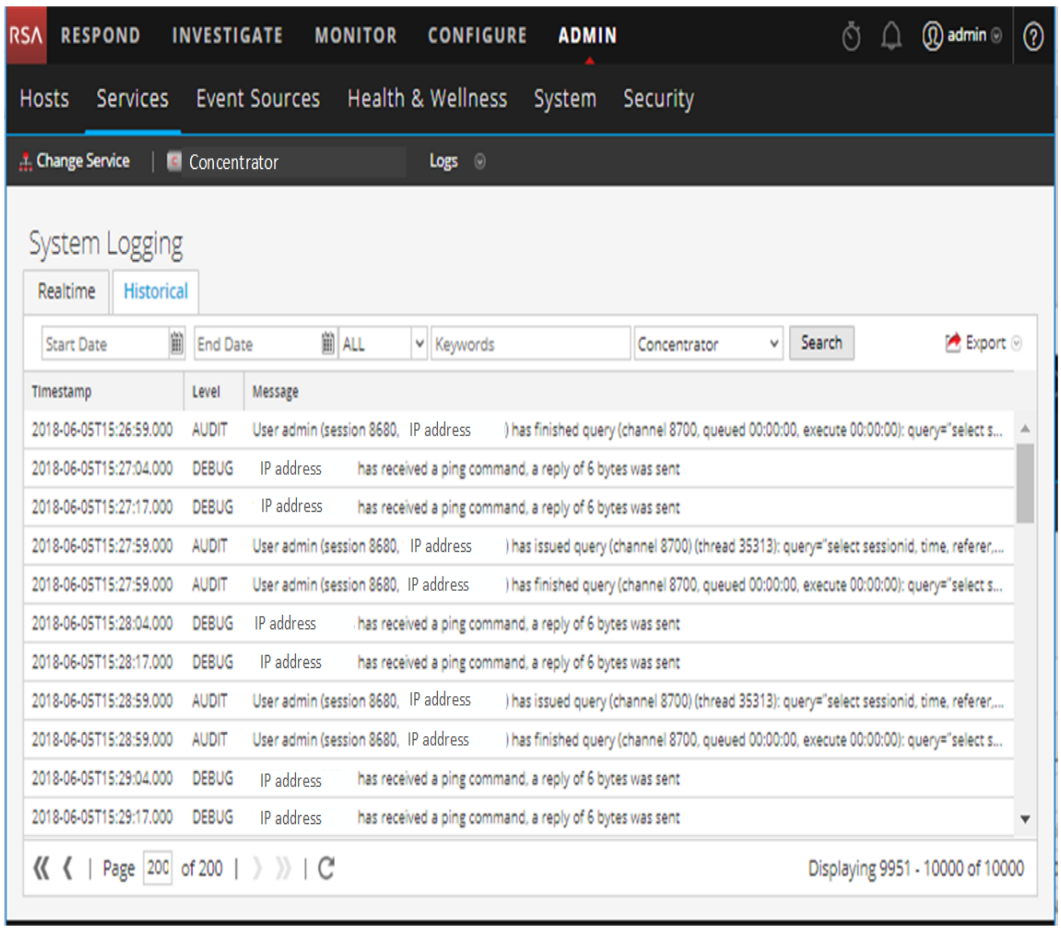
So zeigen Sie ein Serviceprotokoll an:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service und dann  **>Ansicht > Protokolle** aus.

In der folgenden Abbildung ist die Ansicht „Services > Protokolle“ mit der Registerkarte „Echtzeit“ dargestellt.



In der folgenden Abbildung ist die Ansicht „Services > Protokolle“ mit der Registerkarte „Historisch“ gezeigt.



Funktionen

Der Bereich „Systemprotokollierung“ weist die unten beschriebenen Registerkarten auf. Die Protokollierungsfunktionen werden in den Themen zur Systemwartung beschrieben (siehe **Überwachen von Integrität und Zustand von NetWitness Platform** im Leitfaden *Systemwartung*).

Funktion	Beschreibung
Registerkarte Echtzeit	Dies ist der Überwachungsmodus des Serviceprotokolls.
Registerkarte Verlauf	Dies ist eine durchsuchbare Ansicht des Serviceprotokolls.

Ansicht „Services-Sicherheit“

Dieses Thema bietet eine Übersicht über das Sicherheitsmanagement für Services in der Ansicht „Services-Sicherheit“.

In NetWitness Platform weist jeder Service eine eigene Konfiguration mit Nutzern, Rollen und Rollenberechtigungen auf, die in der Ansicht Services > Sicherheit gemanagt wird.

Um auf Serviceinformationen zugreifen und Serviceabläufe über NetWitness Platform durchführen zu können, muss der Nutzer einer Rolle angehören, die Berechtigungen für diesen Service umfasst. Für NetWitness Platform Core-Services der Version 10.4 oder höher, die vertrauenswürdige Verbindungen verwenden, müssen keine NetWitness PlatformCore-Nutzerkonten für Nutzer erstellt werden, die sich über den Webclient anmelden. Sie müssen nur NetWitness PlatformCore-Nutzerkonten für Nutzer von Aggregation, Thick-Client und REST-API erstellen.

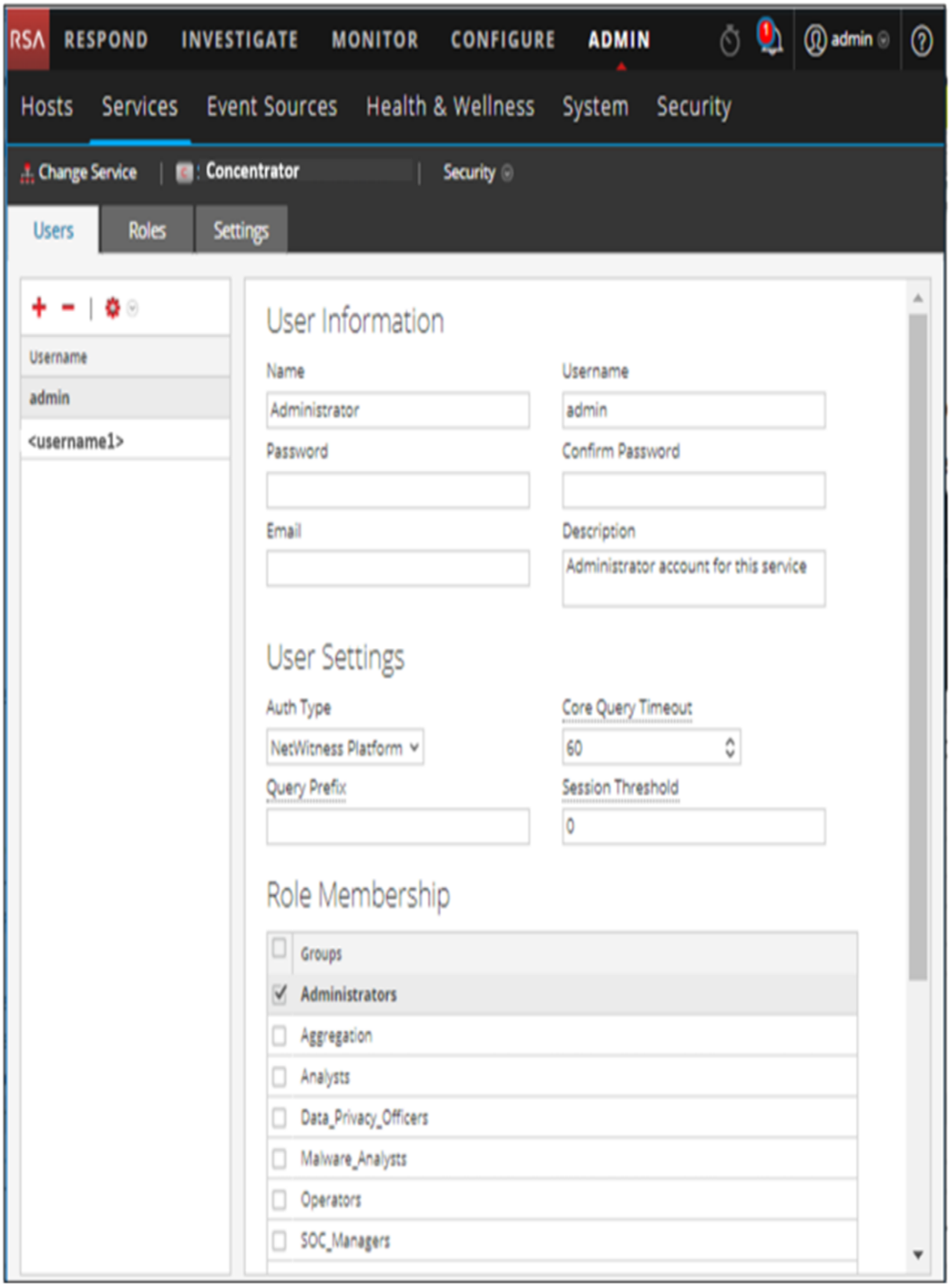
Hinweis: Nur der Admin-Standardbenutzer in NetWitness Platform wird standardmäßig in allen Services erstellt. Als Voraussetzung für das Managen der Sicherheit muss das Admin-Standardbenutzerkonto in der NetWitness Platform-Ansicht Administration > Services vorhanden sein. Für jeden anderen Nutzer muss der Zugriff auf einen bestimmten Service über NetWitness Platform konfiguriert werden.

Verfahren im Zusammenhang mit dieser Registerkarte sind unter Hosts und Services – Verfahren beschrieben.

So greifen Sie auf die Ansicht „Services > Sicherheit“ zu:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.

2. Wählen Sie einen Service und dann > **Ansicht > Sicherheit** aus.
   Die Ansicht „Services-Sicherheit“ für die ausgewählten Services wird angezeigt.



Funktionen

Die Ansicht Services-Sicherheit enthält drei Registerkarten: Nutzer, Rollen und Einstellungen.

Rollen und Servicezugriff

Die wichtigsten Schritte beim Konfigurieren der Sicherheit sind die Definition der Rollen und das Zuweisen der Rollen zu Nutzern. In der Ansicht Services-Sicherheit befinden sich diese Funktionen auf der Registerkarte Nutzer bzw. auf der Registerkarte Rollen.

- Auf der Registerkarte Rollen können Sie Rollen erstellen und den Rollen Berechtigungen für einen bestimmten Service zuweisen.
- Auf der Registerkarte Nutzer können Sie für einen ausgewählten Service einen Nutzer hinzufügen, Nutzereinstellungen bearbeiten, das Nutzerpasswort ändern und die Rollenmitgliedschaft des Nutzers bearbeiten. Auch wenn Sie in der Ansicht Services-Sicherheit nur einen einzigen Service ausgewählt haben, können Sie die Einstellungen dieses Service auf andere Services anwenden.

Themen

- Registerkarte „Rollen“
- Servicebenutzerrollen und -berechtigungen
- Rolle „Aggregation“
- Registerkarte „Einstellungen“
- Registerkarte „Nutzer“

Registerkarte „Rollen“

In diesem Thema werden die Funktionen der Ansicht Services > Sicherheit Registerkarte Rollen eingeführt.

In der Registerkarte **Rollen** haben Sie die Möglichkeit, Rollen zu erstellen und Berechtigungen zuzuweisen. Jede Rolle kann unterschiedliche Berechtigungen für verschiedene Services haben. Die Rolle Analysten kann zum Beispiel verschiedene Rollenberechtigungen basierend auf dem ausgewählten Service haben.

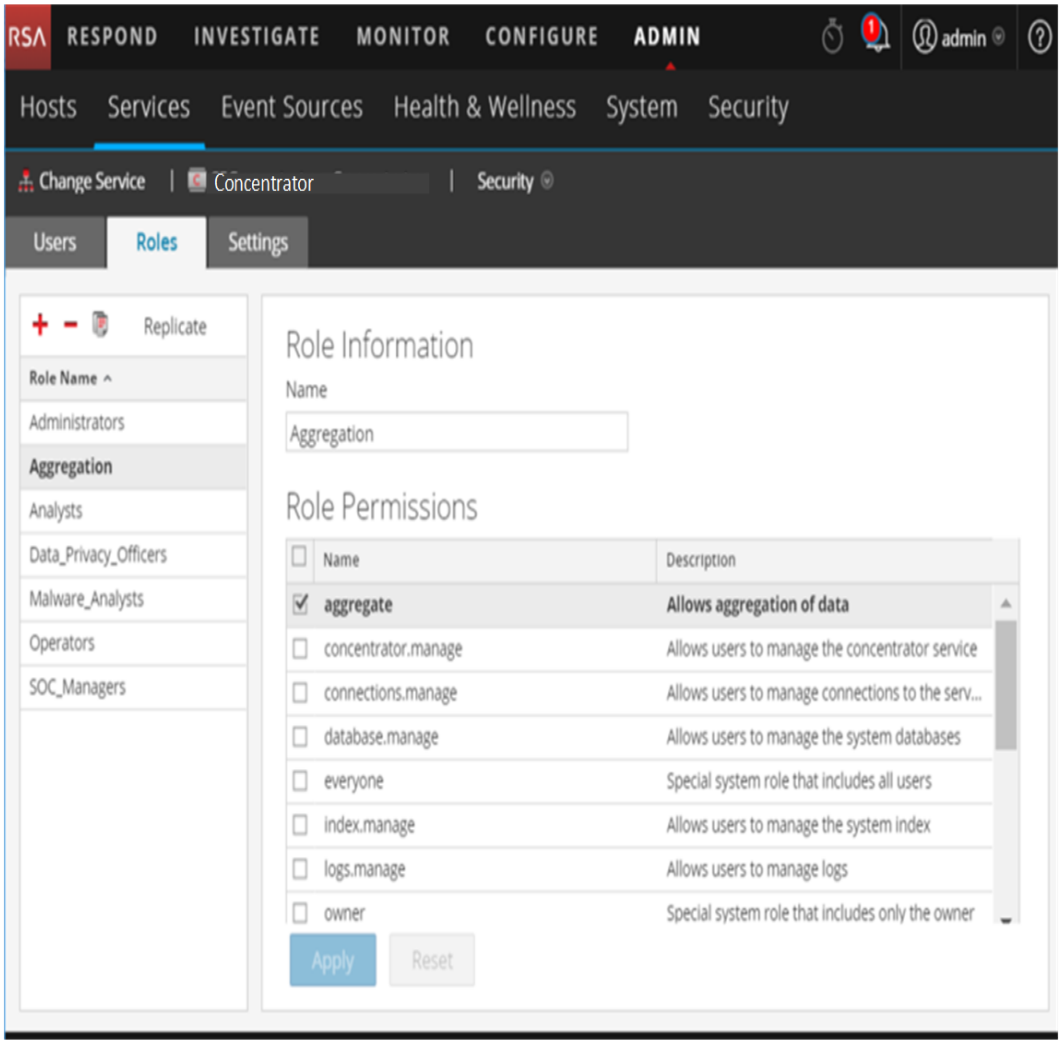
Bevor Sie Nutzer zu Rollen hinzufügen können, müssen Sie Nutzerrollen, normalerweise nach Funktion, definieren und den Rollen Berechtigungen zuteilen.

Verfahren im Zusammenhang mit dieser Registerkarte sind unter Hosts und Services – Verfahren beschrieben.

So zeigen Sie die Registerkarte **Ansicht Services Sicherheit > Rollen** an:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service aus, zu dem Sie einen Nutzer hinzufügen möchten, und wählen Sie dann  **> Ansicht > Sicherheit** aus.
3. Wählen Sie die Registerkarte **Rollen** aus.

In der folgenden Abbildung ist die Registerkarte „Rollen“ in der Ansicht „Services > Sicherheit“ dargestellt.



Funktionen

Die Registerkarte Rollen hat links den Bereich **Rollen-ID**. Bei der Auswahl einer Rollen-ID wird rechts der Bereich **Rolleninformationen** für die ausgewählte Rolle angezeigt.

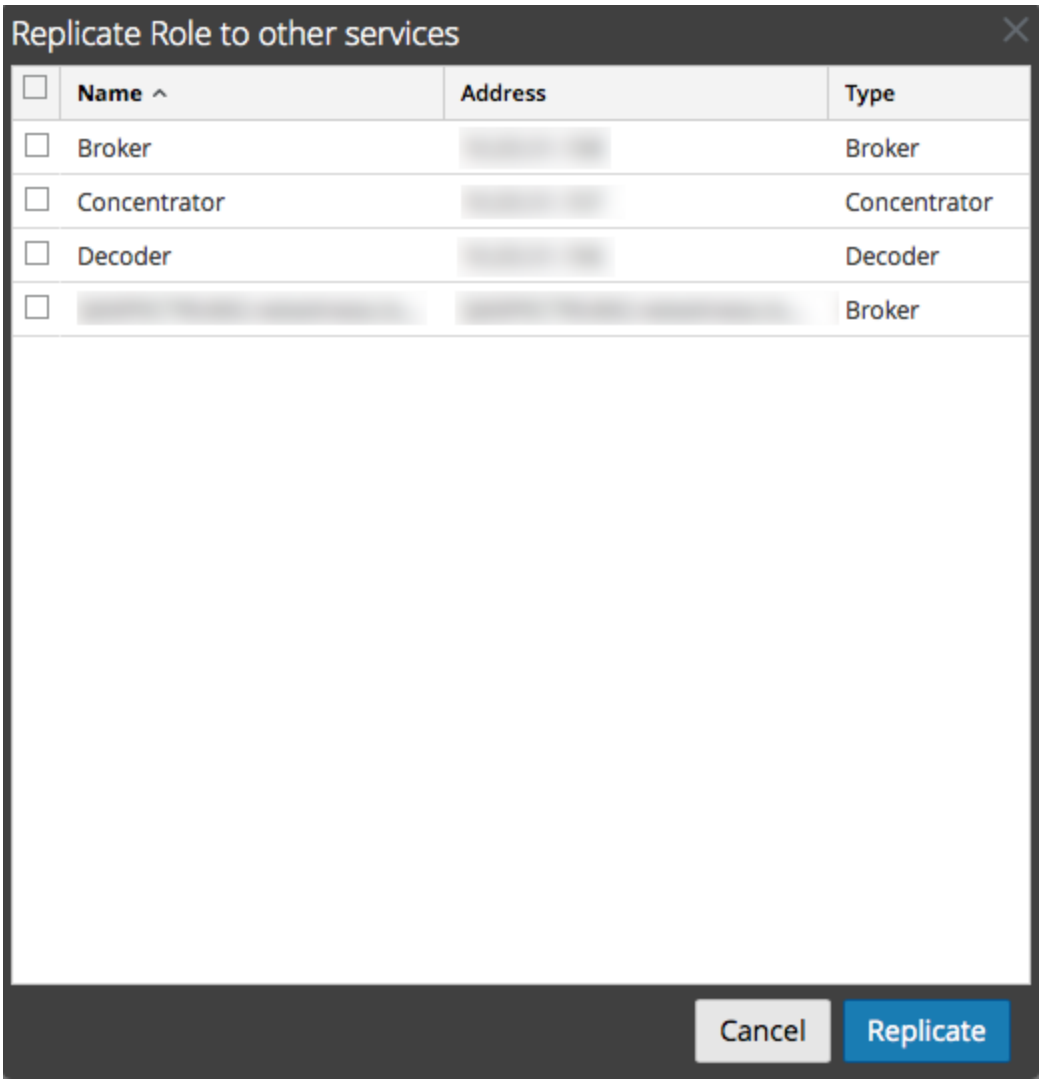
Bereich Rollen-ID

Der Bereich **Rollen-ID** bietet folgende Funktionen:

Funktion	Beschreibung
+	Fügt eine neue Gruppe zum aktuellen Service hinzu.
−	Löscht die ausgewählte Gruppe vom aktuellen Service.

Funktion	Beschreibung
	Kopiert eine Rolle und Ihre zugeteilten Berechtigungen auf eine neue Rolle. Der Name der neuen Rolle muss eindeutig sein. Sie können zum Beispiel die Rolle **Analysten** kopieren und eine andere Rolle mit einem neuen Namen erstellen, wie zum Beispiel **Analysten-Manager**.
Replizieren	Überträgt eine Rolle und ihre zugeteilten Berechtigungen auf einen anderen Service. Nachdem Sie eine Rolle ausgewählt und auf **Replizieren** geklickt haben, wird das Dialogfeld **Rolle nach anderen Services replizieren** angezeigt. Sie können im Dialogfeld die Services auswählen, auf die Sie die Rollen replizieren möchten.

In der folgenden Abbildung wird das Dialogfeld **Rolle nach anderen Services replizieren** gezeigt.



Bereich „Rolleninformationen und -berechtigungen“

Im Bereich **Rolleninformationen und Berechtigungen** werden die Rollenberechtigungen definiert.

Es gibt zwei Schaltflächen:

- Mit der Schaltfläche **Anwenden** werden die Änderungen gespeichert, die im Bereich Rollenberechtigungen durchgeführt wurden, und diese werden sofort aktiv.
- Wenn Sie die Änderungen nicht im Bereich Rollenberechtigungen gespeichert haben, werden mit der Schaltfläche **Zurücksetzen** alle Felder und Einstellungen auf die Werte vor der Bearbeitung zurückgesetzt.

Servicebenutzerrollen und -berechtigungen

In diesem Thema werden die vorkonfigurierten Servicebenutzerrollen und Berechtigungen beschrieben.

In der Registerkarte Rollen der Ansicht Services > Sicherheit können Sie Servicebenutzerrollen erstellen und Berechtigungen zuweisen. Sie können auch die in NetWitness Platform enthaltenen vorkonfigurierten Rollen verwenden, um Nutzerberechtigungen zuzuweisen.

Servicebenutzerrollen

NetWitness Platform umfasst die folgenden vorkonfigurierten Servicebenutzerrollen.

Rolle	Zugewiesene Berechtigungen	Personal/Konto
Administratoren	Alle Berechtigungen	NetWitness Platform Systemadministrator
Aggregation	aggregate sdk.content sdk.meta sdk.packets	Sie können diese Rolle verwenden, um ein Aggregationskonto zu erstellen. Diese Rolle verfügt über die zur Aggregation von Daten mindestens erforderlichen Berechtigungen. Sie ist nur in Services ab NetWitness Platform 10.5 verfügbar.
Analysts, Malware_ Analysts und SOC_ Managers	sdk.meta sdk.content sdk.packets storedproc.execute	Nutzer können bestimmte Anwendungen verwenden, Abfragen ausführen und Inhalte zu Analysezwecken einsehen.
Data_Privacy_ Officers	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	Data Privacy Officer Data Privacy Officer verfügen auf Decodern und Log Decodern über die Berechtigung dpo.manage.

Rolle	Zugewiesene Berechtigungen	Personal/Konto
Operatoren	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	Operator sind verantwortlich für den täglichen Betrieb der Services.

Servicebenutzerberechtigungen

Sie können einer Servicerolle in NetWitness Platform viele verschiedene Berechtigungen zuweisen. Nutzer können abhängig von den ihnen zugewiesenen Rollen und den für jede Rolle ausgewählten Berechtigungen für jeden Service andere Berechtigungen haben. In dieser Tabelle sind die Berechtigungen beschrieben, die Sie einer Rolle zuweisen können.

Berechtigung	Definition
sys.manage	Ermöglicht das Bearbeiten der Servicekonfigurationseinstellungen.
services.manage	Ermöglicht das Managen von Verbindungen zu anderen Services.
connections.manage	Ermöglicht das Managen von Verbindungen zu dem Service.
users.manage	Ermöglicht das Erstellen individueller Nutzer und Nutzerrollen sowie das Festlegen von Nutzerberechtigungen.
aggregate	Ermöglicht das Ausführen der Datenaggregation.
sdk.meta	Ermöglicht das Ausführen von Abfragen in den Anwendungen Investigation und Reporting sowie das Anzeigen der von der Abfrage zurückgegebenen Metadaten.
sdk.content	Ermöglicht den Zugriff auf Rohdatenpakete und Protokolle einer beliebigen Clientanwendung (Investigation und Reporting).
sdk.packets	Ermöglicht den Zugriff auf Rohdatenpakete und Protokolle einer beliebigen Clientanwendung.
appliance.manage	Ermöglicht das Managen der Appliance- bzw. Hostaufgaben. Diese Berechtigung wird vom Appliance-Service obligatorisch abgefragt.

Berechtigung	Definition
decoder.manage	Ermöglicht das Bearbeiten der Konfigurationseinstellungen für den Decoder-Service.
concentrator.manage	Ermöglicht das Bearbeiten der Konfigurationseinstellungen für den Concentrator-/Broker-Service
logs.manage	Ermöglicht das Anzeigen von Serviceprotokollen und das Bearbeiten der Protokollierungs-Konfigurationseinstellungen für den angegebenen Service.
parsers.manage	Ermöglicht das Managen aller Attribute unter dem Parser-Node.
rules.manage	Ermöglicht das Hinzufügen und Löschen aller Regeln.
database.manage	Ermöglicht das Festlegen von Datenbankstandorten und -größen sowie der verschiedenen Konfigurationseinstellungen für die Sitzungs-, Metadaten- und/oder Paket-/Protokolldatenbanken.
index.manage	Ermöglicht das Managen aller indexbezogenen Attribute.
sdk.manage	Ermöglicht das Anzeigen und Festlegen aller SDK-Konfigurationselemente.
storedproc.execute	Ermöglicht das Ausführen eines gespeicherten Lua-Verfahrens.
storedproc.manage	Ermöglicht das Managen gespeicherter Lua-Verfahren.
archiver.manage	Ermöglicht das Ändern der Archiver-Konfiguration.
dpo.manage	Ermöglicht das Managen der Transformationskonfiguration und der entsprechenden Schlüssel.

Rolle „Aggregation“

In diesem Thema werden die Rolle Aggregation und die Berechtigungen beschrieben, mit denen die Servicebenutzer die Aggregation ausführen können.

Die Rolle „Aggregation“ ist eine Servicebenutzerrolle, die nur zur Aggregation von Daten dient. Die Rolle verfügt über die mindestens zum Ausführen der Aggregation erforderlichen Berechtigungen:

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

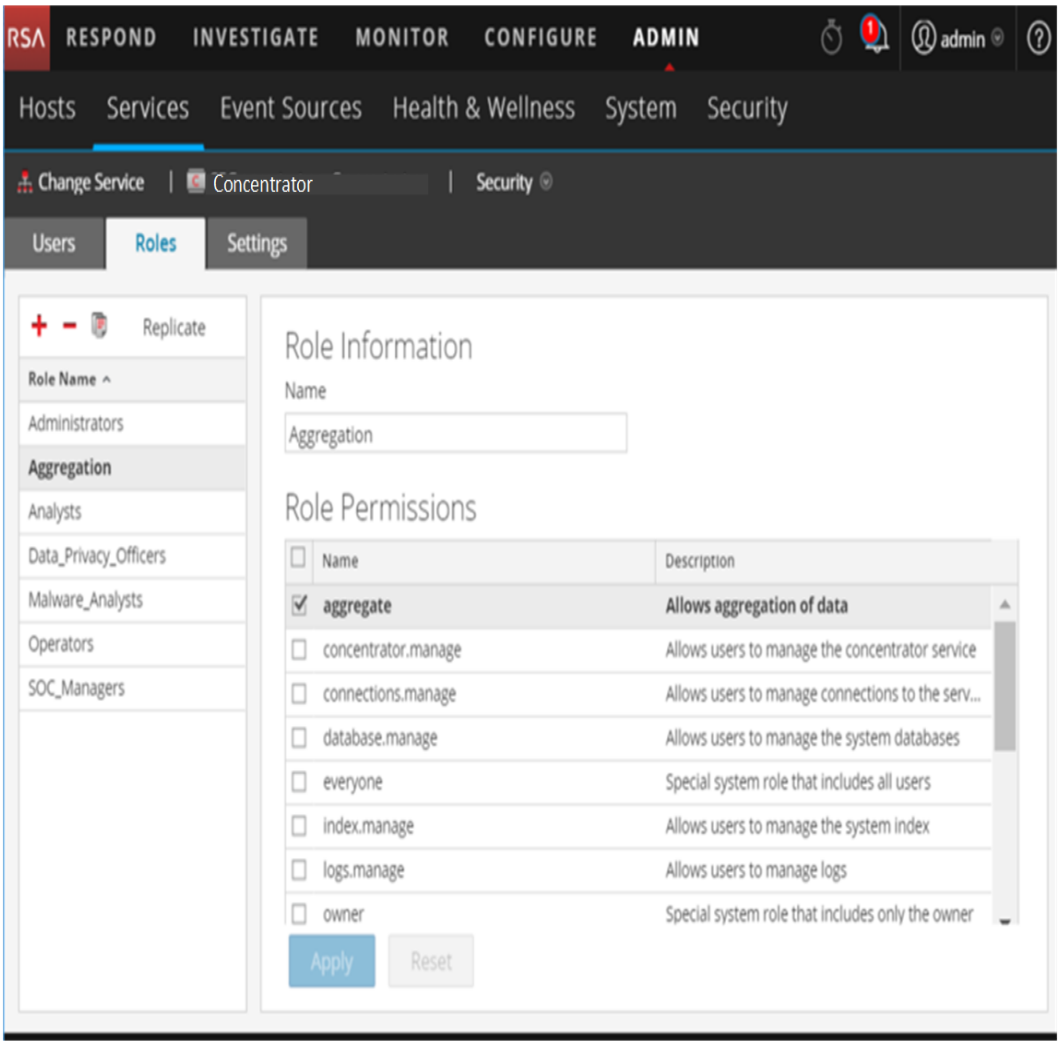
Die Rolle „Aggregation“ ist nur für NetWitness Platform-Services ab Version 10.5 verfügbar und kann für ein Aggregationskonto verwendet werden. Mitglieder dieser Rolle oder Servicebenutzer mit diesen Berechtigungen können die Aggregation auf Decodern, Concentrators, Archivers und Brokers ausführen. Mit der Berechtigung **aggregate** können Servicebenutzer die Aggregation auf Sitzungen und Metadaten zusammen mit Rohdatenpaketen und Protokollen ausführen.

Sie können die Berechtigungen decoder.manage, concentrator.manage und archiver.manage zwar verwenden, aber die Berechtigungen der Rolle Aggregation lassen nur die Aggregation zu und verhindern die anderen verfügbaren Vorgänge.

Der Zugriff auf die Servicerollen erfolgt über die Registerkarte **Administration** > **Services** (einen Service auswählen) > **Aktionen** > **Ansicht** > **Sicherheit** > **Rollen**.

Verfahren im Zusammenhang mit Rollen sind unter Hosts und Services – Verfahren beschrieben. Weitere Informationen zu vorkonfigurierten Rollen erhalten Sie unter Servicebenutzerrollen und -berechtigungen.

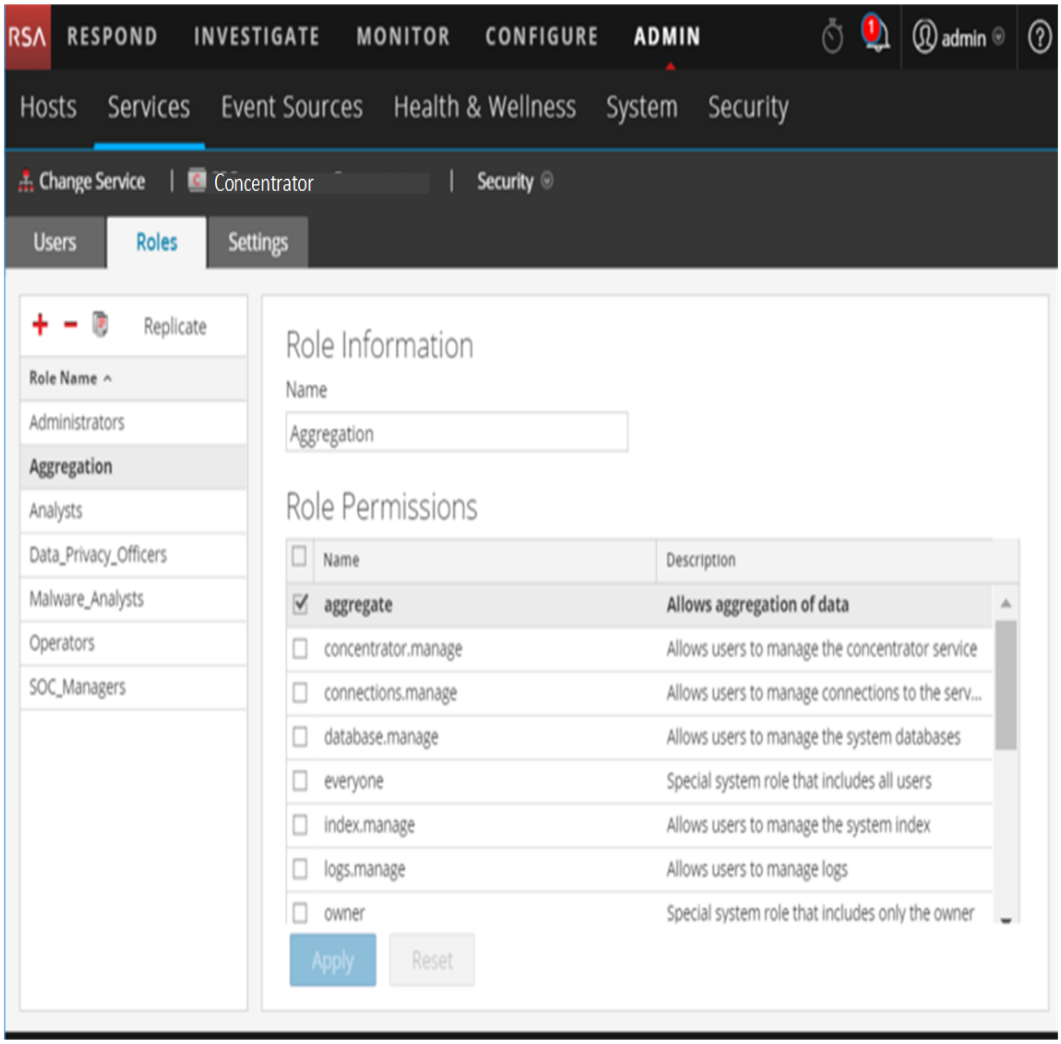
In der folgenden Abbildung sind die Berechtigungen in der Rolle „Aggregation“ dargestellt.



Registerkarte „Einstellungen“

In diesem Thema werden die Funktionen der Registerkarte Einstellungen der Ansicht Services > Sicherheit erklärt.

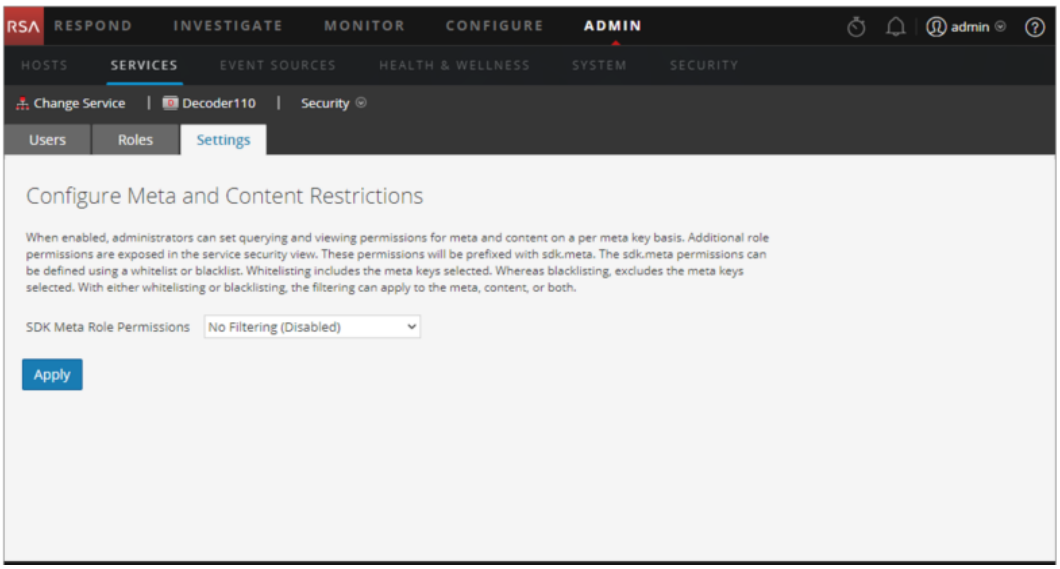
Auf der Registerkarte „Einstellungen“ der Ansicht „Services > Sicherheit“ können Administratoren Systemrollen aktivieren und konfigurieren, die Berechtigungen auf Metaschlüsselbasis für einzelne Broker, Concentrator, Decoder und Log Decoder definieren. Durch das Konfigurieren dieser Funktion werden konfigurierbare Metaschlüssel zur Registerkarte Rollen der Ansicht Services > Sicherheit hinzugefügt, sodass auf spezifische Rollen in einem bestimmten Service individuelle Metaschlüssel angewendet werden können. In der folgenden Abbildung ist dieser Vorgang dargestellt.



Diese Konfiguration ist im Allgemeinen Teil eines Datenschutzplans, durch den sichergestellt werden soll, dass bestimmte von einem Service verarbeitete oder aggregierte Contenttypen geschützt werden, indem die Sichtbarkeit von Metadaten und Content auf Nutzer mit den nötigen Berechtigungen beschränkt wird (siehe *Datenschutzmanagement*).

So zeigen Sie die Registerkarte an:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie im Raster **Services** einen Decoder- oder Log Decoder-Service aus, klicken Sie auf  **> Ansicht > Sicherheit** und klicken Sie dann auf die Registerkarte **Einstellungen**.



Funktionen

Die Registerkarte umfasst zwei Funktionen.

Funktion	Beschreibung
Feld SDK-Meta-Rollenberechtigungen	Bietet eine Option zum Deaktivieren oder Konfigurieren von Beschränkungen für Metaschlüssel und Content. Die Filteroptionen werden beschrieben.
Schaltfläche Anwenden	Wendet die ausgewählte Konfiguration sofort an. Wenn Sie nicht deaktiviert werden, werden die Metaschlüssel der Registerkarte Rollen hinzugefügt, sodass Sie bestimmten Rollen zugewiesen werden können.

Optionen für SDK-Meta-Rollenberechtigungen

In der folgenden Tabelle sind die in der Auswahlliste SDK-Meta-Rollenberechtigungen verfügbaren Filteroptionen aufgeführt sowie die numerischen Werte, die zur Deaktivierung (0) und für andere Arten des Filterns verwendet werden (1 bis 6).

Hinweis: Es ist nicht notwendig, die numerischen Werte zu kennen, es sei denn, Sie konfigurieren die Metadaten- und Inhaltssichtbarkeit im system.roles-Node manuell.

system.roles-Node-Wert	Option der Registerkarte Einstellungen	Beschreibung
0	Keine Filterung (Deaktiviert)	Systemrollen, die Berechtigungen auf Metaschlüsselbasis definieren, sind deaktiviert.
1	Metadaten und Content in der weißen Liste	Metadaten und Content für die angegebenen SDK-Metarollen werden der weißen Liste hinzugefügt oder sind sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.

system.roles-Node-Wert	Option der Registerkarte Einstellungen	Beschreibung
2	Nur Metadaten in der weißen Liste	Metadaten für die angegebenen SDK-Metarollen werden der weißen Liste hinzugefügt oder sind sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.
3	Nur Content in der weißen Liste	Content für die angegebenen SDK-Metarollen wird der weißen Liste hinzugefügt oder ist sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.
4	Metadaten und Content in der schwarzen Liste	Metadaten und Content für die angegebenen SDK-Metarollen werden der schwarzen Liste hinzugefügt oder sind nicht sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.
5	Nur Metadaten in der schwarzen Liste	Metadaten für die angegebenen SDK-Metarollen werden der schwarzen Liste hinzugefügt oder sind nicht sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.
6	Nur Content in der schwarzen Liste	Content für die angegebenen SDK-Metarollen wird der schwarzen Liste hinzugefügt oder ist nicht sichtbar für Nutzer, denen die Systemrolle zugewiesen wurde.

Registerkarte „Nutzer“

In diesem Thema werden die Funktionen der Registerkarte Nutzer in der Ansicht Services > Sicherheit erklärt.

Auf der Registerkarte Nutzer in der Ansicht Services-Sicherheit können sie Folgendes für einen Service konfigurieren:

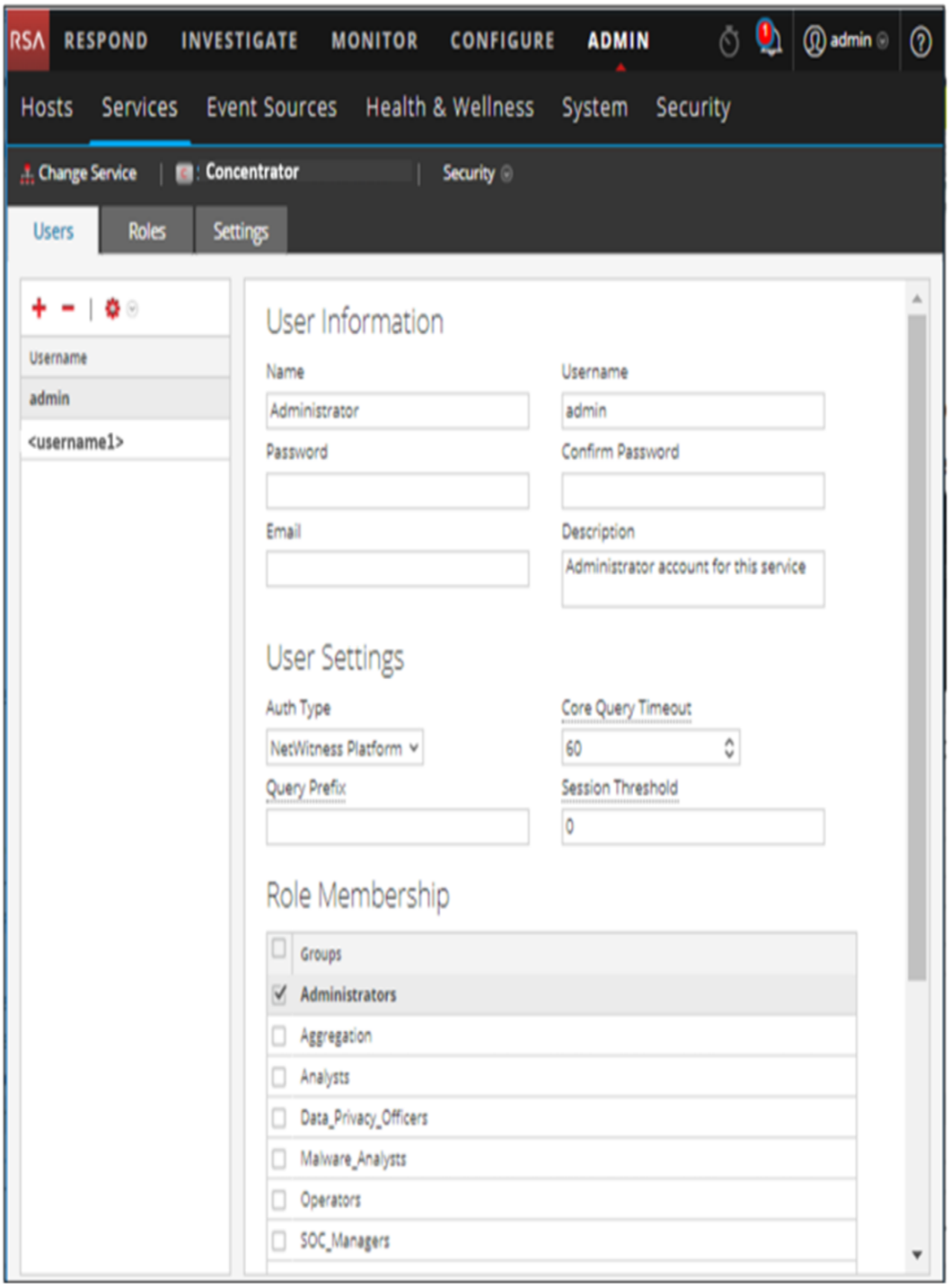
- Fügen Sie Nutzerkonten hinzu.
- Ändern Sie Servicebenutzerpasswörter.
- Konfigurieren Sie Nutzerauthentifizierungseigenschaften und Abfragebehandlungseigenschaften für den Service.
- Geben Sie die Nutzerrollenmitgliedschaft an, die die Rollen angegeben, denen der Nutzer auf dem ausgewählten Service angehört.

Hinweis: Für NetWitness Platform Core-Services der Version 10.4 oder höher, die vertrauenswürdige Verbindungen verwenden, müssen keine NetWitness Platform Core-Nutzerkonten für Nutzer erstellt werden, die sich über den Webclient anmelden. Sie müssen nur NetWitness Platform Core-Nutzerkonten für Nutzer von Aggregation, Thick-Client und REST-API erstellen.

Verfahren im Zusammenhang mit dieser Registerkarte sind unter Hosts und Services – Verfahren beschrieben.

So rufen Sie die Registerkarte Nutzer in der Ansicht Services-Sicherheit auf:

1. Navigieren Sie in **NetWitness Platform** zu **ADMIN > Services**.
2. Wählen Sie einen Service aus, dem Sie einen Nutzer hinzufügen möchten, und wählen Sie dann  **> Ansicht > Sicherheit** aus.



Funktionen

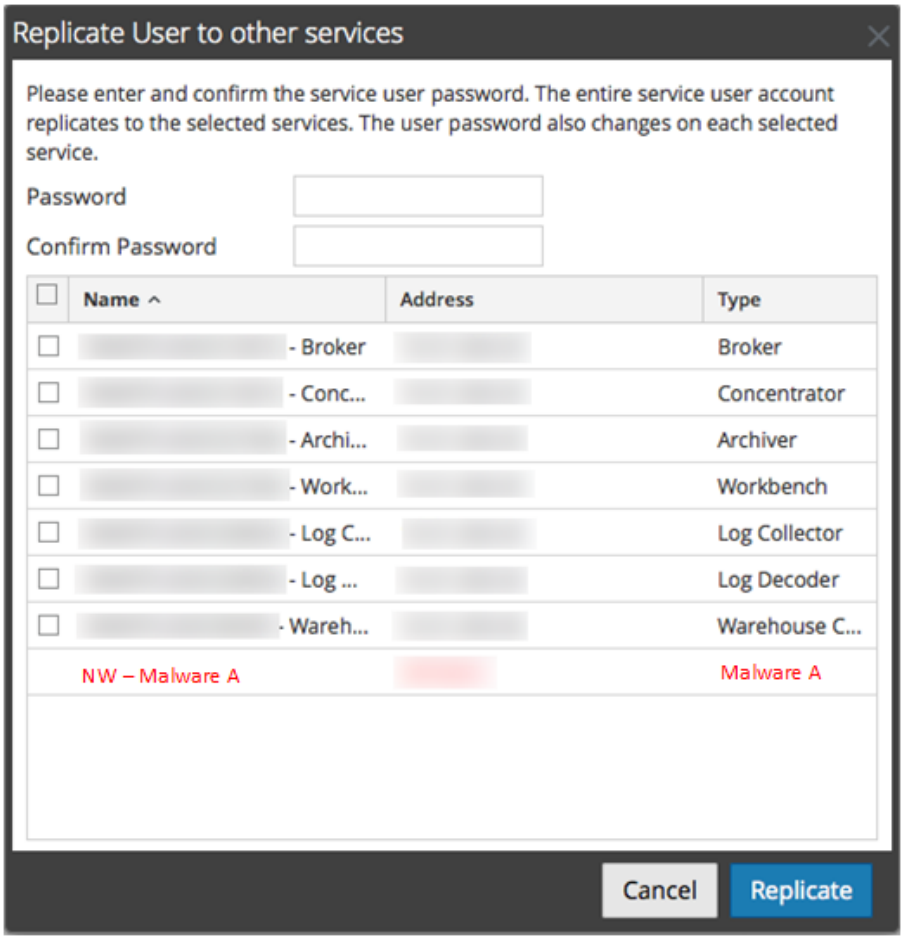
Auf der linken Seite der Registerkarte Nutzer befindet sich ein Nutzerlistenbereich. Wenn Sie einen Nutzernamen auswählen, wird der Nutzerdefinitionsbereich auf der rechten Seite verfügbar.

Nutzerlistenbereich

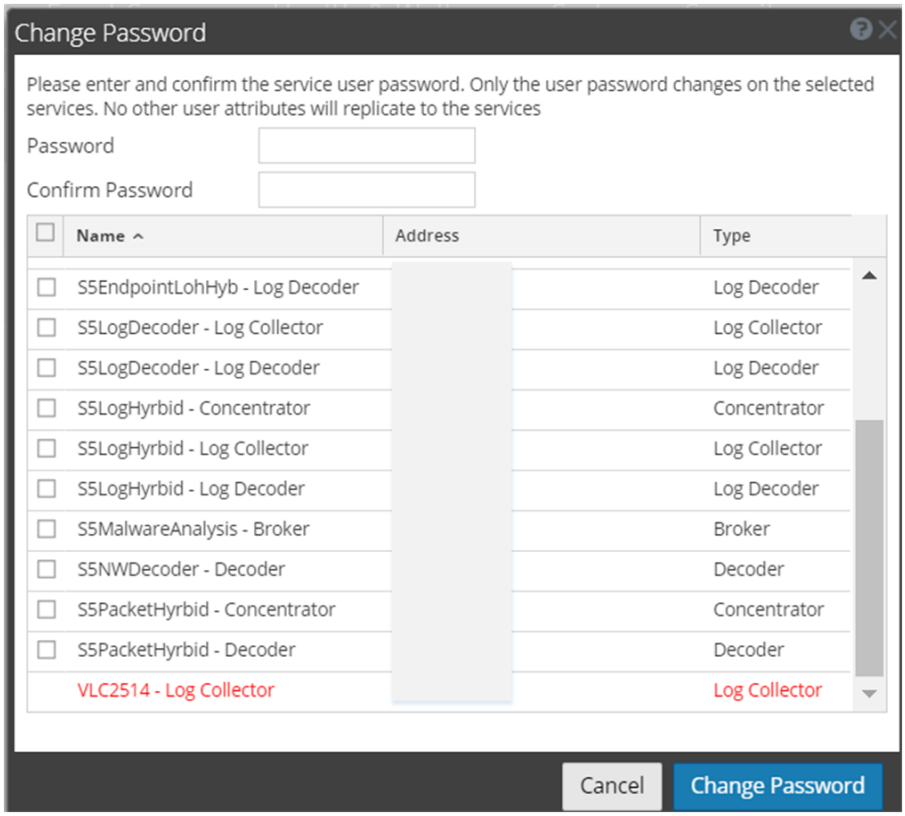
Der Nutzerlistenbereich enthält die folgenden Komponenten:

Funktion	Beschreibung
	Fügt dem aktuellen Service einen neuen Nutzer hinzu.
	Löscht die ausgewählten Nutzer von dem Service.
	Führt am ausgewählten Servicebenutzerkonto eine der folgenden Aktionen durch: • **Replizieren:** Repliziert das gesamte Servicebenutzerkonto zu den ausgewählten Services. • **Passwort ändern:** Ändert das Passwort eines Servicebenutzers und repliziert das neue Passwort zu Core-Services, in denen dieses Nutzerkonto definiert ist. Bei der Option Passwort ändern wird nur die Passwortänderung zu den betreffenden Core-Services repliziert, nicht jedoch das gesamte Nutzerkonto
Nutzername	Die Nutzernamen für alle Nutzerkonten, die auf den Service zugreifen. Der Nutzername muss einer sein, der zur Anmeldung bei NetWitness Platform verwendet wird.

Die folgende Abbildung zeigt das Dialogfeld **Nutzer in anderen Services replizieren**.



Die folgende Abbildung zeigt das Dialogfeld **Passwort ändern**.



Nutzerdefinitionsbereich

Der Nutzerdefinitionsbereich enthält drei Abschnitte:

- In Nutzerinformationen wird der Nutzer angegeben, so wie er in der Ansicht Administration-Sicherheit erstellt wurde.
- Nutzereinstellungen definieren Parameter, die für den Zugriff dieses Nutzers auf den Service gelten.
- Unter Rollenmitgliedschaft werden die Nutzerrollen definiert, zu denen der Nutzer gehört.

Es gibt zwei Schaltflächen:

- Die Schaltfläche **Speichern** speichert die Änderungen, die im Nutzerdefinitionsbereich vorgenommen wurden, und sie werden sofort wirksam.
- Wenn Sie keine Änderungen im Nutzerdefinitionsbereich gespeichert haben, setzt die Schaltfläche **Zurücksetzen** alle Felder und Einstellungen auf ihre Werte vor der Bearbeitung zurück.

Nutzerinformationen

Der Abschnitt Nutzerinformationen weist folgende Funktionen auf.

Feld	Beschreibung
Name	Der Name des Nutzers.

Feld	Beschreibung
Nutzername	Der Nutzername, den dieser Nutzer eingibt, um sich am Service anzumelden. Dies ist der NetWitness Platform-Nutzername, der erzeugt wurde, als der Administrator den Nutzer und die zugehörigen Anmeldedaten in der Ansicht **Administrationssicherheit** („Administration > Sicherheit“) hinzugefügt hat.
Passwort /Passwort bestätigen)	Das Passwort, das der Nutzer eingibt, um sich am Service anzumelden Dies ist das NetWitness Platform-Passwort, das erzeugt wurde, als der Administrator den Nutzer und die zugehörigen Anmeldedaten in der Ansicht **Administration > Sicherheit** hinzugefügt hat. Das NetWitness Platform-Kontopasswort und das Servicepasswort müssen übereinstimmen, damit der Nutzer sich über NetWitness Platform mit dem Service verbinden kann.
E-Mail	(Optional) Die E-Mail-Adresse des Nutzers
Beschreibung	(Optional) Ein allgemeines Beschreibungsfeld, um den Nutzer zu beschreiben

Nutzereinstellungen

Der Abschnitt Nutzereinstellungen hat folgende Funktionen.

Feld	Beschreibung
Authentifizierungstyp	Das Authentifizierungsschema für diesen Nutzer Die Produktlinie unterstützt interne und externe Authentifizierung. • **NetWitness** gibt die interne Authentifizierung an und ist standardmäßig aktiviert. In diesem Modus müssen sich alle Nutzer mit dem Nutzerkonto und Passwort authentifizieren, die erzeugt wurden, als der Administrator den Nutzer und die zugehörigen Anmeldedaten in der NetWitness Platform-Ansicht „Administrationssicherheit“ („Administration“ > „Sicherheit“) erstellt hat. • **Extern** gibt an, dass die Authentifizierung mit PAM (Pluggable Authentication Modules) über die Hostschnittstelle aktiviert wird. Weitere Informationen finden Sie unter **Konfigurieren der PAM-Anmeldefunktion** im Handbuch *Systemsicherheit und Nutzerverwaltung*.
Abfragepräfix	(Optional) Hängen Sie die Abfragesyntax immer an alle Abfragen von diesem Nutzer an. Zum Beispiel verhindert das Hinzufügen des Abfragepräfix **email != ceo@company.com**, dass diese E-Mail-Ergebnisse in den Sitzungen angezeigt werden.

Feld	Beschreibung
SA Core-Abfragetimeout	**Hinweis:** Dieses Feld ist nur bei NetWitness Platform-Services ab Version 10.5 verfügbar. Bei Services der Version 10.4 und niedriger wird es nicht angezeigt. In NetWitness Platform 10.4 und niedriger wird anstelle von SA Core-Abfragetimeout die Funktion „Abfrageebene“ verwendet. Gibt die maximale Dauer in Minuten an, in der ein Nutzer eine Abfrage am Service ausführen kann. Wenn dieser Wert auf Null (0) gesetzt ist, wird das Timeout für Abfrage für den Nutzer an diesem Service nicht durchgesetzt. Beim Replizieren eines Nutzers von einem NetWitness Platform-Service der Version 10.5 oder höher zu einem NetWitness Platform-Service der Version 10.4 wird das Timeout für Abfrage in die nächstmögliche Abfrageebene umgewandelt. Wenn ein Nutzer beispielsweise ein Timeout für Abfrage von 15 Minuten hat, erhält er nach der Migration die Abfrageebene 3. Hat er ein Timeout für Abfrage von 35 Minuten, erhält er nach der Migration ebenfalls die Abfrageebene 2. Hat er ein Timeout für Abfrage von 45 Minuten, erhält er nach der Migration ebenfalls die Abfrageebene 2.
Sitzungsschwellenwert	(Optional) Steuert das Verhalten dieser Anwendung beim Scannen von Metawerten zur Feststellung der Sitzungsanzahl. Jeder Metawert mit einer Sitzungsanzahl, die über dem eingestellten Schwellenwert liegt, beendet die Feststellung der tatsächlichen Sitzungsanzahl, wenn der Schwellenwert erreicht wird. Wenn ein Schwellenwert für eine Sitzung festgelegt ist, werden in der Ansicht Navigation das Erreichen des Schwellenwerts sowie der Prozentsatz der Abfragezeit, der zum Erreichen des Schwellenwertes verwendet wurde, angezeigt.

Rollenmitgliedschaft

Der Abschnitt Rollenmitgliedschaft zeigt die Rollen an, die ein Nutzer für den ausgewählten Service innehat.

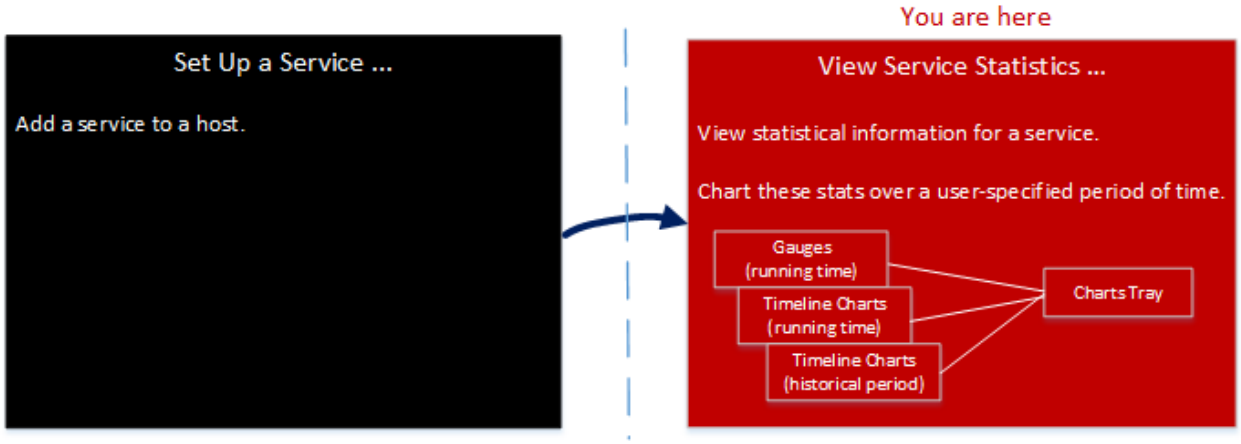
Ansicht „Services-Statistik“

In diesem Thema werden die Funktionen beschrieben, die in der NetWitness Platform-Ansicht Service-Statistik verfügbar sind.

Die Ansicht Service-Statistik ermöglicht, den Status und Betrieb von Services zu überwachen. In dieser Ansicht werden wichtige Statistiken sowie service- und hostbezogene Systeminformationen für einen Service angezeigt. Darüber hinaus können mehr als 80 Statistiken in Form von Mess- und Zeitachsendiagrammen angezeigt werden. In Verlaufs-Zeitachsendiagrammen werden ausschließlich Statistiken für Sitzungsgröße, Sitzungen und Pakete angezeigt.

Workflow

Dieser Workflow zeigt die Aufgaben, die Sie aus der Ansicht „Statistik“ ausführen.

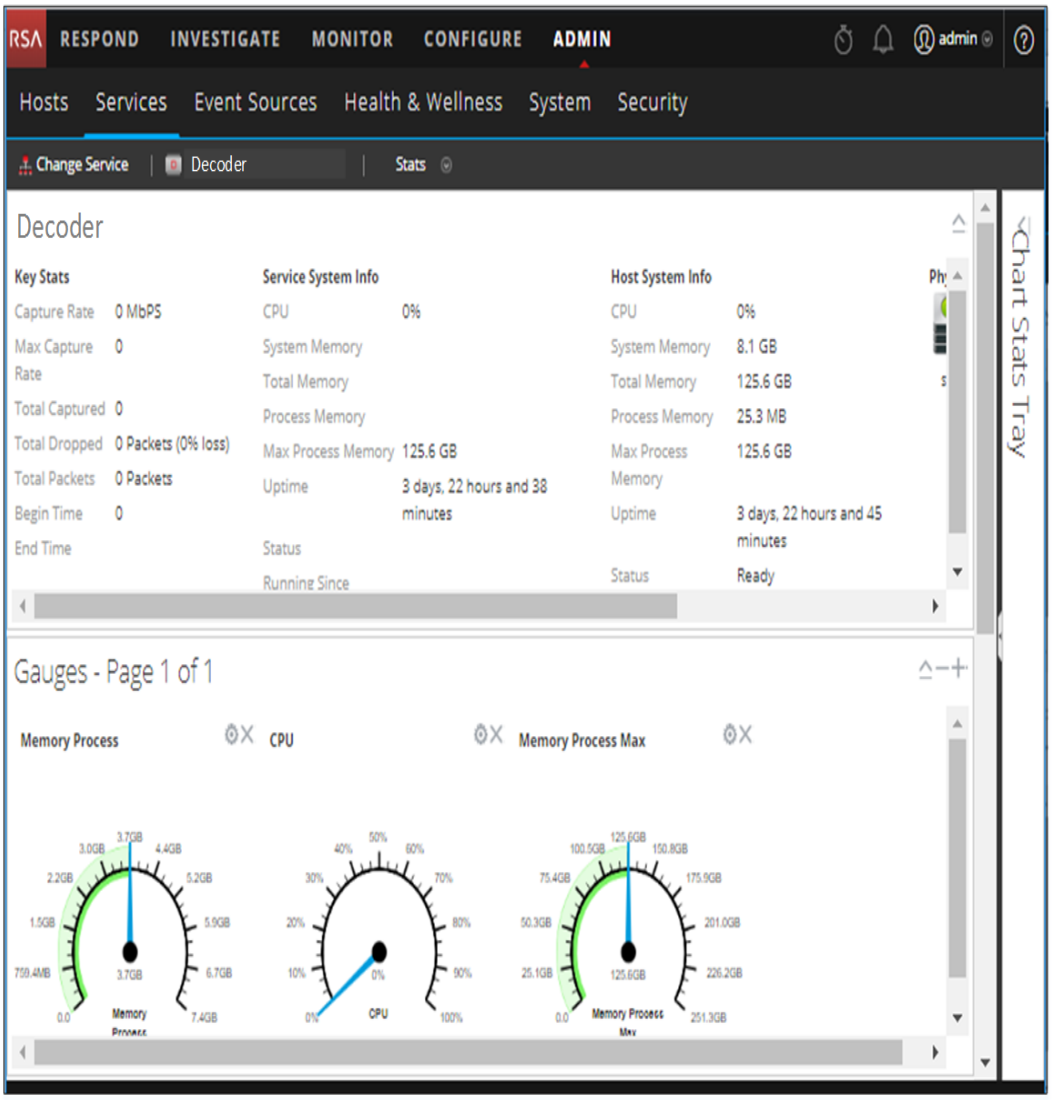


In der Ansicht „Statistik“ können Sie die überwachten Statistiken für einzelne Services anpassen.

Das folgende Beispiel zeigt, wie Sie die Ansicht Statistik für eine Decoder verwenden. Die Ansicht Statistik für alle Services bietet Ihnen die gleichen Informationen für jeden Service.

So greifen Sie auf die Ansicht Services > Statistiken zu:

1. In **NetWitness Platform** , navigieren Sie zu **ADMIN > Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie einen Service und die Optionen  **> Ansicht > Statistik** aus.



Funktionen

Zwar sind für die unterschiedlichen Servicearten verschiedene Statistiken verfügbar, aber bestimmte Elemente werden für jeden Core-Service in der Ansicht „Services-Statistik“ angezeigt:

- Abschnitt Statistikübersicht
- Abschnitt Messdiagramme
- Abschnitt Zeitachsen
- Abschnitt Verlaufszeitachsen
- Diagrammstatistikbereich

Abschnitt Statistikübersicht

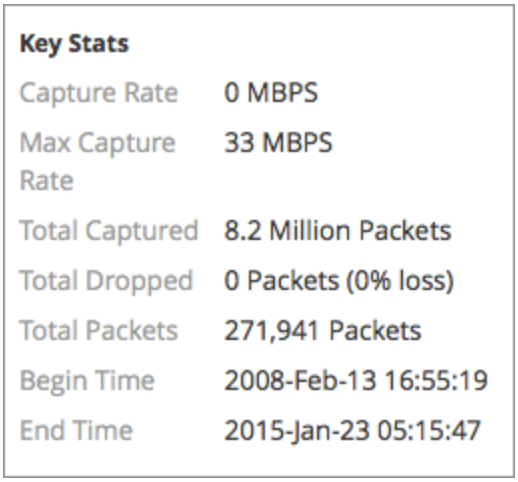
Der Abschnitt Statistikübersicht befindet sich oben in der Standardansicht und enthält keine bearbeitbaren Felder.

Der Abschnitt Statistikübersicht besteht aus fünf Bereichen. Im Bereich **Schlüsselstatistiken** werden verschiedene Statistiken für die unterschiedlichen Arten von Services angezeigt. Die verbleibenden Bereiche im Abschnitt „Statistikübersicht“ sind für alle Servicearten identisch.

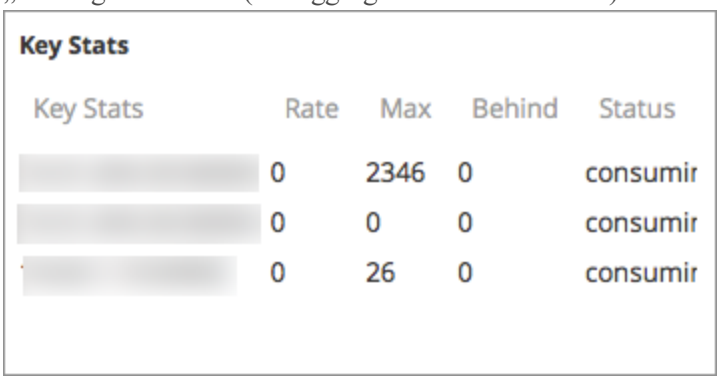
Schlüsselstatistiken

Im Bereich „Schlüsselstatistiken“ werden verschiedene Statistiken für die unterschiedlichen Arten von Services angezeigt.

- Bei einem Decoder oder Log Decoder werden Erfassungsstatistiken angezeigt, zum Beispiel Erfassungsrate, Gesamtzahl der erfassten Pakete oder Protokolle, Gesamtzahl der gelöschten Pakete oder Protokolle sowie Start- und Endzeit der Datenerfassung.

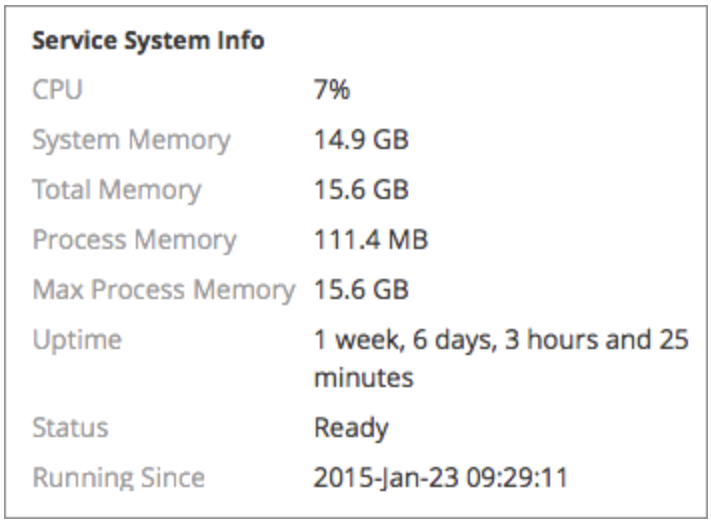


- Ein Broker oder Concentrator aggregiert Daten von mehreren Services. Aus diesem Grund werden Schlüsselstatistiken für alle aggregierten Services in einem Raster dargestellt. Die Rasterspalten geben den Namen des Services, die Erfassungsrate, die maximale Erfassungsrate, die Anzahl für „Sitzungen zurück“ (die aggregiert werden müssen) sowie den Servicestatus an.



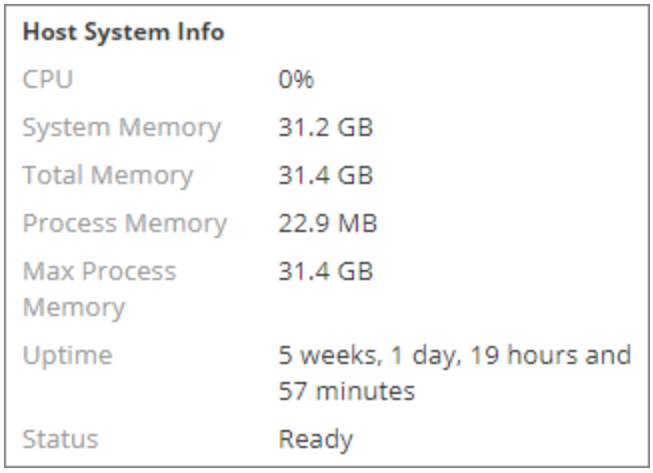
Servicesysteminformationen

Im Bereich „Servicesysteminformationen“ werden die prozentuale Auslastung der CPU durch den Service, die Statistik zur Speicherauslastung (System, gesamt, Prozess und maximaler Prozess), die Betriebszeit des Services, der Status, die Startzeit der aktuellen Ausführung und die aktuelle Zeit angegeben.



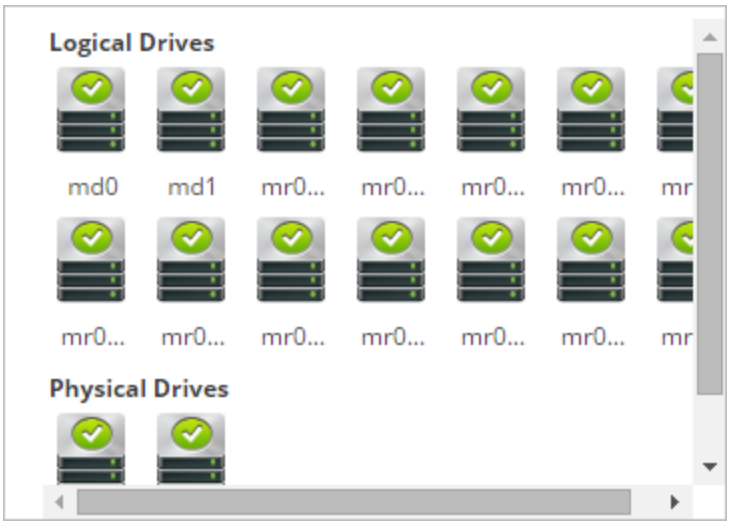
Service System Info	
CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	111.4 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 25 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

Hostsysteminformationen enthält die prozentuale Auslastung der CPU durch den Host, die Statistik zur Speicherauslastung (System, gesamt, Prozess und maximal), die Betriebszeit des Hosts, den Status, die Startzeit der aktuellen Ausführung und die aktuelle Zeit.



Host System Info	
CPU	0%
System Memory	31.2 GB
Total Memory	31.4 GB
Process Memory	22.9 MB
Max Process Memory	31.4 GB
Uptime	5 weeks, 1 day, 19 hours and 57 minutes
Status	Ready

Logische Laufwerke und **Physische Laufwerke** werden jeweils zusammen mit einem Symbol für den Laufwerksnamen und Status angezeigt. Darunter werden die in den Namen verwendeten Laufwerkstypen und die Statusoptionen für das Laufwerk angegeben.



Laufwerkstypen und -status

Laufwerkstyp	Beschreibung	Anmerkung	Status-Optionen
sd	SCSI-Blockgerät	Direkt verbundene SAS-, SATA-MegaRAID-Volumes	OK (grün) FAIL (rot)
ld	Logisches MegaRAID-Volume	Im BIOS oder mit dem MegaCLI-Tool definiert	OK (grün) DEGRADED (gelb) BUILDING (gelb) FAIL (rot)
pd	Physische MegaRAID-Festplatten	Keine direkte Verbindung mit Linux	OK (grün) FAIL (rot)
md	RAID-Volume mit Linux-Software		OK (grün) DEGRADED (gelb) BUILDING (gelb) FAIL (rot)

Messdiagramme

Im Abschnitt Messdiagramme in der Statistik-Ansicht werden Statistiken in Form von analogen Messdiagrammen angezeigt. Weitere Informationen zur Konfiguration von Messdiagrammen erhalten Sie unter Funktionen.

Zeitachsen

Zeitachsendiagramme zeigen die ausgewählten Statistiken in einem laufenden Zeitplan an, wobei der Schwerpunkt auf dem aktuellen Zeitpunkt liegt. Dies gilt für alle Arten von Services und nur der angezeigte Name des Zeitplans kann bearbeitet werden. Weitere Informationen zur Konfiguration von Zeitplänen erhalten Sie unter Zeitachsendiagramm.

Verlaufszeitachsen

Verlaufs-Zeitachsendiagramme zeigen Statistiken mit Sitzungsgröße, Sitzungen und Paketen auf einer Verlaufszeitachse dar. Dies gilt für alle Arten von Services und es können jeweils der angezeigte Name, das Start- und das Enddatum bearbeitet werden. Weitere Informationen zur Konfiguration von Zeitplänen erhalten Sie unter Zeitachsendiagramm.

Hinweis: Das Verlaufs-Zeitachsendiagramm für Log Collector, Virtual Log Collector (VLC) und Windows Legacy Collector-Services ist veraltet.

Diagrammstatistikbereich

Im Diagrammstatistikbereich werden alle verfügbaren Statistiken für den ausgewählten Servicetyp aufgeführt. Verschiedene Services überwachen unterschiedliche Statistiken. Eine ausführliche Beschreibung finden Sie unter Komponenten.

Themen

- Komponenten
- Funktionen
- Zeitachsendiagramm

Diagrammstatistikbereich

In diesem Thema wird der Diagrammstatistikbereich in der Ansicht Service-Statistik dargestellt.

In der Ansicht Service-Statistik bietet der Diagrammstatistikbereich eine Möglichkeit, die angezeigten Statistiken für individuelle Services anzupassen. Die Diagrammstatistikbereich listet alle verfügbaren Statistiken für den Service auf. Die Anzahl an Statistiken variiert je nach überwachtem Servicetyp. Jede Statistik im Diagrammstatistikbereich kann in einem Messdiagramm oder in einem Zeitplandiagramm angezeigt werden. Nur Statistiken für Sitzungsgröße, Sitzungen und Pakete sind in Verlaufs-Zeitachsendiagrammen sichtbar.

So greifen Sie auf die Ansicht „Service-Statistik“ zu:

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **Administration > Services** aus.

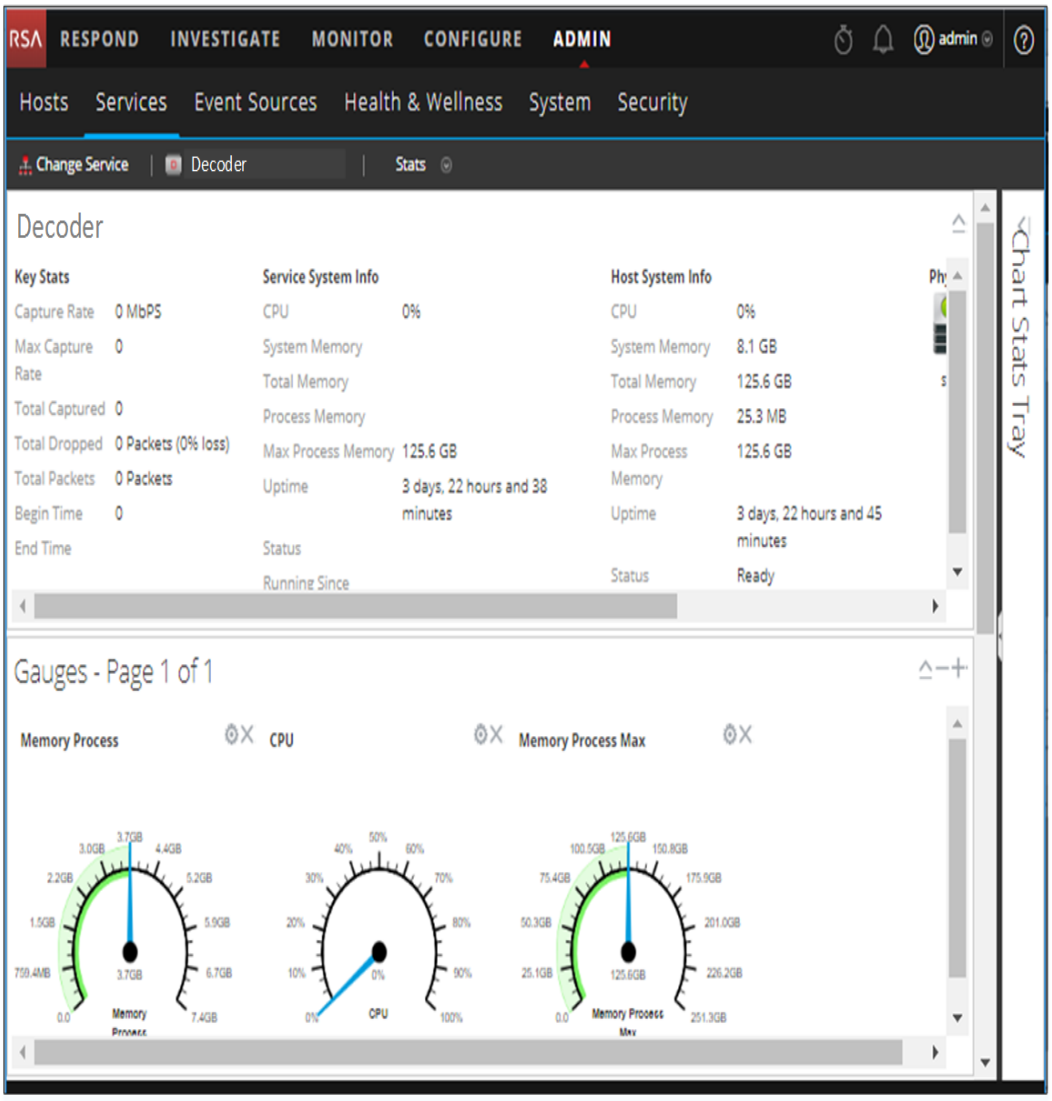
   Die Ansicht „Administrationsservices“ wird angezeigt.

2. Wählen Sie einen Service aus und klicken Sie auf  **> Ansicht > Statistiken**.

   Der Diagrammstatistikbereich befindet sich auf der rechten Seite.

3. Wenn der Bereich ausgeblendet wird, klicken Sie auf  , um die Liste der verfügbaren Statistiken anzuzeigen.

Das folgende Beispiel zeigt die Ansicht Services-Statistik für einen Decoder. Der Diagrammstatistikbereich wird reduziert.



Komponenten

Der Diagrammstatistikbereich verfügt über verschiedene Statistiken für unterschiedliche Servicetypen. In dem oben stehenden Beispiel stehen 111 Statistiken für den Decoder zur Verfügung. Die folgende Tabelle beschreibt die Funktionen des Diagrammstatistikbereichs.

Funktion	Beschreibung
<|	Klicken Sie hier, um den Bereich horizontal zu vergrößern.
|>	Klicken Sie hier, um den Bereich horizontal zu verkleinern.

Funktion	Beschreibung
Suchen	Geben Sie einen Suchbegriff in das Feld ein und drücken Sie die **RETURN**-Taste. Passende Statistiken werden mit markiertem passenden Wort angezeigt.
«	Klicken Sie hier, um die erste Seite anzuzeigen.
‹	Klicken Sie hier, um die vorherige Seite anzuzeigen.
Page 5 of 200	Geben Sie eine Seitennummer in das Seitenfeld ein.
›	Klicken Sie hier, um die nächste Seite anzuzeigen.
»	Klicken Sie hier, um die letzte Seite anzuzeigen.
↻	Klicken Sie hier, um die Ansicht zu aktualisieren.
Stats 1 - 12 of 111	Zeigt die angezeigte Reihe an Statistiken an. Die Gesamtanzahl an Statistiken variiert je nach Servicetyp.

Messdiagramme

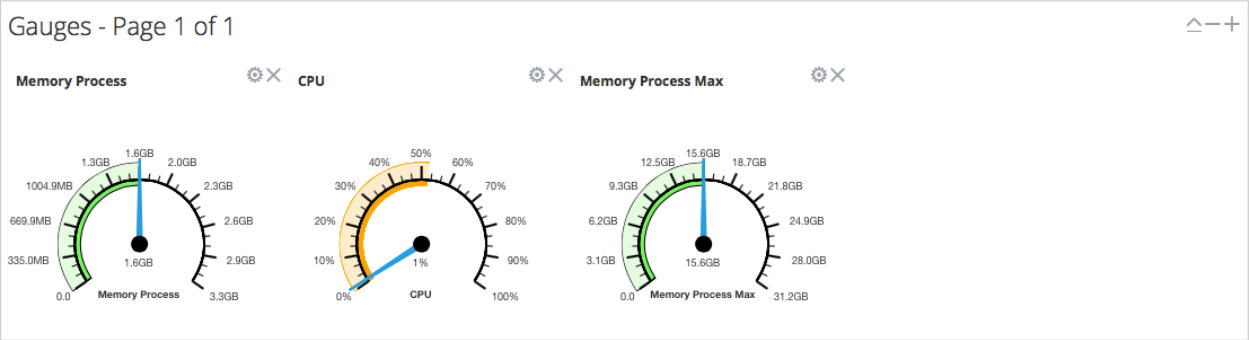
In diesem Thema werden die Funktionen des Abschnitts Messdiagramme der Ansicht Service-Statistik eingeführt.

Der Abschnitt Messdiagramme der Ansicht Service-Statistik präsentiert Statistiken in Form eines analogen Rundinstruments. Sie können jede beliebige verfügbare Statistik im Diagrammstatistikbereich im Abschnitt Messdiagramme ziehen und dort ablegen. Die Eigenschaften jedes einzelnen Messdiagramms sind bearbeitbar; alle Messdiagramme haben einen bearbeitbaren Titel und einige verfügen über zusätzliche bearbeitbare Eigenschaften.

So greifen Sie auf die Ansicht Service-Statistik zu:

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **ADMIN > Services** aus.
   Die Ansicht „Administration“ > „Services“ wird angezeigt.
2. Wählen Sie einen Service und die Optionen  **> Ansicht > Statistik** aus.
   Die Ansicht Service-Statistik beinhaltet den Abschnitt Messdiagramme.

In der folgenden Abbildung werden die Standardmessdiagramme in der Ansicht „Servicestatistik“ für einen Log Decoder gezeigt.



Funktionen

Die Standardmessdiagramme zeigen folgende Statistiken:

- Prozess-Speichernutzung
- CPU-Nutzung
- Maximal verwendeter Prozess-Speicher

Die Steuerelemente in der Titelleiste Messdiagramme und in den einzelnen Messdiagrammen sind die Standardsteuerelemente für Dashlets.

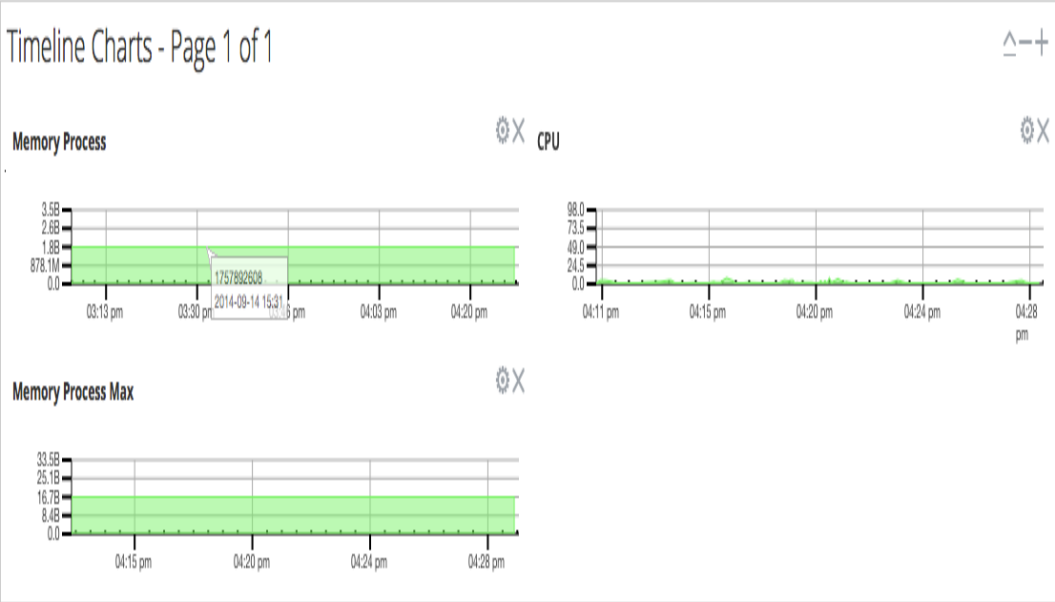
- In der Titelleiste „Messdiagramme“ können Sie den Abschnitt ausblenden und einblenden und eine Seite vor oder zurück gehen.
- In jedem Messdiagramm können Sie Eigenschaften bearbeiten ( ) und das Messdiagramm löschen ( ).

Zeitachsendiagramm

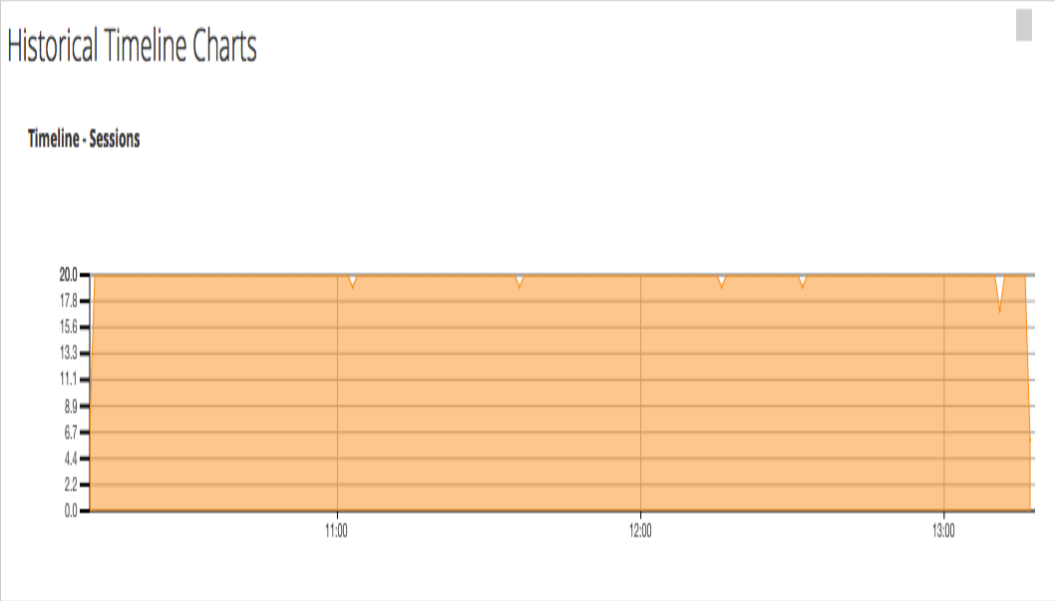
In diesem Thema werden die Funktionen der Zeitachsendiagramme in der Ansicht Services-Statistik erläutert.

Zeitachsendiagramme zeigen Statistiken in einem laufenden Zeitplan an. Die Ansicht Services-Statistik umfasst zwei Zeitplantypen: Aktueller Zeitplan und historischer Zeitplan. Sie können jede beliebige verfügbare Statistik in die Diagrammstatistikbereich im Bereich „Zeitachsendiagramm“ ziehen und ablegen. Nur Statistiken für Sitzungsgröße, Sitzungen und Pakete sind in Verlaufs-Zeitachsendiagrammen sichtbar. Die Eigenschaften eines Zeitachsendiagramms lassen sich bearbeiten, ebenso wie die Titel aller Zeitachsendiagramme. Außerdem lassen sich bei einigen Zeitachsendiagrammen weitere Eigenschaften bearbeiten.

In der folgenden Abbildung ist ein Beispiel für einen aktuellen Zeitplan mit dem Wert und dem Zeitstempel eines Datenpunktes dargestellt.



Die folgende Abbildung zeigt ein Beispiel für ein Verlaufs-Zeitachsendiagramm.



In den standardmäßigen Zeitachsendiagrammen werden folgende Statistiken angezeigt:

- Speicherprozess
- CPU
- Max. Speicherprozess

In den Verlaufs-Zeitachsendiagrammen werden folgende Statistiken angezeigt:

- Sitzungen
- Pakete

- Sitzungsgröße

Die Steuerelemente in der Titelleiste „Zeitachsendiagramm“ und in den einzelnen Zeitplänen sind Standard-Dashlet-Steuerelemente.

- In der Titelleiste „Zeitachsendiagramm“ können Sie den Abschnitt aus- und einblenden und vor- und zurückblättern.
- In jedem Zeitplan können Sie die Eigenschaften bearbeiten ( ) und den Zeitplan löschen ( ).
- Wenn Sie den Mauszeiger über einen Datenpunkt im Diagramm bewegen, werden der Wert und der Zeitstempel für den ausgewählten Punkt angezeigt.

Systemansicht

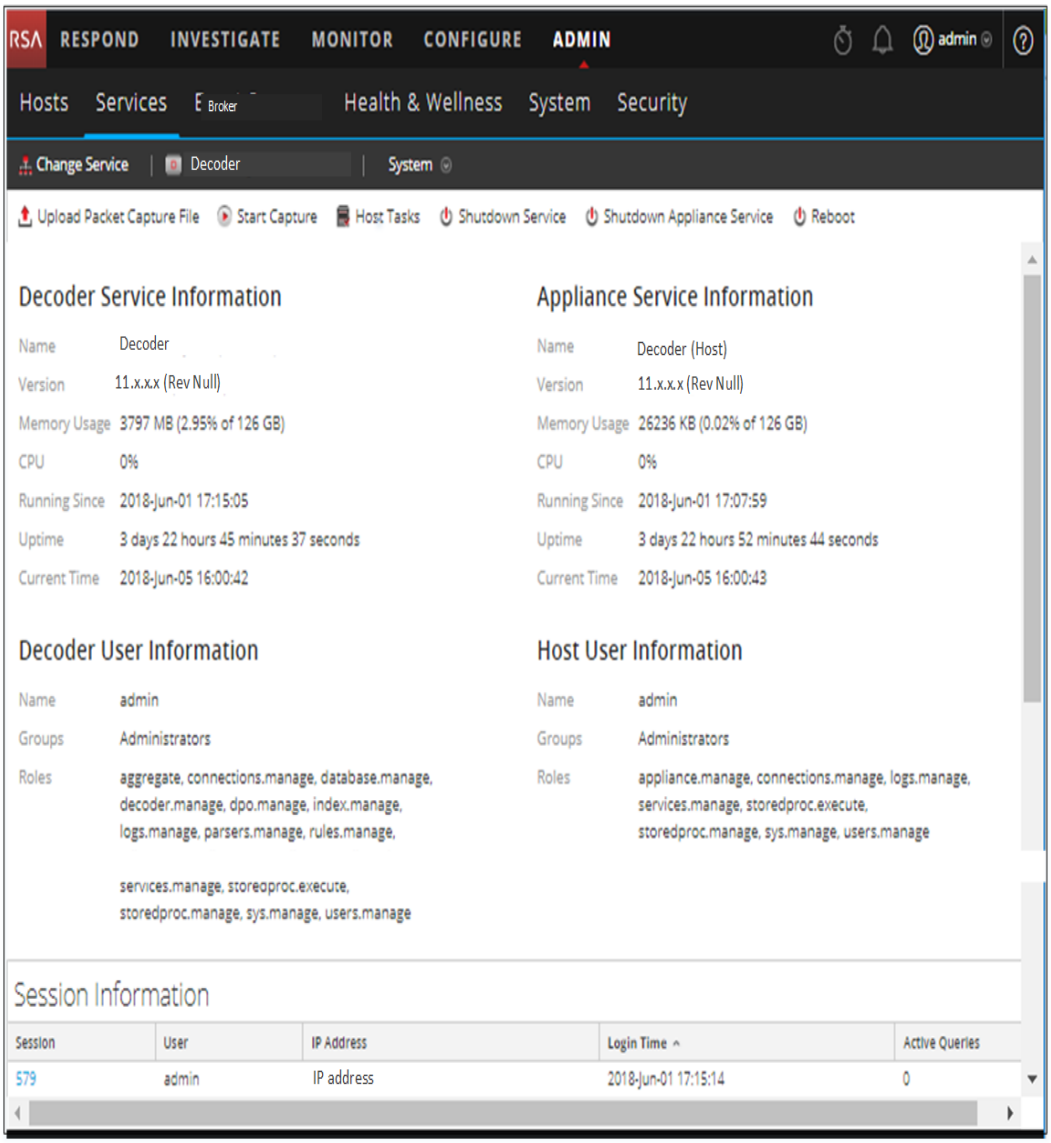
In diesem Thema werden Funktionen in der Ansicht System am Beispiel von Decoder und Log Decoder vorgestellt. Weitere Informationen finden Sie in den Konfigurationsleitfäden der einzelnen Services (z. B. im *Broker- und Concentrator-Konfigurationsleitfaden* für den *RSA NetWitness® Platform*) unter **Administration > Services > System**.

Ein Log Decoder ist ein spezieller Typ Decoder und wird ähnlich wie ein solcher konfiguriert und gemanagt. Daher bezieht sich ein Großteil der Informationen in diesem Abschnitt auf beide Arten Decoder. Auf Unterschiede für Log Decoder wird hingewiesen.

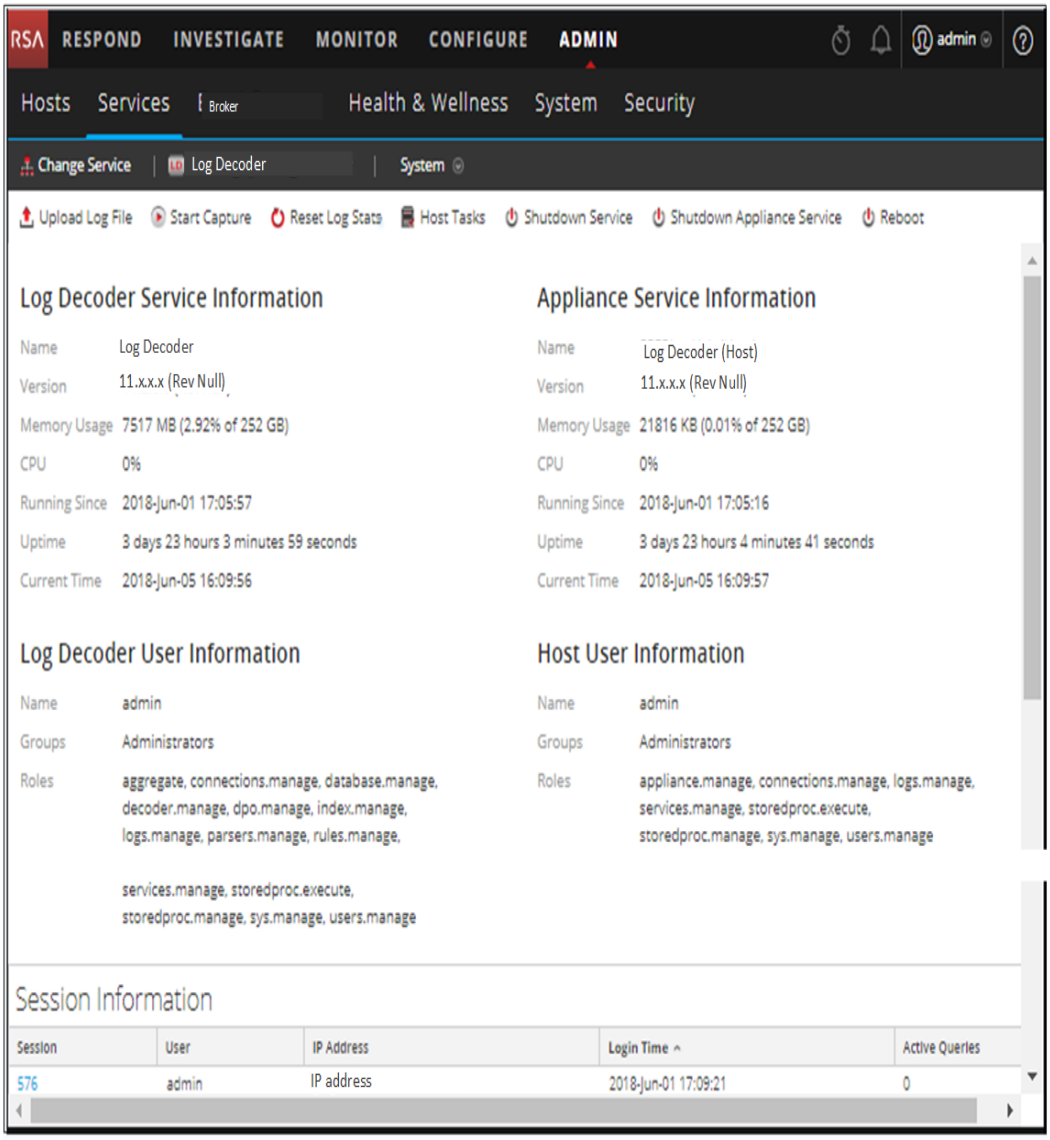
So greifen Sie auf die Ansicht System zu einem Decoder zu:

1. Navigieren Sie im Menü **NetWitness Platform** zu **Administration > Services.**
   Die Ansicht -Services wird angezeigt.
2. Wählen Sie einen Service und dann  **> Ansicht > System** aus.

Die folgende Abbildung zeigt ein Beispiel der Servicesystemansicht für einen Decoder.



Die folgende Abbildung zeigt die Servicesystemansicht für einen Log Decoder.



Funktionen

Symbolleiste Serviceinfo

In den folgenden Symbolleisten sind die spezifischen Optionen für Decoder und Log Decoder gezeigt.

Zusätzlich zu den gemeinsamen Optionen in der Symbolleiste der Ansicht „Services > System“ können Sie die Erfassung von Paketen oder Protokollen starten und beenden. Die Uploaddateioptionen für den Standard-Decoder (Paketerfassungsdatei) und den Log Decoder (Protokolldatei) sind unterschiedlich.

Aktion	Beschreibung
Hochladen einer Paketerfassungsdatei	Es wird ein Dialogfeld angezeigt, in dem eine Paketerfassungsdatei (.pcap) für das Hochladen zu dem ausgewählten Decoder ausgewählt werden kann. Weitere Informationen finden Sie unter **Hochladen einer Paketerfassungsdatei** im *Konfigurationsleitfaden für Decoder und Log Decoder*. **Hinweis:** Diese Option gilt nicht für Log Decoder.
Hochladen einer Protokolldatei	Es wird ein Dialogfeld angezeigt, in dem eine Protokolldatei (.log) für das Hochladen zu dem gewählten Log Decoder ausgewählt werden kann. Weitere Informationen finden Sie unter **Hochladen einer Protokolldatei an einen Log Decoder** im *Konfigurationsleitfaden für Decoder und Log Decoder*.
Starten/Beenden der Erfassung	Startet die Paketerfassung auf dem ausgewählten Decoder. Wenn die Paketerfassung ausgeführt wird, ändert sich die Option in der Symbolleiste zu Erfassung beenden und die Option zum Hochladen einer Datei ist nicht verfügbar.

Dialogfeld „Hostaufgabenliste“

In diesem Thema wird das Dialogfeld Hostaufgabenliste in der Ansicht Services > System beschrieben.

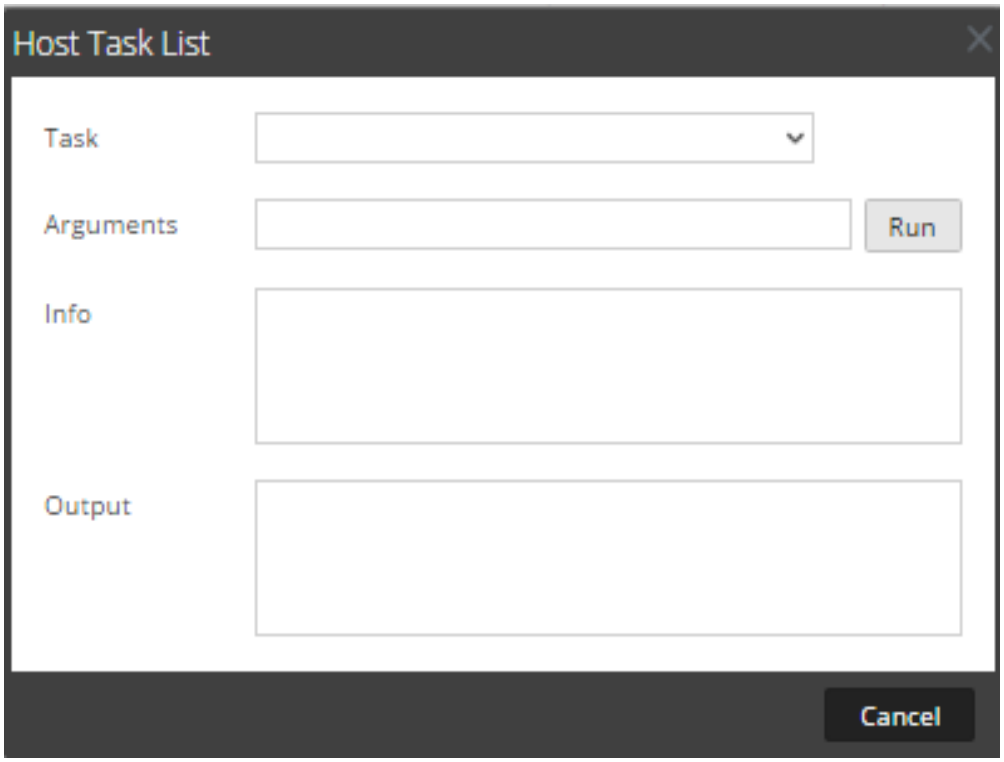
Sie können in der RSA NetWitness Platform-Ansicht Services > System die Option Hostaufgaben verwenden, um Aufgaben zu verwalten, die einen Host und dessen Kommunikation mit dem Netzwerk betreffen. Mehrere Service- und Hostkonfigurationsoptionen sind für Core-Services verfügbar.

So greifen Sie auf das Dialogfeld Hostaufgaben zu:

1. Wählen Sie in **NetWitness Platform** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Service aus und klicken Sie auf  > **Ansicht** > **System**.

   Die Ansicht „System“ für den Service wird angezeigt.
3. Klicken Sie in der Ansicht **Services > System** auf **Hostaufgaben**.

   Das Dialogfeld „Hostaufgabenliste“ wird angezeigt. Die **Aufgabenliste** stellt eine Liste mit unterstützen Meldungen für den entsprechenden Host zur Verfügung.



Funktionen

Die unten stehende Tabelle beschreibt die Funktionen des Dialogfelds.

Feld	Beschreibung
Aufgabe	Ein Eingabefeld, in das Sie eine Meldung für einen Core-Host eingeben oder aus dem Sie diese auswählen. Wenn Sie auf dieses Feld klicken, wird eine Drop-down-Liste mit verfügbaren Hostaufgaben angezeigt.

Feld	Beschreibung
Argumente	Ein Eingabefeld, in das Sie Argumente für die Meldung eingeben
Ausführen	Führt die in den Eingabefeldern erfassten Aufgaben und Argumente aus
Info	Informationen zum Zweck und der Syntax der Meldung
Ausgabe	Ausgabe oder Ergebnis einer ausgeführten Aufgabe
Abbrechen	Schließt das Dialogfeld Hostaufgabenliste

Auswahlliste Hostaufgaben

Diese Aufgaben werden als Drop-down-Liste im Feld „Aufgabe“ angezeigt. Die verfügbaren Optionen werden durch die Sicherheitsrolle bestimmt, die zur Ausführung der Option benötigt wird.

Aufgabe	Beschreibung
Dateisystemüberwachung hinzufügen	Startet die Überwachung der Speicherservices, die mit dem angegebenen Dateisystem zusammenhängen (siehe Hinzufügen und Löschen einer Dateisystemüberwachung).
Dateisystemüberwachung löschen	Beendet die Überwachung der Speicherservices, die mit dem angegebenen Dateisystem zusammenhängen.
Host neu starten	Fährt den Host herunter und startet ihn neu (siehe Neustarten eines Hosts).
Interne Uhr des Hosts einstellen	Stellt die lokale Uhrzeit des Hosts ein (siehe Einstellen der internen Uhr des Hosts).
Hostnamen des Hosts festlegen	Diese Methode der Änderung des Hostnamens ist in NetWitness Platform 10.6 veraltet und wird durch das unter Hosts und Services – Verfahren beschriebene Verfahren ersetzt
Netzwerkkonfiguration festlegen	Legt Netzwerkadressen-Parameter fest (siehe Festlegen der Netzwerkkonfiguration).
Quelle für die Netzwerkzeit festlegen	Legt die Uhrzeitquelle für diesen Host fest (siehe Festlegen der Quelle für die Netzwerkzeit)
Syslog-Weiterleitung einrichten	Aktiviert oder deaktiviert die Syslog-Weiterleitung von einem Remoteserver zum ausgewählten Service (siehe Einrichten der Syslog-Weiterleitung).
Netzwerkportstatus anzeigen	Zeigt die Netzwerkschnittstelleninformationen für einen Host an (siehe Anzeigen des Netzwerkportstatus).
Seriennummer anzeigen	Ruft die Seriennummer des Hosts ab (siehe Anzeigen der Seriennummer).
Host herunterfahren	Fährt den physischen Host herunter und der Host bleibt ausgeschaltet (siehe Herunterfahren des Hosts).

Aufgabe	Beschreibung
Service starten	Startet einen Service auf diesem Host (siehe Starten, Beenden oder Neustarten eines Service).
Service anhalten	Beendet einen Service auf diesem Host.
setSNMP	Aktiviert oder deaktiviert den SNMP-Service auf einem Host (siehe Festlegen des SNMP).

Servicekonfigurationseinstellungen

In diesem Thema werden die verfügbaren Servicekonfigurationseinstellungen für RSA NetWitness Platform Core-Services erläutert.

Zu den NetWitness Platform Core-Services gehören Broker, Concentrator, Decoder, Log Decoder, Archiver und der Appliance-Service. Die in diesen Tabellen aufgeführten Servicekonfigurationsparameter beinhalten alle anzeigbaren und konfigurierbaren Parameter. Einige Parameter können in verschiedenen Bereichen der NetWitness Platform-Benutzeroberfläche konfiguriert werden, während andere nur in der Serviceübersicht angezeigt und konfiguriert werden können.

Appliance-Servicekonfigurationsparameter

In diesem Thema werden die verfügbaren Konfigurationsparameter für den NetWitness Platform Core Appliance-Service aufgelistet und beschrieben.

Der NetWitness Platform Core Appliance-Service bietet Hardwareüberwachung auf Legacy-NetWitness-Hardware.

In dieser Tabelle werden die Konfigurationsparameter der Appliance beschrieben.

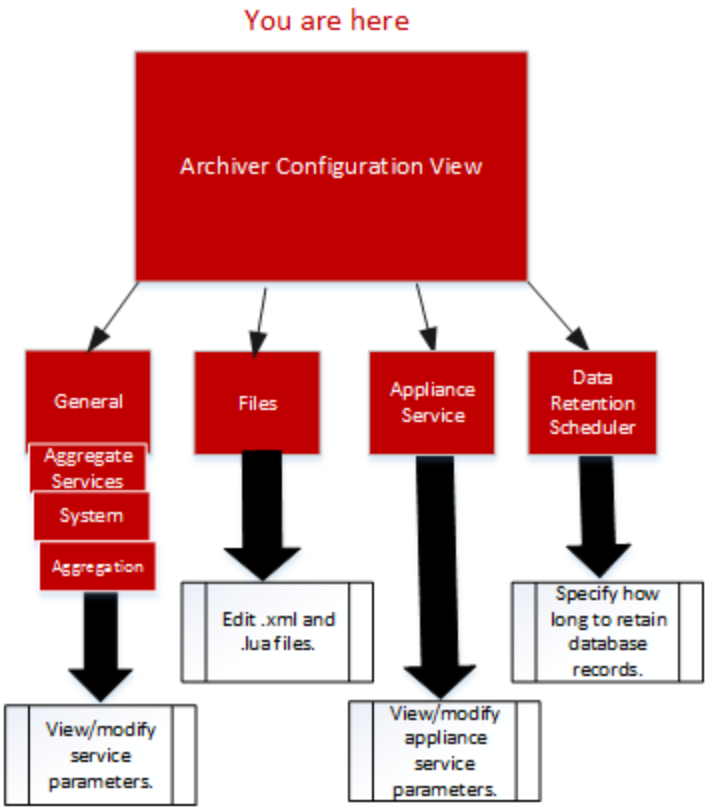
Appliance-Parameterfeld	Beschreibung
Protokolle	/logs/config, siehe Konfigurationsparameter der Core-Service-Protokollierung
REST	/rest/config, siehe Konfigurationsparameter für die REST-Schnittstelle
Services	/services/<service name>/config, siehe Core-Service-to-Service-Konfigurationsparameter
System	/sys/config, siehe Core-Service-Systemkonfigurationsparameter

Ansicht Archiver-Servicekonfiguration

In diesem Thema werden die verfügbaren Konfigurationseinstellungen für NetWitness Platform-Archiver aufgeführt und beschrieben.

Workflow

Der folgende Workflow zeigt die Konfigurationsaufgaben für den Archiver-Service.



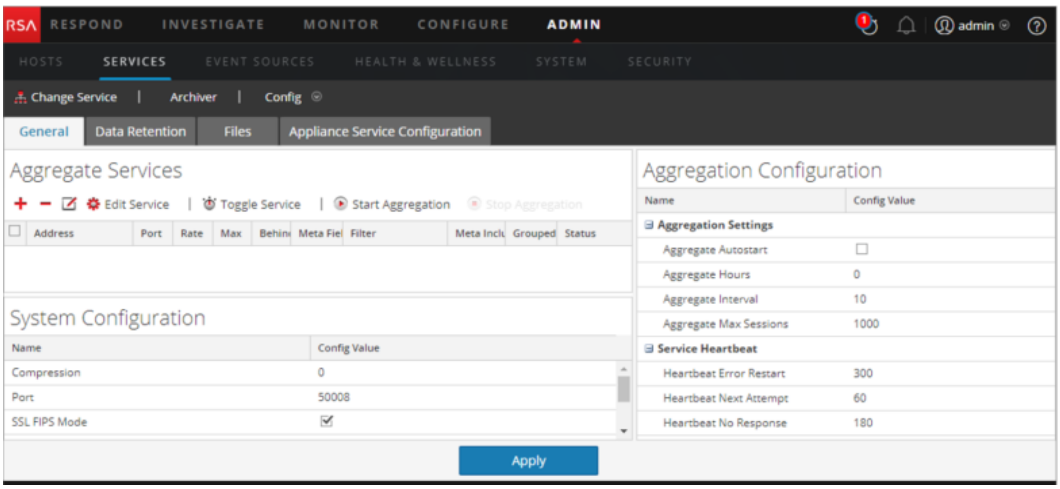
Rolle	Ziel
Administrator	Konfigurieren von Metafiltern für Aggregation Anweisungen finden Sie unter „(Optional) Konfigurieren von Metafiltern für Aggregation“ im *RSA-NetWitness PlatformKonfigurationsleitfaden Archiver*.
Administrator	Konfiguration der Gruppenaggregation Weitere Informationen finden Sie unter „Konfiguration der Gruppenaggregation“ im *RSA-NetWitness PlatformLeitfaden zur Bereitstellung*.

Überblick

So greifen Sie auf die Ansicht „Service-Konfiguration“ zu:

1. Wählen Sie in **NetWitness Platform** die Option **ADMINISTRATION > Services** aus.
   Die Ansicht „Admin > Services“ wird angezeigt.
2. Wählen Sie einen Archiver-Service und dann  **>Ansicht > Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ für den Archiver-Service wird angezeigt.

Im folgenden Beispiel ist die Ansicht „Services > Konfiguration“ für einen Archiver gezeigt.



Broker-Servicekonfigurationsparameter

Dieses Thema beschreibt die Konfigurationsparameter für NetWitness Platform-Broker.

In dieser Tabelle werden die Broker-Konfigurationsparameter aufgeführt und erläutert.

Broker-Parameterfeld	Beschreibung
Broker	/broker/config, siehe Aggregationskonfigurationsparameter
aggregate.interval.behind	Mindestanzahl an Millisekunden, bevor eine weitere Aggregationsrunde angefordert wird, wenn der Broker im Rückstand ist. Die Änderung wird sofort wirksam.
Datenbank	/database/config, siehe **Datenbankkonfigurations-Nodes** im *NetWitness Platform Core-Services-Datenbank-Tuning-Leitfaden*
Index	/index/config
index.dir	Das Verzeichnis, in dem die Broker-Gerätezuordnungsdateien gespeichert werden. Die Änderung wirkt sich beim Serviceneustart aus.
language.filename	Die Indexsprachspezifikation (XML), die beim Starten geladen wird. Änderungen erfordern einen Neustart des Service.
Protokolle	/logs/config, siehe Konfigurationsparameter der Core-Service-Protokollierung
REST	/rest/config, siehe Konfigurationsparameter für die REST-Schnittstelle
SDK	/sdk/config, siehe **SDK-Konfigurations-Nodes** im *NetWitness Platform Core-Services-Datenbank-Tuning-Leitfaden* und Modi für Systemrollen der NetWitness Platform Core-Services
Services	/services/<servicename>/config, siehe Core-Service-to-Service-Konfigurationsparameter
System	/sys/config, siehe Core-Service-Systemkonfigurationsparameter

Aggregationskonfigurationsparameter

In diesem Thema werden die Konfigurationsparameter aufgeführt und beschrieben, die für alle Services verfügbar sind, die Aggregationen ausführen, z. B. NetWitness Platform-Concentrator und -Archiver.

In dieser Tabelle sind die Parameter enthalten, die die Aggregation in einem Aggregationsservice steuern.

Konfigurationspfad	/concentrator/config oder /archiver/config
aggregate.autostart	Startet die Aggregation nach einem Serviceneustart automatisch neu, sofern aktiviert. Die Änderung wird sofort wirksam.
aggregate.buffer.size	Zeigt die Größe des bei jeder Aggregationsrunde verwendeten Puffers an (Standardeinheit ist KB). Größere Puffer verbessern möglicherweise die Aggregationsperformance, könnten aber die Abfrageperformance beeinträchtigen. Die Änderung wird nach einem Aggregationsneustart wirksam.
aggregate.crc	Ist dies aktiviert, werden alle Aggregationsstreams durch CRC-Prüfsummen validiert. Die Änderung wird sofort wirksam.
aggregate.hours	Zeigt die maximale Anzahl der Stunden an, nach denen ein Service mit der Aggregation beginnen soll. Die Änderung wird sofort wirksam.
aggregate.interval	Gibt die Mindestanzahl der Millisekunden an, die vergehen sollen, bis eine neue Aggregationsrunde angefordert wird. Die Änderung wird sofort wirksam.
aggregate.meta.page.factor	Gibt die zugeordnete Anzahl der Metaseiten pro Sitzung an, die für die Aggregation verwendet werden. Die Änderung wirkt sich beim Serviceneustart aus.
aggregate.meta.perpage	Gibt die zugeordnete Anzahl der Metadaten an, die auf einer Datenseite gespeichert werden. Die Änderung wirkt sich beim Serviceneustart aus.
aggregate.precache	Bestimmt, ob der Concentrator ein Precaching der nächsten Aggregationsrunde für vorgelagerte Services durchführt. Dies kann die Aggregationsperformance verbessern, könnte aber die Abfrageperformance beeinträchtigen. Die Änderung wird sofort wirksam.
aggregate.sessions.max	Gibt die Anzahl der in jeder Runde zu aggregierenden Sitzungen an. Die Änderung wird nach einem Aggregationsneustart wirksam.
aggregate.sessions.perpage	Gibt die Anzahl der Sitzungen an, die auf einer Datenseite gespeichert werden. Die Änderung wirkt sich beim Serviceneustart aus.
aggregate.time.window	Zeigt das maximale +/- -Zeitfenster in Sekunden an, in dem sich alle Services befinden müssen, bevor eine weitere Aggregationsrunde angefordert wird. Bei der Angabe von null wird das Zeitfenster deaktiviert. Die Änderung wird sofort wirksam.
consume.mode	Legt fest, ob der Concentrator je nach Lizenzeinschränkungen nur lokal oder auch über ein Netzwerk aggregieren kann. Die Änderung wirkt sich beim Serviceneustart aus.

Konfigurationspfad	/concentrator/config oder /archiver/config
export.enabled	Ermöglicht den Export von Sitzungsdaten, sofern aktiviert. Die Änderung wirkt sich beim Serviceneustart aus.
export.expire.minutes	Listet die Anzahl der Minuten bis zum Ablauf und zur Leerung von Exportcachedateien auf. Die Änderung wird sofort wirksam.
export.format	Bestimmt das beim Datenexport verwendete Dateiformat. Die Änderung wirkt sich beim Serviceneustart aus.
export.local.path	Zeigt den lokalen Speicherort zum Cachen exportierter Daten an. Optionale zugewiesene maximale Größe (=#Einheit). Einheiten sind: t für TB; g für GB, m für MB. Die Änderung wirkt sich beim Serviceneustart aus.
export.meta.fields	Bestimmt, welche Metafelder exportiert werden. Kommaliste von Feldern. Stern bedeutet alle Felder. Stern plus Feldliste bedeutet alle Felder mit Ausnahme der aufgelisteten Felder. Nur Feldliste bedeutet, es werden nur diese Felder eingeschlossen. Die Änderung wird sofort wirksam.
export.remote.path	Zeigt das Remoteprotokoll (nfs://) und den für den Export verwendeten Speicherort an. Die Änderung wirkt sich beim Serviceneustart aus.
export.rollup	Bestimmt das Rollupintervall für exportierte Dateien. Die Änderung wirkt sich beim Serviceneustart aus.
export.session.max	Zeigt die maximale Anzahl Sitzungen pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.size.max	Zeigt die maximale Anzahl Bytes pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.usage.max	Zeigt den maximalen Prozentsatz an verwendeten Cachespeichers an, bevor die Aggregation angehalten wird. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
heartbeat.error	Gibt die Anzahl der Sekunden an, die nach einem Servicefehler gewartet werden soll, bevor eine erneute Serviceverbindung versucht wird. Die Änderung wird sofort wirksam.
heartbeat.interval	Gibt die Anzahl der Millisekunden zwischen Heartbeat-Serviceprüfungen an. Die Änderung wird sofort wirksam.
heartbeat.next.attempt	Gibt die Anzahl der Sekunden an, die gewartet werden soll, bevor eine erneute Serviceverbindung versucht wird. Die Änderung wird sofort wirksam.
heartbeat.no.response	Gibt die Anzahl der Sekunden an, die gewartet werden soll, bevor ein nicht reagierender Service offline geschaltet wird. Die Änderung wird sofort wirksam.

Concentrator-Servicekonfigurationsparameter

In diesem Thema werden die verfügbaren Konfigurationsparameter für NetWitness Platform-Concentrator aufgeführt und beschrieben.

In dieser Tabelle werden die Concentrator-Konfigurationsparameter aufgeführt und beschrieben.

Concentrator-Parameterfeld	Beschreibung
Concentrator	/concentrator/config, siehe Aggregationskonfigurationsparameter
Datenbank	/database/config, siehe **Datenbankkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Index	/index/config, siehe **Indexkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Protokolle	/logs/config, siehe Konfigurationsparameter der Core-Service-Protokollierung
REST	/rest/config, siehe Konfigurationsparameter für die REST-Schnittstelle
SDK	/sdk/config, siehe **SDK-Konfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden* und Modi für Systemrollen der NetWitness Platform Core-Services
Services	/services/<servicename>/config, siehe Core-Service-to-Service-Konfigurationsparameter
System	/sys/config, siehe Core-Service-Systemkonfigurationsparameter

Konfigurationsparameter der Core-Service-Protokollierung

In diesem Thema werden die Konfigurationsparameter für die Protokollierung für alle NetWitness Platform Core-Services aufgeführt und beschrieben.

Die Protokollierungskonfiguration ist für alle NetWitness Platform Core-Services identisch.

In der folgenden Tabelle werden die Protokollkonfigurationsparameter beschrieben:

Protokollierungskonfigurationsordner	/logs/config
log.dir	Zeigt das Verzeichnis an, in dem die Protokolldatenbank gespeichert ist. Optional zugewiesene maximale Größe (=#) in MB Die Änderung wirkt sich beim Serviceneustart aus.
log.levels	Steuert, welche Arten Protokollmeldungen gespeichert werden (durch Kommas getrennt). Modulspezifische Einstellungen werden wie folgt definiert: <Modul>= [debug|info|audit|warning|failure|all|none]. Die Änderung wird sofort wirksam.

Protokollierungskonfigurationsordner	/logs/config
log.snmp.agent	Legt einen Remote-SNMP-Trap-Empfänger-Agent fest.
snmp.trap.version	Legt die für Gets und Traps zu verwendende SNMP-Version (2c oder 3) fest.
snmpv3.engine.boots	Zeigt die Bootanzahl der SNMPv3-Engine an. Dieses Feld zählt automatisch beim Start hoch und sollte nicht vom Benutzer festgelegt werden müssen.
snmpv3.engine.id	Legt die ID der SNMPv3-Engine fest. Dabei handelt es sich um eine hexadezimale Zahl mit 10–64 Stellen, der optional 0x vorangestellt ist. Sie können für jeden der SA Core-Services, der auf demselben Host ausgeführt wird, Suffixwerte am Ende der Engine-ID hinzufügen. Beispiel: Wenn die erzeugte Engine-ID für den SA Core-Host 0x1234512345 ist, können Sie die Engine-ID für den Decoder-Service als 0x123451234501 und 0x123451234504 für den Appliance-Service festlegen.
snmpv3.trap.auth.local.key	Legt den lokalen SNMPv3-Trap-Authentifizierungsschlüssel fest. Dabei handelt es sich um eine hexadezimale Zahl mit 16 oder 20 Stellen (je nach verwendetem Authentifizierungsprotokoll), der 0x vorangestellt ist. Für MD5 hat der Schlüssel 16 Hexadezimalstellen, während SHA 20 Hexadezimalstellen verwendet. Sie können einen beliebigen gewünschten Algorithmus zur Erzeugung der lokalen Schlüssel verwenden. Es wird empfohlen, bei der Erzeugung der Schlüsselwerte Methoden zu verwenden, die Zufälligkeit beinhalten, anstatt sie manuell auszuwählen.
snmpv3.trap.auth.protocol	Zeigt das SNMPv3-Trap-Authentifizierungsprotokoll an (keines, MD5 oder SHA).
snmpv3.trap.priv.local.key	Legt den lokalen SNMPv3-Trap-Datensicherheitsschlüssel fest. Dabei handelt es sich um eine hexadezimale Zahl mit 16 Stellen, der 0x vorangestellt ist.
snmpv3.trap.priv.protocol	Zeigt das SNMPv3-Trap-Datenschutzprotokoll an (keines oder AES).

Protokollierungskonfigurationsordner	/logs/config
snmpv3.trap.security.level	Zeigt die SNMPv3 Trap-Sicherheitsebene an, die angibt, ob Authentifizierung und Datensicherheit verwendet bzw. nicht verwendet werden. Mögliche Werte sind noAuthNoPriv, authNoPriv oder authPriv.
snmpv3.trap.security.name	Legt den SNMPv3-Trap-Sicherheitsnamen fest, der bei der SNMPv3-Trap-Authentifizierung verwendet wird.
syslog.size.max	Zeigt die maximale Größe eines an Syslog gesendeten Protokolls an (einige Syslog-Daemons haben Probleme mit sehr großen Meldungen). Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.

Core-Service-to-Service-Konfigurationsparameter

In diesem Thema sind die Konfigurationsparameter aufgeführt und beschrieben, die steuern, wie ein Core-Service eine Verbindung zu einem anderen Core-Service herstellt. Beispiel: Wenn ein Concentrator eine Verbindung zu einem Decoder herstellt, werden die Parameter dieser Verbindung durch diese Einstellungen bestimmt.

Immer wenn ein Core-Service eine Verbindung zu einem anderen Core-Service herstellt, wird von dem Service, der als **Client** agiert, ein neuer Unterordner im Ordner /services der Konfigurationsstruktur erstellt. Der Name des Unterordners entspricht dem Namen des Service und hat das Format `host:port`. Der Serviceverbindungsordner einer Concentrator-Verbindung zu einem Decoder könnte zum Beispiel `/services/reston-va-decoder:50004` sein. In jedem Serviceverbindungsordner befinden sich ein `config`-Unterordner, der konfigurierbare Parameter enthält.

In der folgenden Tabelle werden die Servicekonfigurationsparameter beschrieben:

Services	/services/host:port/config
allow.nonssl.to.ssl	Ermöglicht es einer Nicht-SSL-Verbindung, sich mit einem SSL-Service zu verbinden, wenn auf true eingestellt. Andernfalls, wenn auf false eingestellt, werden nicht-sicher-zu-sicher-Verbindungen abgelehnt. Die Änderung wird sofort wirksam.
Komprimierung	Zeigt einen Konfigurations-Node an, der festlegt, ob Daten vor dem Senden komprimiert werden. Ein positiver Wert bestimmt die Anzahl der Byte, die gesendet werden müssen, bevor es komprimiert wird. Null bedeutet keine Komprimierung.
crc.checksum	Zeigt einen Konfigurations-Node an, der festlegt, ob Datenströme mit einer CRC-Prüfsumme validiert werden. Ein positiver Wert bestimmt die Anzahl der Byte, die gesendet werden müssen, bevor es CRC-validiert wird. Null bedeutet keine CRC-Validierung.
ssl	Zeigt einen Konfigurations-Node an, der die SSL-Verschlüsselung für die Verbindung aktiviert oder deaktiviert.

Core-Service-Systemkonfigurationsparameter

In diesem Thema sind die gemeinsamen Konfigurationsparameter für alle NetWitness Platform Core-Services aufgeführt und beschrieben.

In der folgenden Tabelle werden die Systemkonfigurationsparameter aufgeführt und beschrieben:

Systemkonfigurationsordner	/sys/config
Komprimierung	Zeigt die Mindestanzahl der Byte an, bevor eine Nachricht komprimiert wird, wenn auf einen positiven Wert eingestellt. Ein Wert von null bedeutet keine Komprimierung von Meldungen. Die Änderung wird bei den folgenden Verbindungen wirksam.
crc.checksum	Zeigt die Mindestanzahl der Byte an, bevor eine Meldung über das Netzwerk mit einer CRC-Prüfsumme (vom Client zu validieren) gesendet wird, wenn auf einen positiven Wert eingestellt. Ein Wert von null bedeutet keine CRC-Prüfsummenvalidierung bei Nachrichten. Die Änderung wird bei den folgenden Verbindungen wirksam.
Laufwerke	Zeigt zu überwachende Laufwerke für Nutzungsstatistiken an. Die Änderung wirkt sich beim Serviceneustart aus.
port	Zeigt den Port an, den der Service abhört. Die Änderung wirkt sich beim Serviceneustart aus.
scheduler	Zeigt den Ordner für geplante Aufgaben an.
service.name.override	Zeigt einen optionalen Servicenamen an, der von vorgelagerten Services anstelle des Hostnamens für die Aggregation verwendet wird.
ssl	Verschlüsselt den gesamten Datenverkehr über SSL, sofern aktiviert. Die Änderung wirkt sich beim Serviceneustart aus.
stat.compression	Komprimiert Statistiken, während sie in die Datenbank geschrieben werden, sofern aktiviert. Die Änderung wirkt sich beim Serviceneustart aus.
stat.dir	Zeigt das Verzeichnis an, in dem die Verlaufsstatistikdatenbank gespeichert wird (mehrere Verzeichnisse durch Semikolon trennen). Optionale zugewiesene maximale Größe (=#Einheit). Einheiten sind: t für TB; g für GB, m für MB. Die Änderung wirkt sich beim Serviceneustart aus.
stat.exclude	Listet Stat-Pfadnamen, die von der Stat-Datenbank ausgeschlossen werden müssen. Die folgenden Platzhalter sind zulässig: ? steht für ein beliebiges einzelnes Zeichen; * steht für eines oder mehrere Zeichen bis zum Trennzeichen /, ** steht für null oder mehrere Zeichen einschließlich Trennzeichen. Die Änderung wird sofort wirksam.

Systemkonfigurationsordner	/sys/config
stat.interval	Legt fest, wie oft (in Millisekunden) Statistik-Nodes im System aktualisiert werden Die Änderung wird sofort wirksam.
threads	Listet die Anzahl der Threads im Threadpool für die Verarbeitung eingehender Anforderungen auf. Die Änderung wird sofort wirksam.

Decoder-Servicekonfigurationsparameter

In diesem Thema werden die verfügbaren Konfigurationsparameter für NetWitness Platform-Decoder aufgeführt und beschrieben.

Decoder-Parameterfeld	Beschreibung
Decoder	/decoder/config, siehe Konfigurationsparameter für Decoder und Log Decoder
Datenbank	/database/config, siehe **Datenbankkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Index	/index/config, siehe **Indexkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Protokolle	/logs/config, siehe Konfigurationsparameter der Core-Service-Protokollierung
REST	/rest/config, siehe Konfigurationsparameter für die REST-Schnittstelle
SDK	/sdk/config, siehe **SDK-Konfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden* und Modi für Systemrollen der NetWitness Platform Core-Services
System	/sys/config, siehe Core-Service-Systemkonfigurationsparameter

Konfigurationsparameter für Decoder und Log Decoder

In diesem Thema werden die Konfigurationsparameter aufgelistet und beschrieben, die bei den Decoder- und Log Decoder-Services identisch sind.

Konfigurationspfad	<service>/config
aggregate.buffer.size	Zeigt die Größe des bei jeder Aggregationsrunde verwendeten Puffers an (Standardeinheit ist KB). Größere Puffer verbessern möglicherweise die Aggregationsperformance, könnten aber die Erfassungsperformance beeinträchtigen. Die Änderung wird nach dem Neustart der Erfassung wirksam.

Konfigurationspfad	<service>/config
aggregate.precache	Bestimmt, ob der Decoder ein Precaching der nächsten Aggregationsrunde für vorgelagerte Services durchführt. Dies kann die Aggregationsperformance verbessern, kann aber die Erfassungsperformance beeinträchtigen. Die Änderung wird sofort wirksam.
assembler.pool.ratio	Zeigt den Prozentsatz der Poolseiten an, die durch den Assembler gemanagt und für den Assembly-Prozess verwendet werden. Die Änderung wirkt sich beim Serviceneustart aus.
assembler.session.flush	Leert Sitzungen, wenn sie beendet sind (1), oder leert Sitzungen, wenn sie analysiert wurden (2). Die Änderung wirkt sich beim Serviceneustart aus.
assembler.session.pool	Listet die Anzahl der Einträge im Sitzungspool auf. Die Änderung wirkt sich beim Serviceneustart aus.
assembler.size.max	Listet die maximale Größe auf, die eine Sitzung erhält. Eine Einstellung von 0 entfernt die Sitzungsgrößenbeschränkung. Die Änderung wird sofort wirksam.
assembler.size.min	Listet die minimale Größe auf, die eine Sitzung für ihre Persistenz aufweisen muss. Die Änderung wird sofort wirksam.
assembler.timeout.packet	Listet die Anzahl der Sekunden vor einem Paket-Timeout auf. Die Änderung wird sofort wirksam.
assembler.timeout.session	Listet die Anzahl der Sekunden vor einem Sitzungs-Timeout auf. Die Änderung wird sofort wirksam.
assembler.voting.weights	Zeigt die Gewichtungen an, die verwendet werden, um festzulegen, welcher Sitzungsstream als Kunde und Server markiert wird. Die Änderung wird sofort wirksam.
capture.autostart	Bestimmt, ob die Erfassung automatisch beginnt, wenn der Service gestartet wird. Die Änderung wirkt sich beim Serviceneustart aus.
capture.buffer.size	Zeigt die Zuordnungsgröße des Arbeitsspeicherpuffers für die Erfassung an (Standardeinheit ist MB). Die Änderung wirkt sich beim Serviceneustart aus.

Konfigurationspfad	<service>/config
capture.device.params	Zeigt spezifische Parameter des Erfassungsservice an. Die Änderung wirkt sich beim Serviceneustart aus. Die Parameter, die von diesem Feld verstanden werden, sind für das aktuell ausgewählte Erfassungsgerät spezifisch. Wenn einer der Parameter nicht vom dem aktuellen Erfassungsgerät erkannt wird, wird er ignoriert. Auf Log Decoders ist nur das Erfassungsgerät für Protokollereignisse vorhanden. Dieses akzeptiert einige optionale Parameter. • **use-envision-time:** Ist dieser Wert auf 1 festgelegt, werden die time-Metadaten für jedes Ereignis aus dem Log Collector-Stream importiert. Wenn dieser Wert auf 0 oder nicht festgelegt ist, wird die importierte Ereigniszeit in den event.time-Metadaten gespeichert. • **port:** Dieser Parameter kann auf einen numerischen Wert festgelegt werden, um den Standard-Syslog-Port-Listener, 514, außer Kraft zu setzen.
capture.selected	Zeigt aktuellen Erfassungsservice und -schnittstelle an. Die Änderung wird sofort wirksam.
export.expire.minutes	Listet die Anzahl der Minuten bis zum Ablauf und zur Leerung von Exportcachedateien auf. Die Änderung wird sofort wirksam.
export.packet.enabled	Ermöglicht den Export von Paketdaten, sofern aktiviert. Die Änderung wirkt sich beim Serviceneustart aus.
export.packet.local.path	Zeigt den lokalen Speicherort zum Cachen exportierter Paketdaten an. Optionale zugewiesene maximale Größe (=#Einheit). Einheiten sind: t für TB; g für GB, m für MB. Die Änderung wirkt sich beim Serviceneustart aus.
export.packet.max	Zeigt die maximale Anzahl Pakete pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.packet.remote.path	Listet das Remoteprotokoll (nfs://) und den Speicherort für Exportdaten auf. Die Änderung wirkt sich beim Serviceneustart aus.
export.packet.size.max	Zeigt die maximale Anzahl Byte für Pakete pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.rollup	Bestimmt das Rollupintervall für exportierte Dateien. Die Änderung wirkt sich beim Serviceneustart aus.
export.session.enabled	Ermöglicht den Export von Sitzungsdaten, sofern aktiviert. Die Änderung wirkt sich beim Serviceneustart aus.

Konfigurationspfad	<service>/config
export.session.format	Bestimmt das beim Sitzungsexport verwendete Dateiformat. Die Änderung wirkt sich beim Serviceneustart aus.
export.session.local.path	Zeigt den lokalen Speicherort für die Zwischenspeicherung exportierter Sitzungsdaten an. Optionale zugewiesene maximale Größe (=#Einheit). Einheiten sind: t für TB; g für GB, m für MB. Die Änderung wirkt sich beim Serviceneustart aus.
export.session.max	Zeigt die maximale Anzahl Sitzungen pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.session.meta.fields	Bestimmt, welche Metafelder exportiert werden. Kommaliste von Feldern. Stern bedeutet alle Felder. Stern plus Feldliste bedeutet alle Felder mit Ausnahme der aufgelisteten Felder. Nur Feldliste bedeutet, es werden nur diese Felder eingeschlossen. Die Änderung wird sofort wirksam.
export.session.remote.path	Zeigt das Remoteprotokoll (nfs://) und den für den Export verwendeten Speicherort an. Die Änderung wirkt sich beim Serviceneustart aus.
export.session.size.max	Zeigt die maximale Anzahl Byte für Sitzungen pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
export.usage.max	Zeigt die maximale Anzahl Byte für Sitzungen pro Exportdatei an. Bei Exportdateitypen, die zwischengespeichert werden, bestimmt dies die Größe des Cachespeichers. Null bedeutet unbeschränkt. Die Änderung wird sofort wirksam.
parse.threads	Listet die Anzahl der für das Sitzungs-Parsing verwendeten Parse-Threads auf. Bei einem Wert von null wird dies durch den Server entscheiden. Die Änderung wirkt sich beim Serviceneustart aus.
pool.packet.page.size	Zeigt die Größe einer Paketseite an (Standard ist KB). Die Änderung wirkt sich beim Serviceneustart aus.
pool.packet.pages	Listet die Anzahl der Paketseiten auf, die der Decoder zuweist und verwendet. Die Änderung wirkt sich beim Serviceneustart aus.
pool.session.page.size	Zeigt die Größe einer Sitzungsseite an (standardmäßig in KB). Die Änderung wirkt sich beim Serviceneustart aus.
pool.session.pages	Listet die Anzahl der Sitzungsseiten auf, die der Decoder zuweist und verwendet. Die Änderung wirkt sich beim Serviceneustart aus.

Log Decoder-Servicekonfigurationsparameter

In diesem Thema werden die verfügbaren Konfigurationsparameter für RSA NetWitness Platform Log Decoder aufgeführt und beschrieben.

Log Decoder-Konfigurationseinstellungen

In dieser Tabelle werden die Log Decoder-Konfigurationseinstellungen aufgelistet und beschrieben.

Log Decoder-Einstellungsfeld	Beschreibung
Datenbank	/database/config, siehe **Datenbankkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Decoder	/decoder/config, siheKonfigurationsparameter für Decoder und Log Decoder
Index	/index/config, siehe **Indexkonfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden*
Protokolle	/logs/config, siehe „Konfiguration der Core-Service-Protokollierung“
REST	/rest/config, siehe REST-Schnittstellenkonfiguration
SDK	/sdk/config, siehe **SDK-Konfigurations-Nodes** im *NetWitness Platform Core-Datenbank-Tuning-Leitfaden* und „Core-Service-system.roles-Modi“
System	/sys/config, siehe „Core-Service-Systemkonfiguration“

Konfigurationseinstellungen für den Protokoll-Tokenizer

Der Log Decoder verfügt über einen Satz an Configuration Items, die steuern, wie der automatische Protokoll-Tokenizer Metaelemente aus nicht analysierten Protokollen erstellt. Der Protokoll-Tokenizer wird als ein Satz von integrierten Parsern implementiert, die jeweils nach einer Teilmenge der erkennbaren Tokens scannen. Die Funktion dieser nativen Parser befindet sich in der folgenden Tabelle. Diese word-Elemente bilden einen Volltextindex, wenn sie an die Indexierungs-Engine auf dem Concentrator und Archiver eingespeist werden. Durch die Modifikation des Konfigurationseintrags „parsers.disabled“ können Sie festlegen, welche Protokoll-Tokenizer aktiviert sind.

Name des Parsers	Beschreibung	Konfigurationsparameter
Protokoll-Tokens	Scannt nach der Ausführung von aufeinander folgenden Zeichen, um „word“-Metaelemente zu erzeugen.	token.device.types, token.char.classes, token.max.length, token.min.length, token.unicode
IPSCAN	Scannt nach Text, der wie eine IPv4-Adresse aussieht, um „ip.addr“-Metaelemente zu erzeugen.	token.device.types
IPV6SCAN	Scannt nach Text, der wie eine IPv6-Adresse aussieht, um „ipv6“-Metaelemente zu erzeugen.	token.device.types

Name des Parsers	Beschreibung	Konfigurationsparameter
URLSCAN	Sucht nach Text, der wie eine URI aussieht, um „alias.host“-, „filename“-, „username“- und „password“-Metaelemente zu erzeugen.	token.device.types
DOMAINSCAN	Sucht nach Text, der wo ein Domainname aussieht, um „alias.host“-, „tld“-, „cctld“- und „sld“-Metaelemente zu erzeugen.	token.device.types
EMAILSCAN	Scannt nach Text, der wie eine E-Mail-Adresse aussieht, um „email“- und „username“-Metaelemente zu erzeugen.	token.device.types
SYSLOGTIMESTAMPSCAN	Scannt nach Text, der wie ein Zeitstempel im syslog-Format aussieht. Im syslog-Format fehlt das Jahr und Zeitzone. Wenn solcher Text gefunden wird, wird er in UTC-Zeit normalisiert, um „event.time“-Metaelemente zu erzeugen.	token.device.types
INTERNETTIMESTAMPSCAN	Scannt nach Text, der wie ein Zeitstempel im RFC 3339-Format aussieht, um „event.time“-Metaelemente zu erzeugen.	token.device.types

Dies sind die Konfigurationsparameter für den Protokoll-Tokenizer.

Einstellungsfeld für den Log Decoder-Parser	Beschreibung
token.device.types	Der Satz von Gerätetypen, der auf Rohtexttoken gescannt wird. Standardmäßig ist hier `unknown` festgelegt, was bedeutet, dass nur nicht analysierte Protokolle auf Rohtext gescannt werden. Sie können hier zusätzliche Protokolltypen hinzufügen, um analysierte Protokolle mit Texttokeninformationen zu optimieren. Wenn dieses Feld leer ist, ist die Protokolltokenisierung deaktiviert.

Einstellungsfeld für den Log Decoder-Parser	Beschreibung
token.char.classes	Dieses Feld steuert den Typ der erzeugten Token. Hier kann eine beliebige Kombination der Werte `alpha`, `digit`, `space` und `punct` verwendet werden. Der Standardwert ist `alpha`. • **alpha:** Token können alphabetische Zeichen enthalten. • **digit:** Token können Zahlen enthalten. • **space:** Token können Leerzeichen und Tabulatoren enthalten. • **punct:** Token können Satzzeichen enthalten.
token.max.length	Mit diesem Feld wird die Länge der Token begrenzt. Der Standardwert ist 5 Zeichen. Mit der Einstellung für die maximale Länge kann der Log Decoder den für das Speichern der word-Metadaten erforderlichen Speicherplatz begrenzen. Beim Verwenden längerer Token ist mehr Speicherplatz in der Metadatenbank erforderlich, das Suchen nach Rohtext wird aber etwas beschleunigt. Beim Verwenden kürzerer Token muss die Textabfrageauflösung bei Suchen mehr Lesevorgänge aus den Rohdatenprotokolle durchführen, dabei wird jedoch viel weniger Speicherplatz in der Metadatenbank und im Index verwendet.
token.min.length	Dies ist die Mindestlänge eines durchsuchbaren Texttokens. Die Mindestlänge für ein Token entspricht die Mindestanzahl von Zeichen, die ein Benutzer in das Suchfeld eingeben kann, um Ergebnisse zu finden. Der der empfohlene Wert ist der Standardwert, 3.
token.unicode	Diese boolesche Einstellung steuert, ob bei der Klassifizierung von Zeichen gemäß der Einstellung token.char.classes Unicode-Klassifizierungsregeln angewendet werden. Bei Festlegung dieses Werts auf „true“ wird jedes Protokoll als eine Sequenz von UTF-8-codierten Codepunkten behandelt und Klassifizierung erfolgt nach Durchführung der UTF-8-Decodierung. Bei Festlegung auf „false“ wird jedes Protokoll als ASCII-Zeichen behandelt und nur eine ASCII-Zeichenklassifizierung durchgeführt. Für die Unicode-Zeichenklassifizierung sind mehr CPU-Ressourcen auf dem Log Decoder erforderlich. Wenn Sie keine Indexierung von nicht englischem Text benötigen, können Sie diese Einstellung deaktivieren, um die CPU-Auslastung auf dem Log Decoder zu reduzieren. Der Standard ist aktiviert.

Konfigurationsparameter für die REST-Schnittstelle

In diesem Thema werden die verfügbaren Konfigurationsparameter für die in alle NetWitness Platform Core-Services integrierte REST-Schnittstelle aufgeführt und beschrieben.

Einstellungen

In der folgenden Tabelle werden die REST-Konfigurationsparameter aufgeführt und beschrieben:

REST-Konfigurationspfad	/rest/config
cache.dir	Zeigt das Hostverzeichnis an, das für die temporäre Erstellung und Speicherung von Dateien verwendet wird. Die Änderung wirkt sich beim Serviceneustart aus.
cache.size	Zeigt die maximale Gesamtgröße (Standardeinheit ist MB) aller Dateien im Cacheverzeichnis an, bevor die ältesten gelöscht werden. Die Änderung wirkt sich beim Serviceneustart aus.
enabled	Kann umgestellt werden, um den REST-Service zu aktivieren oder zu deaktivieren: 1 ist an, 0 ist aus. Die Änderung wirkt sich beim Serviceneustart aus.
port	Zeigt den Port an, den der REST-Service abhört. Die Änderung wirkt sich beim Serviceneustart aus.
ssl	Verschlüsselt den gesamten REST-Datenverkehr mithilfe von SSL, sofern aktiviert. Der Standard „System“ bedeutet, dass die Einstellung unter /sys/config/ssl verwendet wird. Die Änderung wirkt sich beim Serviceneustart aus.

Modi für Systemrollen der NetWitness Platform Core-Services

Alle NetWitness Platform Core-Services bieten rollenbasierte Autorisierungsmodi. In diesem Thema werden die verfügbaren Modi und ihre Konfiguration innerhalb von jedem Service beschrieben

Der Konfigurations-Node `/sdk/config/system.roles` legt Abfrage- und Anzeigeberechtigungen für Metadaten und Inhalte auf Schlüsselbasis fest. Dieser Parameter unterstützt die Datenschutzmanagementfunktion. Wenn er unter Verwendung von einem Wert, der nicht Null ist, aktiviert wird, hilft er Data Privacy Officers, den Zugriff auf bestimmte Metaschlüssel und Inhalte zu kontrollieren. Dieser Parameter ist auf der NetWitness Platform-Benutzeroberfläche konfigurierbar (weitere Informationen im Thema **Registerkarte „Datenschutz“** des *Leitfadens Datenschutzmanagement*). Wenn der Wert bearbeitet wird, tritt die Änderung sofort in Kraft.

Null bedeutet, dass die Serviceberechtigungen auf Basis von SDK-Metaschlüsseln deaktiviert sind.

- 0 – deaktiviert

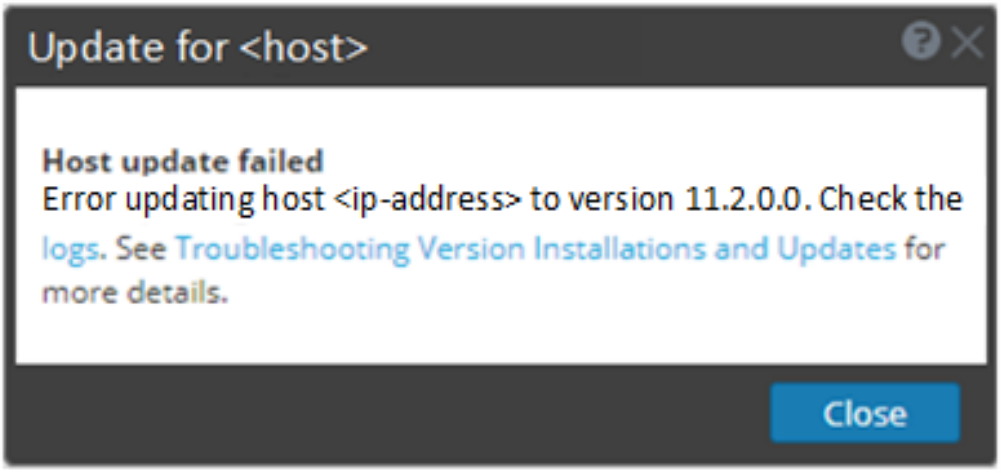
Wird einer der Werte angegeben, die nicht Null sind, kann ein Data Privacy Officer einen Metaschlüssel auswählen, um die Anzeige der zugehörigen Metadaten, Inhalte oder die Anzeige von beidem für eine bestimmte Benutzerrolle in einem Service einer Whitelist oder einer schwarzen Liste hinzuzufügen.

- 1 – gefilterte Metadaten und Inhalte in der Whitelist
- 2 – gefilterte Metadaten in der Whitelist
- 3 – gefilterte Inhalte in der Whitelist
- 4 – gefilterte Metadaten und Inhalte auf der schwarzen Liste
- 5 – gefilterte Metadaten auf der schwarzen Liste
- 6 – gefilterte Inhalte auf der schwarzen Liste

Troubleshooting von Versionsinstallationen und -aktualisierungen

In diesem Abschnitt werden die Fehlermeldungen beschrieben, die in der Ansicht **Hosts** angezeigt werden, wenn beim Aktualisieren von Hostversionen und der Installation von Services auf Hosts in der Ansicht **Hosts** Probleme auftreten. Wenn Sie Probleme bei der Aktualisierung oder Installation mithilfe der folgenden Troubleshooting-Lösungen nicht beheben können, wenden Sie sich an den Kundensupport (https://community.rsa.com/docs/DOC-1294).

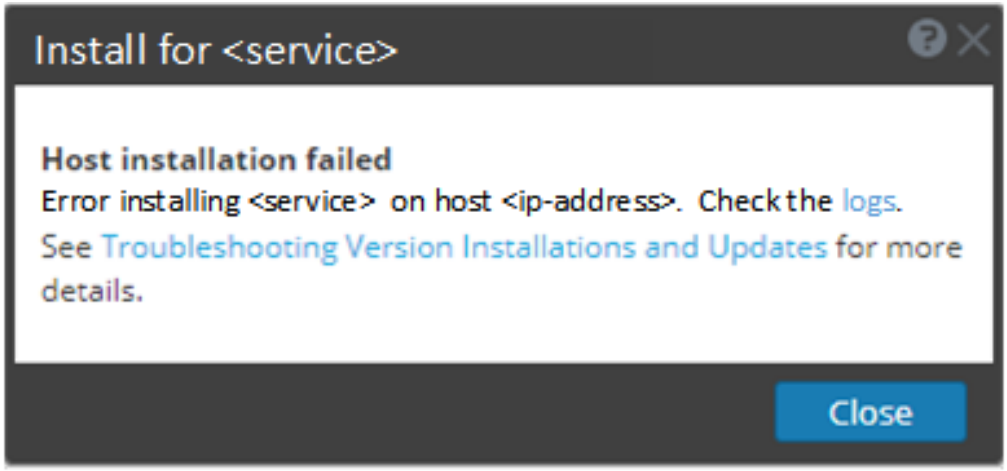
Update für Host fehlgeschlagen

Fehlermeldung	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren** >**Host aktualisieren** klicken, ist zwar der Download erfolgreich, aber die Aktualisierung schlägt fehl.

Lösung	1. **Versuchen Sie, die Versionsaktualisierung erneut auf den Host anzuwenden.**
	Häufig ist das alles, was Sie tun müssen.
	2. Gehen Sie folgendermaßen vor, wenn Sie die neue Aktualisierungsversion weiterhin nicht anwenden können:
	a. Überwachen Sie während der Verarbeitung die folgenden Protokolle auf dem NW-Server (Senden Sie beispielsweise die Befehlszeichenfolge `tail -f` über die Befehlszeile.):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.

	b. Versuchen Sie, das Problem zu lösen, und wenden Sie die Versionsaktualisierung erneut an. • Ursache 1: Das `deploy_admin`-Passwort ist abgelaufen. **Lösung**: Setzen Sie das `deploy_admin`-Passwort zurück. Weitere Informationen zum Zurücksetzen Ihres `deploy_admin`-Passworts finden Sie im nachfolgend beschriebenen Verfahren unter deploy_admin-Passwort abgelaufen • Ursache 2: Das `deploy_admin`-Passwort wurde auf dem NW-Serverhost geändert, nicht aber auf den Nicht-NW-Serverhosts. Führen Sie in diesem Fall auf allen Nicht-NW-Serverhosts unter 11.x den folgenden Befehl mit dem übereinstimmenden `deploy_admin`-Passwort vom NW-Serverhost aus. `/opt/rsa/saTools/bin/set-deploy-admin-password` 3. Wenn Sie die Aktualisierung weiterhin nicht anwenden können, wenden Sie sich mit den Protokollen aus Schritt 2 an den Kundensupport: https://community.rsa.com/docs/DOC-1294.

Update für Service fehlgeschlagen

Fehlermeldung	
Problem	Wenn Sie einen Host auswählen und auf **Installieren** klicken, schlägt der Service für den Installationsprozess fehl.
Lösung	1. **Versuchen Sie, den Service erneut zu installieren.** Häufig ist das alles, was Sie tun müssen. 2. Versuchen Sie Folgendes, wenn der Service weiterhin nicht installiert werden kann: a. Überwachen Sie während der Verarbeitung die folgenden Protokolle auf dem NW-Server (Senden Sie beispielsweise die Befehlszeichenfolge `tail -f` über die Befehlszeile.):

```
/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out
```

Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.

b. Versuchen Sie, das Problem zu lösen, und wenden Sie den Service erneut an.

- Ursache 1: Das falsche `deploy_admin`-Passwort wurde in nwsetup-tui eingegeben.

  Lösung: Rufen Sie Ihr `deploy_admin`-Passwort ab.

  So rufen Sie Ihr `deploy_admin`-Passwort ab:

  1. Wählen Sie im Menü NetWitness Platform **ADMIN** > **Sicherheit** > Registerkarte **Nutzer** aus.
  2. Wählen Sie `deploy_admin` aus und klicken Sie auf **Passwort zurücksetzen**.
  3. (Bedingungsabhängig) Wenn NetWitness Platform Ihnen nicht erlaubt, das abgelaufene `deploy_admin`Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus.
     a. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.

     ```
     security-cli-client --get-config-prop --prop-hierarchy
     nw.security-client --prop-name
     platform.deployment.password -quiet
     ```

     b. Stellen Sie über SSH eine Verbindung mit dem Host her, auf dem die Installation/Orchestrierung fehlgeschlagen ist.

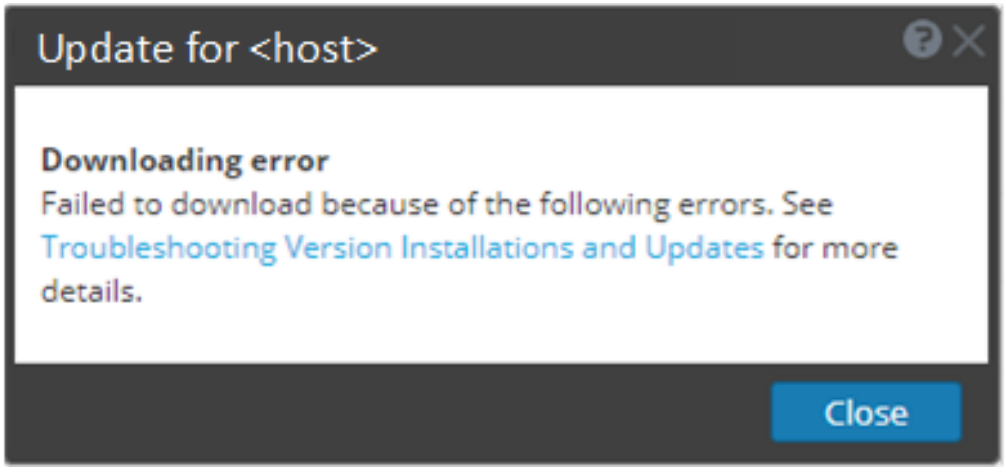
     c. Führen Sie den Befehl nwsetup-tui erneut mit dem korrekten `deploy_admin`-Passwort aus.

- Ursache 2: Das `deploy_admin`-Passwort ist abgelaufen.

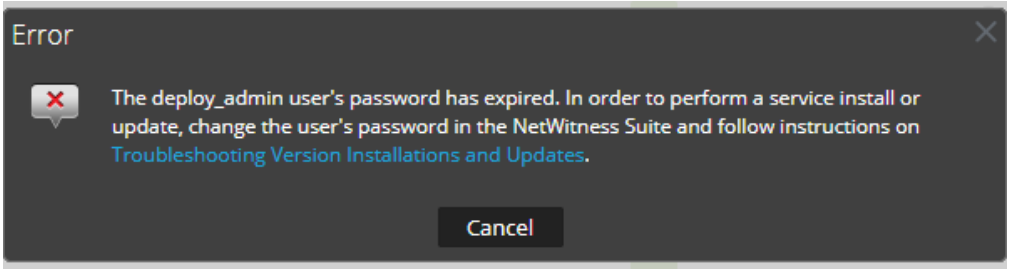
  Lösung: Setzen Sie das `deploy_admin`-Passwort zurück. Weitere Informationen zum Zurücksetzen Ihres `deploy_admin`-Passwords finden Sie in dem unter deploy_admin-Passwort abgelaufen beschriebenen Verfahren.

3. Wenn Sie die Aktualisierung weiterhin nicht anwenden können, wenden Sie sich mit den Protokollen aus Schritt 2 an den Kundensupport: https://community.rsa.com/docs/DOC-1294.

Fehler beim Host-Download

Fehlermeldung	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren** > **Host aktualisieren** klicken, wird der Download zwar gestartet, kann aber nicht abgeschlossen werden.
Ursache	Die Downloaddateien der Version können groß sein und das Herunterladen kann daher lange dauern. Wenn beim Download Kommunikationsprobleme auftreten, schlägt er fehl.
Lösung	1. Versuchen Sie erneut, die Dateien herunterzuladen. 2. Wenn der Download weiterhin fehlschlägt, versuchen Sie, die Dateien außerhalb von NetWitness Platform herunterzuladen. Eine entsprechende Beschreibung finden Sie unter Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff). 3. Wenn Sie die Aktualisierungsdatei weiterhin nicht herunterladen können, wenden Sie sich an den Kundensupport: https://community.rsa.com/docs/DOC-1294.

deploy_admin-Passwort abgelaufen

Fehlermeldung	
Ursache	Das `deploy_admin`-Benutzerpasswort ist abgelaufen.

Lösung	Setzen Sie das `deploy_admin`-Passwort zurück. 1. Wählen Sie im Menü NetWitness Platform **ADMIN** > **Sicherheit** > Registerkarte **Nutzer** aus. 2. Wählen Sie **deploy_admin** aus und klicken Sie auf **Passwort zurücksetzen**. • Wenn NetWitness Platform Ihnen erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus. a. Geben Sie das abgelaufene `deploy_admin`-Passwort ein. b. Deaktivieren Sie das Kontrollkästchen **Passwortänderung bei nächster Anmeldung erzwingen**. c. Klicken Sie auf **Speichern**. • Wenn NetWitness Platform`deploy_admin`Ihnen nicht erlaubt, das abgelaufene -Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus. a. Führen Sie auf dem NW-Server-Host und allen anderen Hosts auf 11.x den folgenden Befehl mit dem neuen `deploy_admin`-Passwort aus. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. Führen Sie auf dem Host mit dem Installations-/Orchestrierungsfehler den Befehl nwsetup-tui aus und verwenden Sie das neue `deploy_admin`-Passwort.