RSA NETWITNESS® SUITE

Protokollsammlung-Konfigurationsleitfaden

für Version 11,1

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Juli 2018

Inhalt

Informationen über die Protokollsammlung

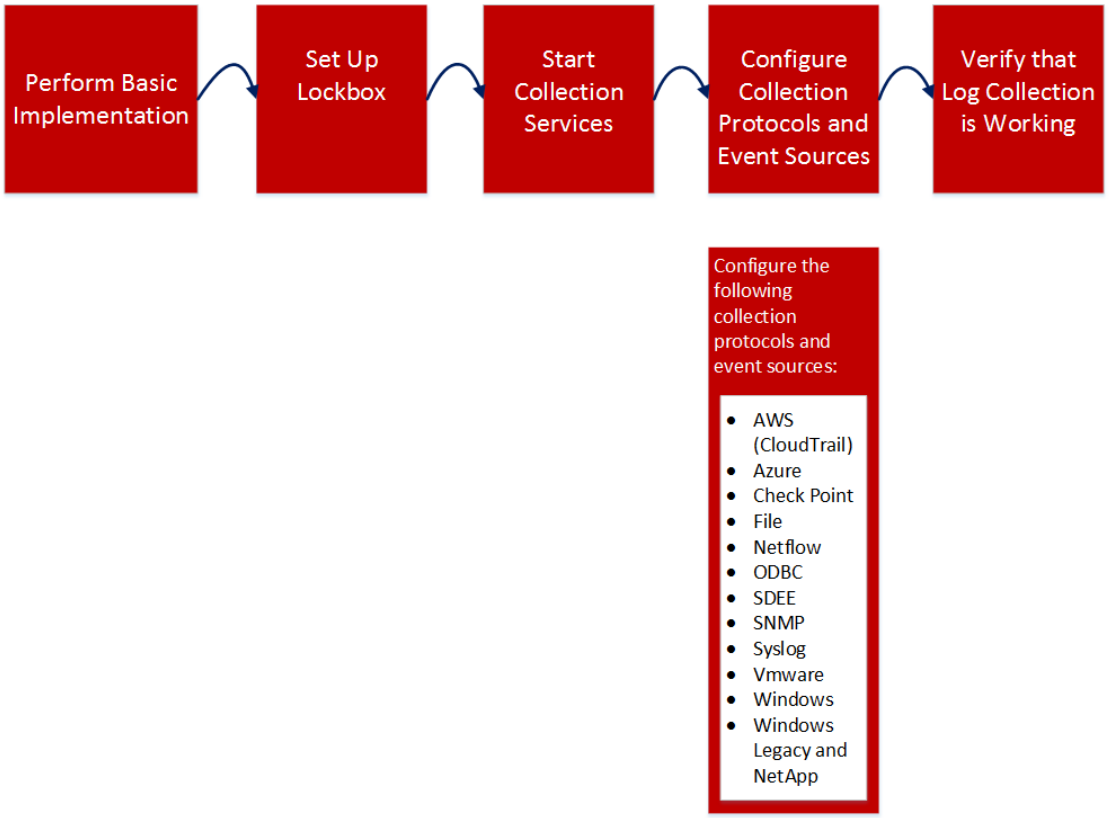
Dieser Leitfaden beschreibt die allgemeinen Schritte und Unteraufgaben beim Einrichten und Konfigurieren der Protokollsammlung für Ereignisquellen. Dazu zählen folgende:

- Was Protokollsammlung tut, wie sie allgemein funktioniert und allgemeine Bereitstellungsdiagramme bietet.
- Wie Sie beginnen, Ereignisse zu erfassen.
- Wo Sie Anweisungen finden, um komplexere Bereitstellungen einzurichten.
- Wie ein Sammlungsprotokoll erstellt wird,
- Wie die Struktur der Benutzeroberfläche zur Konfiguration der Protokollsammlung ist.
- Welche Tools für das Troubleshooting von Problemen bei der Protokollsammlung zu verwenden sind und weitere globale Anweisungen zum Troubleshooting.
- Wie Sie die Protokollsammlung in Ihrer Umgebung fein einstellen und anpassen.
- Wie Sie individuelle Sammlungsprotokolle konfigurieren. Anweisungen finden Sie in den einzelnen Abschnitten zur Protokollsammlung.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zur Erfassung von Ereignissen

durch die Protokollsammlung zunächst durchgeführt werden müssen.



Grundlegende Verfahren

Dies sind die grundlegenden Verfahren, die Sie für die Protokollsammlung befolgen müssen:

I. Hinzufügen von Local und Remote Collectors zu RSA NetWitness Suite.

Richten Sie einen Log Collector lokal für einen Log Decoder (hier als „Local Collector“ bezeichnet) ein. Sie können zudem Log Collectors an so vielen Remotestandorten (d. h. Remote Collectors) einrichten, wie Sie für Ihr Unternehmen benötigen. Weitere Informationen finden Sie unter Grundlegende Implementierung.

II. Aktuelle Inhalte von Live herunterladen. Dies ist eine Aufgabe, die Sie regelmäßig durchführen, da die Inhalte auf Live regelmäßig aktualisiert werden.

LIVE ist das Contentmanagementsystem für RSA NetWitness® Suite, von dem Sie die aktuellen Inhalte herunterladen. Die beiden Ressourcentypen, die Sie verwenden, um Inhalte der Protokollsammlung herunterzuladen, sind:

- **RSA Log Collector**: Contentaktivierung der Sammlung von Ereignisquelltypen.
- **RSA Log Device**: die aktuellen unterstützten Ereignisquellen-Parser.

Sie können Inhalte auf Live auch abonnieren. Weitere Informationen finden Sie im *Handbuch Live-Servicemanagement*.

III. Konfigurieren von Einstellungen: Einrichten der Lockbox und Zertifikate.

Weitere Informationen finden Sie unter Einrichten einer Lockbox und Konfigurieren von Zertifikaten.

IV. Konfigurieren von Ereignisquellen.

Sie konfigurieren alle Ereignisquellen in Ihrem Netzwerk, um deren Protokollinformationen an RSA NetWitness Suite zu senden. Wenn Sie neue Ereignisquellen hinzufügen, müssen Sie dieses Verfahren auch ausführen. Alle Ereignisquellen-Konfigurationsleitfäden finden Sie im Bereich Von RSA unterstützte Ereignisquellen in RSA Link.

V. Starten und Beenden von Services für konfigurierte Protokolle. Gelegentlich müssen Sie basierend auf neuen Ereignisquellen, die Sie zu RSA NetWitness Suite hinzufügen, Services möglicherweise beenden und neu starten.

VI. Überprüfen Sie, ob die Protokollsammlung funktioniert.

Stellen Sie sicher, dass die richtigen Protokolle an RSA NetWitness Suite gesendet werden, wenn Sie eine neue Ereignisquelle einrichten oder ein neues Sammlungsprotokoll hinzufügen.

Architektur der Protokollsammlung

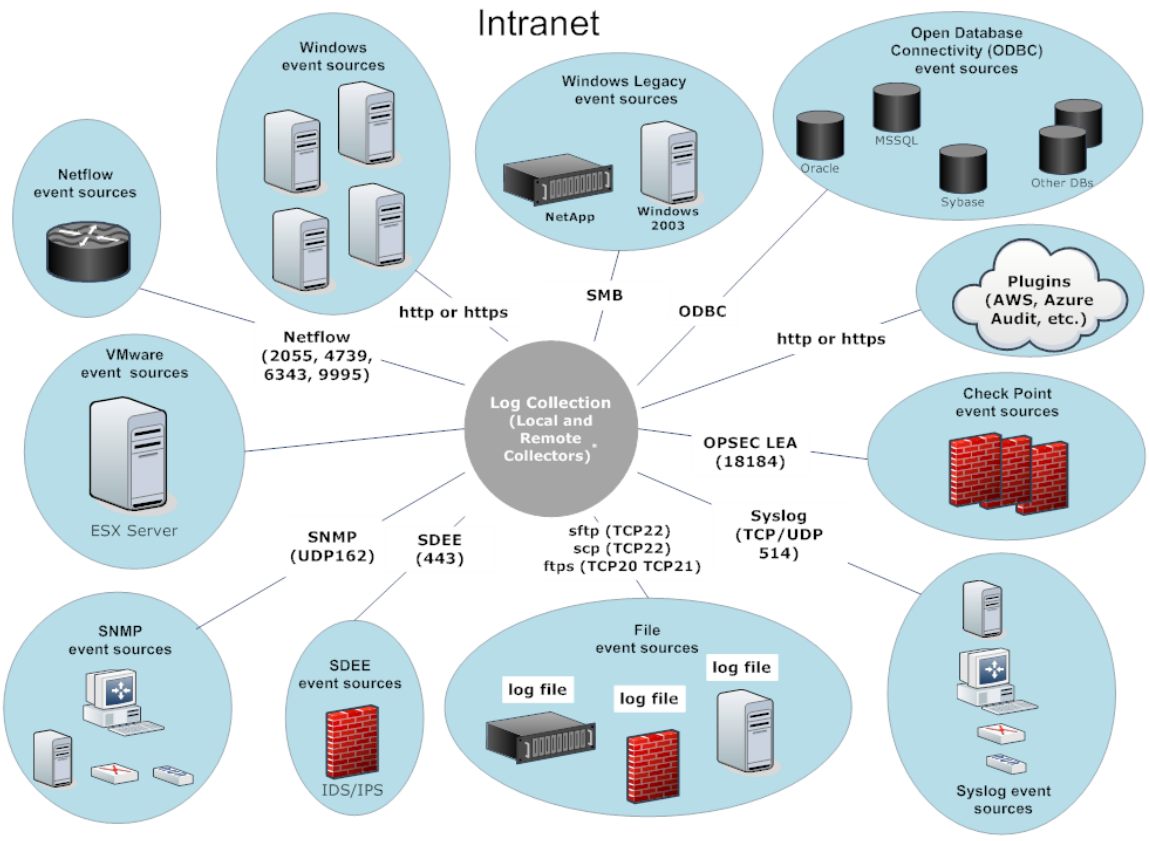
In diesem Thema wird beschrieben, wie NetWitness Suite eine Protokollsammlung durchführt.

Bereitstellen der Protokollsammlung

Sie können die Protokollsammlung entsprechend den Anforderungen und Präferenzen Ihres Unternehmens bereitstellen. Dazu gehört die Bereitstellung der Protokollsammlung über mehrere Standorte hinweg und die Sammlung von Daten aus verschiedenen Sätzen von Ereignisquellen. Zu diesem Zweck richten Sie einen Local Collector mit einem oder vielen Remote Collectors ein.

Komponenten der Protokollsammlung

Die folgende Abbildung zeigt alle Komponenten, die an der Ereignissammlung durch den NetWitness Suite Log Collector beteiligt sind.



*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Local und Remote Collectors

Die folgende Abbildung stellt dar, wie Local und Remote Collectors interagieren, um Ereignisse von allen Ihren Standorten zu sammeln.

In diesem Szenario erfolgt die Protokollsammlung von verschiedenen Protokollen, wie Windows, ODBC usw., sowohl durch den Remote Collector- als auch den Log Collector-Service. Bei der Protokollsammlung durch den Local Collector wird sie dem lokalen Bereitstellungsszenario entsprechend an den Log Decoder-Service weitergeleitet. Bei der Protokollsammlung durch einen Remote Collector gibt es zwei Methoden zur Weiterleitung an den Local Collector:

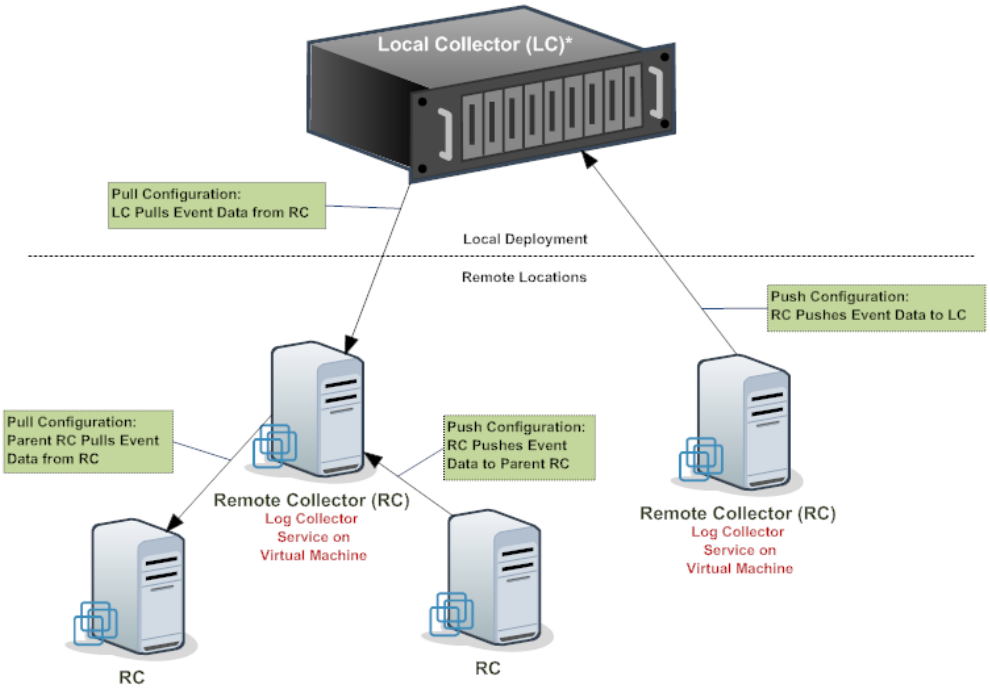
- **Pull-Konfiguration**: Wählen Sie von einem Local Collector die Remote Collectors aus, von denen Sie Ereignisse abrufen möchten.
- **Push-Konfiguration**: Wählen Sie von einem Remote Collector den Local Collector aus, an den Sie Ereignisse übertragen möchten.

Hinweis: Das typische Anwendungsbeispiel ist die Übertragung per Push. Pull ist verfügbar, wenn Sie eine DMZ in Ihrer Umgebung haben. Weniger sichere Netzwerksegmente dürfen keine Verbindungen zu sichereren Netzwerksegmenten herstellen. Bei Pull initiiert der Log Collector (oder Virtual Log Collector) im sicheren Netzwerk die Verbindung mit der VLC im weniger sicheren Netzwerk und die Protokolle werden dann übertragen, ohne dass die Verbindungsregeln gebrochen werden.

Sie können einen oder mehrere Remote Collectors konfigurieren, um Ereignisdaten auf einen Local Collector zu übertragen, oder Sie können einen Local Collector konfigurieren, um Ereignisdaten von einem oder mehreren Remote Collectors abzurufen.

Darüber hinaus können Sie eine Kette von Remote Collectors festlegen, für die Sie Folgendes konfigurieren können:

- Einen oder mehrere Remote Collectors zum Übertragen von Ereignisdaten an einen Remote Collector.
- Einen Remote Collector zum Abrufen von Ereignisdaten aus einem oder mehreren Remote Collectors.



* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

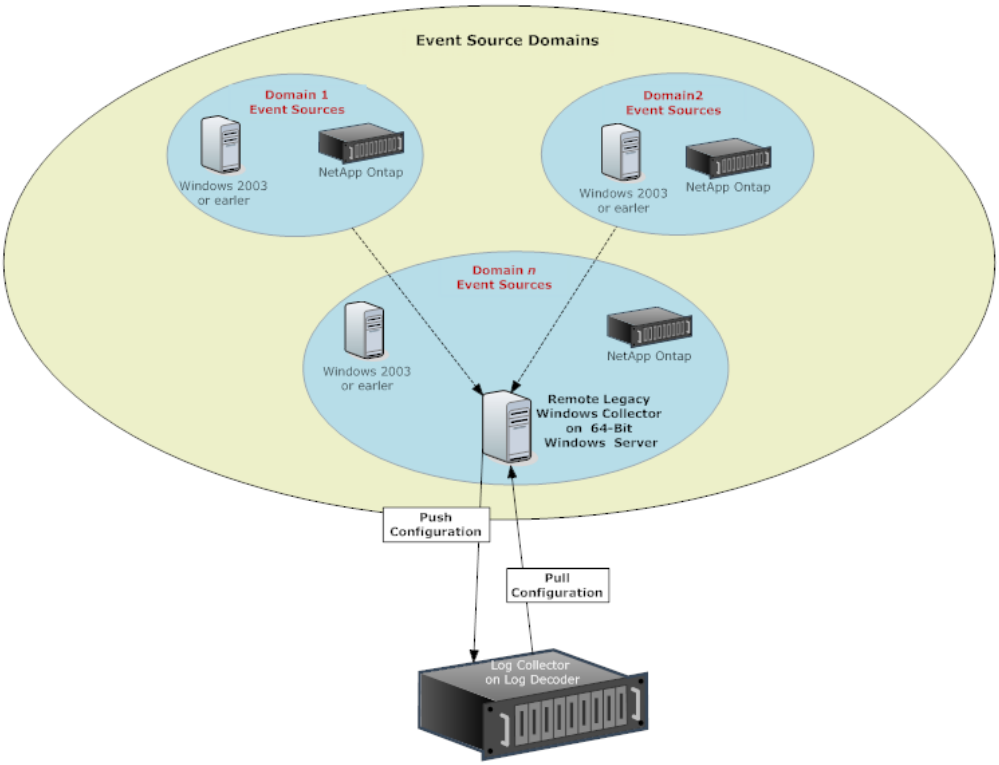
Windows-Legacy-Remote Collector

Der RSA NetWitness® Suite Windows Legacy Collector ist ein Microsoft Windows-basierter Remote Log Collector (RC), der in einer Windows-Domäne installiert werden kann.

Sie unterstützt die Sammlung von :

- Ereignisquellen aus Windows 2003 und früher
- NetApp ONTAP-Host-Ereignisdateien

Die folgende Abbildung zeigt die Bereitstellung, die erforderlich ist, um Ereignisse von Windows-Legacy-Ereignisquellen zu sammeln.


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

Setup

Grundlegende Implementierung

In diesem Thema wird die Ersteinrichtung von Local Collectors und Remote Collectors beschrieben.

Voraussetzungen

Überprüfen, ob der eingerichtete Log Decoder:

- Daten sammelt.
- den aktuellen Inhalt geladen hat.
- korrekt lizenziert ist.

Rollen der Local und Remote Collectors

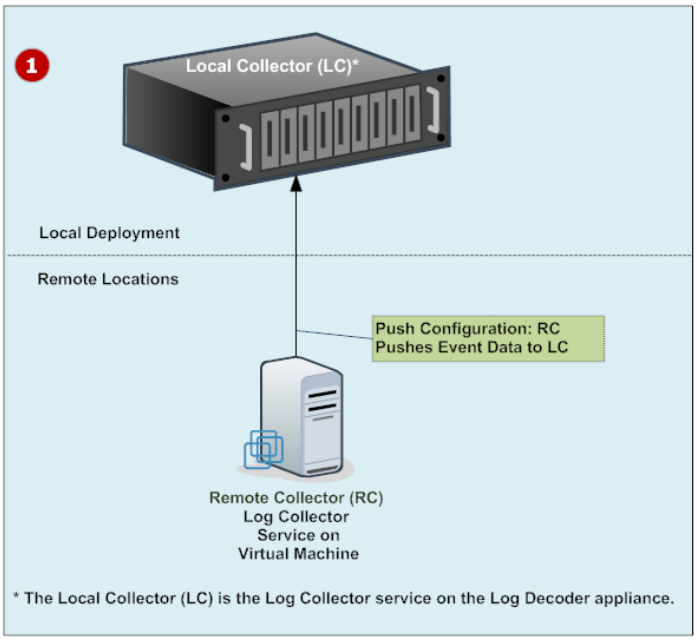
Ein Local Collector (LC) ist ein Log Collector-Service, der auf einem Log Decoder-Host ausgeführt wird. In einem lokalen Bereitstellungsszenario wird der Log Collector-Service auf einem Log Decoder-Host mit dem Log Decoder-Service bereitgestellt. Die Protokollsammlung aus verschiedenen Protokollen wie Windows, ODBC usw. wird durch den Log Collector-Service durchgeführt und an den Log Decoder-Service weitergegeben. Der Local Collector sendet alle gesammelten Ereignisdaten an den Log Decoder-Service.

Sie müssen über mindestens einen Local Collector verfügen, um Nicht-Syslog-Ereignisse sammeln zu können.

Ein Remote Collector (RC), auch bezeichnet als virtueller Log Collector (Virtual Log Collector, VLC), ist ein Log Collector-Service, der auf einer eigenständigen virtuellen Maschine ausgeführt wird. Remote Collectors sind optional und müssen die gesammelten Ereignisse an einen Local Collector senden. Die Remote Collector-Bereitstellung ist ideal, wenn Sie Protokolle aus Remotestandorten sammeln müssen. Remote Collectors komprimieren und verschlüsseln die Protokolle, bevor sie diese an einen Local Collector senden.

Bereitstellen und Konfigurieren von Protokollsammlung

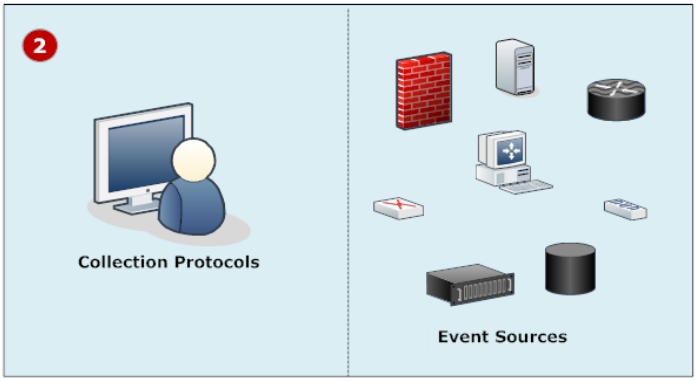
Die folgende Abbildung zeigt die grundlegenden Aufgaben für die Bereitstellung und Konfiguration von Protokollsammlung. Um Protokollsammlung bereitzustellen, müssen Sie einen Local Collector einrichten. Sie können auch einen oder mehrere Remote Collectors bereitstellen. Nach der Bereitstellung der Protokollsammlung müssen Sie die Ereignisquellen in NetWitness Suite und den Ereignisquellen selbst konfigurieren. Im folgenden Diagramm wird der Local Collector mit einem Remote Collector dargestellt, der Ereignisse an den Local Collector weitergibt.



1 Einrichten von Local und Remote Collectors

Der Local Collector ist der Log Collector-Service, der auf dem Log Decoder-Host ausgeführt wird.

Ein Remote Collector ist der Log Collector-Service, der auf einer virtuellen Maschine oder einem Windows-Server an einem Remotestandort ausgeführt wird.



2 Konfigurieren von Ereignisquellen:

- Konfigurieren Sie Sammlungsprotokolle im Verzeichnis C:\Temp\Malware Analysis Configuration Guide für Version 11.0.
- Konfigurieren Sie jede Ereignisquelle für die Kommunikation mit dem NetWitness SuiteLog Collector.

Hinzufügen eines Local und Remote Collector zu NetWitness Suite

So fügen Sie einen Local Collector oder Remote Collector zu NetWitness Suite hinzu:

1. Navigieren Sie zu **ADMIN > Services**.
2. Klicken Sie auf + und wählen Sie im Menü **Log Collector** aus.

   Das Dialogfeld **Service hinzufügen** wird angezeigt.
3. Definieren Sie die Details des Service **Protokollsammlung**.
4. Wählen Sie **Verbindung testen** aus, um sicherzustellen, dass der Local oder Remote Collector hinzugefügt wurde.

Konfigurieren von Protokollsammlung

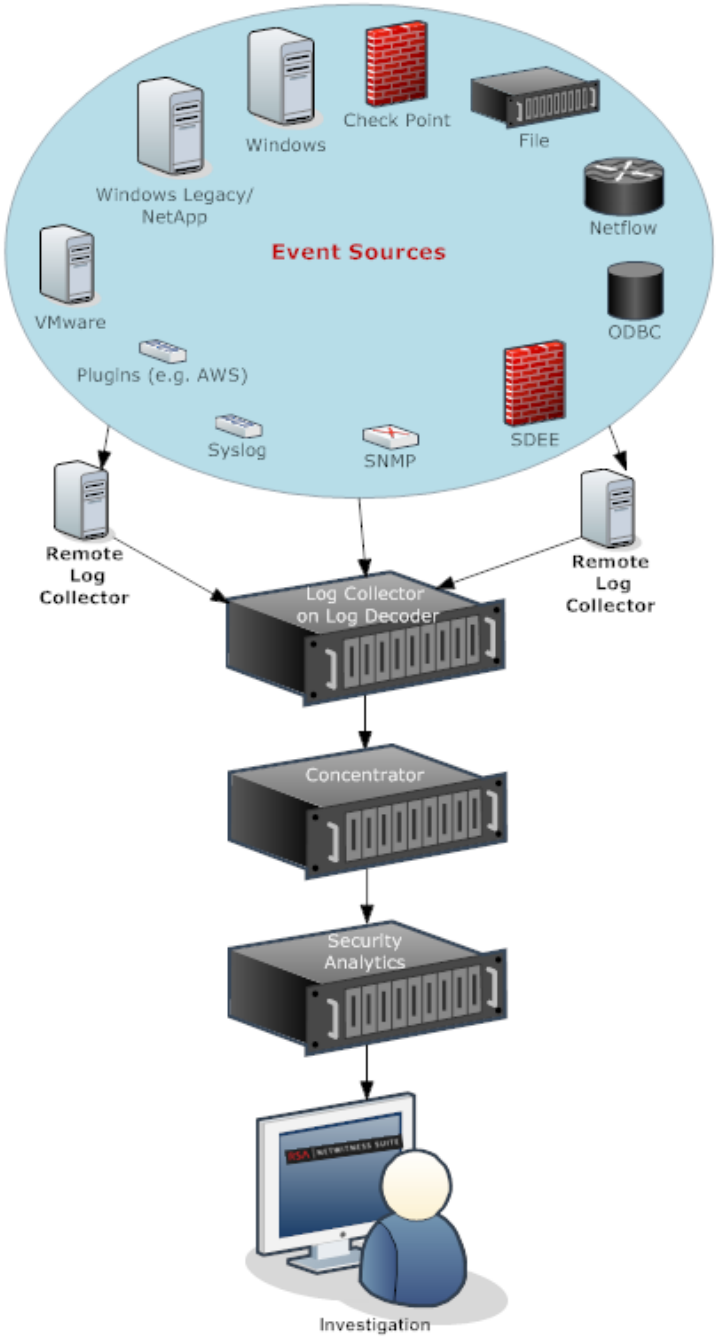
Sie wählen den Log Collector, d. h. entweder einen Local Collector (LC) oder einen Remote Collector (RC), aus, für den Sie Parameter in der Ansicht „Services“ definieren möchten. In der folgenden Abbildung wird dargestellt, wie die Ansicht „Services“ angezeigt und ein Log Collector-Service ausgewählt werden kann. Außerdem wird die Konfigurationsparameterschnittstelle für diesen Service dargestellt.

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Klicken Sie unter **Aktionen** auf ⚙ und wählen Sie **Ansicht** > **Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Definieren Sie globale Protokollsammlungsparameter in der Registerkarte **Allgemein**.
5. Bei einem
   - Local Collector zeigt NetWitness Suite die Registerkarte **Remote Collectors** an. Wählen Sie auf dieser Registerkarte die Remote Collectors aus, von denen der Local Collector Ereignisse abruft.
   - Remote Collector zeigt NetWitness Suite die Registerkarte **Local Collectors** an. Wählen Sie auf dieser Registerkarte die Local Collectors aus, an die der Remote Collector Ereignisse weitergibt.
6. Bearbeiten Sie Konfigurationsdateien als Textdateien in der Registerkarte **Dateien.**
7. Definieren Sie die Sammlungsprotokollparameter in der Registerkarte **Ereignisquellen**.
8. Definieren Sie eine Lockbox, Chiffrierschlüssel und Zertifikate in der Registerkarte „Einstellungen“.

9. Definieren Sie die Parameter des Appliance-Services in der Registerkarte **Appliance-Servicekonfiguration**.

Datenflussdiagramm

Sie verwenden die durch den Log Collector-Service gesammelten Protokolldaten, um den Zustand Ihres Unternehmens zu überwachen und Ermittlungen durchzuführen. Die folgende Abbildung zeigt, wie Daten durch die NetWitness Suite-Protokollsammlung zu Investigation fließen.



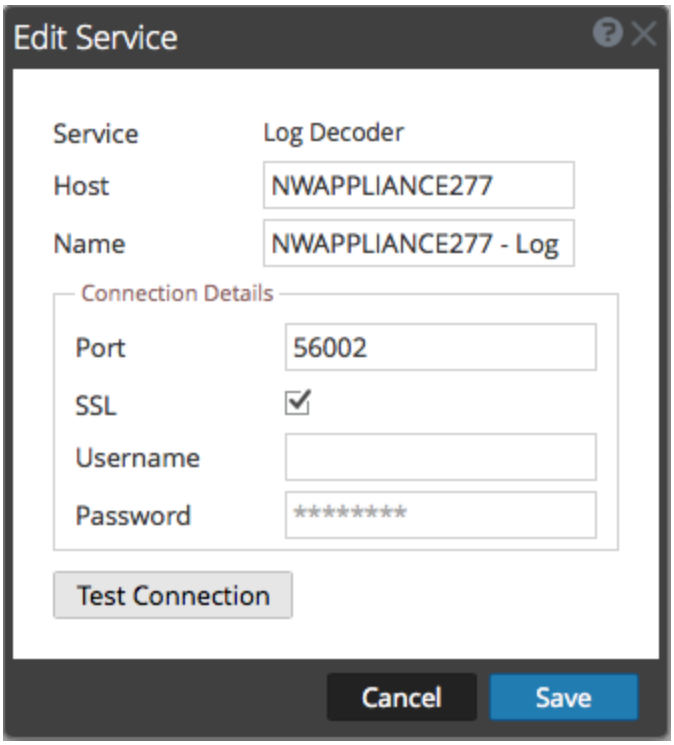
Provisioning von Local Collectors und Remote Collectors

Der NetWitness Suite-Server prüft, ob eine Appliance einen Log Decoder-Service hat. Wenn ein Log Decoder-Service vorhanden ist, wird er zu einem Local Collector. Wenn ein Log Decoder-Service fehlt, wird er zu einem Remote Collector. Ein lokaler Log Collector hat ein Ereignisziel und verbindet sich standardmäßig mit dem lokalen Log Decoder-Service. Ein Remote Collector hat kein Ereignisziel. Der NW-Server-Server identifiziert einen Legacy Windows Collector als Remote Collector.

So bearbeiten Sie einen Local Collector oder Remote Collector:

1. Navigieren Sie zu **ADMIN > Services.**
2. Wählen Sie in der Ansicht **Services** in der Symbolleiste aus.

   Das Dialogfeld **Service bearbeiten** wird angezeigt.



3. Geben Sie im Dialogfeld **Service bearbeiten** die folgenden Informationen an.

Feld	Beschreibung
Service	Wählen Sie Log Collector als Servicetyp aus.
Host	Wählen Sie einen Log Decoder-Host aus.
Name	Geben Sie den Namen ein, den Sie dem Service geben möchten.

Feld	Beschreibung
Port	Standardport ist 50001 für Klartext und 56001 für SSL-verschlüsselten Text.
SSL	Wählen Sie **SSL**, wenn Sie möchten, dass NetWitness Suite mit dem Host mithilfe von SSL kommuniziert. Die Sicherheit der Datenübertragung erfolgt durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten.
(Optional) Benutzername	Geben Sie den Benutzernamen für den Local Collector ein.
(Optional) Passwort	Geben Sie das Passwort für den Local Collector ein.

4. Klicken Sie auf **Verbindung testen**, um festzustellen, ob NetWitness Suite sich mit dem Service verbindet.
5. Wenn das Ergebnis erfolgreich ist, klicken Sie auf **Speichern**.

   Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Serviceinformationen und versuchen Sie es erneut.

Konfigurieren von Local und Remote Collectors

In diesem Thema wird beschrieben, wie Sie Local und Remote Collectors konfigurieren.

Wenn Sie Protokollsammlung bereitstellen, müssen Sie die Log Collectors so konfigurieren, dass diese die Protokollereignisse von unterschiedlichen Ereignisquellen sammeln und diese Ereignisse verlässlich und sicher an den Log Decoder-Service weitergeben. Dort werden die Ereignisse dann analysiert und für weitere Analysen gespeichert.

Sie können einen oder mehrere Remote Collectors konfigurieren, um Ereignisdaten auf einen Local Collector zu übertragen, oder Sie können einen Local Collector konfigurieren, um Ereignisdaten von einem oder mehreren Remote Collectors abzurufen.

In diesem Thema wird Folgendes beschrieben:

- **Konfigurieren des Local Collector für den Abruf von Ereignissen vom Remote Collector**

  Wenn Sie möchten, dass der Local Collector Ereignisse vom Remote Collector abruft, richten Sie dies auf der Registerkarte „Remote Collectors“ in der Konfigurationsansicht des Local Collector ein.

- **Konfigurieren des Remote Collector für die Übertragung von Ereignissen an Local**

Collectors

Wenn Sie möchten, dass ein Remote Collector Ereignisse an einen Local Collector überträgt, richten Sie dies auf der Registerkarte „Local Collector“ in der Konfigurationsansicht des Remote Collector ein. In der Übertragungskonfiguration können Sie auch Folgendes tun:

- **Konfigurieren des Failover Local Collector für den Remote Collector**

  Sie richten ein Ziel ein, das aus Local Collectors besteht. Ist der primäre Local Collector nicht erreichbar, versucht der Remote Collector, mit jedem Local Collector an diesem Ziel eine Verbindung aufzubauen, bis eine erfolgreiche Verbindung hergestellt werden konnte.

- **Replikation konfigurieren**

  Sie können mehrere Zielgruppen einrichten, sodass NetWitness die Ereignisdaten in jeder Gruppe repliziert. Wird die Verbindung zu einer der Zielgruppen unterbrochen, können Sie die erforderlichen Daten wiederherstellen, da sie in einer anderen Zielgruppe repliziert wurden.

- **Konfigurieren der Protokollweiterleitung für bestimmte Protokolle**

  Sie können mehrere Ziele in einer Zielgruppe einrichten, sodass Ereignisdaten je nach Protokolltyp an bestimmte Ziele weitergeleitet werden.

- **Konfigurieren einer Kette von Remote Collectors**

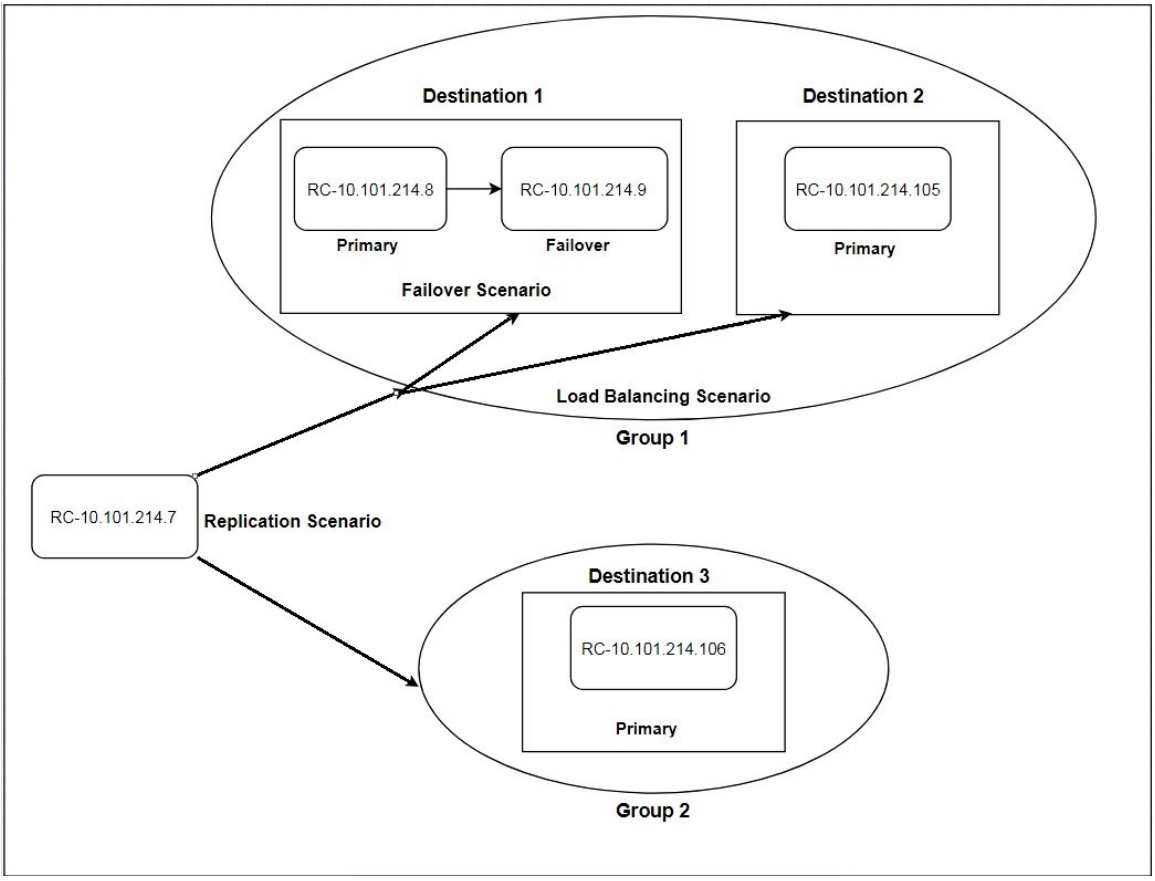
  Sie können eine Kette von Remote Collectors konfigurieren, um Ereignisdaten auf einen Local Collector zu übertragen, oder Sie können einen Local Collector konfigurieren, um Ereignisdaten von einer Kette von Remote Collectors abzurufen.

  - Sie können einen oder mehrere Remote Collectors zum Übertragen von Ereignisdaten an einen Remote Collector konfigurieren.
  - Sie können einen Remote Collector zum Abrufen von Ereignissen von einem oder mehreren Remote Collectors konfigurieren.

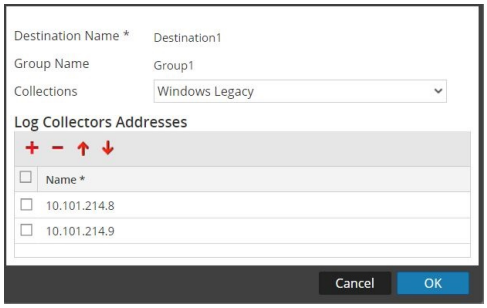
Failover, Replikation und Lastenausgleich

In diesem Abschnitt wird die Funktionsweise von Failover, Replikation und Lastenausgleich in RSA NetWitness Suite beschrieben.

Die folgende Abbildung veranschaulicht einen für Lastenausgleich, Failover und Replikation konfigurierten Remote Collector.

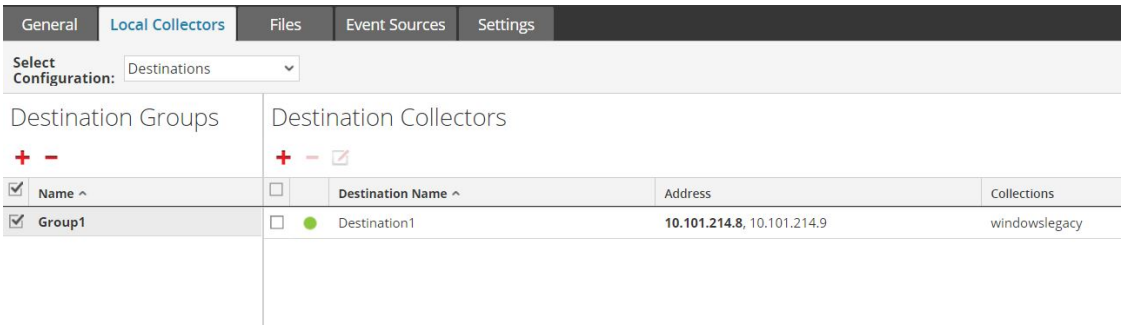


- **Failover** wird erreicht, indem mehrere Collectors auf demselben Ziel eingerichtet werden. Ziel 1 verfügt über einen primären Collector und einen zweiten Collector, den Failover-Collector. Dies wird in NetWitness Suite durch Hinzufügen mehrerer Log Collectors zum gleichen Ziel erreicht.

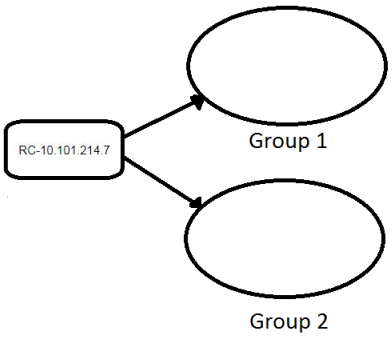


Da 10.101.214.8 zuerst aufgeführt ist, wird diese Adresse der primäre Collector und 10.101.214.9 wird der Failover-Collector. Um 10.101.214.9 zum primären Collector zu machen, ändern Sie die Reihenfolge mithilfe des Nach-oben-Pfeils.

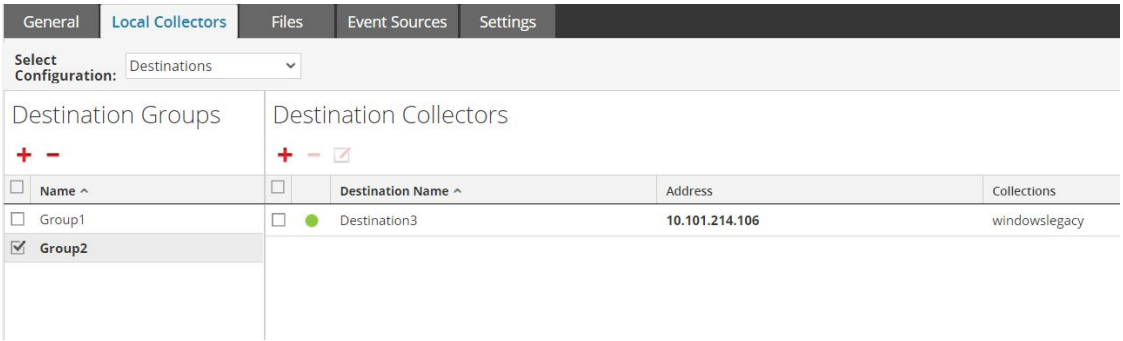
Im Folgenden sehen Sie, wie die zwei Collectors beide für Ziel 1 aufgeführt sind. Der primäre Collector (10.101.214.8) ist fett markiert.



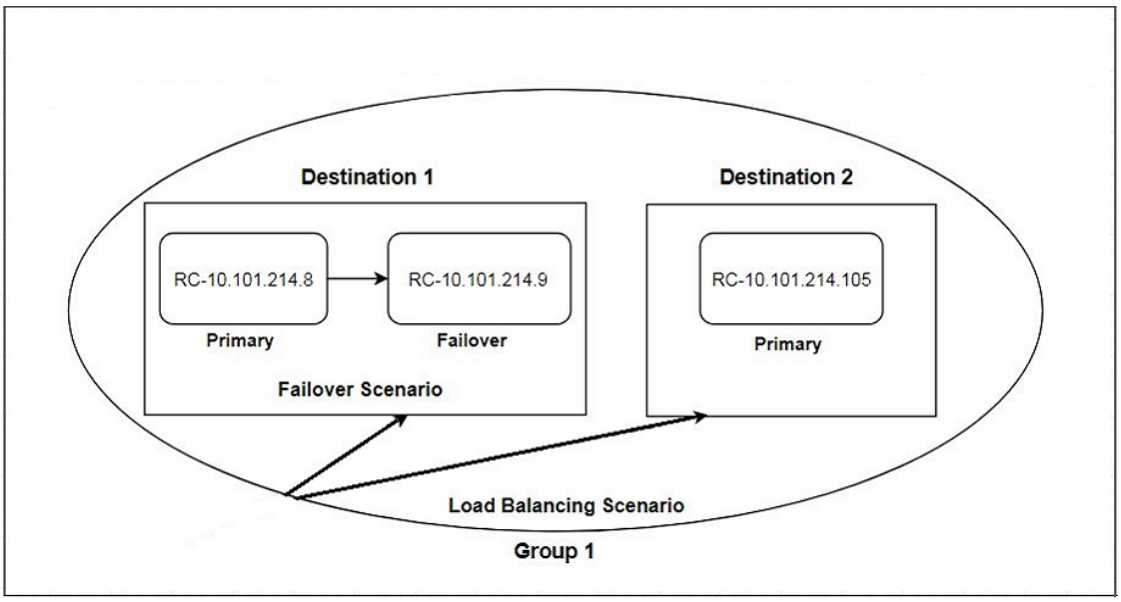
- **Replikation** wird mithilfe mehrerer Zielgruppen erreicht: Jede Gruppe erhält den gesamten Satz an Nachrichtendaten.



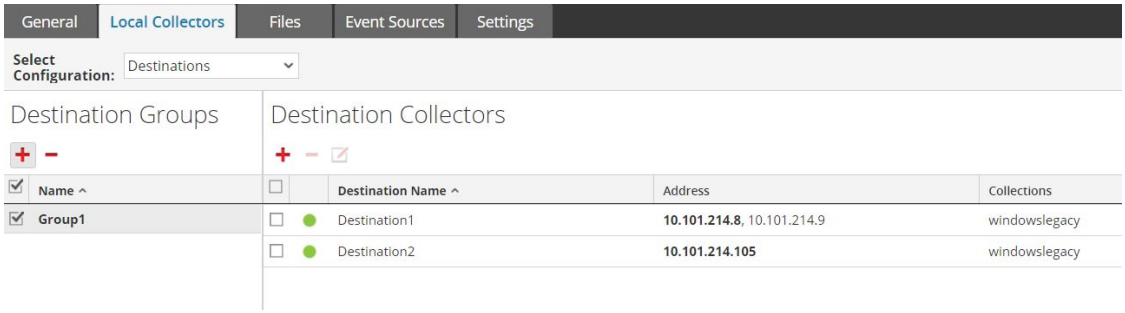
Auf dem folgenden Bildschirm können Sie sehen, dass Nachrichtendaten an die Collectors in Gruppe 1 *und* Gruppe 2 gesendet werden.



- **Lastenausgleich** wird erreicht, indem mehrere Ziele innerhalb einer Gruppe eingerichtet werden.



Im folgenden Bildschirm können Sie sehen, dass die Gruppe 1 zwei Ziele hat, Ziel 1 und Ziel 2. Die Nachrichtendaten werden gleichmäßig auf die Ziele in der Gruppe verteilt.



Bei zwei Zielen erhält jedes Ziel die Hälfte der Nachrichtendaten. Bei drei Zielen würde jedes Ziel jeweils 1/3 der gesamten Nachrichtendaten erhalten. Fügen Sie weitere Ziele hinzu, um die Last auf den Collectors in jedem Ziel zu verringern.

Hinweis: Sie können auch eine Protokollweiterleitung einrichten, sodass Ereignisdaten für bestimmte Protokolle an bestimmte Ziele gesendet werden.

Konfigurieren eines Local oder Remote Collector

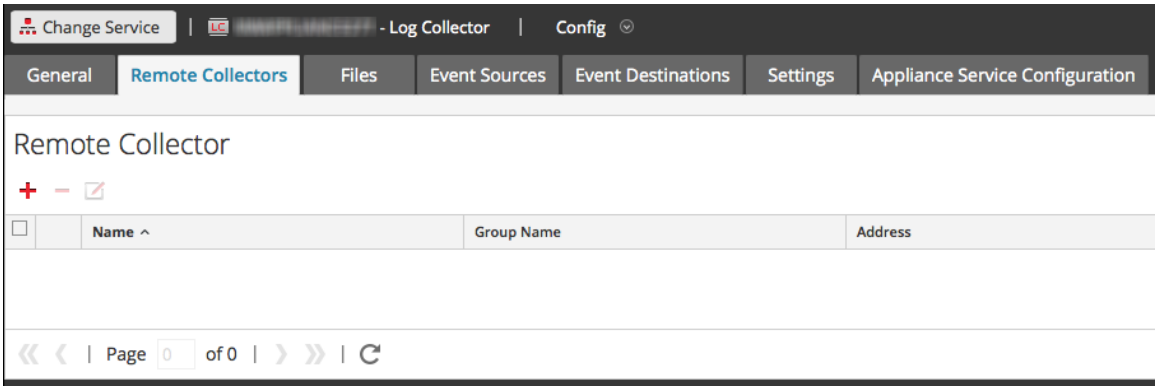
Sie wählen den Log Collector aus, also einen Local Collector (LC) oder Remote Collector (RC), für den Sie in der Ansicht „Services“ die Bereitstellungsparamater definieren möchten. Im folgenden Verfahren wird gezeigt, wie Sie zur Ansicht Services gelangen, einen Local oder Remote Collector auswählen und die Bereitstellungsparameteroberfläche für diesen Service aufrufen.

So konfigurieren Sie einen Local oder Remote Collector:

1. Navigieren Sie zu **ADMIN > Services.**
2. Wählen Sie einen Local- oder Remote-Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Führen Sie je nach Ihrer Auswahl in Schritt 2 folgende Schritte durch:
   - Bei Auswahl eines Local Collector wird die Registerkarte **Remote Collectors** angezeigt. Wählen Sie auf dieser Registerkarte die Remote Collectors aus, von denen der Local Collector Ereignisse abruft.
   - Wenn Sie einen Remote Collector ausgewählt haben, werden die **Local Collectors** angezeigt. Wählen Sie auf dieser Registerkarte die Local Collectors aus, an die der Remote Collector Ereignisse überträgt.

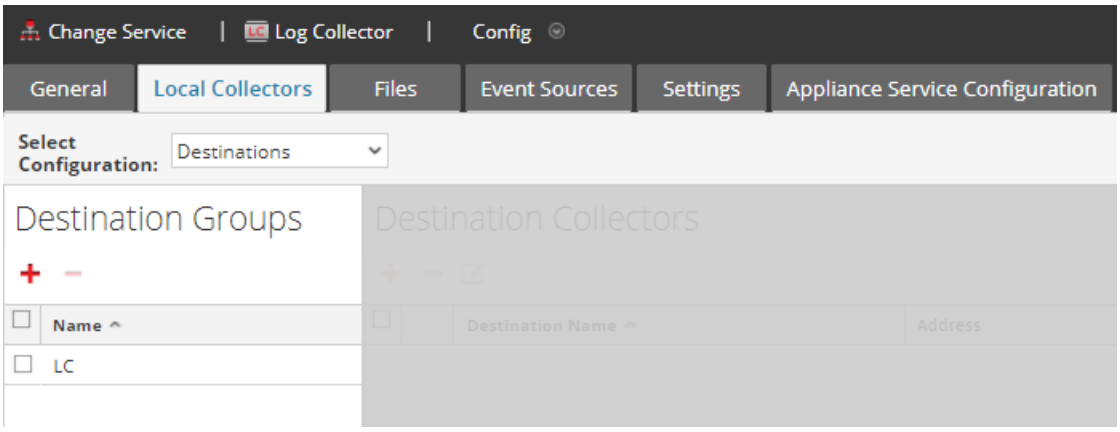
Registerkarte „Remote Collectors“

In der folgenden Abbildung ist die Registerkarte **Remote Collectors** für einen Local Collector dargestellt, der zum Abrufen von Ereignissen aus einem Remote Collector konfiguriert ist. NetWitness Suite zeigt diese Registerkarte an, wenn Sie einen Local Collector in **Administration > Services** ausgewählt haben.

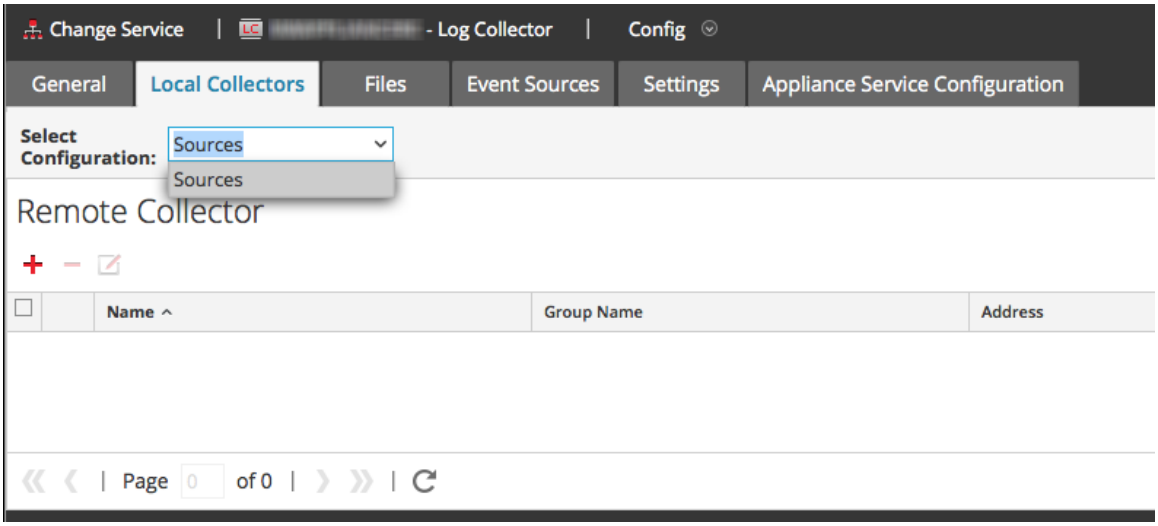


Registerkarte „Local Collectors“ für einen Remote Collector

In der folgenden Abbildung ist die Registerkarte **Local Collectors** für einen Remote Collector dargestellt, der zum Übertragen von Ereignissen an einem Local Collector oder einen anderen Remote Collector konfiguriert ist.



In der folgenden Abbildung ist die Registerkarte „Local Collectors“ für einen Remote Collector dargestellt, der zum Abrufen von Ereignissen aus einem Remote Collector konfiguriert ist. NetWitness Suite zeigt diese Registerkarte an, wenn Sie einen Remote Collector in **Administration > Services** ausgewählt haben.



Parameter

Konfigurationsparameter für Remote/Local Collectors

Konfigurieren des Failover Local Collector

In diesem Thema erfahren Sie, wie Sie einen Failover-Local Collector oder Failover-Remote Collector einrichten.

Einrichten eines Failover Local Collector

Sie können einen Failover Local Collector einrichten, zu dem RSA NetWitness® Suite ein Failover ausführt, wenn der primäre Local Collector aus einem beliebigen Grund nicht mehr funktioniert.

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie unter **Services** einen Remote Collector-Service aus.
3. Klicken Sie auf unter **Aktionen** und wählen Sie **Ansicht > Konfiguration** aus.

   Die Ansicht „Service-Konfiguration“ wird mit geöffneter Registerkarte **Log CollectorAllgemein** angezeigt.
4. Wählen Sie die Registerkarte **Local Collectors** aus.
5. Wählen Sie im Abschnitt **Zielgruppenbereich** aus.

   Das Dialogfeld Remoteziel hinzufügen wird angezeigt.
6. Richten Sie eine Zielgruppe ein und wählen Sie einen primären Local Collector aus (zum Beispiel **LC-PRIMARY**).
7. Wählen Sie im Bereich „Zielgruppen“ die Gruppe aus (zum Beispiel **Primary_Standby_LCs**) und klicken Sie auf .

   Die ausgewählte Gruppe wird im Bereich „Local Collectors“ angezeigt.
8. Fügen Sie den Failover Local Collector hinzu (zum Beispiel **LC-STANDBY**).

   Die folgenden Beispiele zeigen die neu hinzugefügten primären und Failover Local Collectors, wobei der primäre Local Collector mit dem Status **Aktiv** und der Failover Local Collector als **Stand-by** angezeigt wird. Der aktive Local Collector ist hervorgehoben (zum Beispiel **LC-PRIMARY**).
9. (Optional) Fügen Sie den einzelnen Remotezielen Local Collectors hinzu, löschen Sie sie oder ändern Sie ihre Reihenfolge.
   a. Klicken Sie auf , um einen Log Collector als Failover-Remoteziel hinzuzufügen.
   b. Beim Herstellen einer Verbindung zu einem Remoteziel versucht der Remote Collector, der Reihe nach eine Verbindung mit jedem Local Collector in dieser Liste herzustellen, bis eine erfolgreiche Verbindung hergestellt wurde.
   c. Wählen Sie einen Local Collector aus und ändern Sie die Verbindungsreihenfolge mithilfe der Pfeilschaltflächen nach oben ( ) und unten ( ).
   d. Wählen Sie einen oder mehrere Local Collectors aus und klicken Sie auf , um sie aus der Liste zu entfernen.

   Die ausgewählten Local Collectors werden zum Abschnitt Log Collector hinzugefügt. Wenn der Remote Collector mit der Datensammlung beginnt, überträgt er Daten an diese Log Collectors.

Einrichten eines Failover Remote Collector

Sie können einen Failover- einrichten, zu dem RSA NetWitness® Suite ein Failover ausführt, wenn der primäre Remote Collector aus einem beliebigen Grund nicht mehr funktioniert.

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie unter **Services** einen Remote Collector-Service aus.
3. Klicken Sie auf  unter **Aktionen** und wählen Sie **Ansicht > Konfiguration** aus.

   Die Ansicht „Service-Konfiguration“ wird mit geöffneter Registerkarte **Log CollectorAllgemein** angezeigt.
4. Wählen Sie die Registerkarte **Local Collectors** aus.
5. Wählen Sie **Quellen** aus dem Drop-down-Menü **Konfiguration auswählen** aus.
6. Klicken Sie auf  , um es im Dialogfeld **Quelle hinzufügen** anzuzeigen.
7. Definieren Sie den Failover Remote Collector und klicken Sie auf **OK**.

Parameter

Konfigurationsparameter für Remote/Local Collectors

Replikation konfigurieren

In diesem Thema wird beschrieben, wie Sie Ereignisdaten, die von einem Remote Collector gesendet wurden, replizieren.

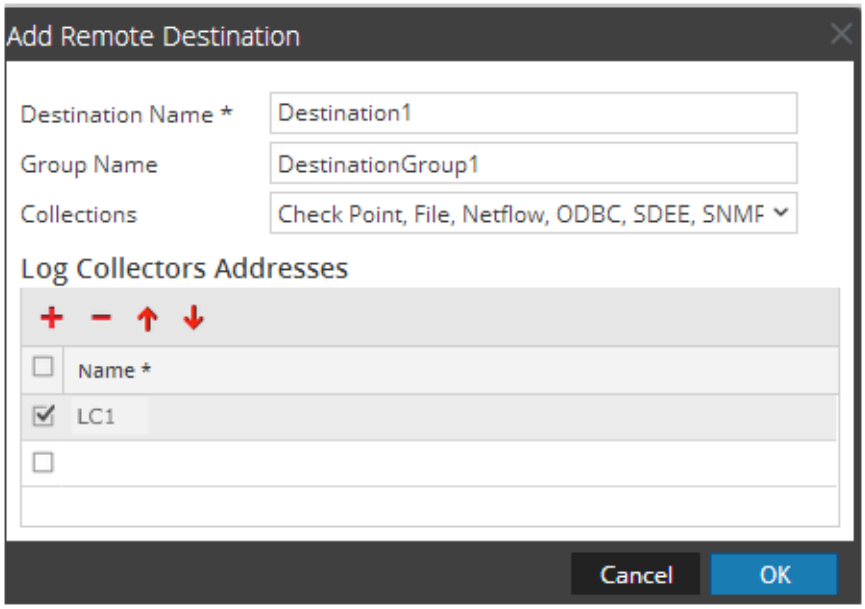
Sie können mehrere Zielgruppen spezifizieren, sodass Ereignisdaten an alle Gruppen repliziert werden.

So replizieren Sie Ereignisdaten zu mehreren Local Collectors:

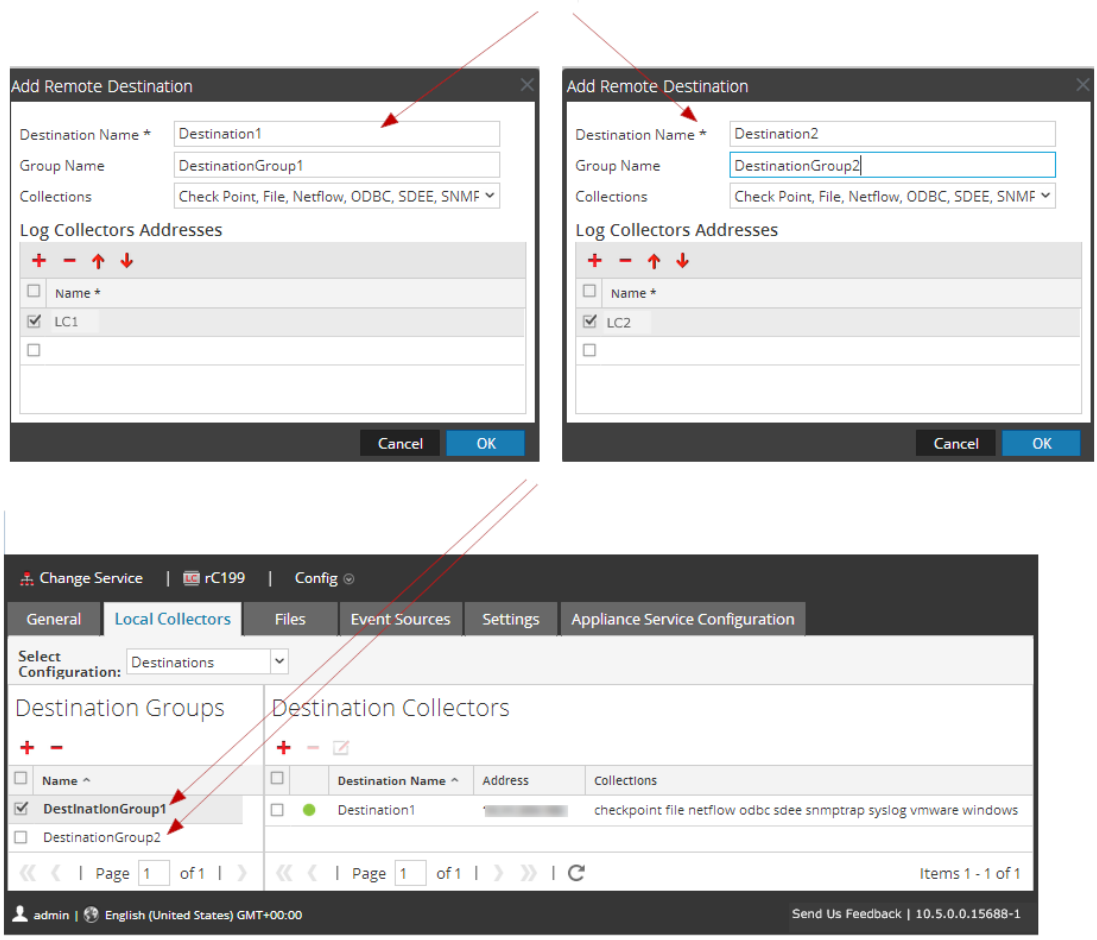
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Remote-Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Service-Konfiguration“ wird mit geöffneter Registerkarte **Log CollectorAllgemein** angezeigt.
4. Wählen Sie die Registerkarte **Local Collectors** aus.
5. Klicken Sie im Bereich **Zielgruppen** auf  .

   Das Dialogfeld **Remoteziel hinzufügen** wird angezeigt.



6. Richten Sie ein separates Ziel für jeden Local Collector ein und bestimmen Sie die Protokolle, für die Ereignismeldungen an diesen Local Collector ausgeführt werden sollen. Folgende Beispiele zeigen die zwei zusätzlichen Ziel-Local Collectors (**Ziel1** und **Ziel2**) für die Sammlungsprotokolle **Kontrollpunkt**, **Datei**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** und **Windows** an:



a. Geben Sie den **Zielnamen** ein.

b. Geben Sie den **Gruppennamen** ein. Wenn Sie keinen Gruppennamen eingeben, wird der Zielname als Gruppenname verwendet.

c. Wählen Sie aus der Drop-down-Liste die Sammelprotokolle aus.

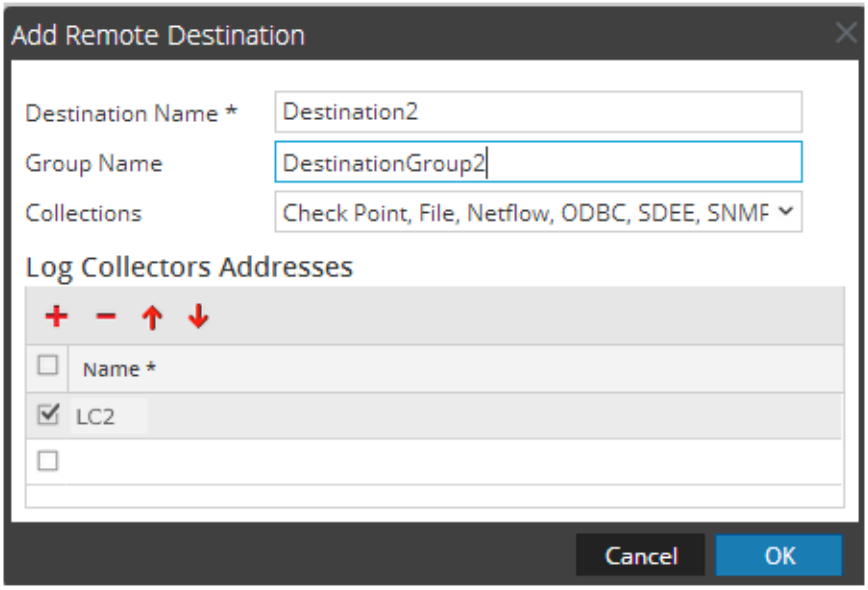
d. Wählen Sie einen Local Collector aus (zum Beispiel **LC1**).

e. Klicken Sie auf **OK**.

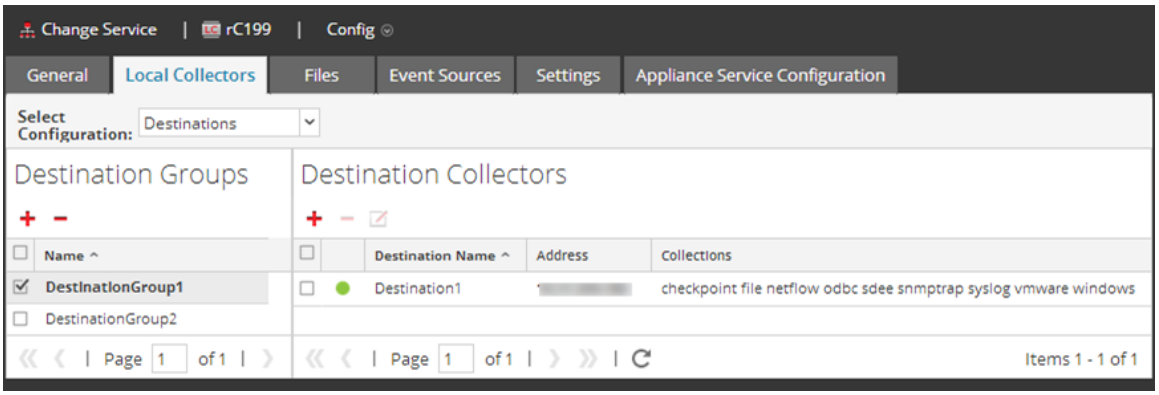
f. Wählen Sie die neue Gruppe (zum Beispiel **DestinationGroup2**) im Bereich **Zielgruppen** aus und klicken Sie im Bereich **Local Collector** auf +.

g. Klicken Sie im Bereich **Local Collector** auf + und füllen Sie das Dialogfeld

Remoteziel hinzufügen aus, wie in der folgenden Abbildung dargestellt.



Die Sammlungsprotokolle **Kontrollpunkt**, **Datei**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** und **Windows** werden an zwei Local Collectors (**LC1** und **LC2**) gesendet. Beide Local Collectors sind aktiv und sammeln Ereignisdaten.



Konfigurieren einer Kette von Remote Collectors

Dieses Thema erklärt, wie man Remote Collectors (auch als VLCs bezeichnet) aneinanderreihen kann.

Sie können eine Kette von Remote Collectors erstellen, um Ereignisdaten an einen Remote Collector zu übertragen, oder einen Remote Collector konfigurieren, um Ereignisdaten von einer Kette von Remote Collectors abzurufen.

- **Remote-Collectors, um Daten zu übertragen.** Übertragen Sie Daten von einem Remote Controller zu anderen Remote Collectors oder Local Collectors.

- **Remote Collector, um Daten abzurufen.** Verwenden Sie einen Remote Collector zum Abrufen von Ereignisdaten aus einem oder mehreren Remote Collectors.

Konfigurieren des Remote Collector für die Übertragung von Ereignissen an einen Remote Collector

Sie können einen Remote Collector für die Übertragung von Ereignisdaten an einen Remote Collector konfigurieren.

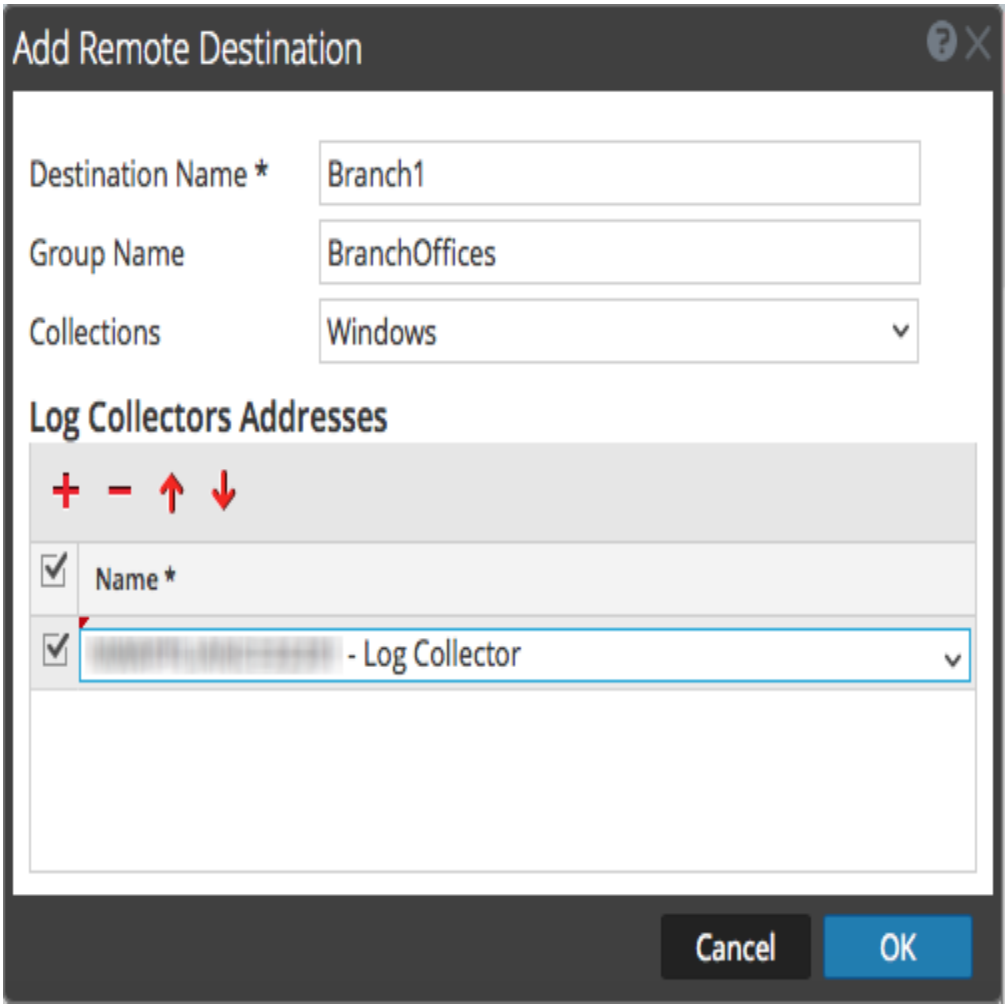
Konfigurieren eines Remote Collectors für die Übertragung von Ereignissen an den angegebenen Remote Collector

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie unter **Services** einen **Remote Collector** aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

   Die Ansicht **Log CollectorService-Konfiguration** wird mit geöffneter Registerkarte **Log CollectorAllgemein** angezeigt.
4. Wählen Sie die Registerkarte **Local Collectors** aus.
5. Wählen Sie im Drop-down-Menü **Konfigurationen auswählen** die Option **Ziele** aus.
6. Wählen Sie im Abschnitt **Zielgruppenbereich**  aus.

   Das Dialogfeld **Remoteziel hinzufügen** wird angezeigt.
7. Richten Sie eine **Zielgruppe** ein:
   a. Geben Sie einen **Zielnamen** ein.
   b. (Optional) **Geben Sie einen Namen für die Gruppe ein**. Wenn Sie den Gruppennamen leer lassen, stellt ihn NetWitness Suite auf den Wert ein, den Sie in „Zielname“ angegeben haben.
   c. Wählen Sie ein oder mehrere Sammlungsprotokolle aus der Drop-down-Liste **Sammlungen** aus.
   d. Klicken Sie im Abschnitt **Log Collector-Adressen** auf  , um einen Remote Collector

auszuwählen.



Hinweis: Wenn Sie kein Sammlungsprotokoll auswählen, leitet der Remote Collector alle Sammlungsprotokolle an die Remote Collectors weiter.

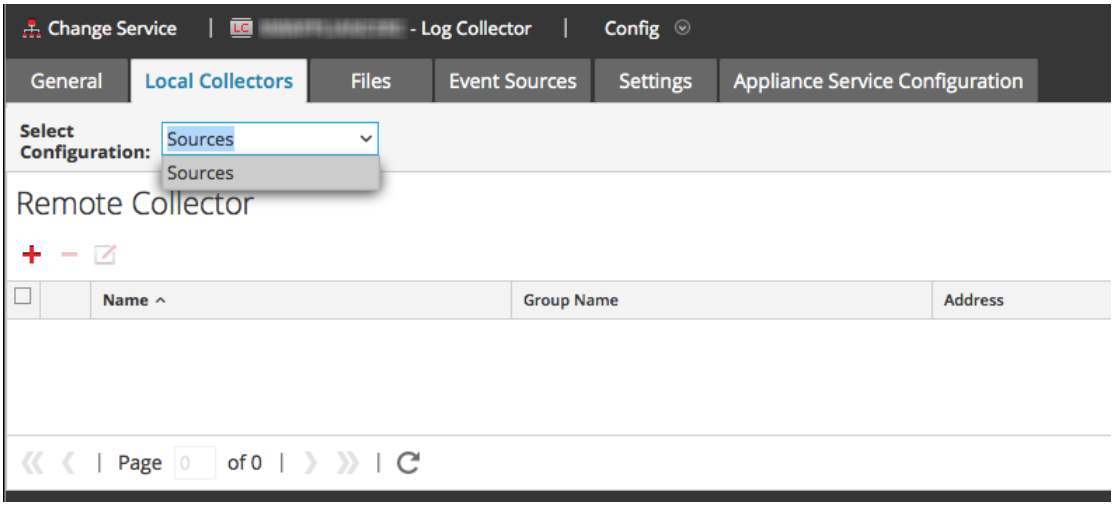
Konfigurieren des Remote Collector für den Abruf von Ereignisdaten von einem Remote Collector

Konfigurieren des ausgewählten Remote Collector für den Abruf von Ereignissen vom angegebenen Remote Collector

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie unter **Services** einen **Remote Collector** aus.
3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

Die Ansicht **Service-Konfiguration** wird mit geöffneter Registerkarte **Log CollectorAllgemein** angezeigt.

4. Wählen Sie die Registerkarte **Local Collectors** aus.
5. Wählen Sie im Drop-down-Menü **Konfigurationen auswählen** die Option **Quellen** aus.



6. Wählen Sie im Bereich **Remote Collectors** die Option + aus.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.

7. Gehen Sie im Dialogfeld **Quelle hinzufügen** wie folgt vor:

   a. Wählen Sie ein oder mehrere Sammlungsprotokolle aus.

      Wenn Sie kein Sammlungsprotokoll auswählen, ruft der Remote Collector alle Sammlungsprotokolle aus dem Remote Collector ab.

   b. Klicken Sie auf **OK**.

      Der Remote Collector wird dem Abschnitt „Remote Collector“ hinzugefügt. Wenn der Log Collector mit der Datensammlung beginnt, werden Ereignisdaten aus diesem Remote Controller abgerufen.

Drosseln des Remote Collector auf die Local Collector-Bandbreite

Um die Performance zu verbessern, können Sie die Bandbreite drosseln, um die Frequenz, mit welcher der Remote Collector Ereignisdaten zum Local Collector oder zwischen Message Brokern sendet, zu steuern. Um dies auszuführen, konfigurieren Sie die Linux-Kernel-Filterung und die IPTable-Funktion.

Dies ist sowohl für Push- als auch für Pull-Konfigurationen des Remote Collector erforderlich. Das Shellskript **set-shovel-transfer-limit.sh**, das sich in **/opt/netwitness/bin** befindet, automatisiert die Konfiguration des mit diesem Port verbundenen Kernel-Filters und der IpTables.

In diesem Thema wird beschrieben, wie Remote Collector mithilfe des Shell-Skripts **set-shovel-transfer-limit.sh** auf Local Collector-Bandbreite gedrosselt werden kann. Es enthält die folgenden Abschnitte:

- Die Befehlszeilenhilfe des Shellskripts **set-shovel-transfer-limit.sh**.

  Hinweis: Der Filterwert, den Sie einstellen müssen, hängt von der Frequenz ab, mit der der Remote Collector Ereignisse zum Local Collector sendet.

- Der Filter wird zum Beispiel auf 4.096 Kilobits pro Sekunde eingestellt.

Befehlszeilenhilfe zum Skript „Set Shovel Transfer Limit“

Geben Sie den `-h`-Befehl aus, um Hilfe zu `set-shovel-transfer-limit.sh` Shell-Skript anzuzeigen.

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

Nutzung:

```
code>set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r
rate]
```

Hierbei gilt:

- -c = Vorhandenes löschen
- -d = Filter anzeigen
- -s = neue Werte einstellen
- -i = Schnittstelle ist der Name der Netzwerkschnittstelle. Der Standardwert ist **eth0**
- -r = Rate ist die Bandbreitenrate. Standardwert ist **256kbps**.

Bandbreiten und Raten können wie folgt angegeben werden:

- **nolimit** = deaktiviert Drosselung
- **Kbit**: Kilobits pro Sekunde
- **mbit**: Megabits pro Sekunde
- **kbps**: Kilobyte pro Sekunde
- **mbps**: Megabyte pro Sekunde
- **bps**: Byte pro Sekunde

Stellen Sie den Filter auf 4.096 Kilobits pro Sekunde

In diesem Beispiel wird der Filter auf 4.096 Kilobits pro Sekunde eingestellt.

```
[root@<hostname> bin]#./set-shovel-transfer-limit.sh -s -r
4096kbit

RATE=4096kbit
 PORTNUMBER=5671
 DEVICE_INTERACE=eth0

iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK
]

Current/new values...

iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source
destination

Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source          destination

Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0     0.0.0.0/0
multiport dports 5671 MARK set 0xa
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0    0.0.0.0/0
multiport sports 5671 MARK set 0xa

Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination

tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000

class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Einrichten einer Lockbox

In diesem Thema erfahren Sie, wie Sie Lockbox-Sicherheitseinstellungen konfigurieren.

Was ist eine Lockbox?

Eine Lockbox ist eine verschlüsselte Datei, die Sie verwenden, um vertrauliche Informationen über eine Anwendung zu speichern. Die NetWitness Suite-Lockbox speichert einen Chiffrierschlüssel für den Log Collector.

Der Chiffrierschlüssel dient zur Verschlüsselung aller Ereignisquellenpasswörter und des Ereignis-Broker-Passworts.

Wenn Sie die Lockbox erstellen, müssen Sie ein Passwort für die Lockbox definieren.

Die Log Collector betreibt die Lockbox in einem Modus während der Datenerfassung, der es nicht erforderlich macht, das Passwort anzugeben (die Log Collector verwendet stattdessen den Host-Systemfingerabdruck).

Dies sind die Lockbox-Sicherheitseinstellungen.

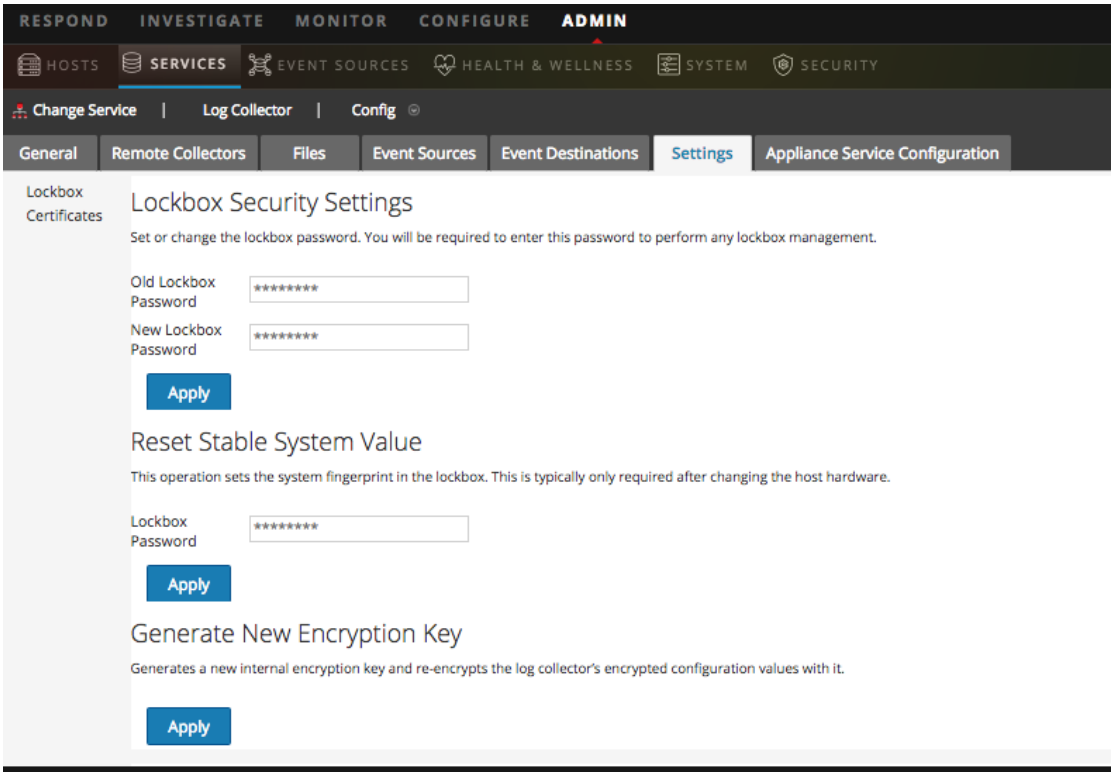
Funktion	Beschreibung
Altes Lockbox-Passwort	Wenn Sie eine Lockbox zum ersten Mal einrichten, ist dieses Feld leer. NetWitness Suite füllt das Feld aus, nachdem Sie ein neues Lockbox-Passwort eingegeben und auf „Anwenden“ geklickt haben.
Neues Lockbox-Passwort	Anfängliches oder neues Lockbox-Passwort. Für optimale Lockbox-Sicherheit geben Sie ein Passwort mit acht oder mehr Zeichen an, das mindestens ein numerisches Zeichen, einen Großbuchstaben und nicht alphanumerische Zeichen wie z. B. # oder ! enthält.
Anwenden	Klicken Sie auf **Anwenden**, um die Änderungen am Lockbox-Passwort zu übernehmen.

Einrichten einer Lockbox

Zur Einrichtung einer Lockbox müssen wie folgt ein Passwort einrichten:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“  **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Einstellungen**.



5. Wählen Sie im Optionsbereich **Lockbox** aus, um die Lockbox-Einstellungen zu konfigurieren.
6. Geben Sie unter **Lockbox-Sicherheitseinstellungen** ein Passwort in das Feld **Neues Lockbox-Passwort** ein und klicken Sie auf **Anwenden**.

Starten von Sammlungsservices

Wenn ein Sammlungsservice anhält, müssen Sie ihn möglicherweise erneut starten. Sie können auch den automatischen Start von Sammlungsservices aktivieren.

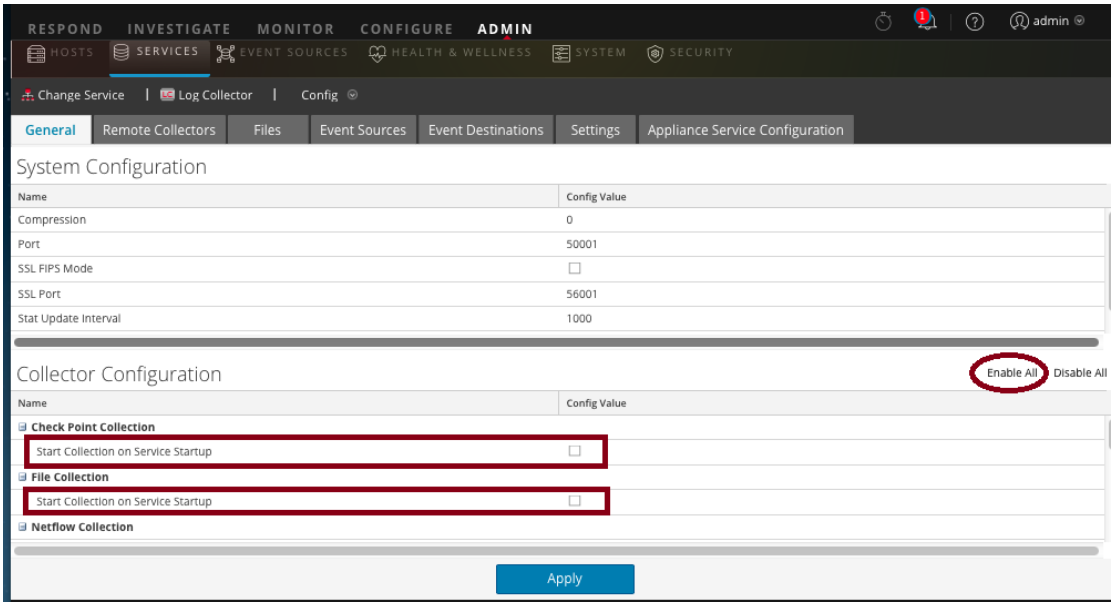
Starten eines Sammlungsservices

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Log Collector-Service aus und klicken Sie unter **Aktionen** auf  .
3. Klicken Sie auf **Ansicht** > **System**.
4. Klicken Sie auf **Sammlung** > ***Service*** (zum Beispiel **Datei**) und klicken Sie auf **Start**.

Aktivieren des automatischen Starts für Servicesammlung

1. Navigieren Sie zu **Admin > Services**.
2. Wählen Sie einen Log Collector-Service aus und klicken Sie unter **Aktionen** auf  .
3. Klicken Sie auf **Ansicht** > **Konfiguration**.

   Die Registerkarte „Allgemein“ wird angezeigt.
4. Wählen Sie im Bereich „Collector-Konfiguration“ für die einzelnen Sammlungsservices, die Sie automatisch starten möchten, die Option **Sammlung bei Start des Services starten** aus. Wählen Sie alternativ **Alle aktivieren** aus, um alle Sammlungsservices automatisch zu starten.



5. Klicken Sie auf **Anwenden**, damit Ihre Änderungen übernommen werden.

Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

In diesem Thema erfahren Sie, wie Sie überprüfen, ob die Protokollsammlung korrekt eingerichtet wurde.

Mithilfe der folgenden Methoden kann überprüft werden, ob die Protokollsammlung funktioniert.

- Überprüfen Sie die Ereignisaktivität auf der Registerkarte „Ereignisquellenüberwachung“ der Ansicht **Administration > Integrität > Zustand**.

- Vergewissern Sie sich, dass in der Ansicht **Investigation > Ereignisse** im Feld **Gerätetyp** in der Spalte **Details** Parser für das von Ihnen konfigurierte Sammlungsprotokoll vorhanden sind.

Informationen zu den Schritten zur Überprüfung der korrekten Protokolleinrichtung finden Sie in den Themen zum jeweiligen Sammlungsprotokoll.

Konfigurieren von Zertifikaten

Sie managen Zertifikate, indem Sie Truststores auf dem Log Collector erstellen. Der Log Collector schlägt in diesen Truststores nach, um festzustellen, ob die Ereignisquellen vertrauenswürdig sind.

Hinzufügen eines Zertifikats

So fügen Sie ein Zertifikat hinzu:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.
3. Klicken Sie auf  unter **Aktionen** und wählen Sie **Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Wählen Sie im Bereich Optionen **Zertifikate** aus.
6. Klicken Sie auf  in der Symbolleiste **Zertifikate**.

   Das Dialogfeld **Zertifikat hinzufügen** wird angezeigt.
7. Klicken Sie auf **Durchsuchen** und wählen Sie ein Zertifikat (***.PEM**) aus Ihrem Netzwerk aus.
8. Geben Sie ein Passwort an (falls erforderlich).
9. Klicken Sie auf **Speichern**.

Bereich „Zertifikate“

In der folgenden Tabelle werden die Schaltflächen und Spalten im Bereich „Zertifikate“ beschrieben.

Feld	Beschreibung
	Öffnet das Dialogfeld „Zertifikat hinzufügen“, in dem Sie ein Zertifikat und ein Passwort hinzufügen können.

Feld	Beschreibung
	Löscht die ausgewählten Zertifikate.
	Wählt Zertifikate aus.
Truststore-Name	Zeigt den Namen des Truststore an.
Distinguished Name des Zertifikats	Zeigt nur für Kontrollpunkt-Ereignisquellen den Distinguished Name für das Zertifikat an.
Zertifikatpasswortname	Zeigt nur für Kontrollpunkt-Ereignisquellen den Zertifikatpasswortnamen an.

Dialogfeld „Zertifikat hinzufügen“

In der folgenden Tabelle werden die Parameter im Dialogfeld **Zertifikat hinzufügen** beschrieben.

Feld	Beschreibung
Truststore-Name	Geben Sie einen Truststore-Namen ein.
Datei	Klicken Sie auf „Durchsuchen“ und wählen Sie ein Zertifikat (*.PEM-Datei) aus Ihrem Netzwerk aus.
Password	Geben Sie das Passwort für dieses Zertifikat ein.
Schließen	Schließt das Dialogfeld, ohne ein Zertifikat hinzuzufügen.
Speichern	Fügt das Zertifikat hinzu.

Grundlagen zur Protokollsammlung

Protokollsammlung – Funktionsweise

Der Log Collector-Service sammelt Protokolle aus Ereignisquellen der gesamten IT-Umgebung in einem Unternehmen und übermittelt diese Protokolle an andere NetWitness Suite-Komponenten. Die Protokolle und der beschreibende Inhalt werden als Metadaten für die Verwendung bei Ermittlungen und Berichten gespeichert.

Ereignisquellen sind die Ressourcen im Netzwerk, zum Beispiel Server, Schalter, Router, Speicherarrays, Betriebssysteme und Firewalls. In den meisten Fällen konfiguriert das IT-Team Ereignisquellen so, dass deren Protokolle an den Log Collector-Service gesendet werden, und der NetWitness Suite-Administrator konfiguriert den Log Collector-Service wiederum so, dass dieser Ereignisquellen abfragt und deren Protokolle abruft. So erhält der Log Collector alle Protokolle in Originalform.

Sammlungsprotokolle

RSA NetWitness Suite kann Protokolle aus einer Vielzahl von Ereignisquellen sammeln. Wenn Sie die Protokollsammlung für eine bestimmte Ereignisquelle konfigurieren, müssen Sie zuallererst das Protokoll kennen, das zum Sammeln der Protokolle verwendet wird.

Sammlungsprotokoll	Beschreibung
Kontrollpunkt	Sammelt Ereignisse von Kontrollpunkt-Ereignisquellen mithilfe von OPSEC LEA. OPSEC LEA ist die Sicherheitsprotokoll-Export-API für Kontrollpunktvorgänge, die die Extrahierung von Protokollen unterstützt. Nähere Informationen finden Sie unter Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite.
Datei	Sammelt Ereignisse aus Protokolldateien. Ereignisquellen generieren Protokolldateien, die mithilfe einer sicheren Dateitransfer-Methode an den Log Collector-Service übermittelt werden. Nähere Informationen finden Sie unter Konfigurieren von Dateiereignisquellen in NetWitness Suite.
Netflow	Akzeptiert Ereignisse von Netflow v5 und Netflow v9. Weitere Informationen finden Sie unter Konfigurieren Sie Netflow-Ereignisquellen in NetWitness Suite.

Sammlungsprotokoll	Beschreibung
ODBC	Sammelt Ereignisse von Ereignisquellen, die Auditdaten in einer Datenbank speichern, mithilfe einer Open Database Connectivity (ODBC)-Softwareschnittstelle Nähere Informationen finden Sie unter Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite.
Plug-ins	Die Plug-ins-Sammlung ist ein allgemeines Sammlungssystem für die Erfassung von Ereignissen mithilfe von externen Skripten, die in anderen Sprachen geschrieben wurden. RSA stellt derzeit Sammlung für Amazon Web Services (AWS) CloudTrail und Microsoft Azure bereit. • **AWS**: Sammelt Ereignisse von Amazon Web Services (AWS) CloudTrail. Im Besonderen CloudTrail-Datensätze, die von der AWS API für ein Konto abgerufen werden. Nähere Informationen finden Sie unter Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite • **Azure**: Sammelt Ereignisse von Microsoft Azure. Weitere Informationen finden Sie unter Konfigurieren von Azure-Ereignisquellen in NetWitness Suite. Kunden können dieses Framework verwenden, um ihre eigenen Sammlungsprotokolle zu entwickeln.
SDEE	Sammelt Meldungen von Systemen zur Erkennung von Eindringversuchen (Intrusion Detection System, IDS) und Services zur Vorbeugung von Eindringversuchen (Intrusion Prevention Service, IPS). Nähere Informationen finden Sie unter Konfigurieren von SDEE-Ereignisquellen in NetWitness Suite.
SNMP-Trap	Akzeptiert SNMP-Traps. Nähere Informationen finden Sie unter Konfigurieren von SNMP-Ereignisquellen in NetWitness Suite.
Syslog	Akzeptiert Meldungen von Ereignisquellen, die Syslog-Meldungen auslösen. Weitere Informationen finden Sie unter Konfigurieren der Syslog-Ereignisquellen für Remote Collector. **Hinweis:** Sie konfigurieren die Syslog-Sammlung nicht für Local Log Collectors. Sie müssen die Syslog-Sammlung nur für Remote Collectors konfigurieren.

Sammlungsprotokoll	Beschreibung
VMware	Sammelt Ereignisse von einer virtuellen VMware-Infrastruktur. Nähere Informationen finden Sie unter Konfigurieren von VMware-Ereignisquellen in NetWitness Suite.
Windows	Sammelt Ereignisse von Windows-Rechnern, die das Microsoft Windows-Modell unterstützen. Windows 6.0 ist ein Framework zur Ereignisprotokollierung und Nachverfolgung, das seit Microsoft Windows Vista und Windows Server 2008 im Umfang des Betriebssystems enthalten ist. Nähere Informationen finden Sie unter Konfigurieren Sie Windows-Ereignisquellen in NetWitness Suite.
Windows-Legacy	Sammelt Ereignisse von: • älteren Windows-Versionen, zum Beispiel Windows 2000 und Windows 2003, und sammelt Ereignisquellen von Windows, die bereits für die Envision-Sammlung ohne den Bedarf einer Neukonfiguration konfiguriert sind. • NetApp ONTAP-Appliance-Ereignisquellen, sodass Sie nun NetApp evt-Dateien sammeln und analysieren können. • Weitere Informationen finden Sie unter Konfiguration für Windows-Legacy- und NetApp-Sammlung. **Hinweis:** Sie installieren den NetWitness Suite-Windows-Legacy-Collector auf einem physischen oder virtuellen Windows 2008 R2 SP1 64-Bit-Server mithilfe der Datei **SALegacyWindowsCollector-*Versionsnummer.exe***.

Grundlegendes Verfahren

Das grundlegende Verfahren gilt für alle unterstützten Sammlungsprotokolle.

1. **Richten Sie die Ereignisquelle für die Sammlung ein.** Für jede unterstützte Ereignisquelle gibt es ein Konfigurationsdokument im Bereich „Von RSA unterstützte Ereignisquellen“ auf RSA Link.
   a. Navigieren Sie zum Bereich Von RSA unterstützte Ereignisquellen auf RSA Link.
   b. Suchen Sie die Anweisungen für Ihre Ereignisquelle.

Auf der Übersichtsseite werden alle aktuell unterstützten Ereignisquellen sowie Informationen zur Sammlungsmethode, Geräteklasse und unterstützten Versionen angezeigt.

c. Laden Sie die Konfigurationsanweisungen für Ihre Ereignisquelle herunter und befolgen Sie diese.

2. **Konfigurieren der Sammlung auf RSA NetWitness Suite .** Der Konfigurationsleitfaden für die Ereignisquelle enthält diese Anweisungen. Dieser Leitfaden enthält jedoch je nach Sammlungsmethode, die von Ihrer Ereignisquelle verwendet wird, auch diese Anweisungen. Nähere Informationen finden Sie unter Sammlungsprotokolle.
3. **Starten Sie den Service für Ihre Sammlungsmethode.** Normalerweise müssen Sie diese Schritte nur für die erste Ereignisquelle ausführen, die diese Sammlungsmethode verwendet. So müssen Sie möglicherweise den Dateiservice in NetWitness Suite starten, wenn Sie zum ersten Mal eine Ereignisquelle konfigurieren, die die Dateisammlung verwendet.
4. **Stellen Sie sicher, dass die Sammlung für Ihre Ereignisquelle funktioniert.**

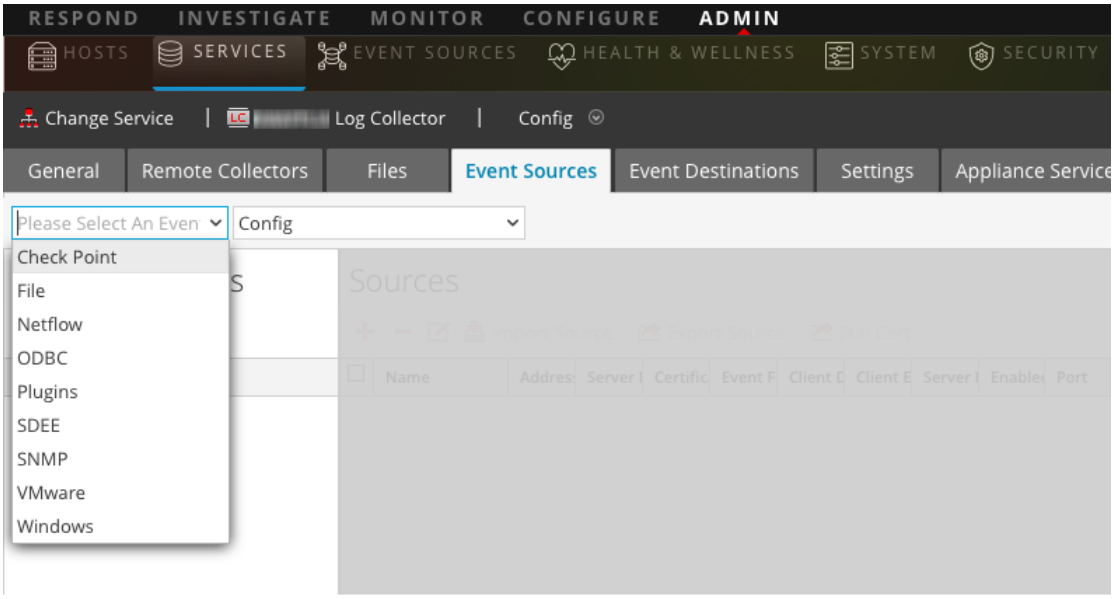
Im weiteren Verlauf dieses Themas werden die Schritte 2, 3 und 4 ausführlicher erläutert.

Konfigurieren der Sammlung in RSA NetWitness Suite

Der Prozess zum Konfigurieren von Ereignisquellen hängt von der Sammlungsmethode ab, die sie verwenden. Beachten Sie jedoch, dass sie sehr ähnlich sind. Das folgende Verfahren ist allgemein gehalten: Weitere Details für einzelne Sammlungsmethoden finden Sie in Themen, welche die Details für die jeweilige Sammlungsmethode behandeln.

1. Navigieren Sie im Menü NetWitness Suite zu **ADMIN> Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** des Log Collector Ihre Sammlungsmethode aus dem Drop-down-Menü aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf +.

   Das Dialogfeld „Verfügbare Ereignisquelltypen“ wird angezeigt.
7. Wählen Sie einen Ereignisquelltyp aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich Ereigniskategorien angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste „Quellen“.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
9. Geben Sie Werte für die verfügbaren Parameter ein.

   Nähere Informationen finden Sie im Abschnitt „Parameter“ der jeweiligen Sammlungsmethode, die Sie konfigurieren.
10. Klicken Sie auf **OK**.

Starten des Service für Ihre Sammlungsmethode

Gehen Sie folgendermaßen vor, um den Service für Ihre Sammlungsmethode zu starten:

1. Navigieren Sie zu **Admin > Services**.
2. Wählen Sie einen **Log Collector** und dann ⚙ **> Ansicht > System** aus.

3. Klicken Sie auf **Sammlung > *Protokoll*> Starten**,

   wobei ***Protokoll*** das Protokoll ist, das Sie starten möchten, z. B. **Netflow**.

Sicherstellen, dass die Sammlung für Ihre Ereignisquelle funktioniert

Ob eine Sammlung funktioniert, prüfen Sie über **Administration > Integrität und Zustand > Registerkarte „Ereignisquellenüberwachung“**.

So stellen Sie sicher, dass die Sammlung für eine Ereignisquelle funktioniert:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**
2. Klicken Sie auf die Registerkarte **Ereignisquellenüberwachung**.
3. Suchen Sie im Raster nach **Log Decoder**, **Ereignisquelle** und **Ereignisquelltyp**.
4. Suchen Sie bei einer Ereignisquelle in der Spalte **Zähler** nach einer Aktivität, um sicherzustellen, dass die Sammlung Ereignisse annimmt.

Konfigurieren von Ereignisfiltern für einen Collector

In diesem Thema erfahren Sie, wie Sie Ereignisfilter für alle Sammlungsprotokolle erstellen und warten.

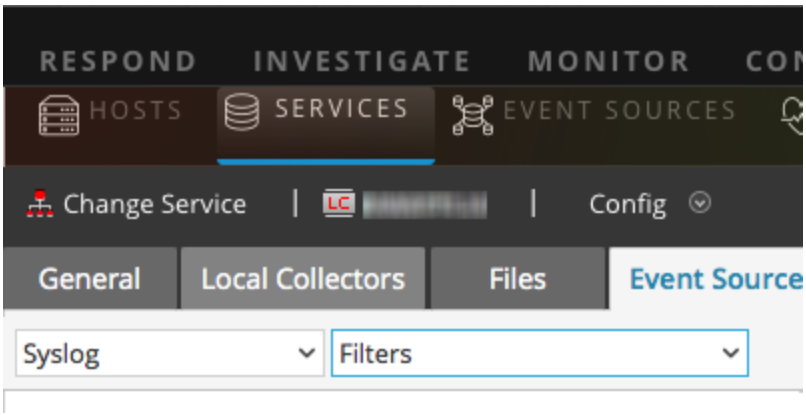
Hinweis: Sie können die Syslog-Sammlung nicht für Local Log Collectors konfigurieren. Sie müssen die Syslog-Sammlung nur für Remote Collectors konfigurieren. Nähere Informationen zur Konfiguration finden Sie unter Konfigurieren von Local und Remote Collectors.

Konfigurieren eines Ereignisfilters

So konfigurieren Sie eine Ereignisquelle:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie auf der Registerkarte **Ereignisquellen** in den Drop-down-Menüs eine Sammlungsmethode/einen **Filter** aus.

   Der folgende Bildschirm zeigt die ausgewählte Option **Syslog** an.

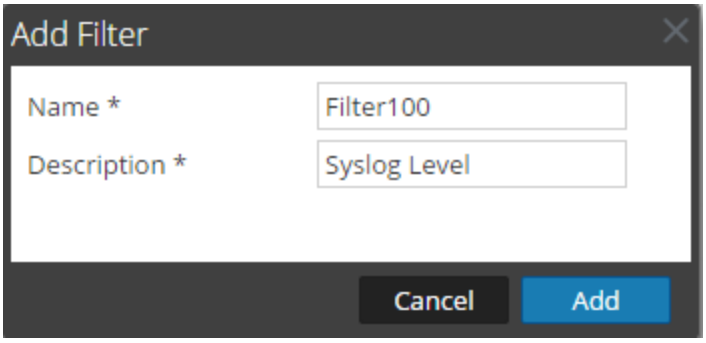


Hinweis: Syslog-Konfiguration ist nur verfügbar auf Remote Collectors: Wenn Sie mit einem Local Collector-Service arbeiten, ist **Syslog** im Drop-down-Menü nicht verfügbar.

Die Ansicht **Filter** zeigt die Filter an, die für die ausgewählte Sammlungsmethode konfiguriert sind, sofern vorhanden.

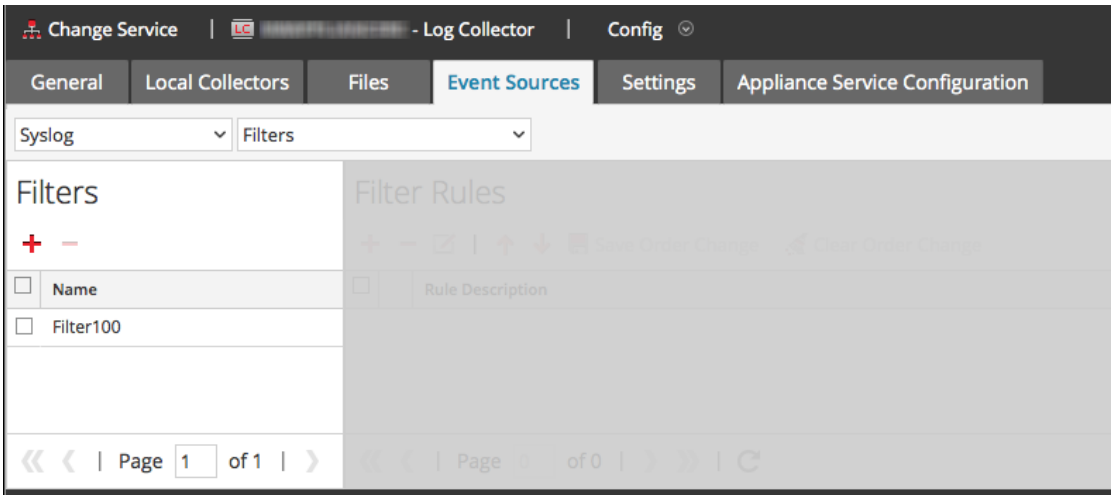
6. Klicken Sie in der Symbolleiste des Bereichs **Filter** auf +.

   Das Dialogfeld **Filter hinzufügen** wird angezeigt.



7. Geben Sie einen Namen und eine Beschreibung für den neuen Filter ein und klicken Sie auf **Hinzufügen**.

   Der neue Filter wird im Bereich **Filter** angezeigt.

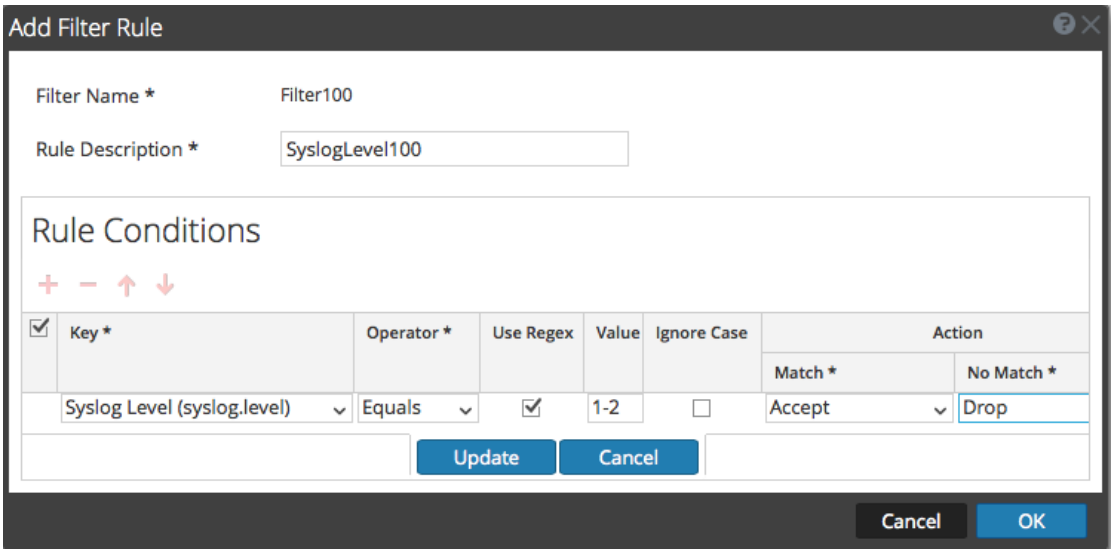


8. Wählen Sie den neuen Filter im Bereich **Filter** aus und klicken Sie in der Symbolleiste des Bereichs **Filterregeln** auf +.

   Das Dialogfeld **Filterregel hinzufügen** wird angezeigt.

9. Klicken Sie unter **Bedingungen der Regel** auf +.

10. Fügen Sie die Parameter für diese Regel hinzu und klicken Sie auf **Update > OK**.



NetWitness Suite aktualisiert den Filter mit der von Ihnen definierten Regel.

Hinweis: Regeln werden von oben nach unten verarbeitet, bis ein Aktionstyp die Verarbeitung abbricht oder die letzte Regel überprüft wurde. Standardmäßig wird die Regel akzeptiert, wenn keine Übereinstimmungen gefunden werden.

In den folgenden Tabellen werden die Parameter für das Hinzufügen einer Filterregel beschrieben.

Ereignisfilterregel Parameter „Schlüssel“

Die Werte für das Feld „Schlüssel“ hängen von der Sammlungsmethode ab, auf die der Filter angewendet wird.

Sammlungsmethode	Werte für das Feld *Schlüssel*
Kontrollpunkt, Datei, Netflow, Plug-in, SDEE SNMP und VMware	• Alle Datenfelder • Ereignisquelltyp • Name der Ereignisquelle • Quell-IP • Rohereignis
ODBC	• Alle Datenfelder • Ereignisquelltyp • Name der Ereignisquelle • Quell-IP • Meldungs-ID • Nachrichtenebene
Syslog	• Alle Datenfelder • Ereignisquelltyp • Name der Ereignisquelle • Quell-IP • Syslog-Stufe • Rohereignis

Sammlungsmethode	Werte für das Feld *Schlüssel*
Windows	• Alle Datenfelder • Ereignisquelltyp • Name der Ereignisquelle • Quell-IP • Ereignis-ID • Provider • Channel • Computer • UserName • DomainName
Windows-Legacy	• Alle Datenfelder • Ereignisquelltyp • Name der Ereignisquelle • Quell-IP • Ereignis-ID

Andere Parameter für Ereignisfilterregeln

Die folgende Tabelle beschreibt alle anderen verfügbaren Felder für die Erstellung einer Ereignisfilterregel.

Feld	Beschreibung
Operator	Gültige Werte: • Enthält • Gleich
Regex verwenden	Optional. Sie können diese Option auswählen, wenn Sie regex verwenden möchten.

Feld	Beschreibung
Wert	Wert ist abhängig von dem gewählten Schlüsselwert. Wenn Sie für Schlüssel beispielsweise **Syslog-Stufe** wählen, ist der Wert eine Zahl, die die Syslog-Stufe angibt.
Groß-/Kleinschreibung ignorieren	Optional. Wählen Sie dies aus, um die Groß-/Kleinschreibung zu ignorieren.
Aktion	Wenn eine Übereinstimmung vorliegt, können Sie eine Aktion für das Akzeptieren, das Verwerfen, die nächste Bedingung oder die nächste Regel auswählen: • **Akzeptieren** : Ereignisse, die mit den bereitgestellten IDs übereinstimmen, sind in Ereignisprotokollen enthalten und werden in der Systems Analytics-Benutzeroberfläche angezeigt. • **Verwerfen**: Ereignisse, die mit den bereitgestellten IDs übereinstimmen, sind in Ereignisprotokollen nicht enthalten und werden in der Systems Analytics-Benutzeroberfläche nicht angezeigt. • **Nächste Bedingung**: Der Filter ignoriert Ereignisse mit übereinstimmenden IDs und fährt mit der nächsten Regelbedingung fort. • **Nächste Regel**: Der Filter ignoriert Ereignisse mit übereinstimmenden IDs und fährt mit der nächsten Regel fort. Wenn keine Übereinstimmung vorliegt, können Sie eine Aktion für das Akzeptieren, das Verwerfen, die nächste Bedingung oder die nächste Regel auswählen.

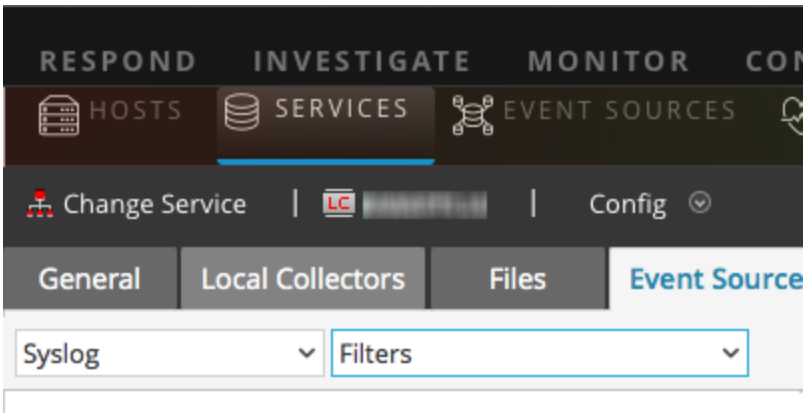
Ändern von Filterregeln

So ändern Sie eine Ereignisquelle:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie auf der Registerkarte **Ereignisquellen** in den Drop-down-Menüs eine

Sammlungsmethode/einen **Filter** aus.

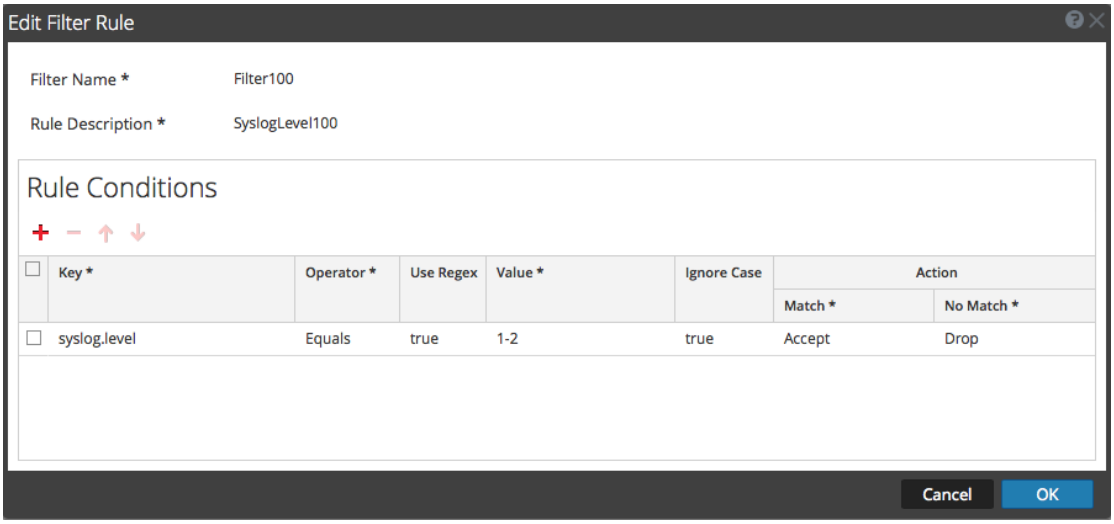
Der folgende Bildschirm zeigt die ausgewählte Option **Kontrollpunkt** an.



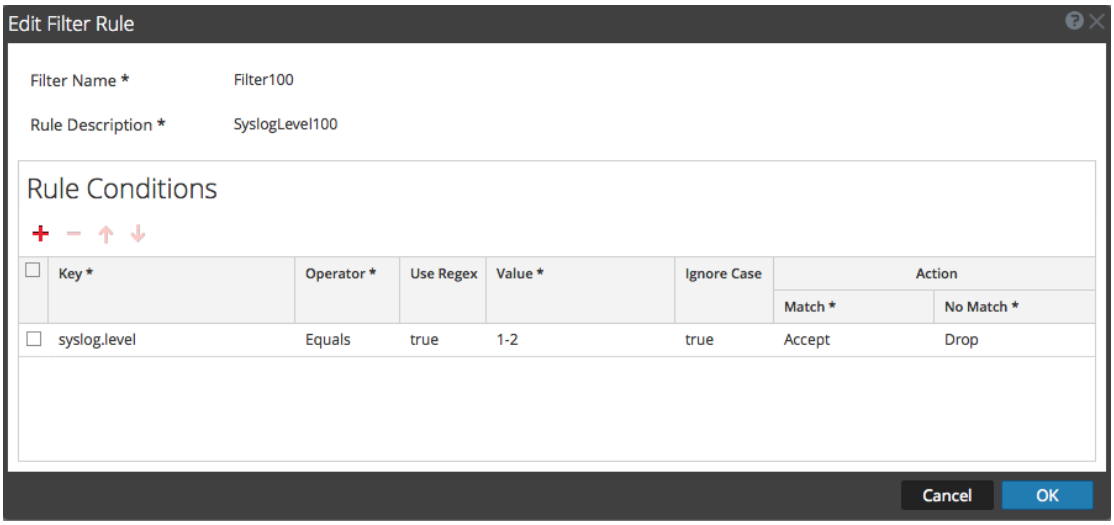
Die Ansicht **Filter** zeigt die Filter an, die für die ausgewählte Sammlungsmethode konfiguriert sind, sofern vorhanden.

6. Wählen Sie in der Liste **Filterregeln** eine Regel aus und klicken Sie auf .

   Das Dialogfeld **Filterregel bearbeiten** wird angezeigt.



7. Wählen Sie die Regelbedingung aus, die Sie ändern möchten.



8. Ändern Sie die Bedingungsparameter, die Änderungen erfordern, und klicken Sie auf **Aktualisieren > OK**.

NetWitness Suite wendet die Bedingungsparameteränderungen auf die ausgewählte Filterregel an.

Gleichzeitiges Importieren, Exportieren, Bearbeiten und Testen mehrerer Ereignisquellen

In diesem Thema wird erläutert, wie Sie mehrere Ereignisquellen gleichzeitig importieren, exportieren, bearbeiten und testen.

Mit der Option zum gleichzeitigen Exportieren können Sie mehrere Ereignisquellendetails der aktuellen Konfiguration exportieren und speichern. Wenn ein Problem mit der aktuellen Konfiguration auftritt und Sie die vorhandenen Ereignisquelldaten benötigen, können diese Daten gleichzeitig importiert werden.

Mit der Funktion zum gleichzeitigen Bearbeiten können Sie mehrere Ereignisquellen gleichzeitig bearbeiten, für die eine bestimmte Änderung erforderlich ist. Sie können alle Quellen auswählen und die Bearbeitungsoption gleichzeitig auf alle anwenden. Damit vermeiden Sie, dass alle einzeln geändert werden müssen.

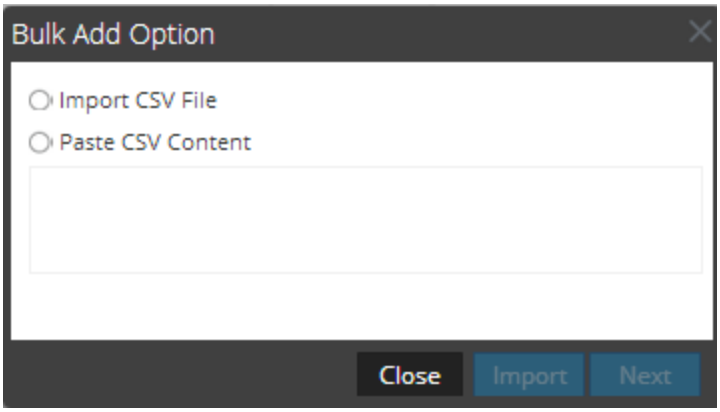
Gleichzeitiges Importieren mehrerer Ereignisquellen

Warnung: Wenn Sie für die Bearbeitung einer CSV-Datei mit exportierten Ereignisquellen ein Tabellenkalkulationsprogramm verwenden, kann es vorkommen, dass einige Datenfelder wie Zahlen und Datumsangaben in die nativen Feldtypen des Tabellenkalkulationsprogramms umformatiert werden. Dies kann Probleme verursachen, wenn Sie diese Informationen erneut importieren, da einige Datenfelder möglicherweise unlesbar oder falsch formatiert sind. Sie können dies vermeiden, indem Sie die CSV-Datei in das Tabellenkalkulationsprogramm importieren und alle Datenfelder als Textwerte angeben.

So importieren Sie mehrere Ereignisquellen gleichzeitig:

1. Navigieren Sie zu **Admin > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie **Kontrollpunkt**, **Datei**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE (Syslog nur für Remote Collectors)**, **VMware**, **Windows** oder **Windows Legacy** aus (SNMP verfügt nicht über eine Importfunktion).
6. Klicken Sie in der Symbolleiste im Bereich **Quellen** auf **Quelle importieren**.

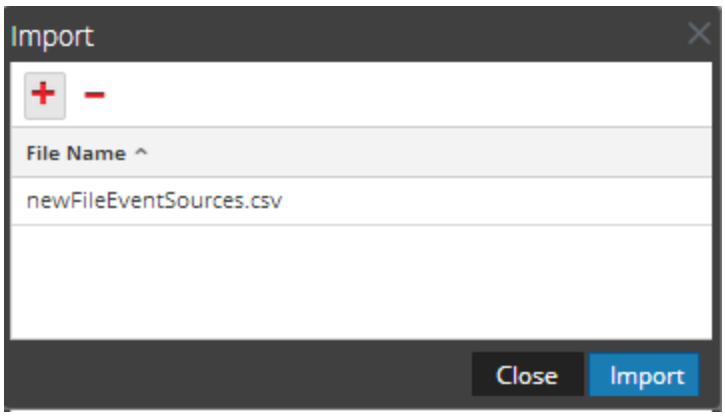
   Das Dialogfeld **Option zum Massenhinzufügen** wird angezeigt.



7. Wählen Sie entweder **CSV-Datei importieren** oder **CSV-Content einfügen** aus. Falls Sie Folgendes ausgewählt haben:
   - CSV-Datei importieren:
     a. Klicken Sie auf **Weiter**.

        Das Dialogfeld **Importieren** wird angezeigt.

b. Klicken Sie auf **Hinzufügen** und wählen Sie eine **CSV**-Datei aus dem Netzwerk aus.

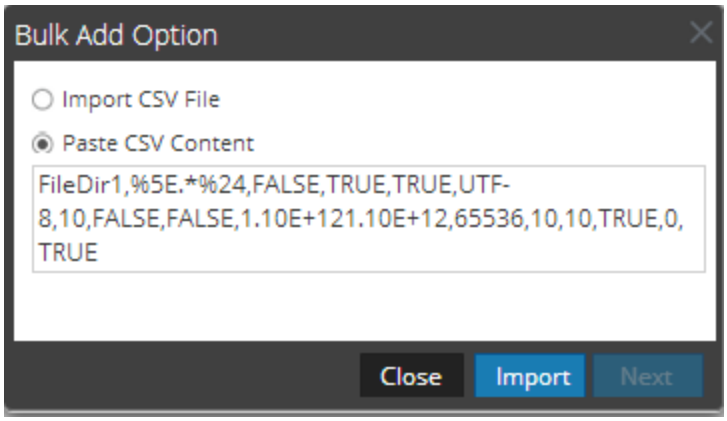


c. Klicken Sie auf **Importieren**.

Die Ereignisquellen werden der Liste **Ereignisquelle** hinzugefügt.

- CSV-Content einfügen:

a. Kopieren Sie den Inhalt aus der **CSV**-Datei und fügen Sie ihn im Dialogfeld ein.



b. Klicken Sie auf **Importieren**.

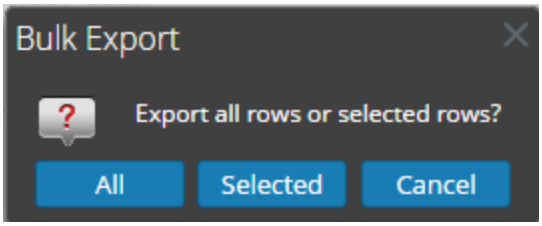
Die Ereignisquellen werden der Liste **Ereignisquelle** hinzugefügt.

Gleichzeitiges Exportieren mehrerer Ereignisquellen

Warnung: Wenn Sie für die Bearbeitung einer CSV-Datei mit exportierten Ereignisquellen ein Tabellenkalkulationsprogramm verwenden, kann es vorkommen, dass einige Datenfelder wie Zahlen und Datumsangaben in die nativen Feldtypen des Tabellenkalkulationsprogramms umformatiert werden. Dies kann Probleme verursachen, wenn Sie diese Informationen erneut importieren, da einige Datenfelder möglicherweise unlesbar oder falsch formatiert sind. Sie können dies vermeiden, indem Sie die CSV-Datei in das Tabellenkalkulationsprogramm importieren und alle Datenfelder als Textwerte angeben.

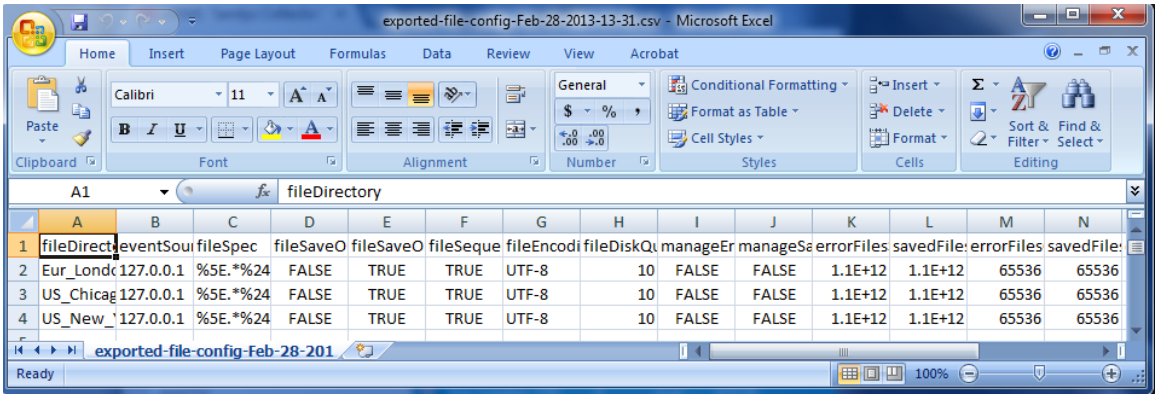
1. Navigieren Sie zu **Admin > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie **Kontrollpunkt**, **Datei**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE (Syslog nur für Remote Collectors)**, **VMware**, **Windows** oder **Windows Legacy** aus (SNMP verfügt nicht über eine Exportfunktion).
6. Wählen Sie im Bereich **Quellen** eine oder mehrere Ereignisquellen aus und klicken Sie auf **Quelle exportieren**.

   Das Dialogfeld **Massenexport** wird angezeigt.



7. Je nach Ihrer Auswahl:
   - **Alle** – NetWitness Suite exportiert alle Ereignisquellen in eine CSV-Datei mit Zeitstempel.
   - **Ausgewählte** – NetWitness Suite exportiert die ausgewählte(n) Ereignisquelle(n) in eine CSV-Datei mit Zeitstempel.
   - **Abbrechen** – NetWitness Suite bricht den Export ab.

Im Folgenden ist ein Beispiel für eine CSV-Datei mit Zeitstempel angegeben, die mit den von Ihnen in der Liste ausgewählten Ereignisquellen erzeugt wird.

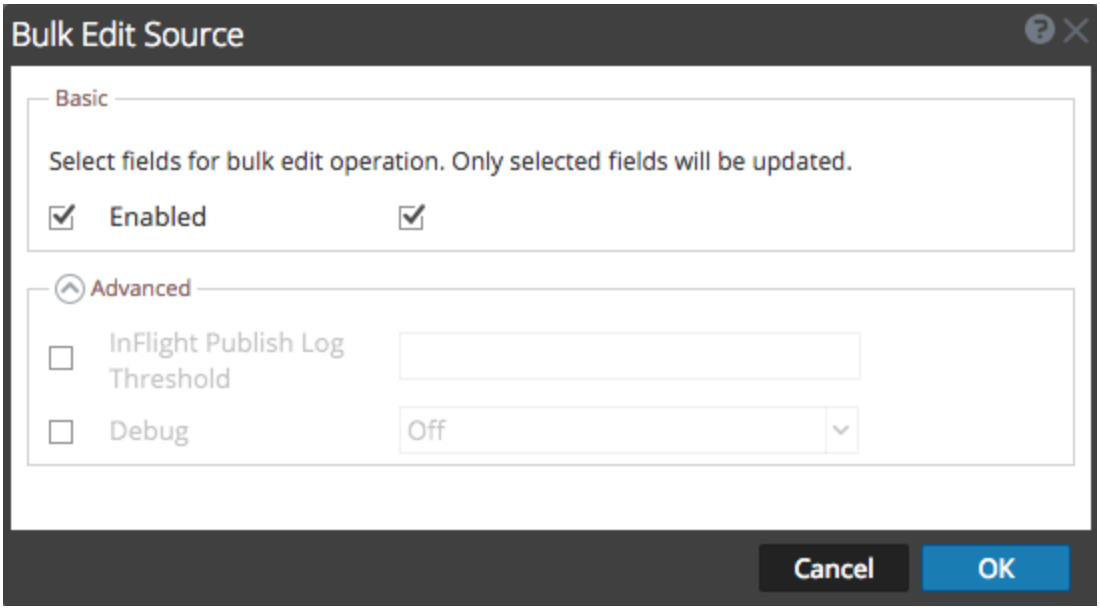


Gleichzeitiges Bearbeiten mehrerer Ereignisquellen

So bearbeiten Sie mehrere Ereignisquellen gleichzeitig:

1. Wählen Sie auf der Registerkarte **Log Collector-Ereignisquellen** die Option **Kontrollpunkt**, **Datei**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **Syslog**, **VMware**, **Windows** oder **Windows Legacy** aus (SNMP verfügt nicht über eine Bearbeitungsfunktion).
2. Wählen Sie im Bereich **Quellen** mehrere Ereignisquellen aus und klicken Sie auf (Bearbeiten-Symbol).

   Für die ausgewählte Ereignisquelle wird das entsprechende Dialogfeld **Massenbearbeitung** angezeigt. Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld **Massenbearbeitung für Quelle** für die Ereignisquellenparameter einer Datei.



3. Aktivieren Sie das Kontrollkästchen links neben den zu ändernden Feldern (z. B. **Debuggen**).
4. Ändern Sie die ausgewählten Parameter (ändern Sie z. B. Debuggen von **Aus** in **Ein**).
5. Klicken Sie auf **OK**.

   NetWitness Suite wendet die gleiche Parameterwertänderung auf alle ausgewählten Ereignisquellen an.

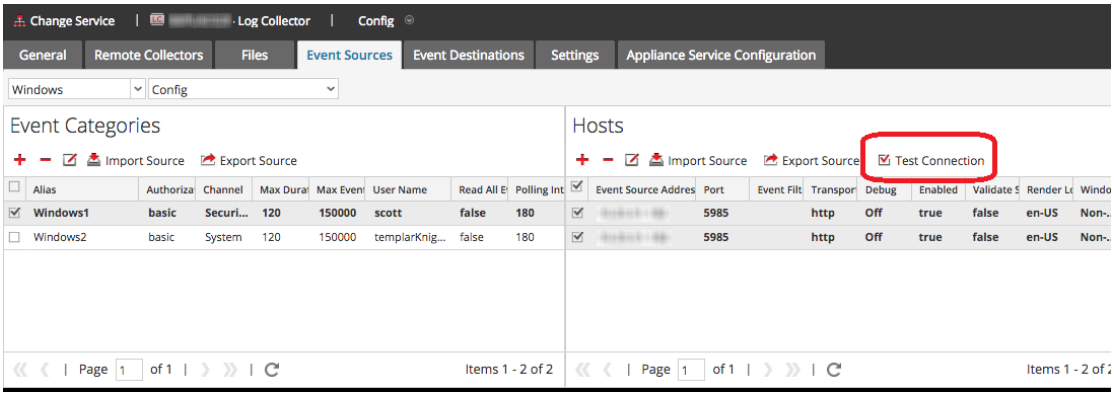
Gleichzeitiges Testen mehrerer Ereignisquellenverbindungen

So testen Sie mehrere Ereignisquellenverbindungen gleichzeitig:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.

3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht** > **Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Wählen Sie die Registerkarte **Ereignisquellen** aus. Wählen Sie dort **Plug-ins**, **ODBC** oder **Windows** aus (die anderen Protokolle verfügen nicht über eine Funktion zum gleichzeitigen Testen von Verbindungen).
5. Wählen Sie eine(n) oder mehrere:
   - Quellen aus dem Bereich **Quellen** für **Plug-ins** oder **ODBC**
   - Hosts aus dem Bereich **Hosts** für **Windows**

   Die Schaltfläche **Verbindung testen** ist aktiviert.



6. Klicken Sie auf Test Connection .

   Das Dialogfeld **Massentest für Verbindungen** wird angezeigt und enthält den aktuellen Status des Tests für die einzelnen Quellen. Der Status kann Warten, Testen, Bestanden oder Fehlgeschlagen sein.

   Wenn Sie den Test schließen, bevor er abgeschlossen ist, wird der Test beendet und das Dialogfeld **Massentest für Verbindungen** wird geschlossen.

Wenn der Test abgeschlossen ist, wird das Ergebnis im Dialogfeld **Massentest für Verbindungen** angezeigt.

Siehe auch

Sie können das Modul **Ereignisquellen** (Administration > Ereignisquellen) verwenden, um Gruppen von Ereignisquellen zu erstellen, die in der Regel aus einer CMDB importiert werden, und um Ereignisquellen basierend auf diesen Gruppen zu überwachen. Weitere Informationen finden Sie unter den folgenden Themen im *Leitfaden für das Ereignisquellenmanagement*:

- Importieren von Ereignisquellen
- Ereignisquellen exportieren

- Massenbearbeitung von Ereignisquellenattributen

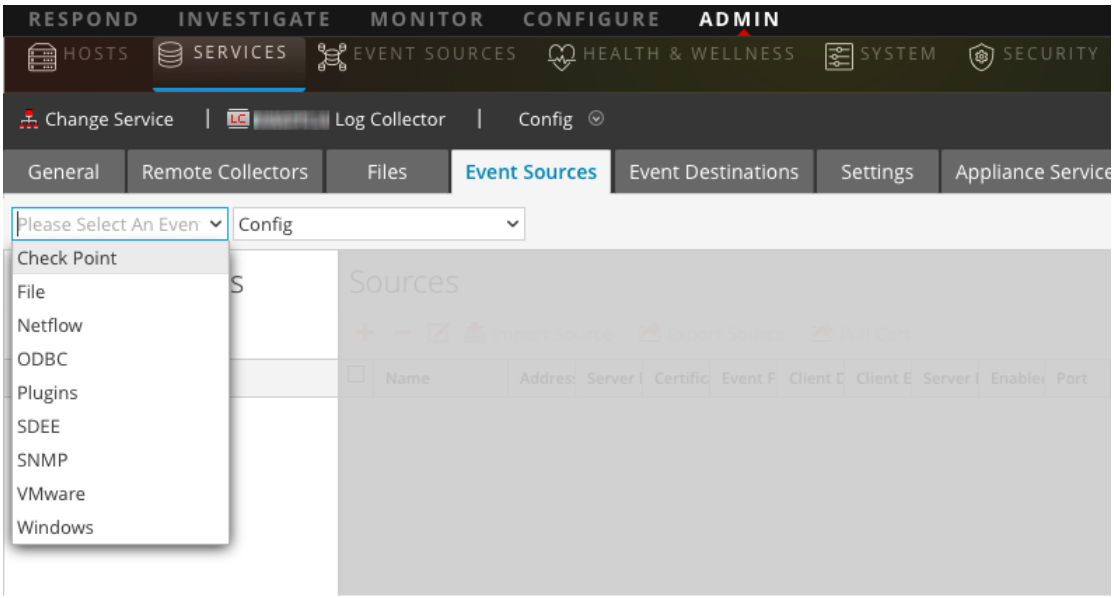
Konfigurieren von Sammlungsprotokollen und Ereignisquellen

In diesem Thema erfahren Sie, wie Sie Sammlungsprotokolle und die Ereignisquellen, die diese Protokolle nutzen, konfigurieren können.

Sie konfigurieren den Log Collector für die Sammlung von Ereignisdaten aus Ihren Ereignisquellen auf der Registerkarte „Ereignisquellen“ der Protokollsammlung-Parameteransicht.

So konfigurieren Sie ein Sammlungsprotokoll:

1. Navigieren Sie im Menü NetWitness Suite zu **ADMIN> Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie ein Sammlungsprotokoll aus (z. B. **Datei**) und wählen Sie dann **Konfiguration**.
6. Klicken Sie auf + und wählen Sie eine Ereignisquelle aus.
7. Wählen Sie die neu hinzugefügte Kategorie aus und klicken Sie auf +.
8. Geben Sie die Parameter für die Ereignisquelle an. Weitere Informationen finden Sie in den Themen zu den einzelnen Sammlungsprotokollen.

Die nachfolgenden Leitfäden enthalten ausführliche Anleitungen in Bezug auf die Konfiguration von Sammlungsprotokollen und ihnen zugeordneten Ereignisquellen in NetWitness Suite. Jeder Leitfaden enthält einen Index zu den Konfigurationsanweisungen für die von diesem Sammlungsprotokoll unterstützten Ereignisquellen.

Informationen über das Konfigurieren einzelner Sammlungsprotokolle finden Sie in den folgenden Themen:

- Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite
- Konfigurieren von Azure-Ereignisquellen in NetWitness Suite
- Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite
- Konfigurieren von Dateiereignisquellen in NetWitness Suite
- Konfigurieren Sie Netflow-Ereignisquellen in NetWitness Suite
- Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite
  - Konfigurieren von DSNs (Data Source Names)
  - Erstellen von angepasstem Typespec für ODBC-Sammlung
  - Parameter der ODBC-Ereignisquellenkonfiguration
  - Parameter der ODBC-DSN-Ereignisquellenkonfiguration
- Konfigurieren von SDEE-Ereignisquellen in NetWitness Suite
- Konfigurieren von SNMP-Ereignisquellen in NetWitness Suite
- Konfigurieren der Syslog-Ereignisquellen für Remote Collector
- Konfigurieren von VMware-Ereignisquellen in NetWitness Suite
- Konfigurieren Sie Windows-Ereignisquellen in NetWitness Suite
- Konfiguration für Windows-Legacy- und NetApp-Sammlung
  - Einrichten des Windows Legacy Collector
  - Konfigurieren von Windows-Legacy- und NetApp-Ereignisquellen
  - Troubleshooting der Windows-Legacy- und NetApp-Sammlung

Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das AWS-Sammlungsprotokoll konfigurieren, das Ereignisse von Amazon Web Services (AWS) CloudTrail sammelt.

Hinweis: Das AWS-Plug-in ist ausschließlich für die Erfassung von AWS CloudTrail-Protokollen gedacht und nicht für die Erfassung aus beliebigen Protokollen in S3-Buckets (unter willkürlichen Verzeichnisse). Die AWS CloudTrail-Protokolle werden im JSON-Format gesendet, wie unter folgendem Link in der AWS-Dokumentation beschrieben: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html.

Funktionsweise der AWS-Sammlung

Der Log Collector-Service sammelt Ereignisse von Amazon Web Services (AWS) CloudTrail. CloudTrail zeichnet AWS-API-Aufrufe für ein Konto auf. Die Ereignisse enthalten die Identität des API-Aufrufers, die Uhrzeit des API-Aufrufs, die Quell-IP-Adresse des API-Aufrufers, die Anforderungsparameter und die vom AWS-Service zurückgegebenen Antwortelemente. Die durch CloudTrail-Ereignisse bereitgestellte AWS-API-Aufrufhistorie ermöglicht Sicherheitsanalyse, Nachverfolgung von Ressourcenänderungen und Compliance-Audits. CloudTrail verwendet Amazon S3 zur Speicherung und Bereitstellung von Protokolldateien. NetWitness Suite kopiert die Protokolldateien aus der Cloud (S3-Bucket) und sendet die in den Dateien enthaltenen Ereignisse an den Log Collector.

Bereitstellungsszenario

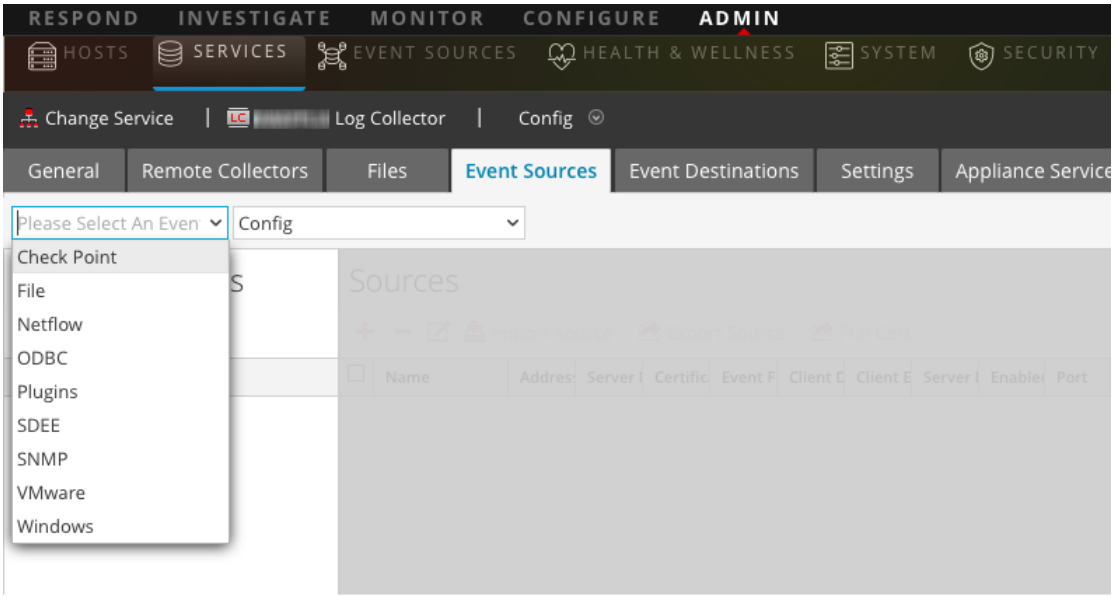
Die folgende Abbildung zeigt die Bereitstellung des AWS-Sammlungsprotokolls in NetWitness Suite.

Konfiguration

So konfigurieren Sie eine AWS (CloudTrail)-Ereignisquelle:

1. Navigieren Sie im Menü NetWitness Suite zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie in der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **Plug-ins/Konfigurieren** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf + .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie **cloudtrail** aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
9. Definieren Sie die Parameterwerte. Weitere Informationen finden Sie unten stehend unter AWS-Parameter.
10. Klicken Sie auf **Verbindung testen**.

    Das Ergebnis des Tests wird im Dialogfeld angezeigt. Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Geräte- oder Serviceinformationen und versuchen Sie es erneut.

    Log Collector braucht etwa 60 Sekunden, um die Testergebnisse zurückzugeben. Wenn das Zeitlimit überschritten wird, wird der Test abgebrochen und NetWitness Suite zeigt eine Fehlermeldung an.
11. Wenn der Test erfolgreich ist, klicken Sie auf **OK**.

    Die neue Ereignisquelle wird im Bereich **Quellen** angezeigt.

AWS-Parameter

In der folgenden Tabelle werden die verfügbaren Konfigurationsparameter für die AWS-Sammlung beschrieben.

Parameter	Beschreibung
Parameter	**Beschreibung**
	Basis
Name*	Name der Ereignisquelle
Aktiviert 	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Konto-ID*	Kontoidentifikationscode des S3 Bucket

Parameter	Beschreibung
S3 Bucketname*	Name des AWS (CloudTrail) S3 Bucket Die Namen von Amazon S3 Buckets sind global eindeutig, unabhängig von der AWS (CloudTrail)-Region, in der der Bucket erstellt wurde. Sie geben den Namen zum Zeitpunkt der Erstellung des Bucket an. Bucket-Namen müssen die DNS-Benennungskonventionen einhalten. Die Regeln für DNS-konforme Bucket-Namen lauten: • Bucket-Namen müssen zwischen 3 und 63 Zeichen lang sein. • Bucket-Namen müssen eine Folge aus einer oder mehreren Bezeichnungen sein. Aneinander grenzende Bezeichnungen werden durch einen einzelnen Punkt getrennt „.“. Bucket-Namen dürfen Kleinbuchstaben, Zahlen und Bindestriche enthalten. Jede Bezeichnung muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. • Bucket-Namen dürfen nicht wie eine IP-Adresse formatiert sein (z. B. 192.168.5.4). Die folgenden Beispiele sind **gültige** Bucket-Namen: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** Die folgenden Beispiele sind **ungültige** Bucket-Namen: • **.myawsbucket** – Bucket-Namen dürfen nicht mit einem Punkt „.“ beginnen. • **myawsbucket.** – Bucket-Namen dürfen nicht mit einem Punkt „.“ enden. • **my..examplebucket** – Zwischen Bezeichnungen darf nur ein Punkt stehen.
Zugangsschlüssel*	Schlüssel für den Zugriff auf den S3 Bucket. Zugriffsschlüssel werden für sichere REST- oder Abfrageprotokollanforderungen an die AWS-Service API verwendet. Weitere Informationen zu Zugriffsschlüsseln erhalten Sie auf der Amazon Web Services-Support-Website unter Manage User Credentials.

Parameter	Beschreibung
Geheimer Schlüssel*	Geheimer Schlüssel für den Zugriff auf den S3 Bucket
Region*	Region des S3-Bucket. **us-east-1** ist der Standardwert.
Region-Endpunkt	Gibt den AWS CloudTrail-Hostnamen an. Zum Beispiel wäre für eine AWS-Public-Cloud für die Region „us-east“ der Region-Endpunkt „s3.amazonaws.com“. Weitere Informationen finden Sie unter http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Dieser Parameter ist erforderlich, um CloudTrail-Protokolle von AWS-Government- oder Private-Clouds zu sammeln.
Proxy verwenden	Aktivieren Sie **Proxy verwenden**, um den Proxy für AWS-Server festzulegen. Diese Option ist standardmäßig deaktiviert.
Proxyserver	Geben Sie den Namen des Proxys ein, mit dem Sie eine Verbindung für den Zugriff auf den AWS-Server herstellen möchten.
Proxyport	Geben Sie die Portnummer ein, die sich mit dem Proxyserver verbindet, um auf den AWS-Server zuzugreifen.
Proxy-Benutzer	Geben Sie den Benutzername zur Authentifizierung mit dem Proxyserver ein.
Proxypasswort	Geben Sie das Passwort zur Authentifizierung beim Proxyport ein.
Startdatum*	Startet die AWS (CloudTrail)-Sammlung von der angegebenen Anzahl Tagen in der Vergangenheit, gemessen vom aktuellen Zeitstempel. Der Standardwert ist 0, also beginnend ab heute. Der Bereich ist 0 bis 89 Tage.
Protokolldateipräfix	Präfix der zu verarbeitenden Datei **Hinweis:** Wenn Sie bei der Einrichtung des CloudTrail-Service ein Präfix festlegen, müssen Sie in diesem Parameter dasselbe Präfix eingeben.
Erweitert	

Parameter	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).
Befehlsargumente	Argumente, die dem Skript hinzugefügt wurden
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist 60. Wenn Sie beispielsweise 60 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 60 Sekunden. Wenn der vorherige Abfragezyklus noch ausgeführt wird, wird gewartet, bis dieser Zyklus abgeschlossen ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 60 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.
SSL aktiviert ☐	Aktivieren Sie für die Kommunikation per SSL das Kontrollkästchen. Die Sicherheit der Datenübertragung erfolgt durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten. Das Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Beschreibung
Verbindung testen	Überprüft, ob die in diesem Dialogfeld angegebenen Konfigurationsparameter korrekt sind. Mit dem folgenden Test wird beispielsweise überprüft, ob: • NetWitness mithilfe der in diesem Dialogfeld angegebenen Anmeldedaten eine Verbindung zu dem S3-Bucket in AWS herstellen kann. • NetWitness eine Protokolldatei von dem Bucket herunterladen kann. (Der Verbindungstest würde fehlschlagen, wenn keine Protokolldateien für den gesamten Bucket vorhanden wären. Dies wäre aber sehr unwahrscheinlich.)
Abbrechen	Das Dialogfeld wird ohne Hinzufügen des AWS (CloudTrail) geschlossen.
OK	Fügt die aktuellen Parameterwerte als neuen AWS (CloudTrail) hinzu.

Konfigurieren von Azure-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das Azure-Sammlungsprotokoll konfigurieren. Microsoft Azure ist eine Cloud-Computing-Plattform und -Infrastruktur für Aufbau, Bereitstellung und Management von Anwendungen und Services über ein globales Netzwerk von Rechenzentren, die von Microsoft verwaltet werden.

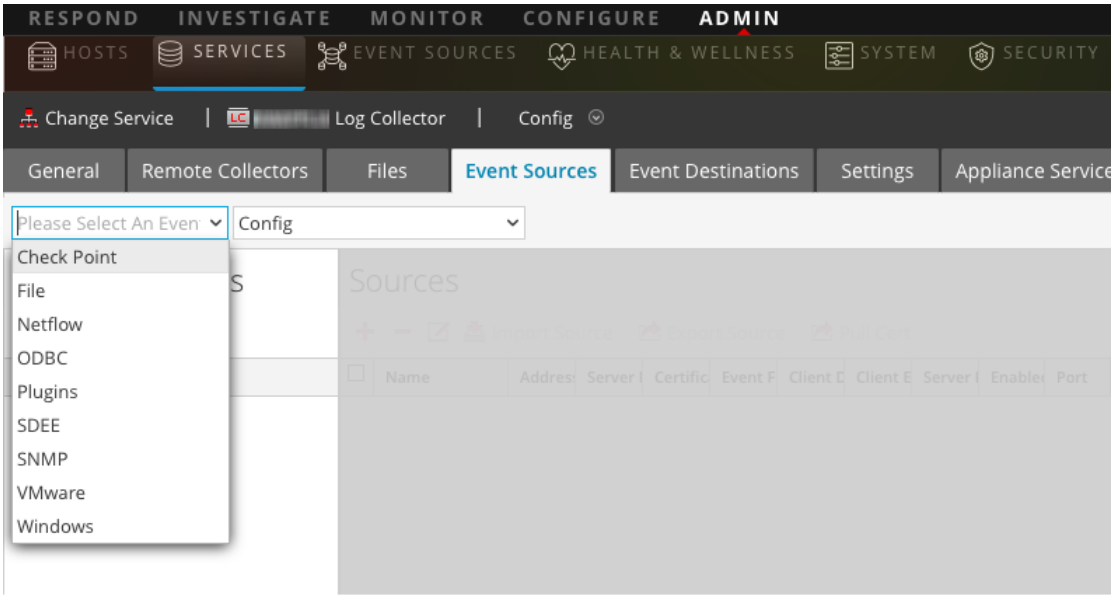
Konfiguration in NetWitness Suite

Ausführliche Informationen zum Konfigurieren von Azure als Ereignisquelle finden Sie im Konfigurationleitfaden für Azure-Ereignisquellen, der auf RSA Link verfügbar ist.

So konfigurieren Sie eine Azure-Ereignisquelle:

1. Navigieren Sie zu **ADMIN > Services** vom NetWitness Suite-Menü aus.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie in der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **Plug-ins/Konfigurieren** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf + .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie **azureaudit** aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
9. Definieren Sie die Parameterwerte. Weitere Informationen finden Sie unten stehend unter Azure-Parameter.
10. Klicken Sie auf **Verbindung testen**.

    Das Ergebnis des Tests wird im Dialogfeld angezeigt. Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Geräte- oder Serviceinformationen und versuchen Sie es erneut.

    Log Collector braucht etwa 60 Sekunden, um die Testergebnisse zurückzugeben. Wenn das Zeitlimit überschritten wird, wird der Test abgebrochen und NetWitness Suite zeigt eine Fehlermeldung an.
11. Wenn der Test erfolgreich ist, klicken Sie auf **OK**.

    Die neue Ereignisquelle wird im Bereich **Quellen** angezeigt.

Azure-Parameter

In diesem Abschnitt werden die Parameter für die Konfiguration der Azure-Ereignisquelle beschrieben.

Hinweis: Elemente, die durch ein Sternchen (*) gekennzeichnet sind, sind erforderlich.

Basisparameter

Name	Beschreibung
Name*	Geben Sie einen alphanumerischen, beschreibenden Namen für die Quelle ein. Dieser Wert wird nur für die Anzeige des Namens auf diesem Bildschirm verwendet.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Client-ID*	Die Client-ID befindet sich auf der Registerkarte „Azure-Anwendungskonfiguration“. Scrollen Sie nach unten, bis Sie sie sehen.
Geheimer Clientschlüssel*	Wenn Sie die Ereignisquelle konfigurieren, wird der geheime Clientschlüssel beim Erstellen eines Schlüssels angezeigt. Wählen Sie eine Gültigkeitsdauer aus. Sie sollten diesen Schlüssel speichern, da er nur einmal angezeigt wird. Er kann später nicht mehr abgerufen werden.
Basis-URL API-Ressource*	Geben Sie `https://management.azure.com/` ein. Achten Sie darauf, den nachgestellten Schrägstrich mit anzugeben (/).
Verbundmetadaten-Endpunkt*	Klicken Sie in der Azure-Anwendung auf die Schaltfläche **Endpunkte anzeigen** (am unteren Rand des Bereichs). Es gibt viele Links, die alle mit der gleichen Zeichenfolge beginnen. Vergleichen Sie die URLs und suchen Sie die Zeichenfolge, mit der die meisten von ihnen beginnt. Diese gemeinsame Zeichenfolge ist der Endpunkt, den Sie hier eingeben müssen.
Abonnement-ID*	Sie finden diese im Microsoft Azure-Dashboard: Klicken Sie unten in der Liste auf der linken Seite auf „Abonnements“.

Name	Beschreibung
Mandantendomain*	Gehen Sie zu Active Directory und klicken Sie auf das Verzeichnis. In der URL der Mandantendomain befindet die Zeichenfolge direkt hinter **manage.windowsazure.com/**. Die Mandantendomain ist die Zeichenfolge bis einschließlich dem **.com**.
Ressourcengruppennamen*	Wählen Sie in Azure im linken Navigationsbereich „Ressourcengruppen“ und dann Ihre Gruppe.
Startdatum*	Wählen Sie das Datum aus, an dem mit der Erfassung begonnen werden soll. Standardwert ist das aktuelle Datum.
Verbindung testen	Überprüft die in diesem Dialogfeld angegebenen Konfigurationsparameter auf ihre Richtigkeit.

Erweiterte Parameter

Klicken Sie auf neben **Erweitert**, um ggf. die erweiterten Parameter anzuzeigen und zu bearbeiten.

Name	Beschreibung
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch durchgeführt wird, wartet der Collector, bis dieser Zyklus beendet ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.
Max. Abrufdauer	Maximale Dauer eines Abfragezyklus in Sekunden. Der Wert 0 bedeutet keine Begrenzung.
Max. Ereignisse-Abruf	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)
Max. Abruf-Inaktivitätsdauer	Maximale Dauer eines Abfragezyklus in Sekunden. Der Wert 0 bedeutet keine Begrenzung.
Befehlsargumente	Optionale Argumente, die beim Skriptaufruf hinzugefügt werden müssen.

Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. **Achtung:** Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich). Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren.

Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das Kontrollpunkt-Sammlungsprotokoll konfigurieren, das Ereignisse aus Kontrollpunkt-Ereignisquellen sammelt.

Dieses Protokoll sammelt Ereignisse aus Kontrollpunkt-Ereignisquellen mit OPSEC LEA. OPSEC LEA ist die Sicherheitsprotokoll-Export-API für Kontrollpunktvorgänge, die die Extrahierung von Protokollen unterstützt.

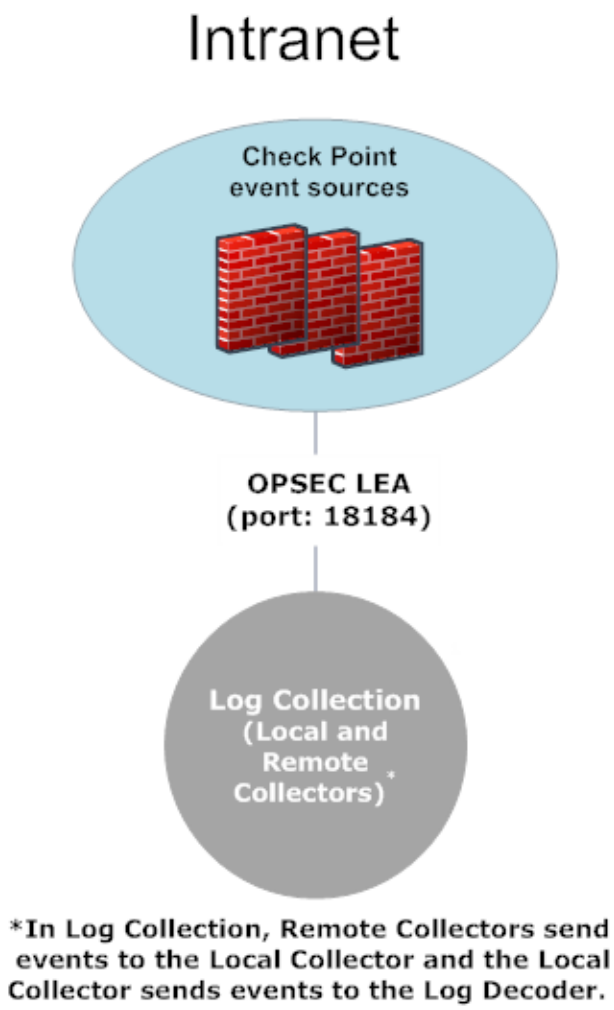
Funktionsweise der Kontrollpunktsammlung

Der Log Collector-Service sammelt Ereignisse von Kontrollpunkt-Ereignisquellen mithilfe von OPSEC LEA. OPSEC LEA ist die Sicherheitsprotokoll-Export-API für Kontrollpunktvorgänge, die die Extrahierung von Protokollen unterstützt.

Hinweis: OPSEC LEA (Protokollexport-API) unterstützt die Extraktion von Protokollen aus Kontrollpunkt-Ereignisquellen, die mit dem SHA-256- oder SHA-1-Zertifikat konfiguriert wurden.

Bereitstellungsszenario

In der folgenden Abbildung wird gezeigt, wie Sie das Kontrollpunkt-Sammlungsprotokoll in NetWitness Suite bereitstellen.

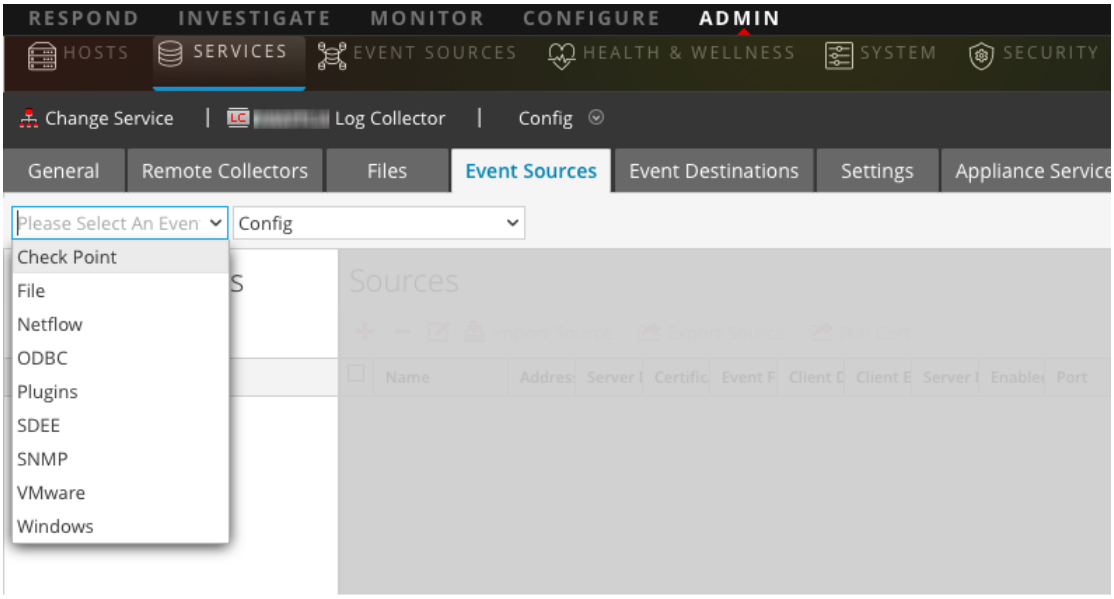


Konfiguration in NetWitness Suite

So konfigurieren Sie eine Kontrollpunkt-Ereignisquelle:

1. Navigieren Sie zu **ADMIN > Services** vom NetWitness Suite-Menü aus.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** die Option **Kontrollpunkt/Konfiguration** aus dem Drop-down-Menü aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf + .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie einen Kontrollpunkt-Ereignisquelltyp aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
9. Definieren Sie die Parameterwerte. Weitere Informationen finden Sie unten stehend unter Kontrollpunktparameter.
10. Klicken Sie auf **Verbindung testen**.

    Das Ergebnis des Tests wird im Dialogfeld angezeigt. Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Geräte- oder Serviceinformationen und versuchen Sie es erneut.

    Log Collector braucht etwa 60 Sekunden, um die Testergebnisse zurückzugeben. Wenn das Zeitlimit überschritten wird, wird der Test abgebrochen und NetWitness Suite zeigt eine Fehlermeldung an.
11. Wenn der Test erfolgreich ist, klicken Sie auf **OK**.

    Die neue Ereignisquelle wird im Bereich **Quellen** angezeigt.

Kontrollpunktparameter

In diesem Abschnitt werden die Parameter für die Konfiguration der Kontrollpunkt-Ereignisquelle beschrieben.

Basisparameter

Parameter	Beschreibung
Name*	Name der Ereignisquelle.
Adresse*	IP-Adresse des Kontrollpunktservers.
Servername*	Name des Kontrollpunktservers.
Zertifikatname	Zertifikatname für sichere Verbindungen zur Verwendung, wenn der Transportmodus https ist Wenn der Name festgelegt wird, muss das Zertifikat im Zertifikat-Truststore enthalten sein, den Sie auf der Registerkarte Einstellungen erstellt haben. Wählen Sie ein Zertifikat aus der Drop-down-Liste aus. Die Dateibenennungskonvention für Kontrollpunkt-Ereignisquellenzertifikate lautet **checkpoint_*Name-der-Ereignisquelle***.
Distinguished-Client	Geben Sie den Distinguished-Client-Namen des Kontrollpunktservers ein.
Cliententitätsname	Geben Sie den Cliententitätsnamen des Kontrollpunktservers ein.
Distinguished-Server	Geben Sie den Distinguished-Server-Namen des Kontrollpunktservers ein.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Zertifikat mithilfe von Pull übertragen	Aktivieren Sie das Kontrollkästchen, um ein Zertifikat das erste Mal abzurufen. Durch das Übertragen eines Zertifikats per Pull wird es vom Truststore zur Verfügung gestellt.
Zertifikatserveradresse	Die IP-Adresse des Servers, auf dem sich das Zertifikat befindet. Der Standardwert ist die Adresse der Ereignisquelle.

Parameter	Beschreibung
Passwort	Nur aktiviert, wenn Sie das Kontrollkästchen Zertifikat mithilfe von Pull übertragen zum ersten Mal aktivieren. Zum Übertragen des Zertifikats per Pull ist ein Passwort erforderlich. Das Passwort ist der Aktivierungsschlüssel, der beim Hinzufügen einer OPSEC-Anwendung zum Kontrollpunkt auf dem Kontrollpunkt erstellt wurde.

Bestimmen der erweiterten Parameterwerte für die Kontrollpunktsammlung

Es werden weniger Systemressourcen verbraucht, wenn Sie eine Kontrollpunkt-Ereignisquellenverbindung dazu konfigurieren, für eine bestimmte Dauer und ein bestimmtes Ereignisvolumen geöffnet zu bleiben (vorübergehende Verbindung). In RSA NetWitness Suite wird standardmäßig eine vorübergehende Verbindung unter Verwendung der folgenden Verbindungsparameter hergestellt:

- Polling-Intervall = **180** (3 Minuten)
- Max. Abrufdauer = **120** (2 Minuten)
- Max. Ereignisse-Abruf = **5.000** (5.000 Ereignisse pro Polling-Intervall)
- Max. Abruf-Inaktivitätsdauer = **0**

Bei Kontrollpunkt-Ereignisquellen mit sehr hoher Aktivität empfiehlt sich die Einrichtung einer Verbindung, die geöffnet bleibt, bis Sie die Sammlung beenden (dauerhafte Verbindung). Dies stellt sicher, dass die Kontrollpunktsammlung die Geschwindigkeit der Ereignisse beibehält, die durch diese aktiven Ereignisquellen erzeugt wird. Die dauerhafte Verbindung vermeidet Neustarts und Verzögerungen bei der Verbindung und verhindert, dass die Kontrollpunktsammlung hinter der Ereigniserzeugung zurückbleibt.

Um eine dauerhafte Verbindung für eine Kontrollpunkt-Ereignisquelle zu etablieren, stellen Sie die folgenden Parameter auf die folgenden Werte ein:

- Polling-Intervall = **-1**
- Max. Abrufdauer = **0**
- Max. Ereignisse-Abruf = **0**
- Max. Abruf-Inaktivitätsdauer = **0**

Parameter	Beschreibung
Port	Der Port auf dem Kontrollpunktserver, mit dem der Log Collector eine Verbindung herstellt. Der Standardwert ist 18184.

Parameter	Beschreibung
Protokolltyp sammeln	Der Typ der Protokolle, die Sie sammeln möchten. Gültige Werte: • **Audit** – Sammelt Auditereignisse. • **Sicherheit** – Sammelt Sicherheitsereignisse. Wenn Sie sowohl Audit- als auch Sicherheitsereignisse sammeln möchten, ist die Erstellung einer doppelten Ereignisquelle erforderlich. Beispiel: Sie erstellen zuerst eine Ereignisquelle mit der Option Audit. Für diese Ereignisquelle wird ein Zertifikat per Pull in den Truststore übertragen. Als Nächstes erstellen Sie eine weitere Ereignisquelle mit denselben Werten, außer dass Sie als Protokolltyp sammelndie Option Sicherheit auswählen. In Zertifikatname wählen Sie dasselbe Zertifikat aus, das Sie bei der Einrichtung des ersten Parametersatzes für diese Ereignisquelle per Pull übertragen haben, und Sie stellen sicher, dass Zertifikat mithilfe von Pull übertragen nicht aktiviert ist.
Protokolle sammeln von	Wenn Sie eine Kontrollpunkt-Ereignisquelle einrichten, werden die Ereignisse von NetWitness aus der aktuellen Protokolldatei gesammelt. Gültige Werte: • **Jetzt** – Beginnt jetzt mit dem Sammeln von Protokollen, also zu diesem Zeitpunkt in der aktuellen Protokolldatei. • **Protokollstart** – Sammelt Protokolle ab dem Anfang der aktuellen Protokolldatei. Wenn Sie als Wert für diesen Parameter „Protokollstart“ auswählen, sammeln Sie möglicherweise eine sehr große Menge von Daten. Dies hängt davon ab, wie lange die derzeitige Protokolldatei bereits Ereignisse sammelt. Beachten Sie, dass diese Option nur für die erste Datenerfassungssitzung wirksam ist.
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch ausgeführt wird, wird gewartet, bis dieser Zyklus abgeschlossen ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.

Parameter	Beschreibung
Max. Abrufdauer	Die maximale Dauer eines Abfragezyklus (wie lange der Zyklus dauert) in Sekunden.
Max. Ereignisse-Abruf	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)
Max. Abruf-Inaktivitätsdauer	Maximale Inaktivitätsdauer, in Sekunden, eines Abfragezyklus. 0 gibt keine Begrenzung an.**> 300** ist der Standardwert.
Weiterleitung	Aktiviert oder deaktiviert den Kontrollpunktserver als Weiterleiter. Diese Option ist standardmäßig deaktiviert.
Protokolltyp (Name-Werte-Paar)	Protokolle von der Ereignisquelle im Name-Wert-Format. Diese Option ist standardmäßig deaktiviert.
Debug	**Achtung:** Aktivieren Sie nur dann das Debugging (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).

Überprüfen, ob die Kontrollpunktsammlung funktioniert

Im folgenden Verfahren wird gezeigt, wie Sie die Funktionsweise der Kontrollpunktsammlung über **Administration > Integrität und Zustand > Registerkarte „Ereignisquellenüberwachung“** prüfen können.

1. Greifen Sie über die Ansicht **Administration > Integrität und Zustand** auf die Registerkarte **Ereignisquellenüberwachung** zu.
2. Suchen Sie in der Spalte **Ereignisquellentyp** nach **checkpointfw1**.
3. Schauen Sie sich den Wert in der Spalte **Anzahl** an, um sicherzustellen, dass bei der Kontrollpunktsammlung Ereignisse erfasst werden.

Im folgenden Verfahren wird gezeigt, wie Sie die Funktionsweise der Kontrollpunktsammlung über **Investigation > Ansicht „Ereignisse“** prüfen können.

1. Greifen Sie auf die Ansicht **Investigation > Ereignisse** zu.
2. Wählen Sie den Log Decoder (z. B. **LD1**), der Kontrollpunktereignisse erfasst, im Dialogfeld **Gerät ermitteln** aus.
3. Suchen Sie in der Spalte **Details** im Feld **device.type** nach einem Kontrollpunkt-Ereignisquellenparser (z. B. **checkpointfw1**), um sicherzustellen, dass bei der Kontrollpunktsammlung Ereignisse erfasst werden.

Hinweis: Wenn die Protokolle vom VSX Checkpoint-Firewallserver durch den Log Collector-Kontrollpunktservice gesammelt werden, müssen Sie, um die VSX-IP der Protokolle in die **ip.orig**-Metadaten zu übersetzen, den VSX-Hostnamen und die VSX-IP-Adresse zur Datei `/etc/hosts` im Log Collector hinzufügen.

Konfigurieren von Dateiereignisquellen in NetWitness Suite

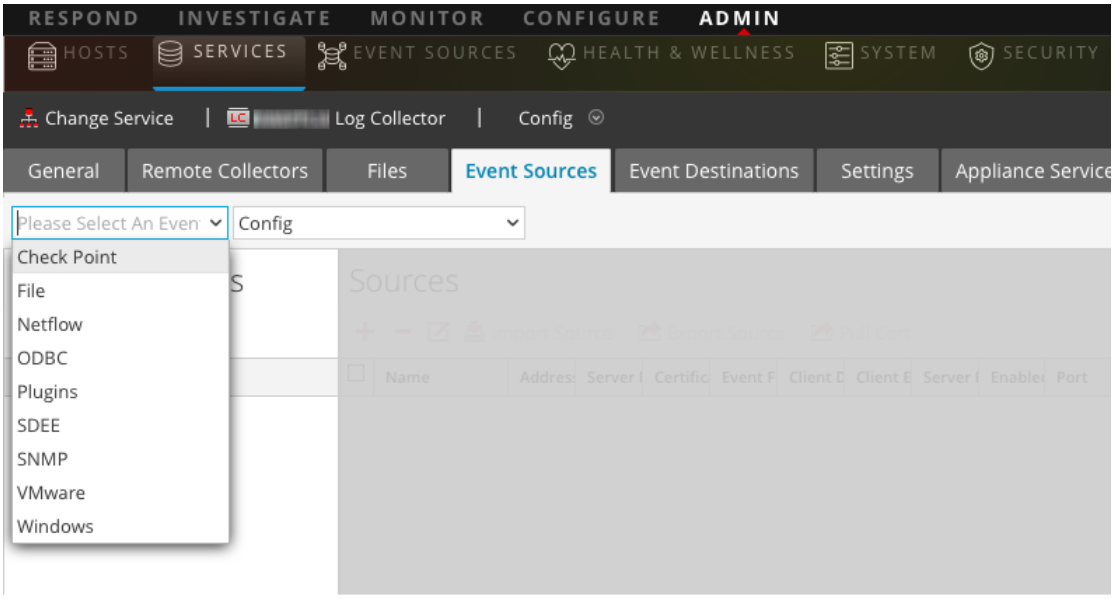
In diesem Thema erfahren Sie, wie Sie das Dateisammlungsprotokoll konfigurieren.

Konfigurieren einer Dateiereignisquelle

So konfigurieren Sie eine Dateiereignisquelle:

1. Navigieren Sie zu **ADMIN > Services** vom NetWitness Suite-Menü aus.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **Datei/Konfigurieren** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf + .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie einen Dateiereignisquelltyp aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
9. Fügen Sie einen **Dateiverzeichnisnamen** hinzu und ändern Sie bei Bedarf andere Parameter. Weitere Informationen finden Sie unten stehend unter Dateisammlungsparameter.
10. Um den öffentlichen Schlüssel zu erhalten und ihn in das Dialogfeld einzugeben, führen Sie die folgenden Schritte aus:
    a. Wählen Sie den öffentlichen Schlüssel aus und kopieren Sie ihn von der Ereignisquelle durch Ausführung von: **cat ~/.ssh/id_rsa.pub**.
    b. Fügen Sie den öffentlichen Schlüssel in das Feld **Ereignisquellen-SSH-Schlüssel** ein.
11. Klicken Sie auf **OK**.

Sie müssen die Dateisammlung neu starten, damit die Änderungen wirksam werden.

Beenden und Neustarten der Dateisammlung

Nachdem Sie eine neue Ereignisquelle hinzugefügt haben, die die Dateisammlung verwendet, müssen Sie den NetWitness Suite-Dateisammlungsservice beenden und neu starten. Dies ist notwendig, um der neuen Ereignisquelle den Schlüssel hinzuzufügen.

Dateisammlungsparameter

Die folgende Tabelle enthält Beschreibungen der Quellparameter für die Dateisammlung.

Name	Beschreibung
	Basis
Dateiverzeichnis*	Sammlungsverzeichnis (zum Beispiel **Eur_London100**), in das die Dateiereignisquelle ihre Dateien platziert. Ein gültiger Wert ist eine Zeichenfolge, die dem folgenden regulären Ausdruck entspricht: **[_a-zA-Z][_a-zA-Z0-9]*** Das bedeutet, dass das Dateiverzeichnis mit einem Buchstaben beginnen muss, auf den Zahlen, Buchstaben und Unterstriche folgen. Dieser Parameter darf nach dem Start der Ereignisdatensammlung nicht geändert werden. Nach der Erstellung der Sammlung erstellt der Log Collector die Arbeits-, Speicher- und Fehlerunterverzeichnisse unter dem Sammlungsverzeichnis.
Adresse*	IP-Adresse der Ereignisquelle. Ein gültiger Wert ist eine **IPv4-Adresse**, eine **IPv6-Adresse** oder ein **Hostname**, der einen vollständig qualifizierten Domainnamen enthält.
Dateispezifikation	Regulärer Ausdruck. Beispiel: **^.*$** = alles wird verarbeitet.

Name	Beschreibung
Dateicodierung	Internationale Dateicodierung. Geben Sie die Dateicodierungsmethode ein. Die folgenden Zeichenfolgen sind Beispiele für gültige Methoden: • UTF-8 (Standard) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Erweitert	
Konvertierungsfehler bei der Codierung ignorieren	Aktivieren Sie dieses Kontrollkästchen, um Konvertierungsfehler bei der Codierung und ungültige Daten zu ignorieren. Das Kontrollkästchen ist standardmäßig aktiviert. **Achtung:** Dies kann zu Analyse- und Transformationsfehlern führen.

Name	Beschreibung
Dateien-Festplatten-Quota	Legt den Zeitpunkt fest, an dem die Speicherung von Dateien beendet wird, unabhängig von den Einstellungen der Parameter **Bei Fehler speichern** und **Bei Erfolg speichern**. Ein Wert von 10 bedeutet beispielsweise: Wenn weniger als 10 % verfügbarer Festplattenspeicher vorhanden ist, beendet der Log Collector die Speicherung von Dateien, um ausreichenden Speicherplatz für die Verarbeitung Ihrer normalen Sammlung zu reservieren. **Achtung:** Der verfügbare Speicherplatz bezieht sich auf eine Partition, in der das Basissammlungsverzeichnis gemountet ist. Wenn der Log Decoder-Server über eine 10-TB-Festplatte verfügt und 2 TB für das Basissammlungsverzeichnis reserviert sind, führt eine Einstellung dieses Werts auf 10 dazu, dass die Protokollsammlung beendet wird, wenn weniger als 0,2 TB (10 % von 2 TB) verfügbarer Speicherplatz vorhanden ist. Es bedeutet nicht 10 % von 10 TB. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.
Sequenzielle Verarbeitung	Flag für sequenzielle Verarbeitung: • Aktivieren Sie das Kontrollkästchen (Standard), um die Ereignisquellendateien in der Reihenfolge der Sammlung zu verarbeiten. • Aktivieren Sie das Kontrollkästchen nicht, um Ereignisquellendateien parallel zu verarbeiten.
Bei Fehler speichern	Flag für Speicherung bei Fehlern. Aktivieren Sie das Kontrollkästchen, um die Datei **eventsource collection** beizubehalten, wenn der Log Collector einen Fehler feststellt. Das Kontrollkästchen ist standardmäßig aktiviert.
Bei Erfolg speichern	Speichert die Datei **eventsource collection** nach der Verarbeitung des Flags. Aktivieren Sie das Kontrollkästchen, um die Datei eventsource collection nach ihrer Verarbeitung zu speichern. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Name	Beschreibung
Ereignisquellen-SSH-Schlüssel	Öffentlicher SSH-Schlüssel, der zum Hochladen von Dateien für diese Ereignisquelle verwendet wird. Weitere Anweisungen zum Erzeugen von Schlüsseln finden Sie im Abschnitt *Erzeugen des Schlüsselpaars auf der Ereignisquelle und Importieren des öffentlichen Schlüssels in den Log Collector* im Handbuch Installieren und Aktualisieren des SFTP-Agent. **Hinweis:** Wenn die Dateisammlung beendet wird, aktualisiert NetWitness Suite nicht die Datei „authorized_keys“ mit dem öffentlichen SSH-Schlüssel, den Sie in diesem Parameter hinzufügen oder ändern. Sie müssen die Dateisammlung neu starten, um den öffentlichen Schlüssel zu aktualisieren. Sie können den Wert des öffentlichen Schlüssels in diesem Parameter in mehreren Dateiereignisquellen hinzufügen oder ändern, ohne dass die Dateisammlung ausgeführt wird. Allerdings aktualisiert NetWitness Suite die Datei **authorized_keys** erst, wenn die Dateisammlung neu gestartet wurde.
Fehlerdateien verwalten	Standardmäßig verwendet der Log Collector den Parameter **Dateien-Festplatten-Quota**, um zu gewährleisten, dass die Festplatte nicht mit Fehlerdateien gefüllt wird. Wenn Sie diesen Parameter auf **true** einstellen, können Sie einen der folgenden Parameter festlegen: • Maximal zugewiesener Speicherplatz für Fehlerdateien im Parameter **Fehlerdateiengröße** • Maximal zulässige Anzahl von Fehlerdateien im Parameter **Anzahl Fehlerdateien** Eine Reduzierungsprozentzahl wird auch angegeben, die das System anwendet, wenn das Maximum erreicht wurde. Aktivieren Sie das Kontrollkästchen zum Managen von Fehlerdateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Name	Beschreibung
Fehlerdateiengröße	Dieser Wert ist nur gültig, wenn die Parameter **Fehlerdateien verwalten** und **Bei Fehler speichern** auf „true“ eingestellt werden. Gibt an, in welchem Umfang NetWitness Suite Fehlerdateien speichert. Bei dem von Ihnen angegebenen Wert handelt es sich um die maximale Gesamtgröße aller Dateien im Fehlerverzeichnis. Ein gültiger Wert ist eine Zahl zwischen **0** und **281474976710655**. Diese Werte werden in **Kilobyte**, **Megabyte** oder **Gigabyte** angegeben. Der Standardwert lautet **100 Megabyte**. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Anzahl Fehlerdateien	Dieser Wert ist nur gültig, wenn die Parameter **Fehlerdateien verwalten** und **Bei Fehler speichern** auf „true“ eingestellt werden. Gibt die maximal zulässige Anzahl von Fehlerdateien im Fehlerverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **65536**. **65536** ist der Standardwert. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Reduzierung Fehlerdateien in %	Der Prozentsatz der Größe oder der Anzahl der Fehlerdateien, die der Log Collector-Service entfernt, wenn die maximale Größe oder die maximale Anzahl erreicht wurde. Der Service löscht die ältesten Dateien zuerst. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.
Gespeicherte Dateien verwalten	Aktivieren Sie das Kontrollkästchen zum Managen von gespeicherten Dateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Standardmäßig verwendet der Log Collector den Parameter **Dateien-Festplatten-Quota**, um zu gewährleisten, dass die Festplatte nicht mit gespeicherten Dateien gefüllt wird. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie einen der folgenden Parameter festlegen: • Maximal zugewiesener Speicherplatz für gespeicherte Dateien im Parameter **Größe gespeicherter Dateien** • Maximal zulässige Anzahl von gespeicherten Dateien im Parameter **Anzahl gespeicherter Dateien** Eine Reduzierungsprozentzahl wird auch angegeben, die das System anwendet, wenn das Maximum erreicht wurde.

Name	Beschreibung
Größe gespeicherter Dateien	Dieser Wert ist nur gültig, wenn die Parameter **Gespeicherte Dateien verwalten** und **Bei Erfolg speichern** auf „true“ eingestellt werden. Gibt die maximale Gesamtgröße aller Dateien im Speicherverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **281474976710655**. Diese Werte werden in **Kilobyte**, **Megabyte** oder **Gigabyte** angegeben. Der Standardwert lautet **100 Megabyte**. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Anzahl gespeicherter Dateien	Dieser Wert ist nur gültig, wenn die Parameter **Gespeicherte Dateien verwalten** und **Bei Erfolg speichern** auf „true“ eingestellt werden. Gibt die maximale Anzahl von gespeicherten Dateien im Speicherverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **65536**. **65536** ist der Standardwert. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Reduzierung gespeicherter Dateien in %	Der Prozentsatz der Größe oder der Anzahl der gespeicherten Dateien, die der Log Collector-Service entfernt, wenn die maximale Größe oder die maximale Anzahl erreicht wurde. Der Service löscht die ältesten Dateien zuerst. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.

Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debugging (legen Sie diesen Parameter auf **Ein** oder **Ausführlich** fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggings wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert/deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).
Abbrechen	Schließt das Dialogfeld, ohne einen Ereignisquelltyp hinzuzufügen.
OK	Fügt die Parameter für die Ereignisquelle hinzu.

Konfigurieren Sie Netflow-Ereignisquellen in NetWitness Suite

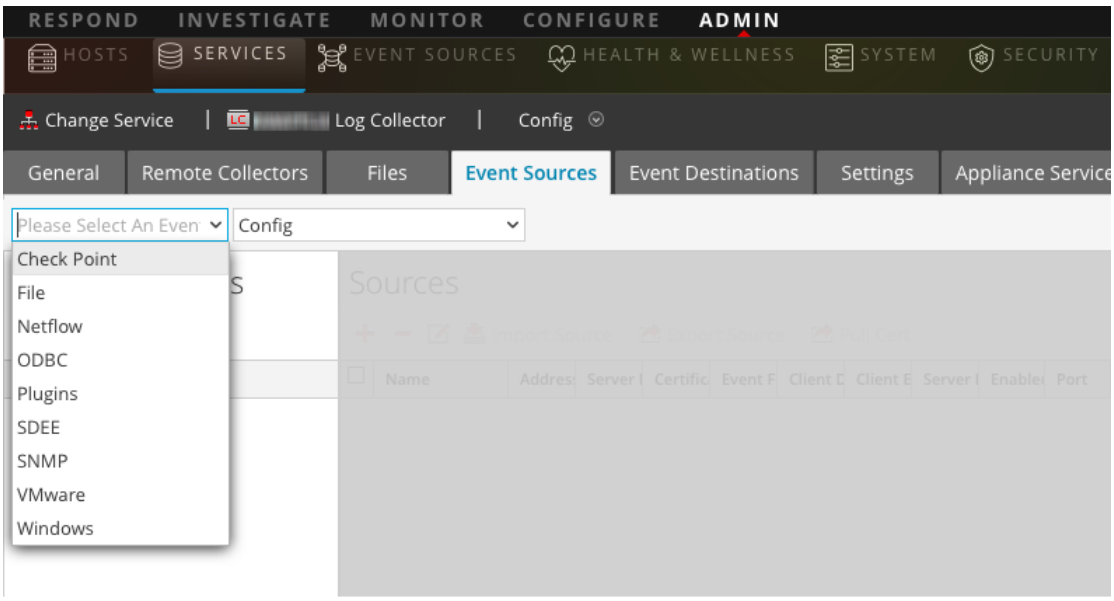
In diesem Thema wird erläutert, wie Sie das Netflow-Sammlungsprotokoll konfigurieren.

Konfigurieren einer Netflow-Ereignisquelle

So konfigurieren Sie eine Netflow-Ereignisquelle:

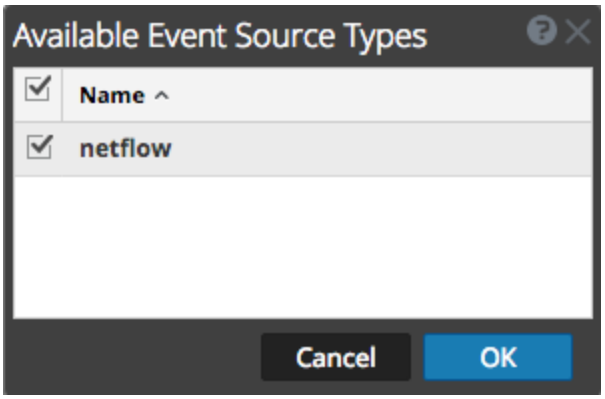
1. Navigieren Sie zu **ADMIN > Services** vom NetWitness Suite-Menü aus.
2. Wählen Sie einen Protokollsammlungsservice aus.

3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht** > **Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **Netflow/Konfigurieren** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf +.

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie den Ereignisquelltyp **netflow** aus und klicken Sie auf **OK**.



   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.
8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.

9. Geben Sie eine Portnummer im Feld **Port** ein und vergewissern Sie sich, dass das Kontrollkästchen „Aktiviert“ aktiviert ist.

   Hinweis: Standardmäßig werden die Ports 2055, 4739, 6343 und 9995 auf der Firewall von NetWitness Suite geöffnet. Sie können andere Ports für Netflow öffnen, falls erforderlich.

   Weitere Informationen zu anderen Parametern finden Sie unten stehend unter Parameter für Netflow-Sammlung.

10. Klicken Sie auf **OK**.

Die neue Ereignisquelle wird in der Liste angezeigt.

Parameter für Netflow-Sammlung

Die folgende Tabelle enthält Beschreibungen der Quellparameter für die Netflow-Sammlung.

Name	Beschreibung
Basis	
Port	Geben Sie die Portnummer ein, die für die Netflow-Ereignisquelle konfiguriert ist. NetWitness Suite öffnet standardmäßig die Ports 2055, 4739, 6343 und 9995 für Netflow. Sie können andere Ports für Netflow öffnen, falls erforderlich.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Erweitert	

Name	Beschreibung
In Flight-Protokollveröffentlichungsschwellenwert	Legt einen Schwellenwert fest. Wenn er erreicht wird, erzeugt NetWitness Suite eine Protokollnachricht, die Sie beim Beheben von Problemen mit dem Ereignisfluss unterstützt. Der Schwellenwert entspricht der Größe der Netflow-Ereignismeldungen, die gegenwärtig von der Ereignisquelle an NetWitness Suite übertragen werden. Gültige Werte: • **0** (Standard) = Deaktiviert die Protokollmeldung. • **100-100000000** = Erzeugt eine Protokollmeldung, wenn diese Log Collector die angegebene Anzahl an Netflow-Ereignissen verarbeitet hat. Wenn Sie diesen Wert zum Beispiel auf 100 festlegen, erzeugt NetWitness Suite eine Protokollmeldung, wenn 100 Netflow-Ereignisse der angegebenen Netflow-Version (v5 oder v9) verarbeitet wurden.

Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggings wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).
Abbrechen	Schließt das Dialogfeld, ohne einen Ereignisquelltyp hinzuzufügen.
OK	Fügt die Parameter für die Ereignisquelle hinzu.

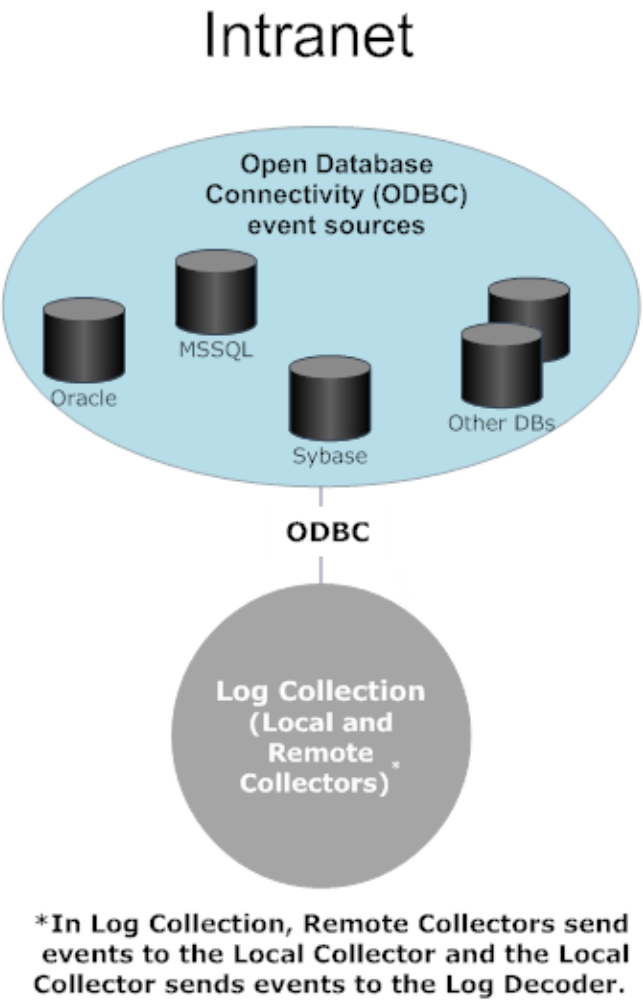
ODBC

Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das ODBC-Sammlungsprotokoll (Open Database Connectivity) konfigurieren, mit dem Ereignisse aus Ereignisquellen abgerufen werden, die Auditdaten mithilfe der ODBC-Softwareschnittstelle in einer Datenbank speichern.

Bereitstellungsszenario

Die folgende Abbildung zeigt die Bereitstellung des ODBC-Sammlungsprotokolls in NetWitness Suite.



Konfigurieren von ODBC-Ereignisquellen

Zum Konfigurieren einer ODBC-Ereignisquelle müssen Sie einen Ereignisquelltyp konfigurieren und auch eine DSN-Vorlage auswählen.

Konfigurieren eines DSN

Das folgende Verfahren beschreibt, wie Sie einen DSN aus einer vorhandenen DSN-Vorlage hinzufügen. Weitere Verfahren im Zusammenhang mit DSNs finden Sie unter Konfigurieren von DSNs (Data Source Names).

Konfigurieren eines DSN:

1. Wechseln Sie zu **Administration** > **Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.
3. Klicken Sie auf  unter **Aktionen** und wählen Sie **Ansicht** > **Konfiguration** aus.
4. Wählen Sie auf der Log Collector-Registerkarte **Ereignisquellen** im Drop-down-Menü **ODBC/DSNs** aus.
5. Der DSNs-Bereich wird mit den vorhandenen DSNs angezeigt, sofern zutreffend.
6. Klicken Sie auf +, um das Dialogfeld **DSN hinzufügen** zu öffnen.
7. Wählen Sie eine DSN-Vorlage im Drop-down-Menü aus und geben Sie einen Namen für den DSN ein. (Sie verwenden den Namen beim Festlegen des ODBC-Ereignisquelltyps.)

   Klicken Sie gegebenenfalls auf 

, um DSN-Vorlagen hinzuzufügen oder zu löschen.
8. Geben Sie die Parameter ein und klicken Sie auf **Speichern**.

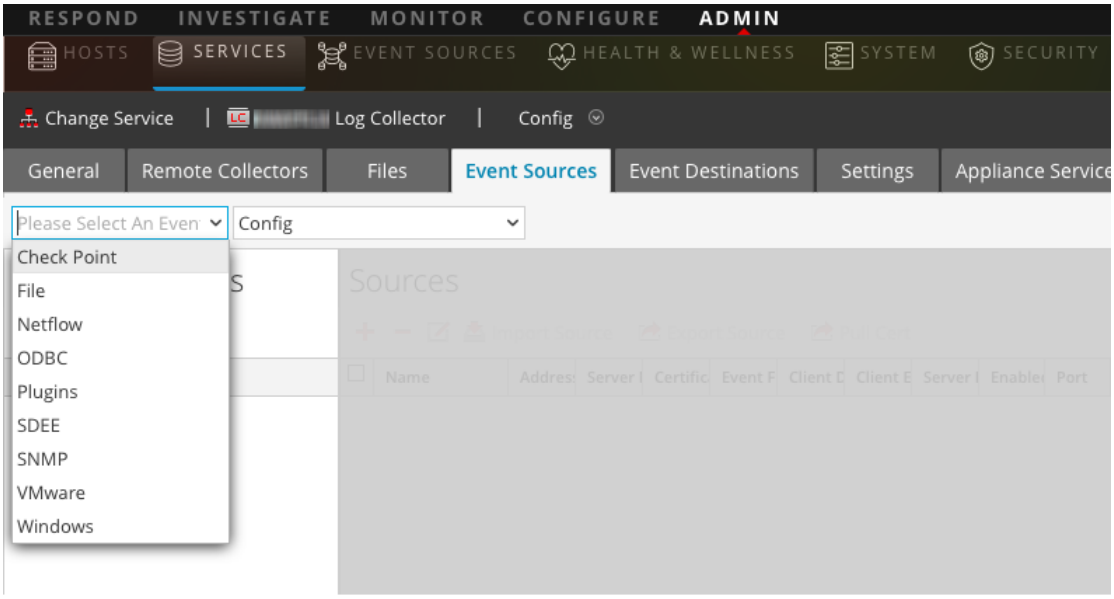
Hinzufügen eines Ereignisquelltyps

Weitere Informationen zu Parametern, die im folgenden Verfahren verwendet werden, finden Sie unter Parameter der ODBC-Ereignisquellenkonfiguration.

So konfigurieren Sie einen ODBC-Ereignisquelltyp:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

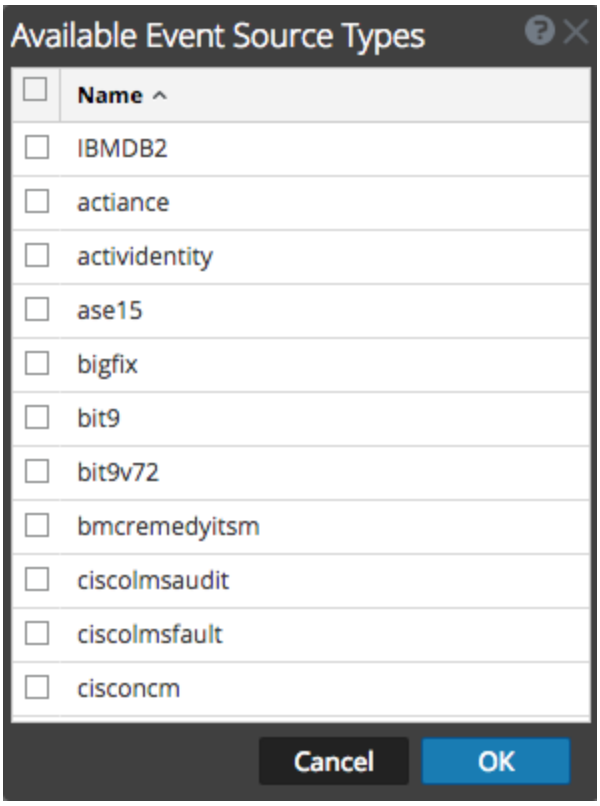
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **ODBC/Konfigurieren** aus.

6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf + .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.

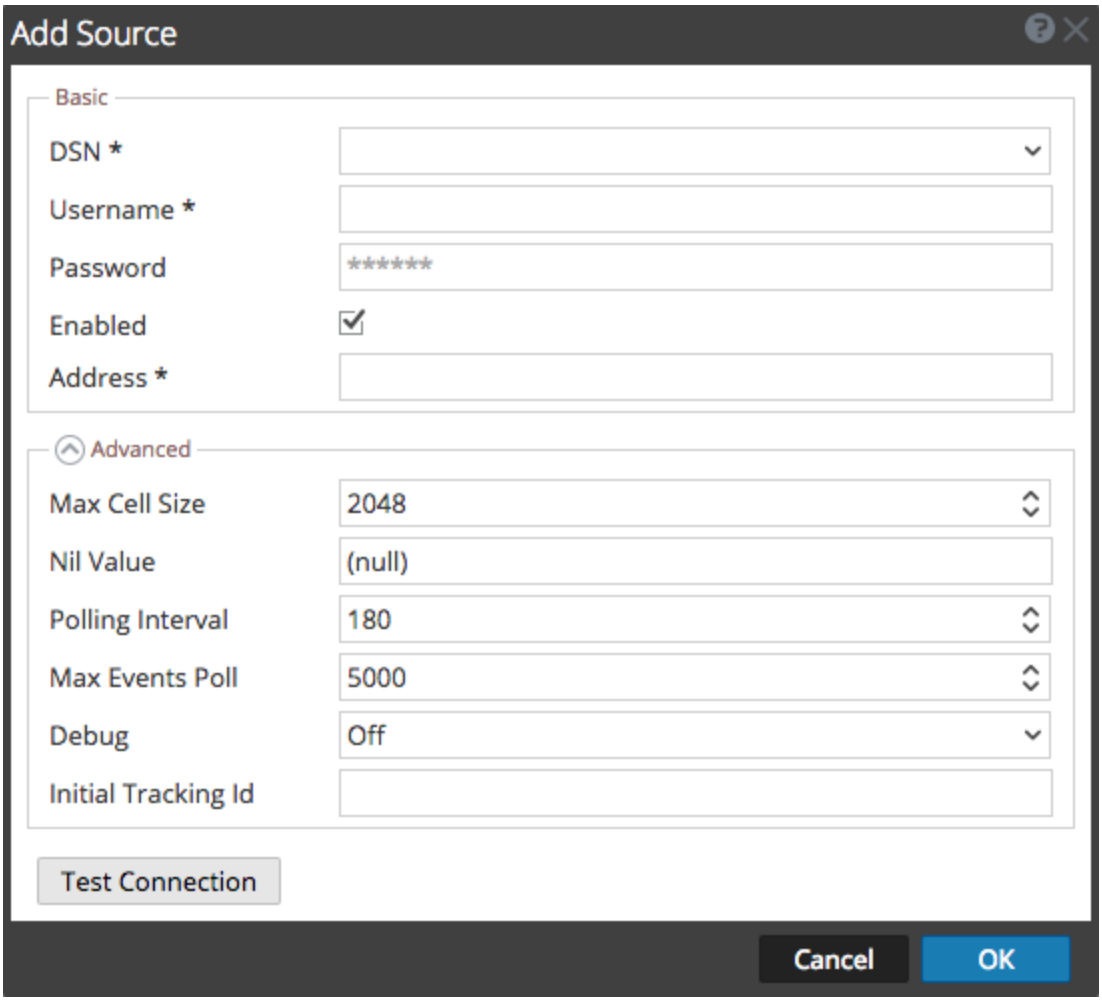


7. Wählen Sie eine Ereignisquellenkategorie aus (z. B. **mssql**) aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.

8. Wählen Sie den neuen Typ im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste **Quellen**.

   Das Dialogfeld **Quelle hinzufügen** wird angezeigt.



9. Wählen Sie einen DSN aus der Drop-down-Liste aus und legen Sie nach Bedarf weitere Parameter fest oder ändern Sie diese. Klicken Sie anschließend auf **OK**.
10. Klicken Sie auf **Verbindung testen**.

    Das Ergebnis des Tests wird im Dialogfeld angezeigt. Wenn der Test nicht erfolgreich ist, bearbeiten Sie die DSN-Informationen und versuchen Sie es erneut.

    Hinweis: Log Collector braucht etwa 60 Sekunden, um die Testergebnisse zurückzugeben. Wenn das Zeitlimit überschritten wird, wird der Test abgebrochen und der NetWitness Suite-Server zeigt eine Fehlermeldung an.
11. Wenn der Test erfolgreich ist, klicken Sie auf **OK**.

Der neu definierte DSN wird im Bereich **Quellen** angezeigt.

Konfigurieren von DSNs (Data Source Names)

In diesem Thema erfahren Sie, wie Sie DSNs für die ODBC-Sammlung erstellen und warten.

Kontext

ODBC-Ereignisquellen (Open Database Connectivity) benötigen DSNs (Data Source Names). Sie müssen daher DSNs mit den zugehörigen Wertepaaren für die ODBC-Ereignisquellenkonfiguration definieren.

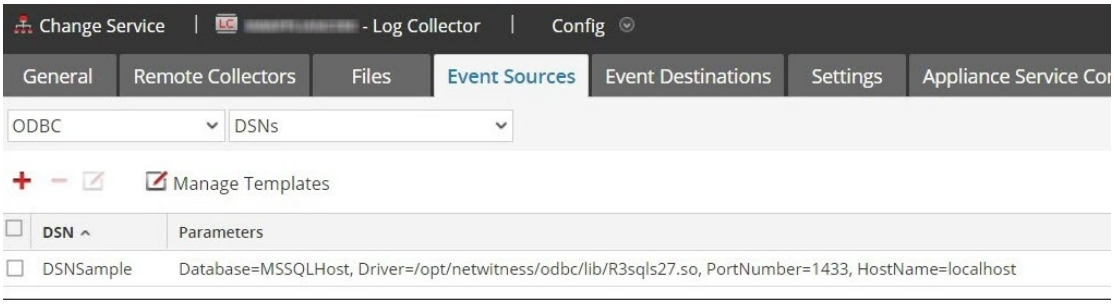
Navigieren zum Bereich „DSN“

Um DSNs oder DSN-Vorlagen hinzuzufügen oder zu bearbeiten, navigieren Sie zuerst zum entsprechenden Bildschirm.

So navigieren Sie zum Bereich „DSN-Vorlagen“:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.
3. Klicken Sie auf  unter **Aktionen** und wählen Sie **Ansicht > Konfiguration** aus.
4. Wählen Sie auf der Registerkarte **Ereignisquellen** des Log Collector im Drop-down-Menü die Option **ODBC/DSNs** aus.

   Der Bereich **DSNs** wird mit den DSNs angezeigt, die hinzugefügt werden, sofern zutreffend.

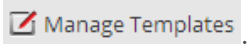


In diesem Bildschirm können Sie die folgenden Aktionen ausführen:

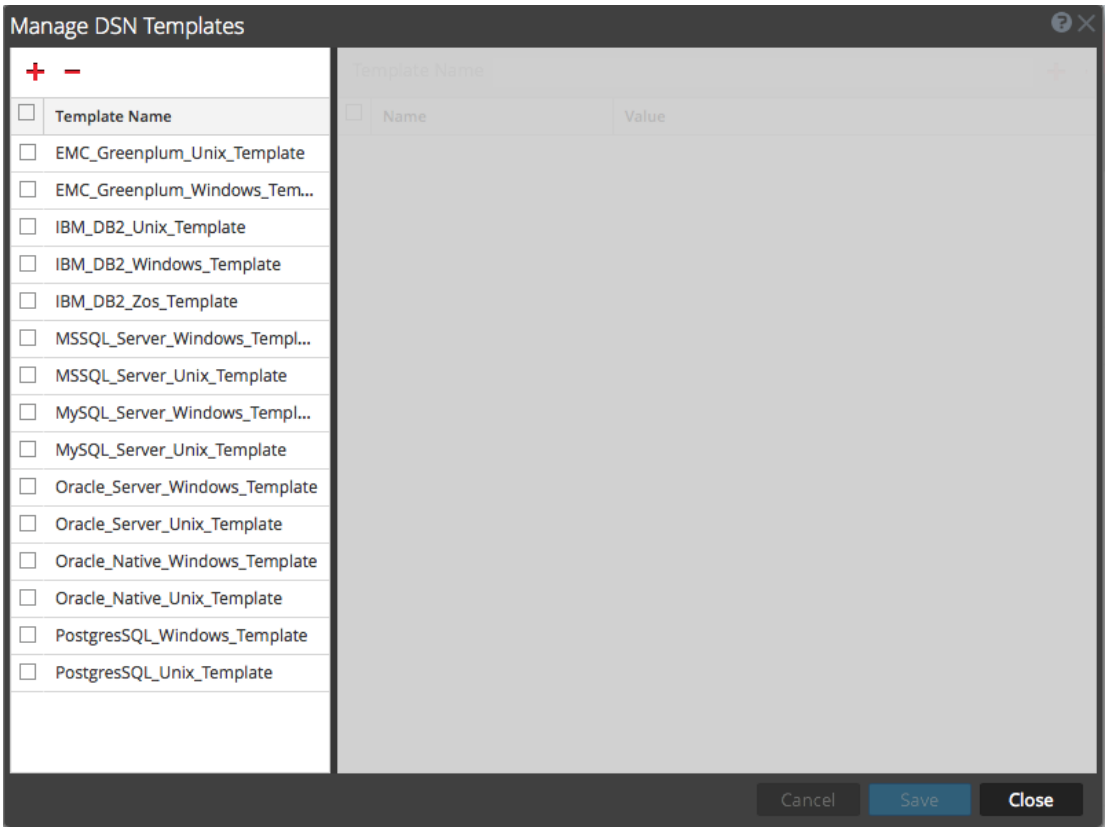
- Hinzufügen einer neuen DSN-Vorlage
- Hinzufügen eines DSN aus einer vorhandenen Vorlage
- Hinzufügen eines DSN durch Bearbeiten einer vorhandenen DSN-Vorlage
- Entfernen eines DSN oder einer DSN Vorlage

Hinzufügen einer neuen DSN-Vorlage

Wenn keine der vordefinierten DSN-Vorlagen Ihren Anforderungen entspricht, verwenden Sie dieses Verfahren, um eine DSN-Vorlage hinzuzufügen.

1. Klicken Sie im Bereich „DSNs“ auf  .

   Das Dialogfeld **DSN-Vorlagen managen** wird angezeigt.



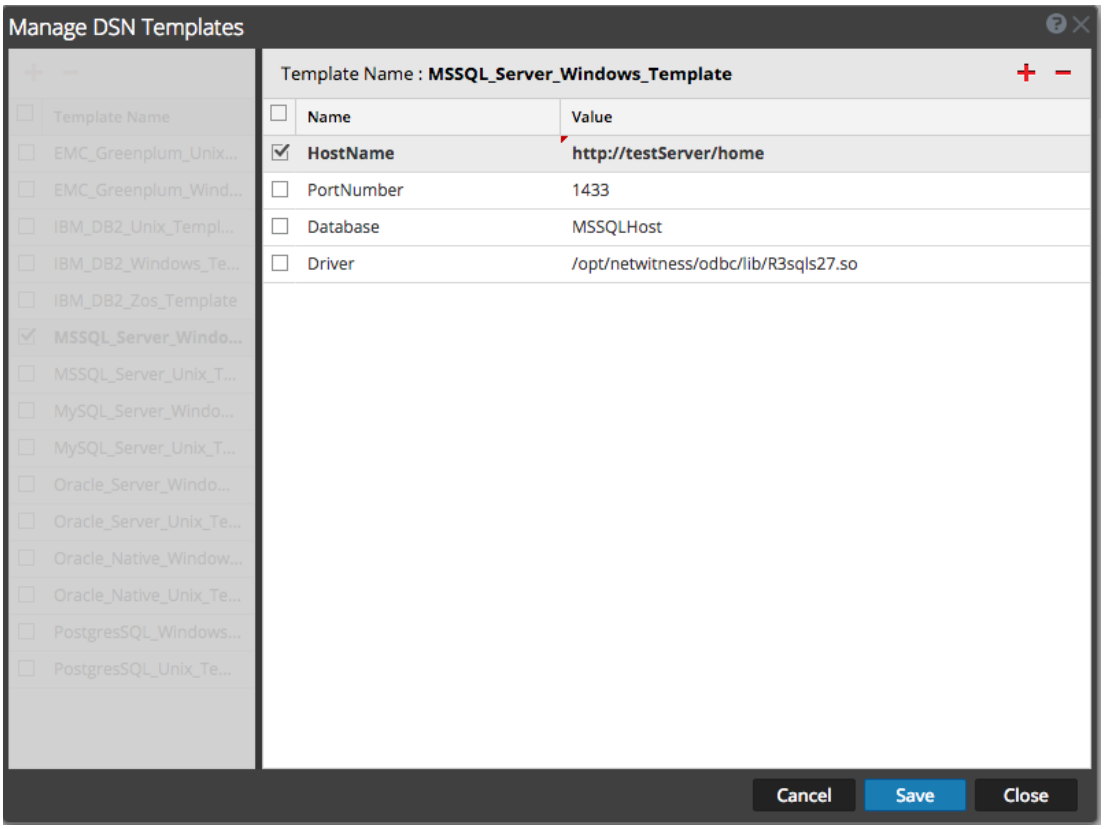
Hinweis: RSA stellt im linken Seitenbereich Standardvorlagen bereit, die Sie verwenden können, wenn Sie einen neuen DSN hinzufügen.

2. Klicken Sie auf + .

   Der rechte Bereich wird aktiviert.

3. Geben Sie einen Vorlagennamen an und klicken Sie auf + im rechten Bereich, um Parameter hinzuzufügen.

4. Geben Sie die Parameter an. Klicken Sie auf **Speichern**.



Die neue DSN-Vorlage wird zu der Liste **DSN-Vorlagen managen** hinzugefügt.

Hinzufügen eines DSN aus einer vorhandenen Vorlage

Sie können eine vorhandene Vorlage auswählen und die Parameter entsprechend Ihren Anforderungen eingeben.

1. Klicken Sie im Bereich „DSNs“ auf +, um das Dialogfeld „DSN hinzufügen“ zu öffnen.

   Das Dialogfeld **DSN hinzufügen** wird mit vorhandenen DSNs angezeigt, sofern zutreffend.

2. Wählen Sie eine DSN-Vorlage im Drop-down-Menü aus und geben Sie einen Namen für den DSN ein. (Sie verwenden den Namen beim Festlegen des ODBC-Ereignisquelltyps.)

3. Geben Sie die Parameter ein und klicken Sie auf **Speichern**.

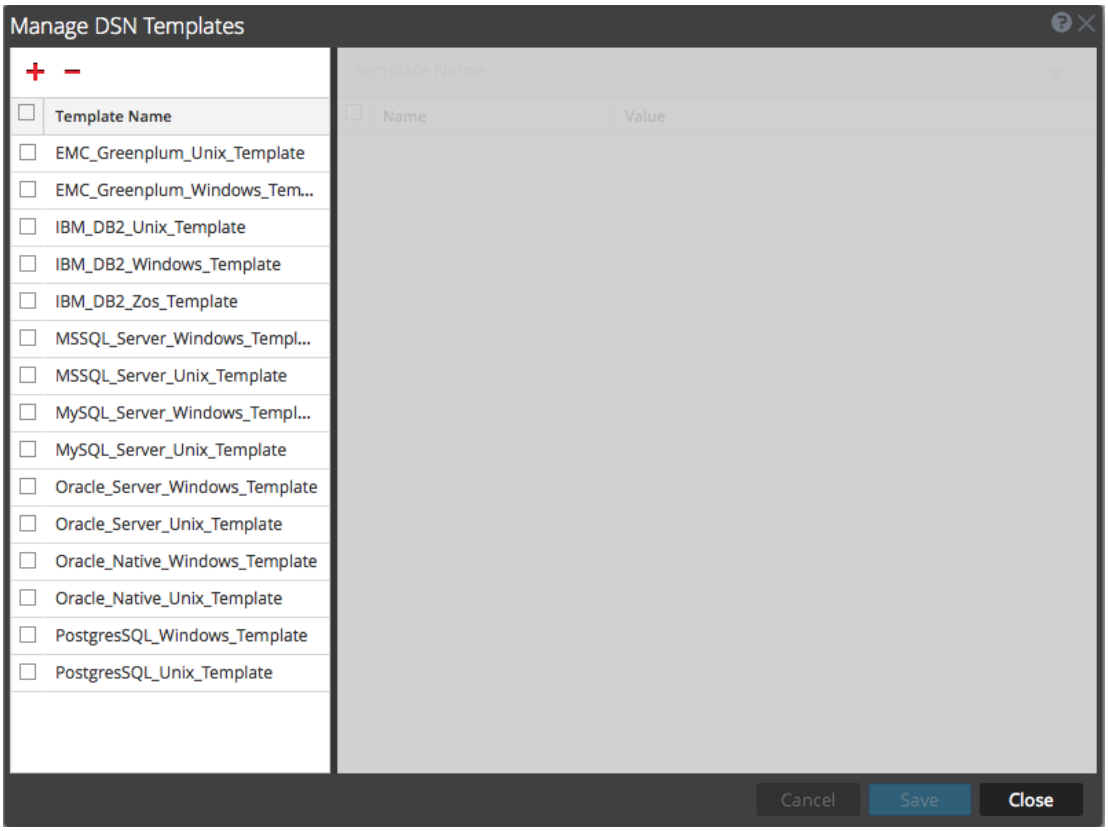
Ihr DSN wurde zur Liste der DSNs hinzugefügt.

Hinzufügen eines neuen DSN durch Bearbeiten einer vorhandenen DSN-Vorlage

Sie können einen DSN hinzufügen, indem Sie eine vorhandene DSN-Vorlage entsprechend Ihren Anforderungen aktualisieren.

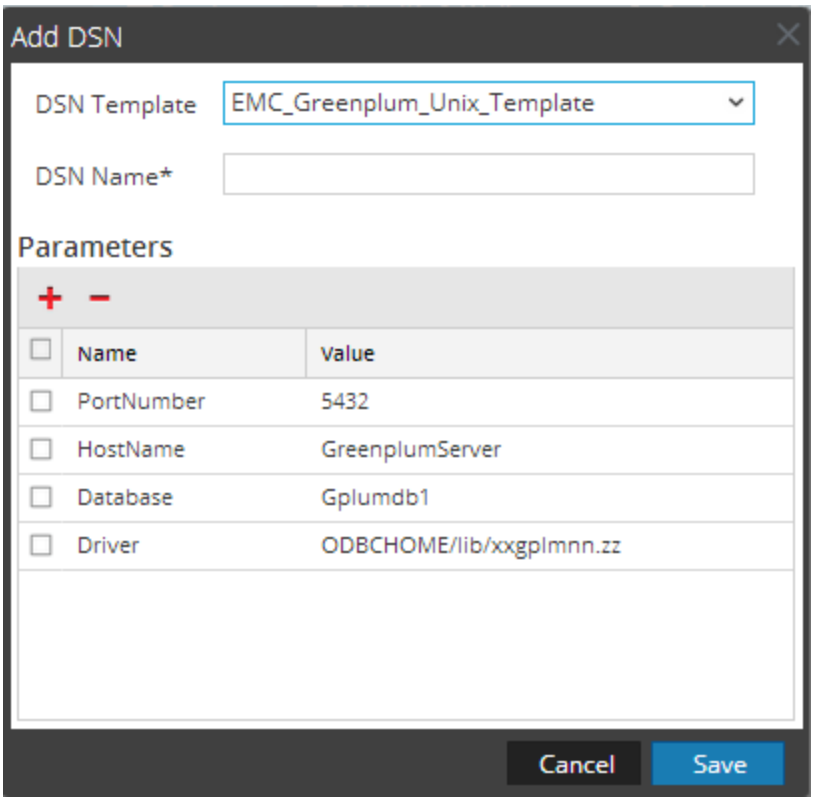
1. Klicken Sie im Bereich „DSNs“ auf Manage Templates.

   Das Dialogfeld **DSN-Vorlagen managen** wird angezeigt.



2. Wählen Sie die vorhandene Vorlage aus, die Sie bearbeiten möchten.

   Der rechte Bereich wird aktiviert und die Standardparameter für die ausgewählte Vorlage werden angezeigt.



3. Geben Sie einen Namen im Feld **DSN-Name** ein.
4. Fügen Sie die Standardparameter hinzu, löschen oder bearbeiten Sie sie.
5. Nachdem Sie die erforderlichen Parameter festgelegt haben, klicken Sie auf **Speichern** und dann auf **Schließen**.
6. Wählen Sie die aktualisierte DSN-Vorlage im Drop-down-Menü aus und geben Sie einen Namen für den DSN ein. (Sie verwenden den Namen beim Festlegen des ODBC-Ereignisquelltyps.)
7. Geben Sie die Parameter ein und klicken Sie auf **Speichern**.

Ihr DSN wurde zur Liste der DSNs hinzugefügt.

Entfernen eines DSN oder einer DSN Vorlage

Wenn Sie einen DSN bzw. eine DSN-Vorlage nicht mehr verwenden, können Sie diese aus dem System entfernen.

So entfernen Sie einen vorhandenen DSN:

1. Wählen Sie im Bereich „DSNs“ einen vorhandenen DSN aus.
2. Klicken Sie auf —.

Eine Warnmeldung wird mit der Frage angezeigt, ob Sie sind sicher, dass Sie den DSN löschen möchten.

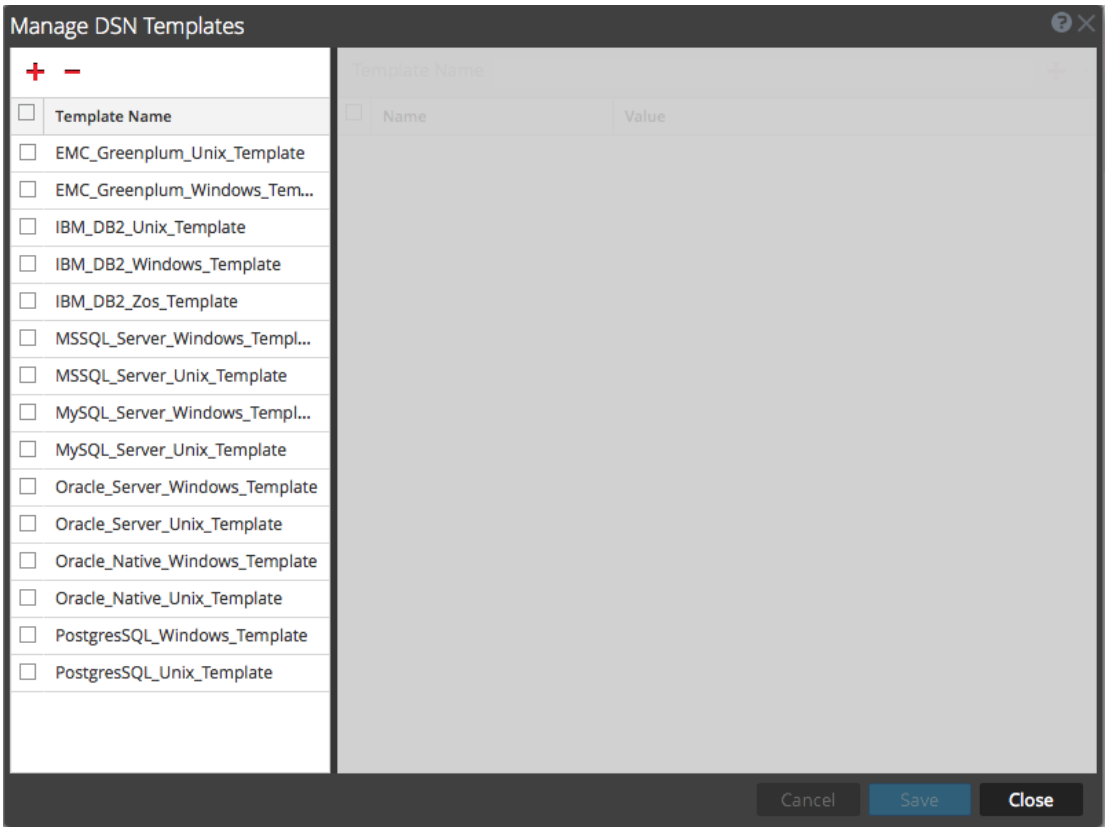
3. Klicken Sie auf **Ja**, um den DSN zu löschen. Um den Löschvorgang abzubrechen, klicken Sie auf **Nein**.

Wenn Sie den Löschvorgang bestätigt haben, wird der ausgewählte DSN aus dem System entfernt.

So entfernen Sie eine vorhandene DSN-Vorlage:

1. Klicken Sie im Bereich „DSNs“ auf Manage Templates.

   Das Dialogfeld **DSN-Vorlagen managen** wird angezeigt.



2. Wählen Sie im Bereich „DSNs“ eine vorhandene DSN-Vorlage aus.
3. Klicken Sie auf −.

   Eine Bestätigungsmeldung wird mit der Frage angezeigt, ob Sie sind sicher, dass Sie die DSNVorlage löschen möchten.

4. Klicken Sie auf **Ja**, um die DSN-Vorlage zu löschen. Um den Löschvorgang abzubrechen, klicken Sie auf **Nein**.

Wenn Sie den Löschvorgang bestätigt haben, wird die ausgewählte DSN-Vorlage aus dem System entfernt.

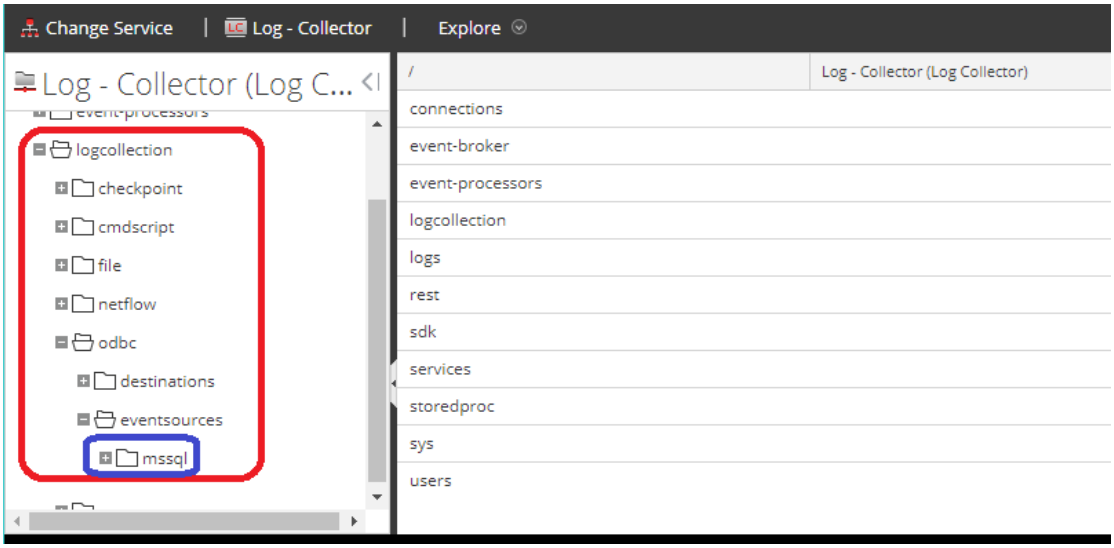
Konfigurieren des Metawerts „device.ip“ für die ODBC-Datenquelle

Sie können für jede ODBC-Ereignisquelle festlegen, ob der ODBC Collector den Metawert **device.ip** mit der IP-Adresse der Ereignisquelle oder der IP der tatsächlichen Quelle, für die Protokolle gesammelt werden, auffüllen soll.

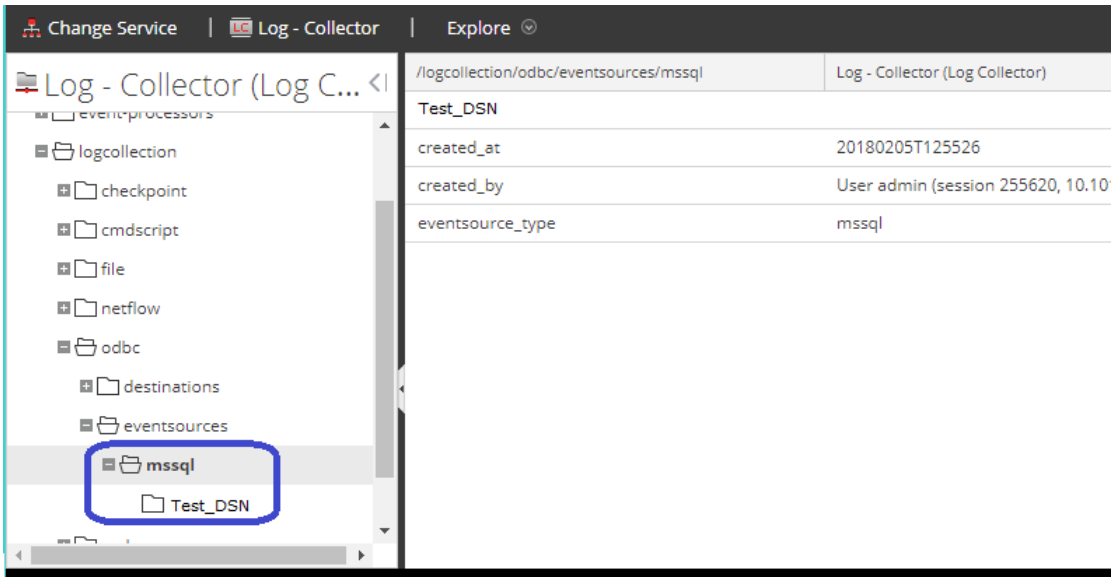
So können Sie diese Parameter anzeigen oder festlegen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.
3. Klicken Sie unter **Aktionen** auf  und wählen Sie **Ansicht > Durchsuchen** aus.
4. Navigieren Sie zu **logcollection > odbc > eventsources**.

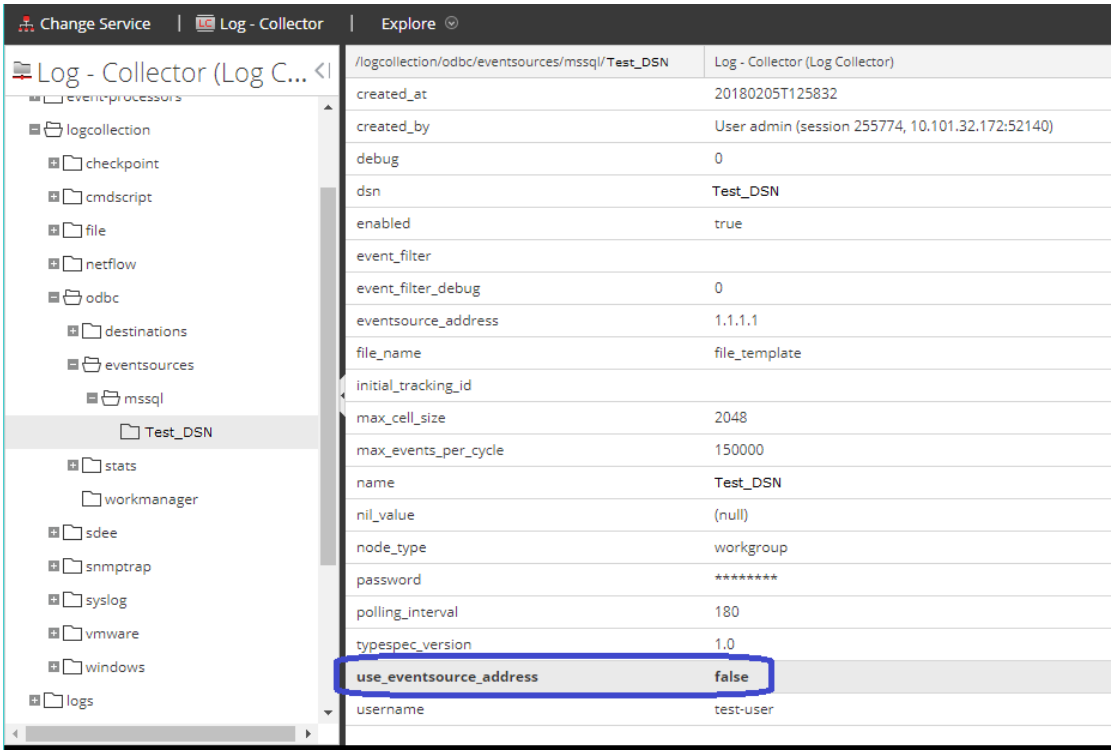
   Sie finden dort Einträge für jede ODBC-Ereignisquelle, die Sie in NetWitness konfiguriert haben. Für diese Installation ist derzeit beispielsweise nur die ODBC-Ereignisquelle MS SQL konfiguriert:



5. Klicken Sie auf + neben einer Ereignisquelle, um sie zu erweitern und ihren DSN-Eintrag anzuzeigen.



6. Klicken Sie auf den DSN-Eintrag (in diesem Beispiel **Test_DSN**), um die Parameter anzuzeigen.
7. Der Parameter **use_eventsource_address** ist aufgeführt.



- **False**: Die IP-Adresse der tatsächlichen Quelle wird verwendet. Dies ist der Standardwert.
- **True**: Die IP-Adresse der Ereignisquelle wird verwendet.

8. Klicken Sie auf den Wert (in diesem Fall **False**) und geben Sie den neuen Wert ein.

> **Hinweis:** Wenn Sie etwas anderes als **true** oder **false** eingeben (Groß- und Kleinschreibung spielt keine Rolle), zeigt eine Fehlermeldung an, dass der eingegebene Wert nicht festgelegt werden kann.

Jegliche Änderungen werden sofort übernommen.

Erstellen von angepasstem Typespec für ODBC-Sammlung

In diesem Thema erfahren Sie, wie Sie ein kundenspezifisches Typespec für den Log Collector erstellen. Das Thema umfasst Folgendes:

- Verfahren zur Erstellung eines kundenspezifischen Typespec
- ODBC-Sammlung-Typespec-Syntax
- Beispiel für eine Typespec-Datei für die ODBC-Sammlung

Erstellen eines kundenspezifischen Typespec

So erstellen Sie eine angepasste Typespec-Datei:

1. Öffnen Sie einen SFTP-Client (z. B. WinSCP) und stellen Sie eine Verbindung zu einem Log Collector oder einem Remote Log Collector her.
2. Navigieren Sie zu **/etc/netwitness/ng/logcollection/content/collection/odbc** und kopieren Sie eine vorhandene Datei, z. B. **bit9.xml**.
3. Ändern die Datei entsprechend Ihren Anforderungen. Details finden Sie unter ODBC-Sammlung-Typespec-Syntax.
4. Benennen Sie die Datei um und speichern Sie sie im selben Verzeichnis.
5. Starten Sie den Log Collector neu.

> **Hinweis:** Der neue Ereignisquelltyp ist nicht sichtbar in NetWitness Suite, bis Sie den Log Collector neu gestartet haben.

ODBC-Sammlung-Typespec-Syntax

In der folgenden Tabelle werden die Typespec-Parameter beschrieben.

Parameter	Beschreibung
Name	Der Anzeigename Ihrer ODBC-Ereignisquelle (z. B. **actividentity**). NetWitness Suite zeigt diesen Namen im Bereich **Quellen** in der Registerkarte **Ansicht > Konfiguration > Ereignisquellen** an. Gültig ist eine alphanumerische Zeichenfolge. - (Bindestrich), _ (Unterstrich) oder Leerzeichen dürfen nicht verwendet werden. Der Name muss für alle Typespec-Dateien im Ordner eindeutig sein.
type	Ereignisquelltyp: **odbc** Ändern Sie diese Zeile nicht.
prettyName	Benutzerdefinierter Name für die Ereignisquelle. Sie können denselben Wert wie für „name“ verwenden (z. B. „apache“) oder einen aussagekräftigeren Namen wählen.
Version	Version dieser Typespec-Datei. Der Standardwert ist 1.0.
author	Person, die die Typespec-Datei erstellt hat. Ersetzen Sie author-name durch Ihren Namen.
Beschreibung	Formelle Beschreibung der Ereignisquelle. Ersetzen Sie formal-description durch Ihre Beschreibung der Ereignisquelle.
<Gerät> Abschnitt	
Parser	Dieser optionale Parameter enthält den Namen des Protokoll-Parsers. Dieser Wert erzwingt die Verwendung des angegebenen Protokoll-Parsers durch den Log Decoder, wenn Protokolle aus dieser Ereignisquelle analysiert werden. **Hinweis:** Bitte lassen Sie das Feld leer, wenn Sie nicht sicher sind, welcher Protokoll-Parser verwendet werden soll.
Name	Geben Sie der ODBC-Ereignisquelle einen Namen (z. B **ActivIdentity ActivCard AAA Server**).
maxVersion	Die Versionsnummer der Ereignisquelle (z. B. **6.4.1**).
Beschreibung	Eine Beschreibung der Ereignisquelle.
<Sammlung> Abschnitt	
odbc	Die Syntax unter `<odbc>` wird zur Ereignissammlung und -verarbeitung verwendet. Sie können mehrere Abfragen für den gleichen Ereignisquelltyp angeben, indem Sie `<query>`-Tags hinzufügen.

Parameter	Beschreibung
query	Dieser Abschnitt enthält die Details der Abfrage, die zum Sammeln von Informationen aus der Ereignisquelle verwendet wird.
etikett	Das Präfix-Tag, das Sie den Ereignissen während der Transformation hinzufügen möchten (z. B. **ActivIdentity**).
outputDelimiter	Geben Sie das Trennzeichen an, mit dem Felder getrennt werden sollen. Geben Sie einen der folgenden Werte ein: • || (senkrechte Striche) • ^ (Caret-Zeichen) • **,** (Komma) • **:** (Doppelpunkt) • **0x20** (zur Darstellung von Leerzeichen)
interval	Geben Sie die Anzahl der Sekunden zwischen Ereignissen an. Der Standardwert ist **60**.
dataQuery	Geben Sie die Abfrage an, mit der Daten aus der ODBC-Ereignisquellen-Datenbank für SQL-syntax abgerufen werden. Beispiel: `SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
maxTrackingQuery	Die Abfrage, die für den ersten Abruf von Ereignissen verwendet wird, um den Ausgangspunkt innerhalb des Datenvolumens zu identifizieren, ab dem mit dem Abrufen von Protokollen begonnen werden soll. Nach dem ersten Abruf wird diese Abfrage nicht mehr verwendet, sofern nicht der Wert **maxTracking** zurückgesetzt oder geändert wurde. Beispiel: `SELECT MAX(Event_Id) from ExEvents`
trackingColumn	Der Verfolgungsspaltenwert, der verwendet wird, wenn der ODBC Collector einen neuen Ereignissatz abruft.

Beispiel für eine Typespec-Datei für die ODBC-Sammlung

Das folgende Beispiel ist die Typespec-Datei für die Ereignisquelle „IBM ISS SiteProtector“.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>
```

```
   <name>siteprotector4_x</name>
   <type>odbc</type>
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

Das folgende Beispiel ist die Typespec-Datei für die Ereignisquelle „Bit9-Sicherheitsplattform“.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
```

```
   <version>1.0</version>
   <author>Administrator</author>
   <description>Bit9 Events</description>

   <device>
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
            SELECT
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from
ExEvents</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
```

```
        </query>
      </odbc>
   </collection>
</typespec>
```

Troubleshooting bei der ODBC-Sammlung

Sie können Probleme beheben und die ODBC-Sammlung überwachen, indem Sie die Informations-, Warn- und Fehlermeldungen im Protokoll des ODBC Collector bei der Ausführung der Sammlung überprüfen.

Jede ODBC-Protokollmeldung umfasst folgende Elemente:

- Zeitstempel
- Kategorie: `debug`, `info`, `warning` oder `failure`
- Sammlungsmethode = `OdbcCollection`
- ODBC-Ereignisquelltyp (GOTS-Name) = Generischer ODBC-Typspezifikationsname, den Sie für die Ereignisquelle konfiguriert haben.
- Sammlungsfunktion abgeschlossen oder versucht (z. B. `[processing]`)
- ODBC-Ereignisquellenname (DSN-Name) = Datenquellenname, den Sie für die Ereignisquelle konfiguriert haben.
- Beschreibung (z. B. Anzahl der vom Log Collector gesammelten Ereignisse)
- Nachverfolgungs-ID = die Log Collector-Position in der Zieldatenbanktabelle

Das folgende Beispiel zeigt die Meldung, die Sie nach erfolgreicher Sammlung eines ODBC-Ereignisse erhalten würden:

```
2014-July-25 17:21:25 info (OdbcCollection) : [event-source]
[processing] [event-source] Published 100 ODBC events: last tracking
id: 2014-July-25 13:22:00.280
```

Das folgende Beispiel zeigt eine Meldung, die Sie erhalten würden, wenn bei der Sammlung eines ODBC-Ereignisses ein Fehler aufgetreten ist:

Protokollmeldung	`timestamp failure (OdbcCollection: [event-source] [processing][event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver] [event-source-type]Invalid object name 'object-name'.`
Mögliche Ursache	ODBC-Sammlung ist beim Zugriff auf den ODBC-Treiber oder auf die Zieldatenbank fehlgeschlagen.

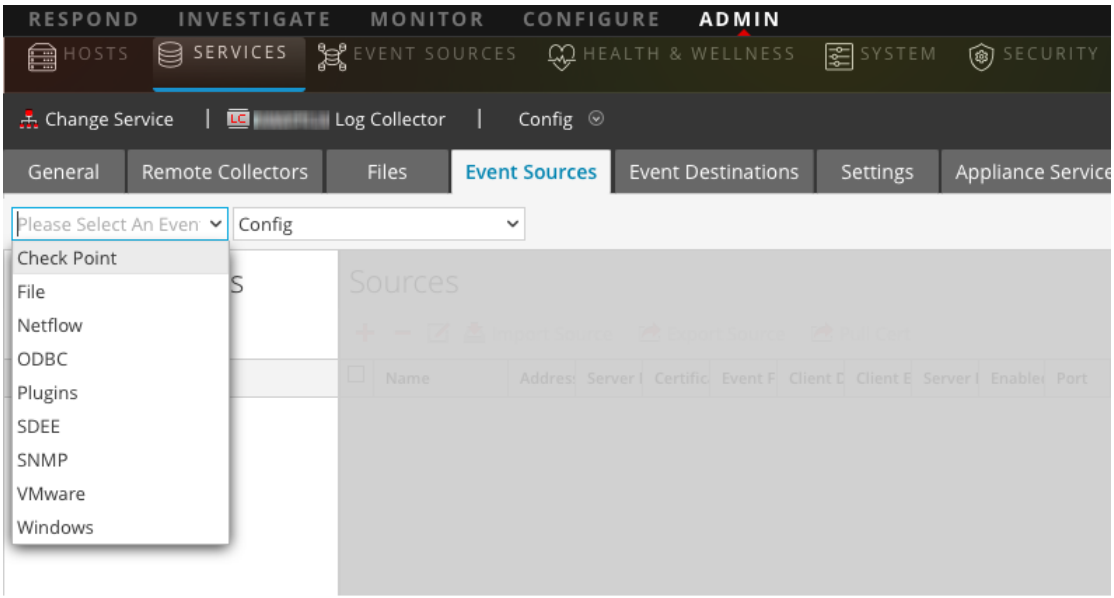
Lösungen	Überprüfen Sie die DSN-Wertpaare für die Ereignisquelle.

Konfigurieren von SDEE-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das SDEE-Sammelprotokoll konfigurieren.

So fügen Sie eine SDEE-Ereignisquelle hinzu:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **SDEE/Konfigurieren** aus.

   Der Bereich „Ereigniskategorien“ zeigt die konfigurierten SDEE-Ereignisquellen an, sofern vorhanden.

6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf +.

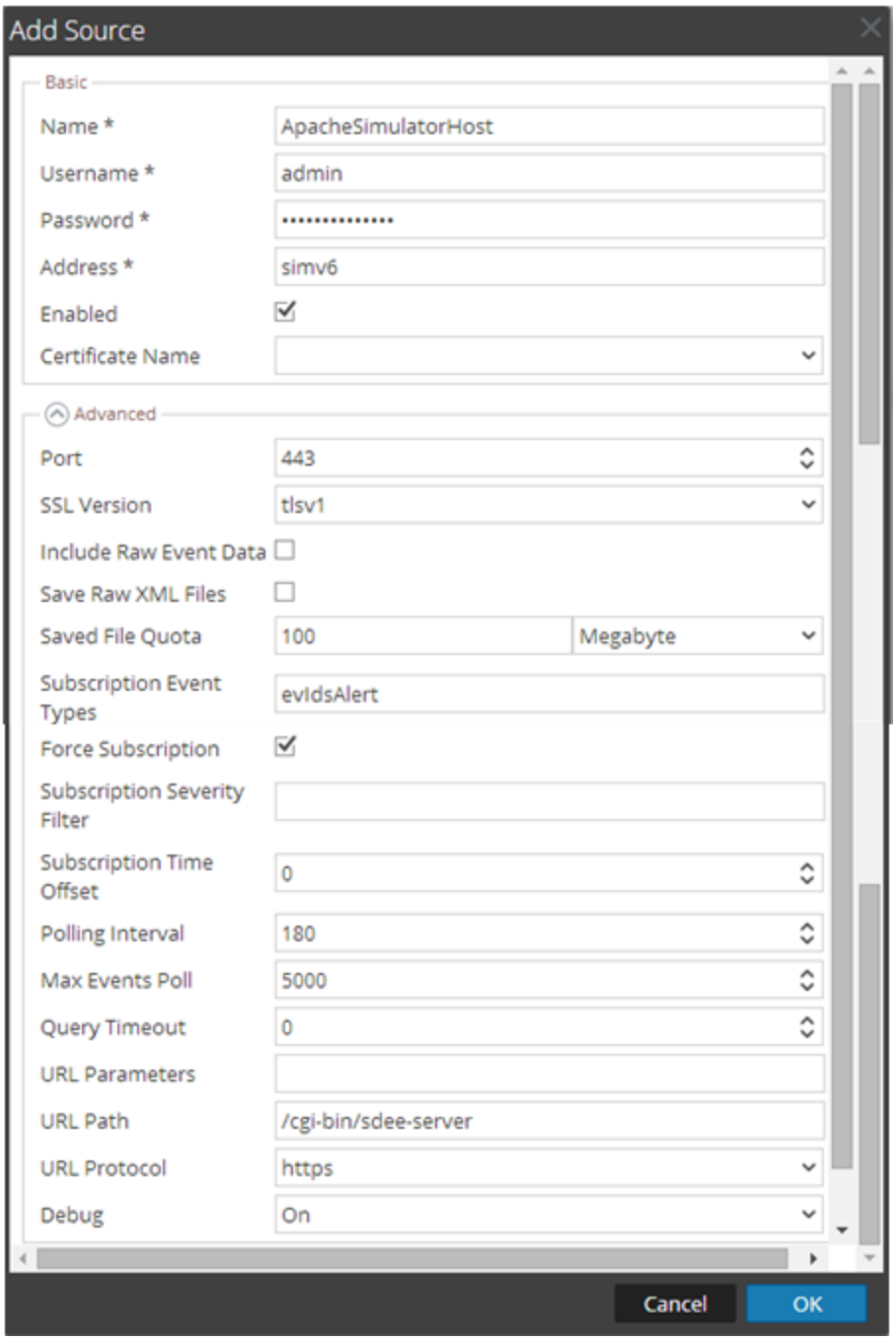
   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.

7. Wählen Sie einen Ereignisquelltyp aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.

8. Wählen Sie den neuen Typ im Bereich „Ereigniskategorien“ aus und klicken Sie in der Symbolleiste „Quellen“ auf +.

   Das Dialogfeld „Quelle hinzufügen“ wird angezeigt.



9. Geben Sie einen Namen, einen Benutzernamen, Adresse und Passwort ein, bearbeiten Sie die zu verändernden Parameter und klicken Sie auf **OK**.

Konfigurieren von SNMP-Ereignisquellen in NetWitness Suite

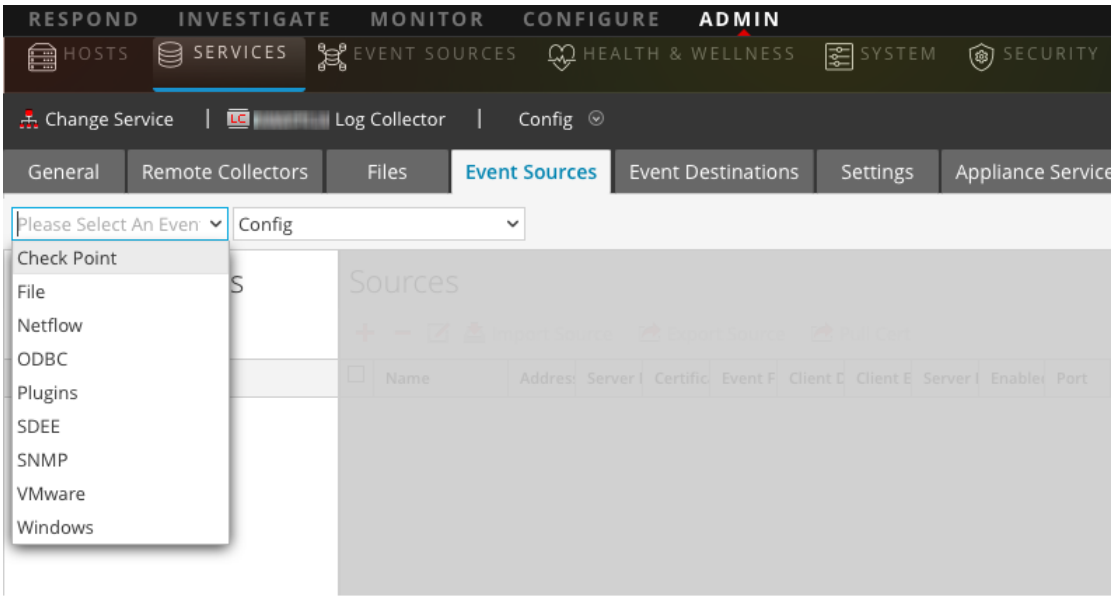
In diesem Thema erfahren Sie, wie Sie das SNMP-Sammlungsprotokoll konfigurieren.

Konfigurieren von SNMP-Trap-Ereignisquellen

So fügen Sie die SNMP-Ereignisquelle hinzu:

Hinweis: Wenn Sie zuvor den Typ **snmptrap** hinzugefügt haben, können Sie ihn nicht erneut hinzufügen. Sie können ihn bearbeiten oder Benutzer managen.

1. Navigieren Sie zu **ADMIN > Services** vom NetWitness Suite-Menü aus.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** im Drop-down-Menü die Option **SNMP/Konfigurieren** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf  .

   Das Dialogfeld **Verfügbare Ereignisquelltypen** wird angezeigt.
7. Wählen Sie den Ereignisquelltyp **snmptrap** aus und klicken Sie auf **OK**.

   Der neu hinzugefügte Ereignisquelltyp wird im Bereich **Ereigniskategorien** angezeigt.

8. Wählen Sie **snmptrap** im Bereich „Ereigniskategorien“ aus.
9. Wählen Sie **snmptrap** im Bereich „Quellen“ aus und klicken Sie auf das Symbol „Bearbeiten“ , um die Parameter bearbeiten.
10. Aktualisieren Sie die Parameter, die Sie ändern müssen, und klicken Sie auf **OK**.

(Optional) Konfigurieren von SNMP-Benutzern

Bei Verwendung von SNMPv3 führen Sie dieses Verfahren aus, um SNMPv3-Benutzer zu aktualisieren und zu verwalten.

Konfigurieren von SNMPv3-Benutzern

1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie im Raster **Services** einen **Log Collector**-Service aus.
3. Klicken Sie auf unter **Aktionen** und wählen Sie **Ansicht** > **Konfiguration** aus.
4. Wählen Sie auf der Registerkarte **Ereignisquellen** des Log Collector die Option **SNMP/SNMPv3-Benutzer-Manager** im Drop-down-Menü aus.

   Der Bereich „SNMPv3-Benutzer“ wird mit den vorhandenen Benutzern angezeigt, sofern vorhanden.
5. Klicken Sie auf , um das Dialogfeld **SNMP-Benutzer hinzufügen** zu öffnen.
6. Geben Sie die erforderlichen Parameter im Dialogfeld ein. Nachfolgend werden die verfügbaren Parameter beschrieben.

SNMP-Benutzerparameter

In der folgenden Tabelle werden die Parameter beschrieben, die Sie beim Erstellen eines SNMPv3-Benutzers eingeben müssen.

Parameter	Beschreibung
Benutzername*	Der Benutzername (oder in der korrekten SNMP-Terminologie: der Sicherheitsname). NetWitness Suite erstellt mit diesem Parameter und dem Parameter **Engine-ID** einen Benutzereintrag in der SNMP-Engine des Sammlungsservices. Die Kombination aus **Benutzername** und **Engine-ID** muss eindeutig sein (z. B. **logcollector**).

Parameter	Beschreibung
Engine-ID	(Optional) Die Engine-ID der Ereignisquelle. Für alle Ereignisquellen, die SNMPv3-Traps an diesen Sammlungsservice senden, müssen Sie den Benutzernamen und die Engine-ID der Ereignisquelle hinzufügen, die das Trap sendet. Für alle Ereignisquellen, die SNMPv3-Informationen senden, müssen Sie nur den Benutzernamen mit einer leeren Engine-ID hinzufügen.
Authentifizierungs-typ	(Optional) Das Authentifizierungprotokoll. Die folgenden Werte sind gültig: • **Keine** (Standard): Für Traps, die an diesen Service gesendet werden, kann nur die Sicherheitsstufe **noAuthNoPriv** verwendet werden. • **SHA**: Sicherer Hashalgorithmus • **MD5**: Message-Digest-Algorithmus **NICHT VERWENDEN: Wählen Sie „MD5“ nicht aus, da dieser Authentifizierungstyp einen Konflikt mit dem im FIPS-Modus ausgeführten Log Collector verursacht.**
Authentifizierungs passphrase	Optional, wenn der **Authentifizierungstyp** nicht festgelegt ist. Die Authentifizierungspassphrase.
Datenschutztyp	(Optional) Das Datenschutzprotokoll. Sie können diesen Parameter nur festlegen, wenn der Parameter „Authentifizierungstyp“ festgelegt ist. Die folgenden Werte sind gültig: • **Keine** (Standard) • **AES**: Advanced Encryption Standard • **DES**: Data Encryption Standard **NICHT VERWENDEN: Wählen Sie „DES“ nicht aus, da dieser Datenschutztyp einen Konflikt mit dem im FIPS-Modus ausgeführten Log Collector verursacht.**
Datenschutz-passphrase	Optional, wenn der **Datenschutztyp** nicht festgelegt ist. Datenschutzpassphrase.
Schließen	Schließt das Dialogfeld, ohne den SNMPv3-Benutzer hinzuzufügen oder Änderungen an den Parametern zu speichern.
Speichern	Fügt die SNMPv3-Benutzerparameter hinzu oder speichert Änderungen an den Parametern.

Konfigurieren der Syslog-Ereignisquellen für Remote Collector

In diesem Thema erfahren Sie, wie Sie Syslog-Ereignisquellen für den Log Collector konfigurieren.

Sie konfigurieren die Syslog-Sammlung nicht für Local Log Collectors. Sie müssen die Syslog-Sammlung nur für Remote Collectors konfigurieren.

Konfigurieren einer Syslog-Ereignisquelle

Syslog-Listener für UDP auf Port 514, TCP auf Port 514 und SSL auf Port 6514 werden standardmäßig erstellt. Sie sollten die SSL-Einstellungen auf den TCP- und SSL-Listenern nicht ändern. Wenn Sie SSL-Zertifikatüberprüfung benötigen, erstellen Sie einen neuen Ereignisquelltyp, um einen anderen Port zu überwachen. Beachten Sie, dass **Iptables** konfiguriert werden muss, um diesen Port zu öffnen.

So konfigurieren Sie den Remote Log Collector für die Syslog-Sammlung:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ einen Remote Log Collector und im Menü „Aktionen“ die Optionen  **> Ansicht > Konfigurieren** aus.
3. Wählen Sie die Registerkarte **Ereignisquellen** aus.
4. Wählen Sie im Drop-down-Menü die Option **Syslog/Konfigurieren** aus.

   Im Bereich Ereigniskategorien werden die konfigurierten Syslog-Ereignisquellen angezeigt, sofern vorhanden.

   Hinweis: Für RSA NetWitness Suite sind einige Syslog-Ereignisquellen standardmäßig verfügbar. In diesem Fall können Sie mit Schritt 6 fortfahren.

5. Klicken Sie in der Symbolleiste des Bereichs „Ereigniskategorien“ auf  .

   Das Dialogfeld „Verfügbare Ereignisquelltypen“ wird angezeigt.

6. Wählen Sie entweder **syslog-tcp** oder **syslog-udp** aus. Sie können je nach den Anforderungen Ihres Unternehmens eine oder beide Ereignisquellentypen festlegen.
7. Wählen Sie den neuen Typ im Bereich „Ereigniskategorien“ aus und klicken Sie in der Symbolleiste „Quellen“ auf  .

   Das Dialogfeld „Quelle hinzufügen“ wird angezeigt.

8. Geben Sie Portnummer ein und wählen Sie **Aktiviert** aus. Konfigurieren Sie optional erweiterte Parameter nach Bedarf.

   Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld zu schließen.

Wenn Sie einen oder beide Syslog-Typen konfiguriert haben, erfasst der Log Decoder oder der Remote Log Collector diese Meldungstypen aus allen verfügbaren Ereignisquellen. Daher können Sie weiterhin Syslog-Ereignisquellen zu Ihrem System hinzufügen, ohne dass Sie weitere Konfigurationen in RSA NetWitness Suite durchführen müssen.

Syslog-Parameter

In der folgenden Tabelle werden die verfügbaren grundlegenden und erweiterten Parameter für die Syslog-Konfiguration beschrieben.

Basisparameter

Name	Beschreibung
Port*	Der Standardport ist **514**.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
SSL-Empfänger	**Hinweis:** Dieser Parameter bezieht sich auf RSA NetWitness® Suite Version 11.1 oder neuer. Es ist nur für die Ereigniskategorie **syslog-Tcp** verfügbar. Wenn Sie das Kontrollkästchen auswählen, akzeptiert die Ereignisquelle nur SSL/TLS-Verbindungen. Wenn Sie diese Einstellung ändern, müssen Sie außerdem die Syslog-Sammlung beenden und neu starten, damit die Änderung wirksam wird.

Erweiterte Parameter

Name	Beschreibung
In Flight-Protokollveröffentlichungsschwellenwert	Legt einen Schwellenwert fest. Wenn dieser erreicht wird, erzeugt NetWitness eine Protokollnachricht, die Sie beim Beheben von Problemen mit dem Ereignisfluss unterstützt. Der Schwellenwert entspricht der Größe der Syslog-Ereignismeldungen, die gegenwärtig von der Ereignisquelle an NetWitness übertragen werden. Gültige Werte: • **0** (Standard): Deaktiviert die Protokollnachricht. • **100-100000000**: Erzeugt eine Protokollnachricht, wenn die aktuell von der Ereignisquelle an NetWitness weitergeleitete Syslog-Ereignismeldungen im Bereich von 100 bis 100.000.000 Byte liegt.
Max. Empfänger	Maximale Anzahl an Empfängerressourcen, die für die Verarbeitung der gesammelten Syslog-Ereignisse verwendet werden. Der Standardwert ist **2**.
Ereignisfilter	Wählen Sie einen Filter. Anweisungen zum Definieren von Filtern finden Sie unter Konfigurieren von Ereignisfiltern für einen Collector.

Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debugging (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).

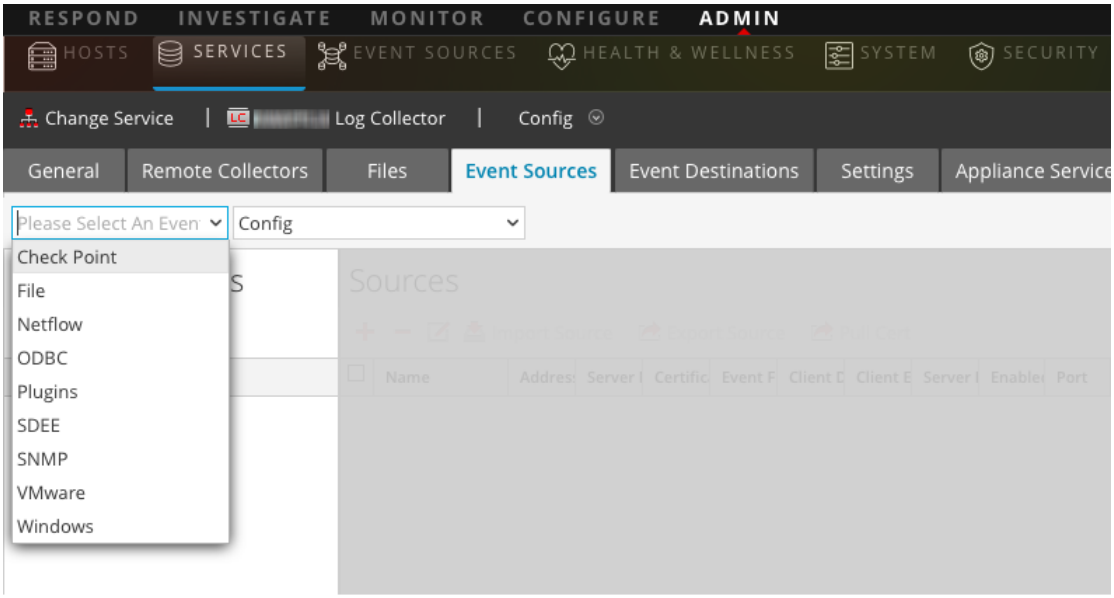
Name	Beschreibung
SSL-Überprüfungsmodus	**Hinweis:** Dieser Parameter bezieht sich auf RSA NetWitness® Suite Version 11.1 oder neuer. Es ist nur für die Ereigniskategorie **syslog-Tcp** verfügbar. Diese Einstellung ist nur relevant, wenn die Einstellung **SSL-Empfänger** ausgewählt ist. Wenn Sie den SSL-Überprüfungsmodus ändern, müssen Sie die Syslog-Sammlung beenden und neu starten, damit die Änderung wirksam wird. Verfügbare Optionen: • **verify-none**: (Standard) Der Server überprüft das Client-Zertifikat nicht, falls vorhanden. Ein Client kann sich verbinden, ohne ein Zertifikat zu präsentieren. • **verify-peer**: Der Server überprüft das Client-Zertifikat, falls vorhanden. Ein Client kann sich verbinden, ohne ein Zertifikat zu präsentieren. **Hinweis:** Wenn die Überprüfung fehlschlägt, wird eine Warnung protokolliert, aber die Nachrichten werden weiterhin akzeptiert. • **verify-peer-fail-if-no-cert**: Der Client muss ein Zertifikat präsentieren und der Server wird es überprüfen. **Hinweis:** Wenn Sie diesen Modus verwenden, ***muss*** das Client-CA-Zertifikat mithilfe der REST-API in den Log Collector-Truststore hochgeladen werden auf `http://LC-ip-address:50101/sys/caupload`

Konfigurieren von VMware-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das VMware-Sammlungsprotokoll konfigurieren.

So fügen Sie eine VMware-Ereignisquelle hinzu:

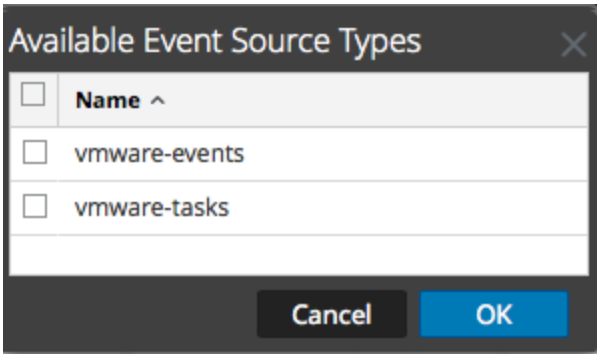
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie auf der Registerkarte **Ereignisquellen** des Log Collector die Option **VMware/Konfigurieren** im Drop-down-Menü aus.

   Im Bereich Ereigniskategorien werden ggf. die konfigurierten VMware-Ereignisquellen angezeigt.

6. Klicken Sie auf +, um das Dialogfeld **Verfügbare Ereignisquelltypen** zu öffnen.



7. Wählen Sie im Dialogfeld „Verfügbare Ereignisquelltypen“ den Eintrag **vmware-events** oder **vmware-tasks** und klicken Sie auf **OK**.

Es gibt die folgenden verfügbaren VMware-Ereignisquelltypen:

- **vmware-events:** Richten Sie vmware-events ein, um Ereignisse von vCenter-Servern und ESX/ESXi-Servern zu sammeln.
- **vmware-tasks:** (Optional) Richten Sie vmware-tasks ein, um Aufgaben von vCenter-Servern zu sammeln.

8. Wählen Sie den neuen Typ im Bereich „Ereigniskategorien“ aus und klicken Sie in der Symbolleiste „Quellen“ auf +.
9. Geben Sie Name, Benutzername und Passwort an und ändern Sie gegebenenfalls weitere Parameter.

   Achtung: Wenn Sie den Domainnamen als Teil des Benutzernamens eingeben müssen, müssen Sie als Trennzeichen einen doppelten umgekehrten Schrägstrich verwenden. Beispiel: Wenn der Domain\Benutzername corp\smithj lautet, müssen Sie **corp\\smithj** angeben.

10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

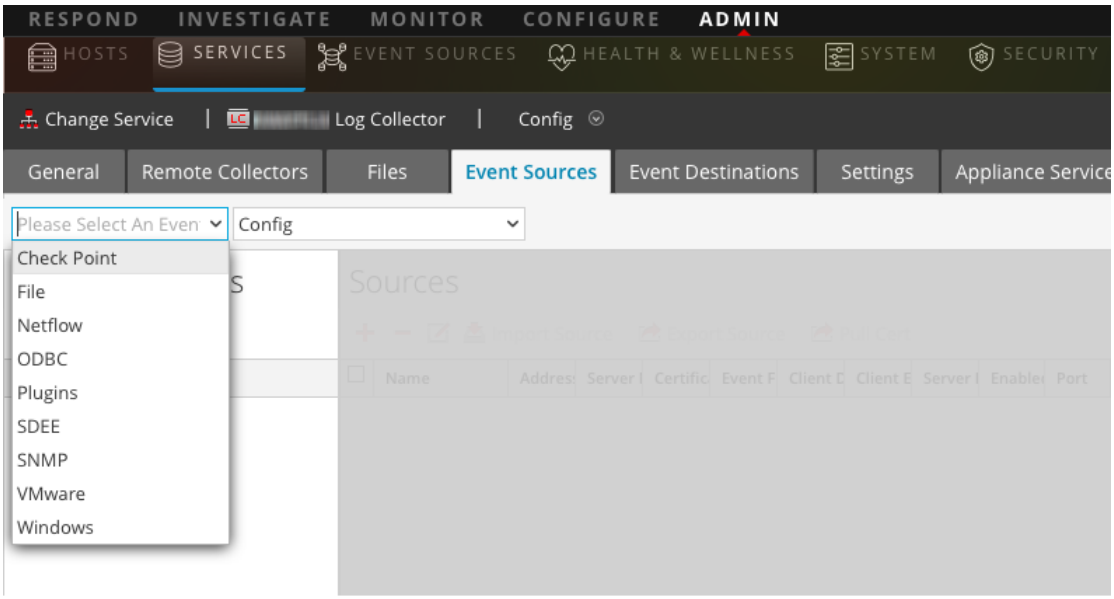
Konfigurieren Sie Windows-Ereignisquellen in NetWitness Suite

In diesem Thema erfahren Sie, wie Sie das Windows-Sammlungsprotokoll konfigurieren.

In RSA NetWitness Suite müssen Sie den Kerberos-Bereich konfigurieren und dann den Typ der Windows-Ereignisquelle hinzufügen.

So konfigurieren Sie den Kerberos-Bereich für die Windows-Sammlung:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.



5. Wählen Sie **Windows/Kerberos-Bereich** im Drop-down-Menü aus.
6. Klicken Sie in der Symbolleiste des Bereichs „Kerberos-Bereichsnamenkonfiguration“ auf +, um einen neuen Bereich hinzuzufügen.

   Das Dialogfeld „Kerberos-Domain hinzufügen“ wird angezeigt.
7. Geben Sie die Parameter anhand der folgenden Guidelines an.

Parameter	Details
Kerberos-Bereichsname	Geben Sie den Bereichsnamen in Großbuchstaben ein. Beispiel: DSNETWORKING.COM. Beachten Sie, dass die Parameter unter „Zuordnungen“ automatisch mit Variationen des Bereichsnamens ausgefüllt werden.
KDC-Hostname	Geben Sie den Namen des Domaincontroller ein. Verwenden Sie hier ***nicht*** einen vollständig qualifizierten Namen: Geben Sie einfach nur den Hostnamen des Domain-Controllers ein. **Hinweis:** Vergewissern Sie sich, dass der Log Collector als DNS-Client für den Unternehmens-DNS-Server konfiguriert ist. Andernfalls hat der Log Collector keine Möglichkeit, den Kerberos-Bereich zu suchen.
Admin-Server	(Optional) Der Name des Kerberos-Administrationsservers im FQDN-Format.

8. Klicken Sie auf **Speichern**, um die Kerberos-Domain hinzuzufügen.

So fügen Sie eine Windows-Ereignisquelle hinzu:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie auf der Registerkarte **Ereignisquellen** des Log Collector die Option **Windows/Konfiguration** im Drop-down-Menü aus.

   Im Bereich Ereigniskategorien werden ggf. die konfigurierten VMware-Ereignisquellen angezeigt.

Fügen Sie dann vom aktuellen Bildschirm aus eine Windows-Ereigniskategorie und einen Windows-Ereignistyp hinzu.

So konfigurieren Sie den Windows-Ereignistyp:

1. Wählen Sie im Drop-down-Menü die Option **Windows/Konfiguration** aus.
2. Klicken Sie in der Symbolleiste des Bereichs „Ereigniskategorien“ auf  , um eine Quelle hinzuzufügen.

   Das Dialogfeld „Quelle hinzufügen“ wird angezeigt.

3. Geben Sie die Parameter anhand der folgenden Guidelines an.

Parameter	Details
Alias	Geben Sie einen beschreibenden Namen ein.
Autorisierungsmethode	Wählen Sie **Verhandeln** aus.
Channel	Für die meisten Ereignisquellen, die die Windows-Sammlung verwenden, sollten Sie Daten aus den Kanälen **Sicherheit**, **System** und **Anwendung** sammeln.
Benutzername	Geben Sie den Kontonamen für das Windows-Benutzerkonto ein, das Sie zuvor für die Kommunikation mit NetWitness festgelegt haben. Beachten Sie, dass Sie den vollständigen Kontonamen eingeben müssen, der die Domain enthält. Beispiel: **rsalog@DSNETWORKING.COM**.
Passwort	Geben Sie das richtige Passwort für das Benutzerkonto ein.
Max. Ereignisse pro Zyklus	(Optional). RSA empfiehlt, dass Sie diesen Wert auf 0 festlegen, mit dem alles gesammelt wird.
Polling-Intervall	(Optional). Für die meisten Benutzer sollte ein Wert von **60** ausreichen.

4. Klicken Sie auf **OK**, um die Quelle hinzuzufügen.

   Die neu hinzugefügte Windows-Ereignisquelle wird im Bereich Ereigniskategorien angezeigt.

5. Wählen Sie die neue Ereignisquelle im Bereich „Ereigniskategorien“ aus.

   Der Bereich **Hosts** wird aktiviert.

6. Klicken Sie in der Symbolleiste des Bereichs „Hosts“ auf  .

7. Geben Sie die Parameter anhand der folgenden Guidelines an.

Parameter	Details
Ereignisquellenadresse	Geben Sie die IP-Adresse des Windows-Hosts ein.
Port	Übernehmen Sie den Standardwert **5985**.
Transportmodus	Geben Sie **http** ein.
Aktiviert	Vergewissern Sie sich, dass das Kontrollkästchen aktiviert ist.

8. Klicken Sie auf **Verbindung testen**.

Hinweis: Sie sollten die Verbindung erfolgreich testen können, selbst wenn der Windows-Service nicht ausgeführt wird.

Weitere Informationen zu den vorherigen Schritten finden Sie in den folgenden Hilfethemen im NetWitness Suite-Benutzerhandbuch:

- Konfigurieren des Windows-Sammlungsprotokolls: https://community.rsa.com/docs/DOC-43410
- Microsoft WinRM-Konfigurationsleitfaden: https://community.rsa.com/docs/DOC-58163
- Leitfaden zum Testen und Troubleshooting von Microsoft WinRM: https://community.rsa.com/docs/DOC-58164

Konfiguration für Windows-Legacy- und NetApp-Sammlung

Dieses **Windows-Legacy**-Protokoll sammelt Ereignisse aus Windows-Legacy-Ereignisquellen (Windows 2003 oder früher) und CIFS-Auditereignisse aus NetApp ONTAP-Ereignisquellen.

Sie müssen die Protokollsammlung bereitstellen, d. h. einen Local Collector und einen Windows-Legacy-Remote-Collector einrichten, bevor Sie das Windows-Legacy-Sammlungsprotokoll konfigurieren können.

Funktionsweise der Windows-Legacy- und NetApp-Sammlung

Sie verwenden das Windows-Legacy-Sammlungsprotokoll zum Konfigurieren von NetWitness Suite für die Sammlung von Ereignissen aus:

- Microsoft Windows-Legacy-Ereignisquellen (Ereignisquellen von Windows 2003 und früher)
- NetApp-Ereignisquellen

Ereignisquellen aus Windows 2003 und früher

Windows-Legacy-Ereignisquellen stammen aus älteren Windows-Versionen (wie Windows 2000 und Windows 2003). Das Windows-Legacy-Sammlungsprotokoll führt Sammlungen aus Windows-Ereignisquellen durch, die bereits für die enVision-Sammlung konfiguriert worden sind, ohne dass sie neu konfiguriert werden müssen. Sie richten diese Ereignisquellen unter dem Ereignisquelltyp Windows ein.

NetApp-Ereignisquellen

NetApp-Appliances, in denen Data ONTAP ausgeführt wird, unterstützen ein aktives Auditing-Framework, das Windows Server ähnelt. Ist dieses Framework konfiguriert, generiert und speichert es Auditereignisse im Windows-Dateiformat .evt. Das Windows-Legacy-Sammlungsprotokoll unterstützt die Sammlung von Ereignissen aus diesen NetApp-Dateien mit der Erweiterung .evt. Sie richten diese Ereignisquellen unter dem Ereignisquelltyp netapp_evt ein.

Die NetApp-Data-ONTAP-Appliance ist so konfiguriert, dass CIFS-Auditingereignisse generiert werden und regelmäßig als .evt-Dateien in einem Format gespeichert werden, das den Zeitstempel im Dateinamen aufweist. Weitere Informationen finden Sie im Konfigurationsleitfaden für ONTAP-Ereignisquelldaten der Network Appliance auf RSA Link. Im Sammlungsprotokoll wird der Zeitstempel der zuletzt verarbeiteten .evt-Datei gespeichert, um den Sammlungsstatus nachzuverfolgen.

Spezifische NetApp-Parameter

Die meisten Parameter, die im Dialogfeld Quelle hinzufügen/bearbeiten zur Verfügung stehen, gelten sowohl für Windows-Legacy- als auch für NetApp-Ereignisquellen.

Folgende zwei Parameter gelten allerdings nur für die NetApp-Ereignisquellen.

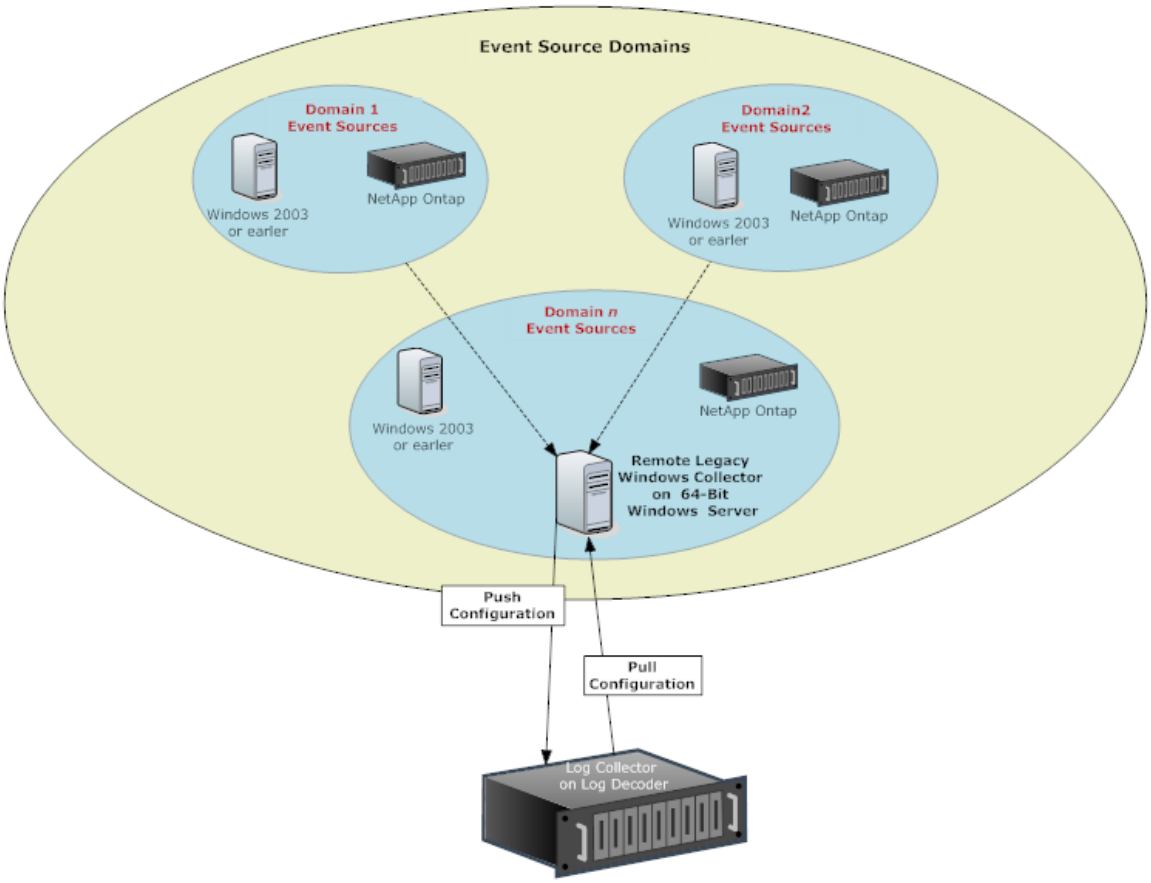
- **Ereignisverzeichnispfad**: Die NetApp-Appliance erzeugt Ereignisdaten und speichert sie in .evt-Dateien in einem gemeinsam nutzbaren Verzeichnis in der NetApp-Appliance. NetWitness Suite erfordert, dass Sie diesen Verzeichnispfad im Parameter „Ereignisverzeichnispfad“ angeben.
- **Ereignisdateipräfix**: Ähnlich wie beim Ereignisverzeichnispfad müssen Sie auch bei NetWitness Suite das Präfix (z. B. adtlog.) der Ereignisdaten in den .evt-Dateien angeben, damit NetWitness Suite diese Daten verarbeiten kann.

In jedem Abfragezyklus sucht NetWitness Suite im konfigurierten freigegebenen NetApp-Pfad nach den **.evt**-Dateien, die Sie über die Parameter „Ereignisverzeichnispfad“ und „Ereignisdateipräfix“ angegeben haben. NetWitness Suite:

- sortiert die Dateien, die dem Format Ereignisdateipräfix.JJMMTThhmmss.evt entsprechen, in aufsteigender Reihenfolge.
- verwendet den Zeitstempel der zuletzt verarbeiteten Datei, um die Dateien zu ermitteln, die noch verarbeitet werden müssen. Wenn NetWitness Suite eine noch nicht vollständig verarbeitete Datei findet, werden die bereits verarbeiteten Ereignisse übersprungen.

Bereitstellungsszenario

Mit dem Windows-Legacy-Protokoll werden Ereignisdaten aus Ereignisquellen von Windows 2003 oder früher und aus Ereignisquellen der NetApp-ONTAP-Appliance gesammelt. Der Windows Legacy Remote Collector ist der Windows Legacy Collector von Security Analytics, der in Ihrer Ereignisquellendomain auf einem physischen oder virtuellen Windows 2008-64-Bit-Server installiert ist.



Einrichten des Windows Legacy Collector

In diesem Thema erfahren Sie, wo Sie die ausführbaren Dateien und Anweisungen finden, die Sie zur Installation oder zum Upgrade des Windows-Legacy-Collectors in Ihren Windows-Legacy-Domains benötigen.

Installieren Sie den Windows Legacy Collector von NetWitness Suite auf einem physischen oder virtuellen 64-Bit-Server mit Windows 2008 R2 SP1. Verwenden Sie hierzu die Datei **NWLegacyWindowsCollector-11.*Versionsnummer.exe***. Laden Sie die Datei **NWLegacyWindowsCollector-11.*Versionsnummer.exe*** von RSA Link herunter. Detaillierte Anweisungen zur Installation oder zur Durchführung eines Upgrades der Windows-Legacy-Sammlung finden Sie in *NetWitness 11.x – Windows Legacy-Sammlung – Upgrade- und Installationsanweisungen*.

Hinweis: Während der Installation sollte die Microsoft Management Console (MMC) geschlossen werden.

Konfigurieren von Windows-Legacy- und NetApp-Ereignisquellen

In diesem Thema erfahren Sie, wie Sie Windows-Legacy-Ereignisquellen in NetWitness Suite konfigurieren.

Mit dem Windows-Legacy-Protokoll werden Ereignisdaten aus Ereignisquellen von Windows 2003 oder früher und aus NetApp-Ereignisquellen gesammelt.

Voraussetzungen

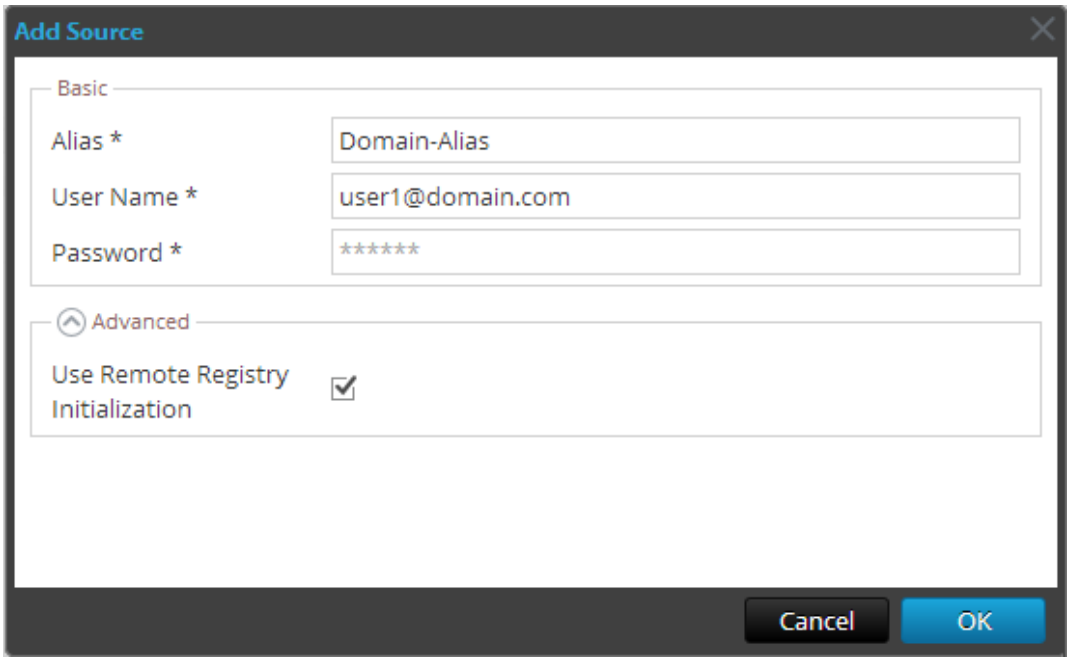
Bevor Sie eine Windows-Legacy-Ereignisquelle konfigurieren, müssen folgende Voraussetzungen erfüllt sein:

1. Der Windows-Legacy-Remote-Collector von NetWitness Suite muss auf einem physischen oder virtuellen 64-Bit-Server mit Windows 2008 installiert sein.
2. Dieser Windows-Legacy-Remote-Collector muss NetWitness Suite hinzugefügt worden sein.

Hinzufügen einer Windows-Legacy-Ereignisquelle

1. Wählen Sie zum Zugreifen auf die Ansicht „Services“ im Menü NetWitness Suite die Optionen **Administration > Services** aus.
2. Wählen Sie im Raster **Services** einen **Windows Legacy Log Decoder**-Service aus.
3. Wählen Sie unter „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisquellen**.
5. Wählen Sie auf der Registerkarte **Ereignisquellen** eine der folgenden Optionen aus dem Drop-down-Menü aus.
   - Windows Legacy/Windows
   - Windows Legacy/NetApp
6. Konfigurieren des Alias:
   a. Klicken Sie in der Symbolleiste des Bereichs **Ereigniskategorien** auf  .

      Das Dialogfeld **Quelle hinzufügen** wird angezeigt.
   b. Geben Sie Werte für die Parameter an und klicken Sie auf **OK**.



Hinweis: Das Kontrollkästchen **Remoteinitialisierung der Registry verwenden** ist standardmäßig aktiviert. Weitere Informationen finden Sie unten stehend unter Remotezugriff auf die Registry.

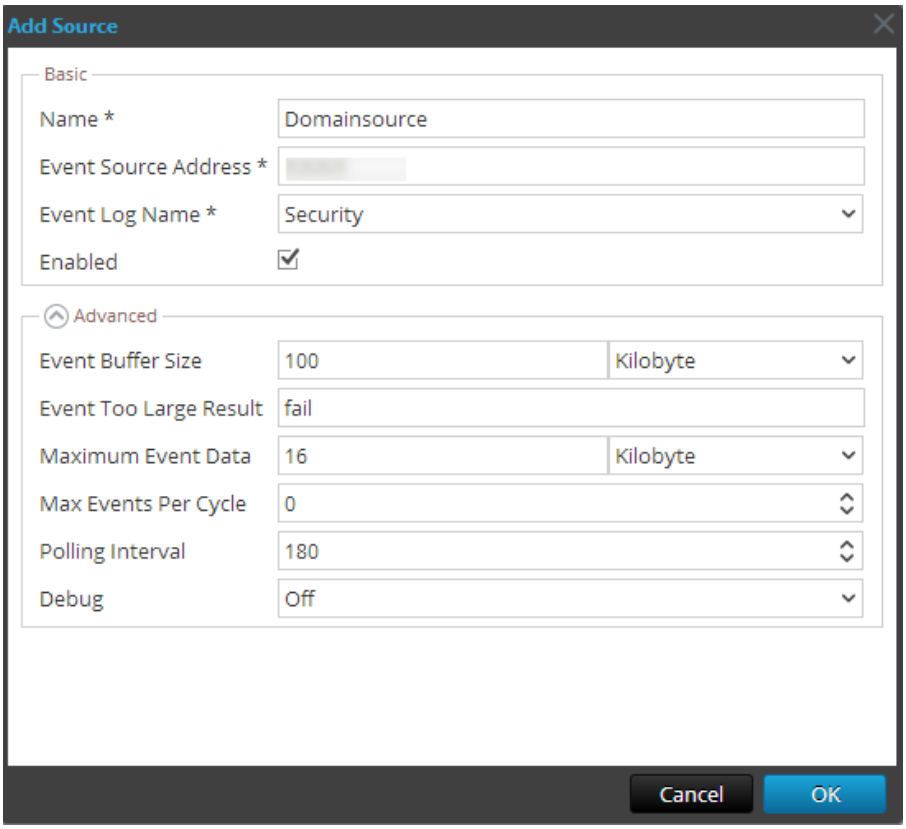
Der neu hinzugefügte **Windows**-Ereignisquelltyp wird im Bereich Ereigniskategorien angezeigt.

7. Fügen Sie die Ereignisquelle hinzu:

   a. Wählen Sie den neuen Alias im Bereich **Ereigniskategorien** aus und klicken Sie auf + in der Symbolleiste des Bereichs **Quelle**.

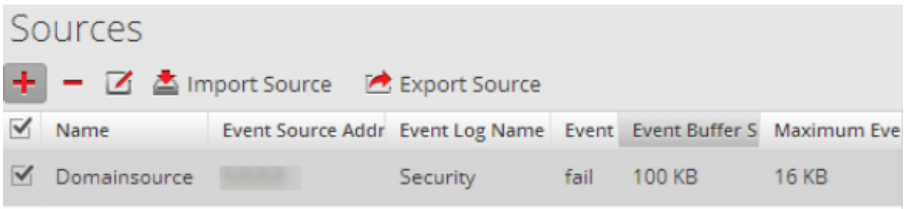
      Das Dialogfeld **Quelle hinzufügen** wird angezeigt.

   b. Geben Sie Werte für die Ereignisquellparameter an und klicken Sie auf **OK**.



Weitere Informationen finden Sie unten stehend unter Konfigurationsparameter für Windows Legacy.

Die neu hinzugefügte Windows-Ereignisquelle wird im Bereich **Ereigniskategorien** angezeigt.



Remotezugriff auf die Registry

Windows Legacy Collector führt vor der Sammlung der Daten zunächst eine Überprüfung der Ereignisquelle durch. Standardmäßig verwendet die Windows Legacy Collector die Methode Windows Management Instrumentation (WMI), um diese anfängliche Überprüfung durchzuführen. Wenn Sie die Methode des Remotezugriffs auf die Registry aktivieren, führt die Windows Legacy Collector eine Remote-Registry-Abfrage durch, um die Ereignisquelle zu überprüfen.

Konfigurieren von Push oder Pull zwischen Log Collector und Windows Legacy Collector

Sie können den Windows Legacy Collector so konfigurieren, dass Ereignisdaten auf einen Local Collector übertragen werden, oder Sie können einen Local Collector so konfigurieren, dass er Ereignisdaten vom Windows Legacy Collector abruft.

So konfigurieren Sie einen Local Collector oder den Windows Legacy Collector:

1. Navigieren Sie zu **ADMIN > Services.**
2. Wählen Sie einen Local Collector oder den Windows Legacy Collection-Service aus.
3. Wählen Sie unter „Aktionen“  **> Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Führen Sie je nach Ihrer Auswahl in Schritt 2 folgende Schritte durch:
   - Bei Auswahl eines Local Collector wird die Registerkarte **Remote Collectors** angezeigt. Wählen Sie auf dieser Registerkarte den Windows Legacy Collector aus, von dem der Local Collector Ereignisse abrufen soll.
   - Wenn Sie einen Windows Legacy Collector ausgewählt haben, wird die Registerkarte **Local Collectors** angezeigt. Wählen Sie auf dieser Registerkarte die Local Collectors aus, auf die der Windows Legacy Collector Ereignisse übertragen soll.

Konfigurationsparameter für Windows Legacy

In der folgenden Tabelle werden die Parameter für eine Windows-Legacy-Ereignisquelle beschrieben.

Funktion	Beschreibung
	Basic
Name*	Der Name der Ereignisquelle. Ein gültiger Wert ist ein Name im Bereich **[_a-zA-Z] [_a-zA-Z0-9]***. Sie können einen Trennstrich **-** als Teil des Namens verwenden.
Ereignisquellenadresse*	IP-Adresse der Ereignisquelle. Ein gültiger Wert ist eine IPv4-Adresse, eine IPv6-Adresse oder ein Hostname, der einen vollständig qualifizierten Domainnamen enthält. NetWitness Suite weist standardmäßig **127.0.0.1** zu. Log Collector konvertiert den Hostnamen in Kleinbuchstaben, um doppelte Einträge zu verhindern.

Funktion	Beschreibung
Ereignisprotokollname	Der Name des Ereignisprotokolls, aus dem Ereignisdaten gesammelt werden (z. B. **System**, **Anwendung** oder **Sicherheit**). Im Folgenden sehen Sie einige Beispiele für diese Kanäle: • **System**: Anwendungen, die unter Systemservicekonten (installierten Systemservices) ausgeführt werden, Treiber oder eine Komponente oder Anwendung, die Ereignisse bezüglich der Integrität des Systems hat. • **Anwendung**: alle Anwendungen auf Benutzerebene. Dieser Kanal ist ungesichert und für jede beliebige Anwendung offen. Wenn eine Anwendung umfangreiche Informationen enthält, sollten Sie für sie einen anwendungsspezifischen Kanal definieren. • **Sicherheit**: das Windows-Auditprotokoll (Ereignisprotokoll), das ausschließlich für die Windows Local Security Authority verwendet wird.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um Daten von dieser Ereignisquelle abzurufen. Wenn Sie dieses Kontrollkästchen nicht aktivieren, ruft der Log Collector keine Ereignisse von dieser Ereignisquelle ab.

Funktion	Beschreibung
Ereignisverzeichnispfad	Verzeichnispfad für **EVT- oder EVTX**-Dateien in NetApp. Es muss ein UNC-Pfad sein. NetApp generiert Ereignisdaten und speichert diese in EVT- oder EVTX-Dateien in einem gemeinsam nutzbaren Verzeichnis in der NetApp-Appliance. • In jedem Abfragezyklus sucht Log Collector im konfigurierten freigegebenen NetApp-Pfad nach den EVT-Dateien, die Sie über die Parameter **Ereignisverzeichnispfad** und **Ereignisdateipräfix** angegeben haben. Log Collector: ◦ sortiert Dateien, die dem Format event-file-prefix.**JJMMTThhmmss.evt** entsprechen, in aufsteigender Reihenfolge. ◦ verwendet den Zeitstempel der letzten verarbeiteten Datei, um die Dateien zu bestimmen, die noch verarbeitet werden müssen. Wenn Log Collector eine noch nicht vollständig verarbeitete Datei findet, werden die bereits verarbeiteten Ereignisse übersprungen. • In jedem Abfragezyklus sucht Log Collector im konfigurierten freigegebenen NetApp-Pfad nach den **EVTX**-Dateien, die Sie über die Parameter **Ereignisverzeichnispfad** und **Ereignisdateipräfix** angegeben haben. Log Collector: ◦ sortiert Dateien, die dem Format **event-file-prefix.JJMMTThhmmssms.evtx** entsprechen, in aufsteigender Reihenfolge. ◦ verwendet den Zeitstempel der letzten verarbeiteten Datei, um die Dateien zu bestimmen, die noch verarbeitet werden müssen. Wenn Log Collector eine noch nicht vollständig verarbeitete Datei findet, werden die bereits verarbeiteten Ereignisse übersprungen.
Ereignisdateipräfix	Präfix der **EVT**-Dateien (z. B. **adtlog.**), die im **Ereignisverzeichnispfad** gespeichert sind.
Erweitert	

Funktion	Beschreibung
Ereignispuffergröße	Maximale Größe der Daten, die der Log Collector bei jeder Abfrage aus der Ereignisquelle abruft. Ein gültiger Wert ist eine Zahl im Bereich von **0** bis **511 Kilobyte**. Dieser Wert wird in **Kilobyte** angegeben.
Ereignisergebnis zu groß	Teilt dem Log Collector mit, was zu tun ist, wenn ein Ereignis zu groß für den Ereignispuffer ist.
Ereignisdatenmaximum	Maximale Größe der Ereignisdaten, die in der Ausgabe enthalten sein können. Ein gültiger Wert ist eine Zahl im Bereich von **0** bis **511 Kilobyte**. Dieser Wert wird in **Kilobyte** oder **Megabyte** angegeben. • 1 Kilobyte – 100 Megabyte • 0 = Keine Ereignisdaten in der Ausgabe einfügen.
Max. Ereignisse pro Zyklus	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch ausgeführt wird, wird gewartet, bis dieser Zyklus abgeschlossen ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.

Funktion	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus - fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu. Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich). Begrenzen Sie die Anzahl der Ereignisquellen, für die Sie ausführliches Debugging verwenden, um Auswirkungen auf die Performance zu minimieren.
Abbrechen	Schließt das Dialogfeld ohne die Windows-Legacy-Ereignisquelle hinzuzufügen.
OK	Fügt die aktuellen Parameterwerte als neue Ereignisquelle hinzu

Troubleshooting der Windows-Legacy- und NetApp-Sammlung

In diesem Thema werden mögliche Probleme behandelt, die im Zusammenhang mit der Windows-Legacy-Sammlung (LWC) auftauchen können, und mögliche Lösungen für diese Probleme vorgestellt.

Hinweis: Im Allgemeinen erhalten Sie robustere Protokollmeldungen, wenn Sie SSL deaktivieren.

Probleme beim Neustart des Protokolls

Problem	Mögliche Ursachen	Lösungen
Sie haben das Windows-Legacy-Sammlungsprotokoll neu gestartet, jedoch erhält NetWitness Suite keine Ereignisse.	Der Log Collector-Service wurde angehalten.	Starten Sie den **Log Collector**-Service neu. 1. Melden Sie sich beim **Windows Legacy Remote Collector** an. 2. Navigieren Sie zu **Start > Verwaltungstools > Aufgabenplaner** und klicken Sie auf **Aufgabenplanungsbibliothek**. 3. Suchen Sie im rechten Bereich nach der Aufgabe **restartnwlogcollector** und überprüfen Sie, ob diese ausgeführt wird. 4. Falls dies nicht der Fall ist, klicken Sie mit der rechten Maustaste auf **restartnwlogcollector** und wählen Sie **Ausführen**.

Installationsprobleme

Falls eine der folgenden Meldungen im **MessageBroker.log** angezeigt wird, liegt möglicherweise ein Problem vor.

Protokollmeldungen	Jede Meldung, die „rabbitmq“ enthält
Mögliche Ursache	Der RabbitMQ-Service wird möglicherweise nicht ausgeführt. Port **5671** ist möglicherweise nicht geöffnet.
Lösungen	Überprüfen Sie, ob der RabbitMQ-Service ausgeführt wird. Überprüfen Sie, ob Port **5671** geöffnet ist.

Protokollmeldungen	Fehler: Hinzufügen eines Log Collector-Benutzerkontos Fehler: Hinzufügen eines Administrator-Tags zum Log Collector-Konto Fehler: Hinzufügen des logcollection-vhosts Fehler: Festlegen der Berechtigungen für das Log Collector-Konto in allen vhosts.
Mögliche Ursache	**rabbitmq-Server** wurde nicht ausgeführt, als das Installationsprogramm versucht hat, Benutzer und vhosts zu erstellen.

Lösungen	Überprüfen Sie, ob der **RabbitMQ**-Service ausgeführt wird und führen Sie die unten stehenden Befehle manuell aus.
	`rabbitmqctl -q add_user logcollector netwitness`
	`rabbitmqctl -q set_user_tags logcollector administrator`
	`rabbitmqctl -q add_vhost logcollection`
	`rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*"`
	`rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"`

Probleme mit dem Windows-Legacy-Federation-Skript

Falls eine der folgenden Meldungen im Protokoll des Federation-Skripts angezeigt wird, liegt möglicherweise ein Problem vor.

Problem	Mögliche Symptome	Lösungen
Das Federation-Skript wurde gestartet, aber der LWC-Service ist ausgefallen.	Das NetWitness Suite-Protokoll zeigt Verbindungsfehlerausnahmen beim Windows Legacy Collector an.	Dieses Problem wird automatisch nach dem Neustart des Windows-Legacy-Services behoben.

Problem	Mögliche Symptome	Lösungen

LWC wird ausgeführt, aber der RabbitMQ-Service ist ausgefallen oder wird neu gestartet.	Die Federation-Protokolldatei auf der Windows-Legacy-Seite zeigt die Fehlermeldung an, dass der RabbitMQ-Service ausgefallen ist.
	Prüfen Sie folgende Protokolldatei: **C:\NetWitness\ng\logcollector**
	Eine Fehlermeldung wie die folgende wird protokolliert, wenn RabbitMQ nicht ausgeführt wird:
	`"Unable to connect to node logcollector@localhost: nodedown"`
	Daraufhin werden Diagnosemeldungen wie die folgenden angezeigt:
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost: * connected to epmd (port 4369) on localhost * epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084'] * suggestion: start the node`
		Führen Sie das Skript **federation.bat** manuell für LWC aus.
		Gehen Sie zur manuellen Ausführung des Skripts **federate.bat** wie folgt vor:
		1. Wechseln Sie zum Ordner **C:\Program Files\NwLogCollector**, in dem die Windows-Legacy-Instanz installiert ist.
		2. Suchen Sie die Datei **federate.bat** in diesem Ordner. Wählen Sie die Datei aus und klicken Sie mit der rechten Maustaste darauf.
		3. Wählen Sie **Als Administrator ausführen** aus.
		4. Zum Überwachen der Protokolldatei navigieren Sie zu **C:\NetWitness\ng\logcollector\federate.log**, während das Skript **federate.bat** ausgeführt wird.
		Hinweis: Vergewissern Sie sich, dass die Protokolldatei keine Fehler während der Ausführung des Skripts anzeigt.

Problem	Mögliche Symptome	Lösungen
Der RabbitMQ-Service ist auf der NetWitness Suite-Seite ausgefallen.	NetWitness Suite-Benutzeroberflächenseiten funktionieren nicht.	Starten Sie den RabbitMQ-Service neu.
Der Kunde erhält eine Benachrichtigung von „Integrität und Zustand“ oder der folgende Alarm von „Integrität und Zustand“ wird angezeigt: „Ausfall der Kommunikation zwischen dem NetWitness Suite-Masterhost und einem Remotehost“ mit dem LWC-Host als Remote-IP.	Das **federate.bat**-Skript konnte nicht erfolgreich ausgeführt werden.	Wenn das Skript **federate.bat** nicht ordnungsgemäß ausgeführt wurde, führen Sie es wie zuvor beschrieben manuell aus.

Windows-Protokollsammlung für Endpunkt-Agents

In Version 11.1 kann die Windows-Protokollsammlung mithilfe des RSA® NetWitness® Endpoint Insights Agent erreicht werden. Wenn der Agent für die Protokollsammlung aktiviert ist, wird eine Protokollkonfigurationsdatei mit dem Agent Packager mitgeliefert, um das Sammeln und Weiterleiten von Windows-Protokollen zusätzlich zu den Endpunktdaten zu ermöglichen. Die erzeugte Konfigurationsdatei enthält Informationen über die Kanäle, von denen Protokolle gesammelt werden sollen, und das Ziel (Log Decoder oder ein Remote Log Collector), um die definierten Windows-Ereignisse weiterzuleiten. Der generierte Agent Packager ist in der Lage, sowohl Endpunkt- als auch Windows-Protokolldaten von Hosts zu sammeln. Der Endpunkt-Agent-Packager wird lokal auf einem Windows-Computer extrahiert, um die Datei des Agent-Installationsprogramms zu erstellen. Die Datei des Installationsprogramms wird dann über ein Softwareverteilungstool eines Drittanbieters an alle Endgeräte in Ihrem Netzwerk verteilt..

Es gibt drei Szenarien für die Windows-Protokollsammlung, und zwar:

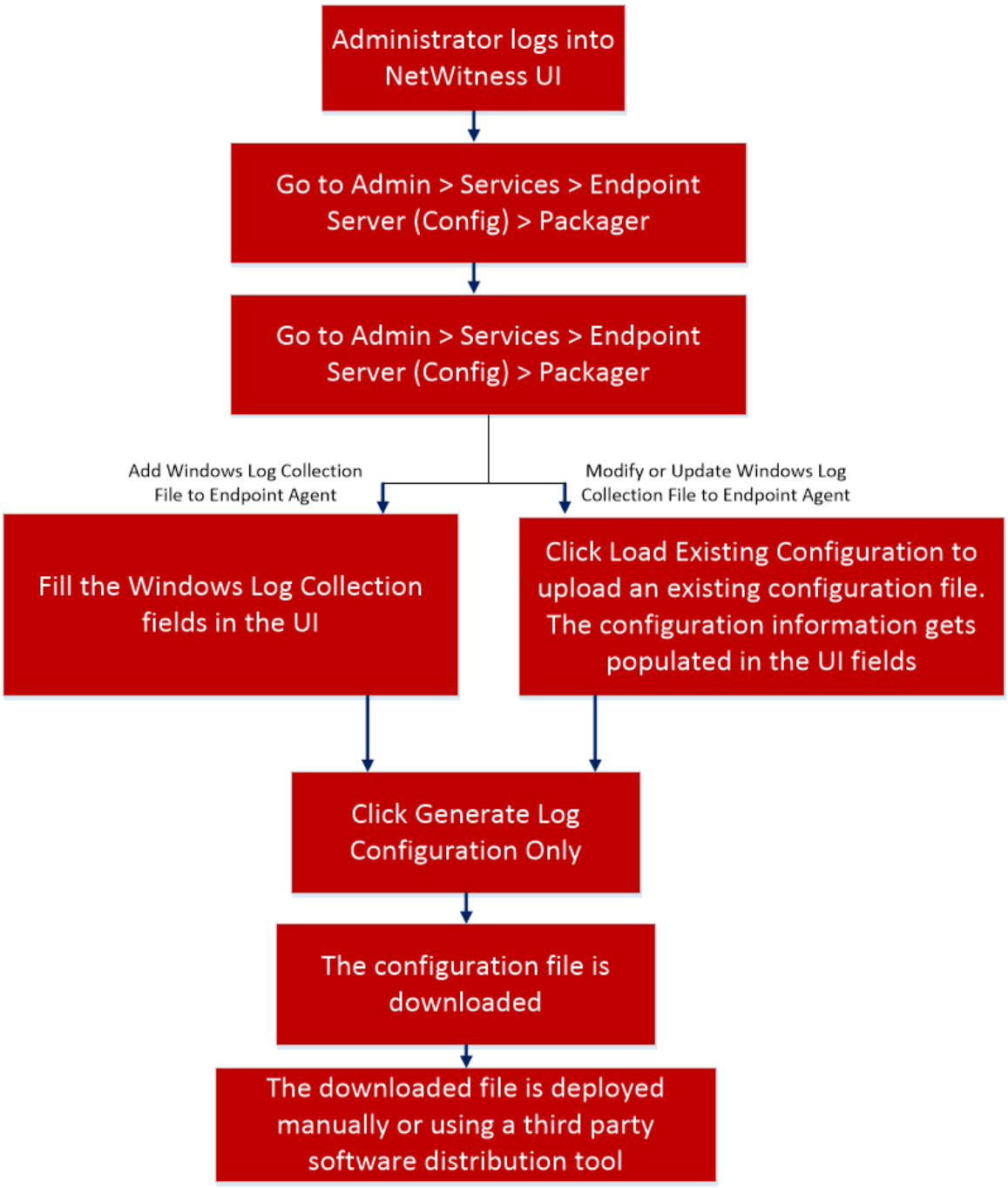
- **Erzeugen des Agent mit der Protokollsammlung**: Wenn die Option **Windows-Protokollsammlung aktivieren** aktiviert ist und Sie auf **Agent erzeugen** klicken, nachdem Sie die Details ausgefüllt haben Die erzeugte Datei AgentPackager.zip enthält die Protokollsammlungsdatei. Weitere Informationen finden Sie unter „Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung“ im *Endpoint Insights Agent-Installationshandbuch*.
- **Erzeugen nur einer Agent-Datei ohne Protokollsammlung**: Wenn **Windows-Protokollsammlung aktivieren** deaktiviert ist und Sie auf **Agent erzeugen** klicken, wird nur die Zip-Datei erstellt, ohne die Protokollsammlungsdatei. Weitere Informationen finden Sie unter „Erzeugen eines Endpoint-Agent-Packager“ im *Endpoint Insights Agent-Installationshandbuch*.
- Wenn Sie auf **Nur Protokollkonfiguration erzeugen** klicken, wird nur die Protokollkonfiguration erzeugt. Dies kann verwendet werden, um die Protokollkonfigurationsdatei in einer vorhandenen Endpoint-Agent-Bereitstellung für die Protokollsammlung zu aktualisieren oder um die Protokollkonfiguration zu einer Endpoint-Agent-Bereitstellung hinzuzufügen. Weitere Informationen finden Sie unter „Hinzufügen oder Aktualisieren einer Windows-Protokollsammlungskonfiguration zu einem installierten Endpoint-Agent“.

Hinzufügen oder Aktualisieren einer Windows-Protokollsammlungskonfiguration zu einem installierten Endpoint-Agent

Sie können eine Windows-Protokollsammlungs-Konfigurationsdatei zu einem Endpoint-Agent hinzufügen und auch eine vorhandene Protokollsammlungs-Konfigurationsdatei ändern. Wenn eine Änderung in der Protokollsammlungskonfiguration für Endpoint-Agents erforderlich ist, müssen die Agents nicht erneut installiert werden. Die Protokollkonfigurationsdatei (`nwelcfg file`) kann über die Packager-Benutzeroberfläche erzeugt und geändert werden.

Workflow

Dieser Workflow zeigt das Verfahren zum Hinzufügen oder Aktualisieren einer Windows-Protokollsammlungs-Konfigurationsdatei.



Es folgen einige Beispiele für Gründe, die eine Änderung in der Konfiguration erforderlich machen würden:

- Das Ziel, an das die Fenster weiterzuleiten sind, muss für ein besseres Lastmanagement auf der Zielseite geändert werden.

- Der Endpunkt wird in eine neue Gruppe verschoben, die von einem Endpunktmanagementsystem eines Drittanbieters definiert wird und eine Änderung des Ziels oder der Liste der weiterzuleitenden Ereignis-IDs erfordert.
- Es gibt Anforderungen, die Liste der Ereignis-IDs, die auf der Zielseite verbraucht werden, zu ändern.

Eine neue Konfigurationsdatei kann erzeugt werden, entweder indem die neuen Werte im Packager-Bildschirm eingegeben werden oder indem eine vorhandene Konfigurationsdatei geladen wird.

Hinweis: Der Endpunkt-Agent ist so konfiguriert, dass er die `nwelcfg`-Datei mit dem aktuellen Zeitstempel unter dem Ordner config liest. Stellen Sie daher sicher, dass das Drittanbieter-Tool zur Verwaltung von Endpunkten den Zeitstempel der Datei auf den aktuellen Zeitpunkt des Endpunkts aktualisiert, während die Konfigurationsdatei verschoben wird.

Befolgen Sie diese Schritte, um eine Windows-Protokollsammlungs-Konfigurationsdatei einem vorhandenen Endpoint-Agent hinzuzufügen oder zu aktualisieren:

1. Führen Sie in der Packager-Benutzeroberfläche einen der folgenden Schritte aus:
   a. Zum Hinzufügen der Windows-Protokollsammlungskonfiguration: Geben Sie die erforderlichen Informationen ein, die unter „Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung“ im *Endpoint Insights Agent-Installationshandbuch* erwähnt sind.
   b. Zum Aktualisieren der Windows-Protokollsammmlungskonfiguration: Klicken Sie auf **Vorhandene Konfiguration wird geladen** und bearbeiten Sie die gewünschten Felder, die unter „Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung“ im *Endpoint Insights Agent-Installationshandbuch* erwähnt sind.
2. Klicken Sie auf **Nur Protokollkonfiguration erzeugen**, um die `nwelcfg`Datei zu erzeugen.
3. Kopieren Sie die heruntergeladene `nwelcfg`-Datei auf den Endpunkt-Agent, von dem aus die Protokolle weitergeleitet werden sollen. Die Konfigurationsdatei sollte in den Ordner %ProgramData%\NWEAgent kopiert werden. Zum Bereitstellen der Konfigurationsdatei für mehrere Agents, verwenden Sie das Drittanbieter-Tool zur Verteilung der Software.

Der Agent ist so konzipiert, dass er die Protokollkonfigurationsdatei mit dem aktuellen Zeitstempel auswählt. Wenn ein Zeitzonenunterschied besteht, stellen Sie sicher, dass die Konfigurationsdatei nach dem Kopieren auf den Zeitstempel des Agent aktualisiert wurde. Dies kann durch Ausführen des Befehls auf dem Agent erreicht werden: `copy /b <filename.nwelcfg> +,,` aus dem Ordner %programdata%\NWEAgent\, in dem die Datei „nwelcfg“ vorhanden ist.

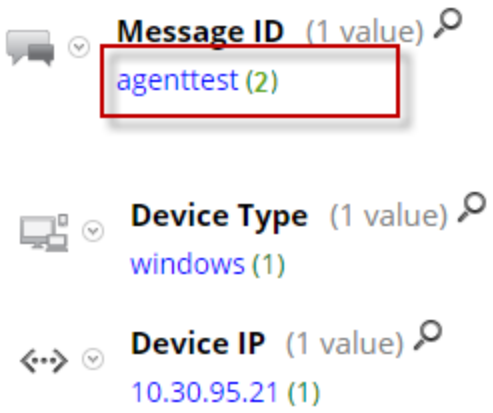
Überprüfen der Windows-Protokollsammlung

Um zu überprüfen, dass die Windows-Protokollsammlung auf einem Endpunkt-Agent erfolgreich bereitgestellt wurde, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu **ADMIN** > **Integrität und Zustand** > **Ereignisquellenüberwachung**.
2. Wählen Sie im Feld „Zeitrahmen“ **Letzte 5 Minuten** oder **Letzte 10 Minuten**, je nachdem, wann die Agents installiert wurden.
3. Klicken Sie auf **Anwenden.**
4. In der angezeigten Liste sollten die IP-Adressen des Agent in der Spalte „Ereignisquelle“ angezeigt werden, mit Ereignisquelltyp als Windows. Damit wird bestätigt, dass der Agent erfolgreich installiert wurde.

Um zu überprüfen, ob eine Windows-Protokollsammlung erfolgreich aktualisiert wurde, gehen Sie folgendermaßen vor:

1. Wechseln Sie zu **UNTERSUCHEN** > **Navigieren**. Warten Sie 2 bis 3 Minuten, bis diese Konfigurationsdatei vom Endpunkt-Agent ausgewählt ist.
2. Wählen Sie den **Concentrator** unter **Untersuchen** aus.
3. Ändern Sie den Zeitrahmen auf **Letzte 5 Minuten** oder nach Bedarf.
4. Klicken Sie auf **Werte laden**.
5. Suchen Sie nach dem Metaschlüssel „Meldung-ID“.
6. Es muss ein Wert „agent.test“ vorhanden sein. Eine Erhöhung der Anzahl der Ereignisse bedeutet, dass die Aktualisierung erfolgreich durchgeführt wurde.



Aktivieren von Protokollweiterleitung und Konfigurieren von Log Decoder

Wenn Sie die Protokollweiterleitungsfunktion aktivieren und den Log Decoder in Endpoint Hybrid als ein Ziel in der Packager-Benutzeroberfläche konfigurieren möchten. Dann müssen Sie die Ports TCP/UDP 514 in der Iptables-Datei auf Endpoint Hybrid hinzufügen.

Um die Ports hinzuzufügen, gehen Sie wie folgt vor:

1. Für TCP, müssen Sie der vorhandenen Liste der Ports in der `/etc/sysconfig/iptables`-Datei auf Endpoint Hybrid den Port „514“ hinzufügen:

   ```
   INPUT -p tcp -m tcp -m multiport --dports 514,
   6514,50002,50102,50202,56002,56202 -m comment --comment
   "nwlogdecoderPorts" -m conntrack --ctstate NEW -j ACCEPT -
   ```

2. Für UDP, müssen Sie in der `/etc/sysconfig/iptables`-Datei in Endpoint Hybrid den Inhalt unten hinzufügen:

   ```
   -A INPUT -p udp -m udp -m multiport --dports 514 -m comment --comment
   "nwlogcollectorUdpPorts" -m conntrack --ctstate NEW -j ACCEPT
   ```

3. Starten Sie den Iptables-Service neu, damit die oben genannten neuen Konfigurationen wirksam werden: `service iptables restart`.

Verwandte Themen

Troubleshooting: Windows-Protokollsammlung mit einem Endpunkt-Agent

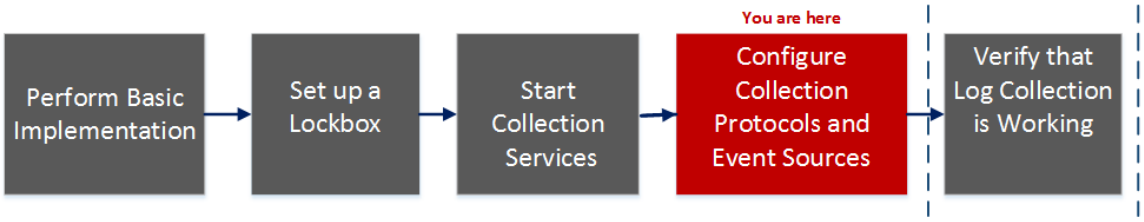
Referenz

AWS-Parameter

Dieses Thema enthält eine Übersicht über die Konfigurationsparameter der AWS-Sammlung für die Bereitstellung eines Remote-Protokollsammlungsservices (VLC) in einer Amazon Web Services (AWS)-Umgebung.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite

In der folgenden Tabelle werden die verfügbaren Konfigurationsparameter für die AWS-Sammlung beschrieben.

Parameter	Beschreibung
Parameter	**Beschreibung**
	Basis
Name*	Name der Ereignisquelle
Aktiviert 	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Konto-ID*	Kontoidentifikationscode des S3 Bucket

Parameter	Beschreibung
S3 Bucketname*	Name des AWS (CloudTrail) S3 Bucket Die Namen von Amazon S3 Buckets sind global eindeutig, unabhängig von der AWS (CloudTrail)-Region, in der der Bucket erstellt wurde. Sie geben den Namen zum Zeitpunkt der Erstellung des Bucket an. Bucket-Namen müssen die DNS-Benennungskonventionen einhalten. Die Regeln für DNS-konforme Bucket-Namen lauten: • Bucket-Namen müssen zwischen 3 und 63 Zeichen lang sein. • Bucket-Namen müssen eine Folge aus einer oder mehreren Bezeichnungen sein. Aneinander grenzende Bezeichnungen werden durch einen einzelnen Punkt getrennt „.“. Bucket-Namen dürfen Kleinbuchstaben, Zahlen und Bindestriche enthalten. Jede Bezeichnung muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. • Bucket-Namen dürfen nicht wie eine IP-Adresse formatiert sein (z. B. 192.168.5.4). Die folgenden Beispiele sind **gültige** Bucket-Namen: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** Die folgenden Beispiele sind **ungültige** Bucket-Namen: • **.myawsbucket** – Bucket-Namen dürfen nicht mit einem Punkt „.“ beginnen. • **myawsbucket.** – Bucket-Namen dürfen nicht mit einem Punkt „.“ enden. • **my..examplebucket** – Zwischen Bezeichnungen darf nur ein Punkt stehen.
Zugangsschlüssel*	Schlüssel für den Zugriff auf den S3 Bucket. Zugriffsschlüssel werden für sichere REST- oder Abfrageprotokollanforderungen an die AWS-Service API verwendet. Weitere Informationen zu Zugriffsschlüsseln erhalten Sie auf der Amazon Web Services-Support-Website unter Manage User Credentials.

Parameter	Beschreibung
Geheimer Schlüssel*	Geheimer Schlüssel für den Zugriff auf den S3 Bucket
Region*	Region des S3-Bucket. **us-east-1** ist der Standardwert.
Region-Endpunkt	Gibt den AWS CloudTrail-Hostnamen an. Zum Beispiel wäre für eine AWS-Public-Cloud für die Region „us-east“ der Region-Endpunkt „s3.amazonaws.com“. Weitere Informationen finden Sie unter http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Dieser Parameter ist erforderlich, um CloudTrail-Protokolle von AWS-Government- oder Private-Clouds zu sammeln.
Proxy verwenden	Aktivieren Sie **Proxy verwenden**, um den Proxy für AWS-Server festzulegen. Diese Option ist standardmäßig deaktiviert.
Proxyserver	Geben Sie den Namen des Proxys ein, mit dem Sie eine Verbindung für den Zugriff auf den AWS-Server herstellen möchten.
Proxyport	Geben Sie die Portnummer ein, die sich mit dem Proxyserver verbindet, um auf den AWS-Server zuzugreifen.
Proxy-Benutzer	Geben Sie den Benutzername zur Authentifizierung mit dem Proxyserver ein.
Proxypasswort	Geben Sie das Passwort zur Authentifizierung beim Proxyport ein.
Startdatum*	Startet die AWS (CloudTrail)-Sammlung von der angegebenen Anzahl Tagen in der Vergangenheit, gemessen vom aktuellen Zeitstempel. Der Standardwert ist 0, also beginnend ab heute. Der Bereich ist 0 bis 89 Tage.
Protokolldateipräfix	Präfix der zu verarbeitenden Datei **Hinweis:** Wenn Sie bei der Einrichtung des CloudTrail-Service ein Präfix festlegen, müssen Sie in diesem Parameter dasselbe Präfix eingeben.
Erweitert	

Parameter	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).
Befehlsargumente	Argumente, die dem Skript hinzugefügt wurden
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist 60. Wenn Sie beispielsweise 60 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 60 Sekunden. Wenn der vorherige Abfragezyklus noch ausgeführt wird, wird gewartet, bis dieser Zyklus abgeschlossen ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 60 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.
SSL aktiviert ☐	Aktivieren Sie für die Kommunikation per SSL das Kontrollkästchen. Die Sicherheit der Datenübertragung erfolgt durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten. Das Kontrollkästchen ist standardmäßig aktiviert.

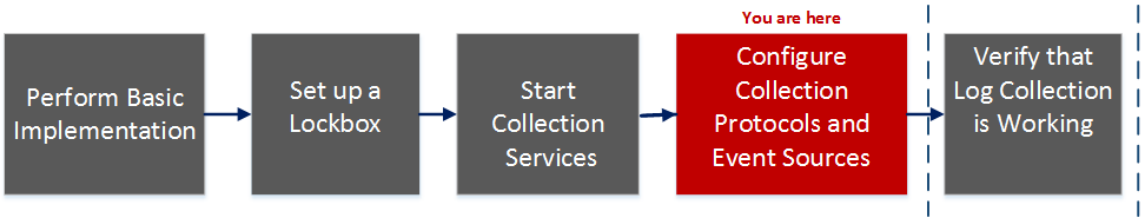
Parameter	Beschreibung
Verbindung testen	Überprüft, ob die in diesem Dialogfeld angegebenen Konfigurationsparameter korrekt sind. Mit dem folgenden Test wird beispielsweise überprüft, ob: • NetWitness mithilfe der in diesem Dialogfeld angegebenen Anmeldedaten eine Verbindung zu dem S3-Bucket in AWS herstellen kann. • NetWitness eine Protokolldatei von dem Bucket herunterladen kann. (Der Verbindungstest würde fehlschlagen, wenn keine Protokolldateien für den gesamten Bucket vorhanden wären. Dies wäre aber sehr unwahrscheinlich.)
Abbrechen	Das Dialogfeld wird ohne Hinzufügen des AWS (CloudTrail) geschlossen.
OK	Fügt die aktuellen Parameterwerte als neuen AWS (CloudTrail) hinzu.

Azure-Parameter

Microsoft Azure ist eine Cloud-Computing-Plattform und -Infrastruktur für Aufbau, Bereitstellung und Management von Anwendungen und Services über ein globales Netzwerk von Rechenzentren, die von Microsoft verwaltet werden.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren von Azure-Ereignisquellen in NetWitness Suite

Parameter für die Azure-Ereignisquellenkonfiguration

Dieses Thema beschreibt die Parameter für die Konfiguration der Azure-Ereignisquelle.

Hinweis: Elemente, die durch ein Sternchen (*) gekennzeichnet sind, sind erforderlich.

Basisparameter

Name	Beschreibung
Name*	Geben Sie einen alphanumerischen, beschreibenden Namen für die Quelle ein. Dieser Wert wird nur für die Anzeige des Namens auf diesem Bildschirm verwendet.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Client-ID*	Die Client-ID befindet sich auf der Registerkarte „Azure-Anwendungskonfiguration“. Scrollen Sie nach unten, bis Sie sie sehen.
Geheimer Clientschlüssel*	Wenn Sie die Ereignisquelle konfigurieren, wird der geheime Clientschlüssel beim Erstellen eines Schlüssels angezeigt. Wählen Sie eine Gültigkeitsdauer aus. Sie sollten diesen Schlüssel speichern, da er nur einmal angezeigt wird. Er kann später nicht mehr abgerufen werden.
Basis-URL API-Ressource*	Geben Sie `https://management.azure.com/` ein. Achten Sie darauf, den nachgestellten Schrägstrich mit anzugeben (/).
Verbundmetadaten-Endpunkt*	Klicken Sie in der Azure-Anwendung auf die Schaltfläche **Endpunkte anzeigen** (am unteren Rand des Bereichs). Es gibt viele Links, die alle mit der gleichen Zeichenfolge beginnen. Vergleichen Sie die URLs und suchen Sie die Zeichenfolge, mit der die meisten von ihnen beginnt. Diese gemeinsame Zeichenfolge ist der Endpunkt, den Sie hier eingeben müssen.
Abonnement-ID*	Sie finden diese im Microsoft Azure-Dashboard: Klicken Sie unten in der Liste auf der linken Seite auf „Abonnements“.

Name	Beschreibung
Mandantendomain*	Gehen Sie zu Active Directory und klicken Sie auf das Verzeichnis. In der URL der Mandantendomain befindet die Zeichenfolge direkt hinter **manage.windowsazure.com/**. Die Mandantendomain ist die Zeichenfolge bis einschließlich dem **.com**.
Ressourcengruppennamen*	Wählen Sie in Azure im linken Navigationsbereich „Ressourcengruppen“ und dann Ihre Gruppe.
Startdatum*	Wählen Sie das Datum aus, an dem mit der Erfassung begonnen werden soll. Standardwert ist das aktuelle Datum.
Verbindung testen	Überprüft die in diesem Dialogfeld angegebenen Konfigurationsparameter auf ihre Richtigkeit.

Erweiterte Parameter

Klicken Sie auf  neben **Erweitert**, um ggf. die erweiterten Parameter anzuzeigen und zu bearbeiten.

Name	Beschreibung
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch durchgeführt wird, wartet der Collector, bis dieser Zyklus beendet ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.
Max. Abrufdauer	Maximale Dauer eines Abfragezyklus in Sekunden. Der Wert 0 bedeutet keine Begrenzung.
Max. Ereignisse-Abruf	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)
Max. Abruf-Inaktivitätsdauer	Maximale Dauer eines Abfragezyklus in Sekunden. Der Wert 0 bedeutet keine Begrenzung.
Befehlsargumente	Optionale Argumente, die beim Skriptaufruf hinzugefügt werden müssen.

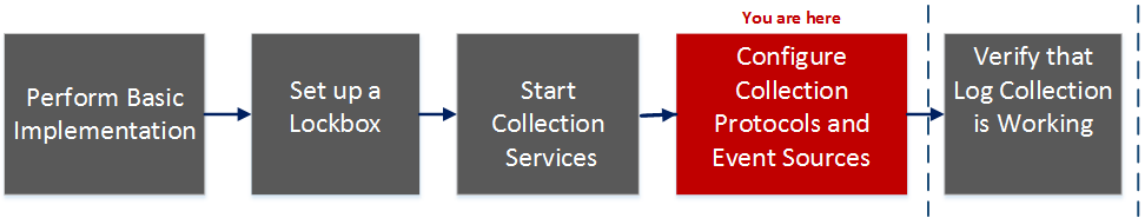
Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. **Achtung:** Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich). Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren.

Kontrollpunktparameter

Das Protokoll „Kontrollpunktsammlung“ erfasst Ereignisse aus Kontrollpunkt-Ereignisquellen mit OPSEC LEA. OPSEC LEA ist die Sicherheitsprotokoll-Export-API für Kontrollpunktvorgänge, die die Extrahierung von Protokollen unterstützt.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite

Konfigurationsparameter für Kontrollpunktsammlung

Basisparameter

Parameter	Beschreibung
Name*	Name der Ereignisquelle.
Adresse*	IP-Adresse des Kontrollpunktservers.
Servername*	Name des Kontrollpunktservers.
Zertifikatname	Zertifikatname für sichere Verbindungen zur Verwendung, wenn der Transportmodus https ist Wenn der Name festgelegt wird, muss das Zertifikat im Zertifikat-Truststore enthalten sein, den Sie auf der Registerkarte Einstellungen erstellt haben. Wählen Sie ein Zertifikat aus der Drop-down-Liste aus. Die Dateibenennungskonvention für Kontrollpunkt-Ereignisquellenzertifikate lautet **checkpoint_*Name-der-Ereignisquelle***.
Distinguished-Client	Geben Sie den Distinguished-Client-Namen des Kontrollpunktservers ein.
Cliententitätsname	Geben Sie den Cliententitätsnamen des Kontrollpunktservers ein.
Distinguished-Server	Geben Sie den Distinguished-Server-Namen des Kontrollpunktservers ein.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Zertifikat mithilfe von Pull übertragen	Aktivieren Sie das Kontrollkästchen, um ein Zertifikat das erste Mal abzurufen. Durch das Übertragen eines Zertifikats per Pull wird es vom Truststore zur Verfügung gestellt.
Zertifikatserveradresse	Die IP-Adresse des Servers, auf dem sich das Zertifikat befindet. Der Standardwert ist die Adresse der Ereignisquelle.

Parameter	Beschreibung
Passwort	Nur aktiviert, wenn Sie das Kontrollkästchen Zertifikat mithilfe von Pull übertragen zum ersten Mal aktivieren. Zum Übertragen des Zertifikats per Pull ist ein Passwort erforderlich. Das Passwort ist der Aktivierungsschlüssel, der beim Hinzufügen einer OPSEC-Anwendung zum Kontrollpunkt auf dem Kontrollpunkt erstellt wurde.

Bestimmen der erweiterten Parameterwerte für die Kontrollpunktsammlung

Es werden weniger Systemressourcen verbraucht, wenn Sie eine Kontrollpunkt-Ereignisquellenverbindung dazu konfigurieren, für eine bestimmte Dauer und ein bestimmtes Ereignisvolumen geöffnet zu bleiben (vorübergehende Verbindung). In RSA NetWitness Suite wird standardmäßig eine vorübergehende Verbindung unter Verwendung der folgenden Verbindungsparameter hergestellt:

- Polling-Intervall = **180** (3 Minuten)
- Max. Abrufdauer = **120** (2 Minuten)
- Max. Ereignisse-Abruf = **5.000** (5.000 Ereignisse pro Polling-Intervall)
- Max. Abruf-Inaktivitätsdauer = **0**

Bei Kontrollpunkt-Ereignisquellen mit sehr hoher Aktivität empfiehlt sich die Einrichtung einer Verbindung, die geöffnet bleibt, bis Sie die Sammlung beenden (dauerhafte Verbindung). Dies stellt sicher, dass die Kontrollpunktsammlung die Geschwindigkeit der Ereignisse beibehält, die durch diese aktiven Ereignisquellen erzeugt wird. Die dauerhafte Verbindung vermeidet Neustarts und Verzögerungen bei der Verbindung und verhindert, dass die Kontrollpunktsammlung hinter der Ereigniserzeugung zurückbleibt.

Um eine dauerhafte Verbindung für eine Kontrollpunkt-Ereignisquelle zu etablieren, stellen Sie die folgenden Parameter auf die folgenden Werte ein:

- Polling-Intervall = **-1**
- Max. Abrufdauer = **0**
- Max. Ereignisse-Abruf = **0**
- Max. Abruf-Inaktivitätsdauer = **0**

Parameter	Beschreibung
Port	Der Port auf dem Kontrollpunktserver, mit dem der Log Collector eine Verbindung herstellt. Der Standardwert ist 18184.

Parameter	Beschreibung
Protokolltyp sammeln	Der Typ der Protokolle, die Sie sammeln möchten. Gültige Werte: • **Audit** – Sammelt Auditereignisse. • **Sicherheit** – Sammelt Sicherheitsereignisse. Wenn Sie sowohl Audit- als auch Sicherheitsereignisse sammeln möchten, ist die Erstellung einer doppelten Ereignisquelle erforderlich. Beispiel: Sie erstellen zuerst eine Ereignisquelle mit der Option Audit. Für diese Ereignisquelle wird ein Zertifikat per Pull in den Truststore übertragen. Als Nächstes erstellen Sie eine weitere Ereignisquelle mit denselben Werten, außer dass Sie als Protokolltyp sammelndie Option Sicherheit auswählen. In Zertifikatname wählen Sie dasselbe Zertifikat aus, das Sie bei der Einrichtung des ersten Parametersatzes für diese Ereignisquelle per Pull übertragen haben, und Sie stellen sicher, dass Zertifikat mithilfe von Pull übertragen nicht aktiviert ist.
Protokolle sammeln von	Wenn Sie eine Kontrollpunkt-Ereignisquelle einrichten, werden die Ereignisse von NetWitness aus der aktuellen Protokolldatei gesammelt. Gültige Werte: • **Jetzt** – Beginnt jetzt mit dem Sammeln von Protokollen, also zu diesem Zeitpunkt in der aktuellen Protokolldatei. • **Protokollstart** – Sammelt Protokolle ab dem Anfang der aktuellen Protokolldatei. Wenn Sie als Wert für diesen Parameter „Protokollstart“ auswählen, sammeln Sie möglicherweise eine sehr große Menge von Daten. Dies hängt davon ab, wie lange die derzeitige Protokolldatei bereits Ereignisse sammelt. Beachten Sie, dass diese Option nur für die erste Datenerfassungssitzung wirksam ist.
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch ausgeführt wird, wird gewartet, bis dieser Zyklus abgeschlossen ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.

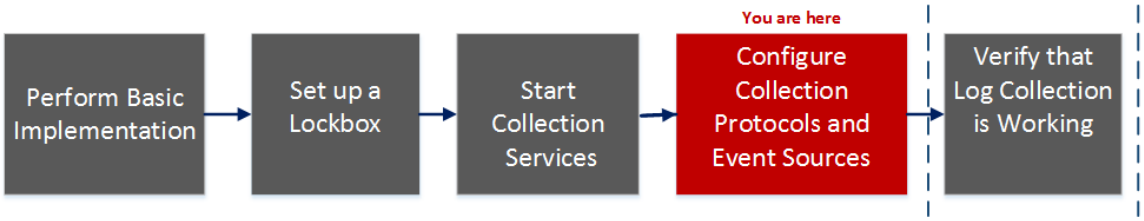
Parameter	Beschreibung
Max. Abrufdauer	Die maximale Dauer eines Abfragezyklus (wie lange der Zyklus dauert) in Sekunden.
Max. Ereignisse-Abruf	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)
Max. Abruf-Inaktivitätsdauer	Maximale Inaktivitätsdauer, in Sekunden, eines Abfragezyklus. 0 gibt keine Begrenzung an.> **300** ist der Standardwert.
Weiterleitung	Aktiviert oder deaktiviert den Kontrollpunktserver als Weiterleiter. Diese Option ist standardmäßig deaktiviert.
Protokolltyp (Name-Werte-Paar)	Protokolle von der Ereignisquelle im Name-Wert-Format. Diese Option ist standardmäßig deaktiviert.
Debug	**Achtung:** Aktivieren Sie nur dann das Debugging (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).

Dateiparameter

In diesem Thema werden die Konfigurationsparameter für die Dateisammlung beschrieben.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren von Dateiereignisquellen in NetWitness Suite

Ereignisquellparameter für die Dateisammlung

Die folgende Tabelle enthält Beschreibungen der Quellparameter für die Dateisammlung.

Name	Beschreibung
	Basis
Dateiverzeichnis*	Sammlungsverzeichnis (zum Beispiel **Eur_London100**), in das die Dateiereignisquelle ihre Dateien platziert. Ein gültiger Wert ist eine Zeichenfolge, die dem folgenden regulären Ausdruck entspricht: **[_a-zA-Z][_a-zA-Z0-9]*** Das bedeutet, dass das Dateiverzeichnis mit einem Buchstaben beginnen muss, auf den Zahlen, Buchstaben und Unterstriche folgen. Dieser Parameter darf nach dem Start der Ereignisdatensammlung nicht geändert werden. Nach der Erstellung der Sammlung erstellt der Log Collector die Arbeits-, Speicher- und Fehlerunterverzeichnisse unter dem Sammlungsverzeichnis.
Adresse*	IP-Adresse der Ereignisquelle. Ein gültiger Wert ist eine **IPv4-Adresse**, eine **IPv6-Adresse** oder ein **Hostname**, der einen vollständig qualifizierten Domainnamen enthält.
Dateispezifikation	Regulärer Ausdruck. Beispiel: **^.*$** = alles wird verarbeitet.
Dateicodierung	Internationale Dateicodierung. Geben Sie die Dateicodierungsmethode ein. Die folgenden Zeichenfolgen sind Beispiele für gültige Methoden: • UTF-8 (Standard) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.

Name	Beschreibung
	Erweitert
Konvertierungsfehler bei der Codierung ignorieren	Aktivieren Sie dieses Kontrollkästchen, um Konvertierungsfehler bei der Codierung und ungültige Daten zu ignorieren. Das Kontrollkästchen ist standardmäßig aktiviert. **Achtung:** Dies kann zu Analyse- und Transformationsfehlern führen.
Dateien-Festplatten-Quota	Legt den Zeitpunkt fest, an dem die Speicherung von Dateien beendet wird, unabhängig von den Einstellungen der Parameter **Bei Fehler speichern** und **Bei Erfolg speichern**. Ein Wert von 10 bedeutet beispielsweise: Wenn weniger als 10 % verfügbarer Festplattenspeicher vorhanden ist, beendet der Log Collector die Speicherung von Dateien, um ausreichenden Speicherplatz für die Verarbeitung Ihrer normalen Sammlung zu reservieren. **Achtung:** Der verfügbare Speicherplatz bezieht sich auf eine Partition, in der das Basissammlungsverzeichnis gemountet ist. Wenn der Log Decoder-Server über eine 10-TB-Festplatte verfügt und 2 TB für das Basissammlungsverzeichnis reserviert sind, führt eine Einstellung dieses Werts auf 10 dazu, dass die Protokollsammlung beendet wird, wenn weniger als 0,2 TB (10 % von 2 TB) verfügbarer Speicherplatz vorhanden ist. Es bedeutet nicht 10 % von 10 TB. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.
Sequenzielle Verarbeitung	Flag für sequenzielle Verarbeitung: • Aktivieren Sie das Kontrollkästchen (Standard), um die Ereignisquellendateien in der Reihenfolge der Sammlung zu verarbeiten. • Aktivieren Sie das Kontrollkästchen nicht, um Ereignisquellendateien parallel zu verarbeiten.
Bei Fehler speichern	Flag für Speicherung bei Fehlern. Aktivieren Sie das Kontrollkästchen, um die Datei **eventsource collection** beizubehalten, wenn der Log Collector einen Fehler feststellt. Das Kontrollkästchen ist standardmäßig aktiviert.

Name	Beschreibung
Bei Erfolg speichern	Speichert die Datei **eventsource collection** nach der Verarbeitung des Flags. Aktivieren Sie das Kontrollkästchen, um die Datei eventsource collection nach ihrer Verarbeitung zu speichern. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Ereignisquellen-SSH-Schlüssel	Öffentlicher SSH-Schlüssel, der zum Hochladen von Dateien für diese Ereignisquelle verwendet wird. Weitere Anweisungen zum Erzeugen von Schlüsseln finden Sie im Abschnitt *Erzeugen des Schlüsselpaars auf der Ereignisquelle und Importieren des öffentlichen Schlüssels in den Log Collector* im Handbuch Installieren und Aktualisieren des SFTP-Agent. **Hinweis:** Wenn die Dateisammlung beendet wird, aktualisiert NetWitness Suite nicht die Datei „authorized_keys“ mit dem öffentlichen SSH-Schlüssel, den Sie in diesem Parameter hinzufügen oder ändern. Sie müssen die Dateisammlung neu starten, um den öffentlichen Schlüssel zu aktualisieren. Sie können den Wert des öffentlichen Schlüssels in diesem Parameter in mehreren Dateiereignisquellen hinzufügen oder ändern, ohne dass die Dateisammlung ausgeführt wird. Allerdings aktualisiert NetWitness Suite die Datei **authorized_keys** erst, wenn die Dateisammlung neu gestartet wurde.
Fehlerdateien verwalten	Standardmäßig verwendet der Log Collector den Parameter **Dateien-Festplatten-Quota**, um zu gewährleisten, dass die Festplatte nicht mit Fehlerdateien gefüllt wird. Wenn Sie diesen Parameter auf **true** einstellen, können Sie einen der folgenden Parameter festlegen: • Maximal zugewiesener Speicherplatz für Fehlerdateien im Parameter **Fehlerdateiengröße** • Maximal zulässige Anzahl von Fehlerdateien im Parameter **Anzahl Fehlerdateien** Eine Reduzierungsprozentzahl wird auch angegeben, die das System anwendet, wenn das Maximum erreicht wurde. Aktivieren Sie das Kontrollkästchen zum Managen von Fehlerdateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Name	Beschreibung
Fehlerdateiengröße	Dieser Wert ist nur gültig, wenn die Parameter **Fehlerdateien verwalten** und **Bei Fehler speichern** auf „true“ eingestellt werden. Gibt an, in welchem Umfang NetWitness Suite Fehlerdateien speichert. Bei dem von Ihnen angegebenen Wert handelt es sich um die maximale Gesamtgröße aller Dateien im Fehlerverzeichnis. Ein gültiger Wert ist eine Zahl zwischen **0** und **281474976710655**. Diese Werte werden in **Kilobyte**, **Megabyte** oder **Gigabyte** angegeben. Der Standardwert lautet **100 Megabyte**. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Anzahl Fehlerdateien	Dieser Wert ist nur gültig, wenn die Parameter **Fehlerdateien verwalten** und **Bei Fehler speichern** auf „true“ eingestellt werden. Gibt die maximal zulässige Anzahl von Fehlerdateien im Fehlerverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **65536**. **65536** ist der Standardwert. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Reduzierung Fehlerdateien in %	Der Prozentsatz der Größe oder der Anzahl der Fehlerdateien, die der Log Collector-Service entfernt, wenn die maximale Größe oder die maximale Anzahl erreicht wurde. Der Service löscht die ältesten Dateien zuerst. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.
Gespeicherte Dateien verwalten	Aktivieren Sie das Kontrollkästchen zum Managen von gespeicherten Dateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Standardmäßig verwendet der Log Collector den Parameter **Dateien-Festplatten-Quota**, um zu gewährleisten, dass die Festplatte nicht mit gespeicherten Dateien gefüllt wird. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie einen der folgenden Parameter festlegen: • Maximal zugewiesener Speicherplatz für gespeicherte Dateien im Parameter **Größe gespeicherter Dateien** • Maximal zulässige Anzahl von gespeicherten Dateien im Parameter **Anzahl gespeicherter Dateien** Eine Reduzierungsprozentzahl wird auch angegeben, die das System anwendet, wenn das Maximum erreicht wurde.

Name	Beschreibung
Größe gespeicherter Dateien	Dieser Wert ist nur gültig, wenn die Parameter **Gespeicherte Dateien verwalten** und **Bei Erfolg speichern** auf „true“ eingestellt werden. Gibt die maximale Gesamtgröße aller Dateien im Speicherverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **281474976710655**. Diese Werte werden in **Kilobyte**, **Megabyte** oder **Gigabyte** angegeben. Der Standardwert lautet **100 Megabyte**. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Anzahl gespeicherter Dateien	Dieser Wert ist nur gültig, wenn die Parameter **Gespeicherte Dateien verwalten** und **Bei Erfolg speichern** auf „true“ eingestellt werden. Gibt die maximale Anzahl von gespeicherten Dateien im Speicherverzeichnis an. Ein gültiger Wert ist eine Zahl zwischen **0** und **65536**. **65536** ist der Standardwert. Nach dem Ändern des Parameters wird die Änderung erst wirksam, wenn Sie die Sammlung oder den Log Collector-Service erneut starten.
Reduzierung gespeicherter Dateien in %	Der Prozentsatz der Größe oder der Anzahl der gespeicherten Dateien, die der Log Collector-Service entfernt, wenn die maximale Größe oder die maximale Anzahl erreicht wurde. Der Service löscht die ältesten Dateien zuerst. Ein gültiger Wert ist eine Zahl zwischen **0** und **100**. **10** ist der Standardwert.

Name	Beschreibung
Debug	**Achtung:** Aktivieren Sie nur dann das Debugging (legen Sie diesen Parameter auf **Ein** oder **Ausführlich** fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggings wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert/deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich).
Abbrechen	Schließt das Dialogfeld, ohne einen Ereignisquelltyp hinzuzufügen.
OK	Fügt die Parameter für die Ereignisquelle hinzu.

Protokollsammlungsservice in der Ansicht „System“

Bei einem Log Collector handelt es sich um einen Service, der auf einem Log Decoder-Host ausgeführt wird (bezeichnet als Log Collector) oder Ereignisse von einem Remote Collector an einen Local Collector sendet und ähnlich wie ein Log Decoder konfiguriert und gemanagt wird.

Um auf den Protokollsammlungsservice in der Ansicht „System“ zuzugreifen, navigieren Sie zu ADMIN > „Services“, wählen einen Log Collector-Service und dann „Ansicht > System“ aus.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.

Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten	Einrichten einer Lockbox
Administrator	*Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

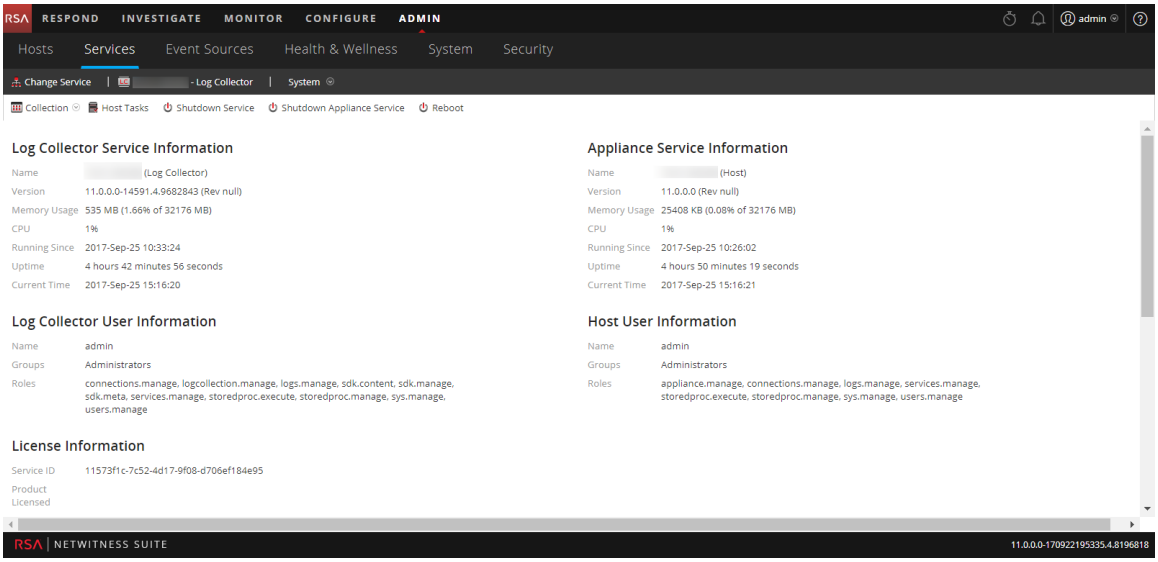
*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

Grundlegende Implementierung

Überblick

In der Symbolleiste „Serviceinformationen“ des Log Collector können Sie mit dem Symbol „Sammlung“ Ereignisdaten aus einem beendeten Protokoll starten oder die Erfassung von Daten aus einem gestartetem Protokoll beenden. Mit dem Symbol „Hostaufgaben“ können Sie Aufgaben auswählen, die Sie ausführen möchten. Außerdem können Sie Ihren Service herunterfahren und in der Symbolleiste „Serviceinformationen“ neu starten.



Parameter der ODBC-Ereignisquellenkonfiguration

In diesem Thema erfahren Sie, wie Sie das ODBC-Sammlungsprotokoll konfigurieren, mit dem Ereignisse aus Ereignisquellen abgerufen werden, die Auditdaten mithilfe der Open Database Connectivity (ODBC)-Softwareschnittstelle in einer Datenbank speichern.

Auf ODBC-Konfigurationsparameter zugreifen

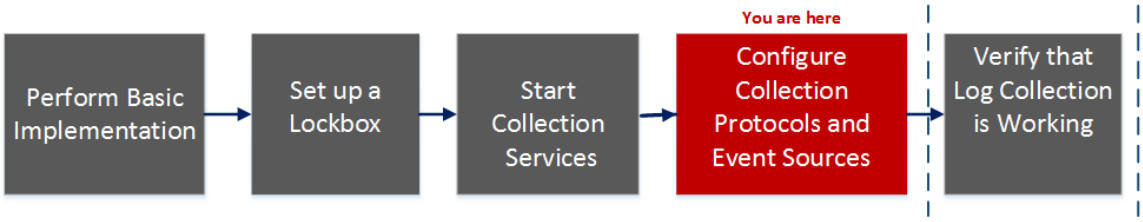
So greifen Sie auf die Konfigurationsparameter für die ODBC-Ereignisquelle zu:

1. Navigieren Sie im Menü NetWitness Suite zu **Administration > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

   Die Ansicht **Services > Konfiguration** wird mit geöffneter Registerkarte **Allgemein** des Log Collector angezeigt.
4. Klicken Sie auf die Registerkarte **Ereignisquellen** und wählen Sie im Drop-down-Menü **ODBC/Konfiguration** aus.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices

Rolle	Ziel	Dokumentation
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite
- Konfigurieren von DSNs (Data Source Names)
- Troubleshooting bei der ODBC-Sammlung
- Erstellen von angepasstem Typespec für ODBC-Sammlung

Parameter für Data Source Name (DSN)

Im Bereich Quellen können Sie die Parameter von Data Source Names (DSN) überprüfen, hinzufügen, ändern oder löschen.

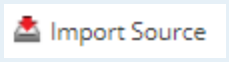
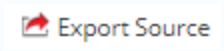
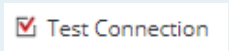
Bereich „Quellen“

Ein ODBC DSN enthält die Informationen für den Log Collector, wie ein ODBC-Endpunkt erreicht werden kann. Nutzen Sie ein ODBC DSN, wenn Sie einen Datenquellennamen mit bestimmten Informationen konfigurieren wollen, z. B. welcher ODBC-Treiber verwendet werden soll, oder den Hostnamen und -Port des ODBC-Endpunktes.

Ein ODBC DSN ist eine Abfolge von Name-Wert-Paaren. Informationen zu den gültigen Namen für einen bestimmten ODBC-Datentyp, z. B. Sybase, Microsoft SQL Server oder Oracle, finden Sie im *Benutzerleitfaden für DataDirect Connect Series für ODBC*, den Sie in der Progress DataDirect Document Library herunterladen können.

Symbolleiste

Die folgende Tabelle enthält Beschreibungen der Symbolleistenoptionen.

Option	Beschreibung
+	Öffnet das Dialogfeld DSN hinzufügen, in dem Sie eine Ereignisquelle für den im Bereich Ereigniskategorien ausgewählten Ereignisquelltyp hinzufügen.
−	Löscht die ausgewählte Ereignisquellen
	Öffnet das Dialogfeld DSN bearbeiten, in dem Sie die Konfigurationsparameter für die ausgewählte Ereignisquelle ändern können. Wenn Sie mehrere Ereignisquellen auswählen, wird mit dieser Option das Dialogfeld „Massenbearbeitung für Quelle“ geöffnet, in dem Sie die Parameterwerte für die ausgewählten Dateiverzeichnisse bearbeiten können.
	Öffnet das Dialogfeld „Option zum Massenhinzufügen“, in dem Sie einen Massenimport von DSN-Parametern aus einer CSV-Datei (durch Kommas getrennte Werte) importieren können. Das Dialogfeld „Option zum Massenhinzufügen“ enthält die folgenden beiden Optionen: • CSV-Datei importieren • CSV-Content einfügen
	Erstellt eine **.csv**-Datei, die die Parameter für die ausgewählten DSNs enthält.
	Überprüft die Konfigurationsparameter für die ausgewählte ODBC-Datenbank.

DSN-Dialogfeld hinzufügen oder bearbeiten

In diesem Dialogfeld können Sie eine Ereignisquelle für die ausgewählte Ereignisquelle hinzufügen oder ändern.

Basisparameter

Name	Beschreibung
DSN*	Der Datenquellenname (DSN), mit dem die Datenbank beschrieben wird, aus der Ereignisse gesammelt werden sollen. Wählen Sie einen vorhandenen DSN aus der Drop-Down-Liste aus. Weitere Informationen finden Sie unter Parameter der ODBC-DSN-Ereignisquellenkonfiguration.

Name	Beschreibung
Benutzername*	Mit dem Benutzernamen verbindet sich der Datenquellenname mit der Datenbank. Sie müssen einen Benutzernamen angeben, wenn Sie die Ereignisquelle erstellen.
Password	Mit dem Passwort verbindet sich der Datenquellenname mit der Datenbank. **Achtung:** Das Passwort wird intern verschlüsselt und in verschlüsselter Form angezeigt.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Ereignisquellenkonfiguration zu aktivieren und die Sammlung zu starten. Das Kontrollkästchen ist standardmäßig aktiviert.
Adresse*	Dieses Feld wird für ODBC nicht verwendet. Der Log Collector verwendet die Adresse in der Datei **ODBC.ini**.

Erweiterte Parameter

Name	Beschreibung
Max. Zellgröße	Maximale Größe der Daten in Byte, die der Log Collector aus einer Zelle in der Datenbank erfassen kann. Der Standardwert ist **2.048**.
Nullwert	Vom Log Collector angezeigte Buchstabenzeichenkette, wenn für eine Zelle in der Datenbank NULL zurückgegeben wird. Standardwert: “” (null).
Polling-Intervall	Intervall (Zeit in Sekunden) zwischen jeder Abfrage. Der Standardwert ist **180**. Wenn Sie beispielsweise 180 angeben, plant der Collector eine Abfrage der Ereignisquelle alle 180 Sekunden. Wenn der vorherige Abfragezyklus noch durchgeführt wird, wartet der Collector, bis dieser Zyklus beendet ist. Wenn eine große Anzahl Ereignisquellen abgefragt wird, kann es länger als 180 Sekunden dauern, bis die Abfrage beginnt, weil die Threads beschäftigt sind.
Max. Ereignisse-Abruf	Die maximale Anzahl der Ereignisse pro Abfragezyklus (wie viele Ereignisse pro Abfragezyklus gesammelt werden)

Name	Beschreibung
Debuggen	**Achtung:** Achtung: Aktivieren Sie nur dann das Debuggen (legen Sie diesen Parameter auf „Ein“ oder „Ausführlich“ fest), wenn Sie ein Problem mit einer Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Die Aktivierung des Debuggens wirkt sich negativ auf die Performance des Log Collector aus. Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisquelle. Gültige Werte: • **Aus** = (Standard) deaktiviert • **Ein** = aktiviert • **Ausführlich** = aktiviert im ausführlichen Modus – fügt Thread-Informationen und Quellkontextinformationen zu den Meldungen hinzu Dieser Parameter ist für das Debugging und die Überwachung isolierter Probleme bei der Ereignisquellensammlung ausgelegt. Wenn Sie diesen Wert ändern, tritt die Änderung sofort in Kraft (kein Neustart erforderlich). Die Debug-Protokollierung ist ausführlich. Begrenzen Sie daher die Anzahl der Ereignisquellen, um die Auswirkungen auf die Performance zu minimieren.
Anfangs-ID der Nachverfolgung	Identifizierungscode, den der Log Collector dieser Ereignisquelle anfangs zuordnet, wenn die Sammlung nicht gestartet wird. Wurde diesem Parameter kein Wert zugewiesen, beginnt der Log Collector am Ende der Tabelle und erfasst lediglich neu hinzugefügte Zeilen am Tabellenende. Der Standardwert lautet “” (null).
Dateiname	Nur für Microsoft SQL Server-Ereignisquellen, Standort des Nachverfolgungsdateiverzeichnisses (z. B. **C:\MyTraceFiles**). Weitere Informationen finden Sie in dem Konfigurationsleitfaden für RSA Microsoft SQL Server-Ereignisquellen auf RSA Link: https://community.rsa.com/docs/DOC-40241.
Verbindung testen	Überprüft die in diesem Dialogfeld angegebenen Konfigurationsparameter auf ihre Richtigkeit.
Abbrechen	Der Dialog wird ohne Hinzufügen oder Ändern von DSN-Parametern geschlossen.
OK	Die Parameter für DSN werden hinzugefügt bzw. geändert.

Parameter der ODBC-DSN-Ereignisquellenkonfiguration

ODBC-Ereignisquellen (Open Database Connectivity) benötigen DSNs (Data Source Names). Sie müssen daher DSNs mit den zugehörigen Wertepaaren für die ODBC-Ereignisquellenkonfiguration definieren.

Auf ODBC-Konfigurationsparameter zugreifen

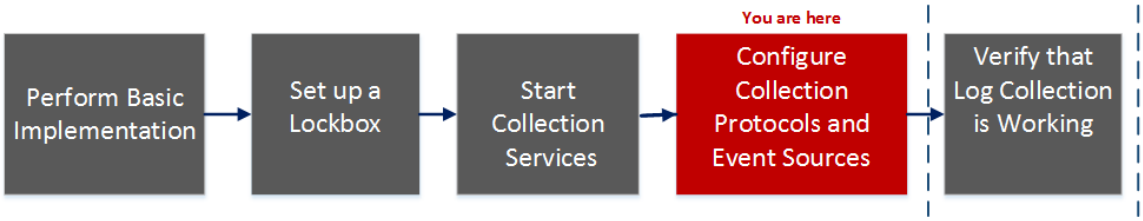
So greifen Sie auf die Konfigurationsparameter für die ODBC-Ereignisquelle zu:

1. Wählen Sie zum Zugreifen auf die Ansicht „Services“ im Menü NetWitness Suite die Optionen **Administration > Services** aus.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

   Die Ansicht **Services > Konfiguration** wird mit geöffneter Registerkarte **Allgemein** des Log Collector angezeigt.
4. Klicken Sie auf die Registerkarte **Ereignisquellen** und wählen Sie im Drop-down-Menü **ODBC/DSNs** aus.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox

Rolle	Ziel	Dokumentation
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite
- Konfigurieren von DSNs (Data Source Names)

ODBC-DSN-Konfigurationsparameter

Dieses Thema beschreibt die Parameter für die Konfiguration der DSNs (Data Source Names).

Bereich DSN

Im Bereich „DSNs“ können Sie DSNs und die Namen-Wert-Paare für DSNs für ODBC-Ereignisquellen hinzufügen, löschen oder bearbeiten.

Funktion	Beschreibung
+	Zeigt das Dialogfeld „DSN hinzufügen“ an, in dem Sie einen DSN und die entsprechenden Parameter definieren können.
−	Löscht die ausgewählten DSNs.
	Zeigt das Dialogfeld „DSN bearbeiten“ an, in dem Sie die Namen-Wert-Paare für den ausgewählten DSN bearbeiten können.
Manage Ter	Zeigt das Dialogfeld „DSN-Vorlagen managen“ an, in dem Sie Vorlagen für Namen-Wert-Paare für DSNs hinzufügen oder löschen können.

Funktion	Beschreibung
	Wählt DSNs aus.
DSN	Name des hinzugefügten DSN.
Parameter	**<name-value for="" p="" pairs="" the=""> </name-value>**

DSN-Dialogfeld hinzufügen oder bearbeiten

In diesem Dialogfeld können Sie ein Dateiverzeichnis für die ausgewählte Ereignisquelle hinzufügen oder ändern.

Funktion	Beschreibung
DSN-Vorlage	Wählen Sie eine vordefinierte Vorlage für die Namen-Wert-Paare für den DSN aus.
DSN-Name*	Zeigt den Namen des DSN an. Sie können den DSN-Namen nach dem Hinzufügen nicht mehr ändern. Der Wert muss einem DSN-Eintrag in der Datei ODBC.ini entsprechen. Ein gültiger Wert ist eine Zeichenfolge, die auf folgende Zeichen beschränkt ist: `[_a-zA-Z][_a-zA-Z0-9]*` Das bedeutet, dass das Dateiverzeichnis mit einem Buchstaben beginnen muss, auf den Zahlen, Buchstaben und Unterstriche folgen (z. B. **oracle_executive_compensation**).
Parameter	 Fügt eine Zeile ein, in der Sie ein Namen-Wert-Paar für einen Parameter definieren können. Löscht das ausgewählte Namen-Wert-Paar für den Parameter.  : Wählt das ausgewählte Namen-Wert-Paar für den Parameter aus. Name: Geben Sie den Parameternamen ein oder ändern Sie ihn. Wert: Geben Sie den Wert zu dem Parameternamen ein oder ändern Sie ihn.
Abbrechen	Schließt das Dialogfeld, ohne das DSN und seine Namen-Wert-Paare hinzuzufügen oder Änderungen an den Namen-Wert-Paaren zu speichern.

Funktion	Beschreibung
Speichern	Fügt das DSN und seine Namen-Wert-Paare hinzu oder speichert Änderungen an den Namen-Wert-Paaren.

Dialogfeld DSN-Vorlagen managen

In diesem Dialogfeld können Sie Vorlagen für die Namen-Wert-Paare für DSNs hinzufügen oder löschen.

Funktion	Beschreibung
	Bereich Vorlagenauswahl
	Öffnet den Bereich „Vorlage hinzufügen“, in dem Sie eine Vorlage für Namen-Wert-Paare für DSNs hinzufügen können.
	Löscht die ausgewählte Vorlage.
	Wählen Sie eine Vorlage zum Löschen oder Ändern aus.
	Bereich Vorlage hinzufügen
	Fügt eine Wertpaarzeile hinzu.
	Löscht eine Wertpaarzeile.
	Wählt eine Wertpaarzeile aus.
Name	Geben Sie den Parameternamen ein.
Wert	Geben Sie den Wert zu dem Parameternamen ein.
Abbrechen	Bricht alle im Dialogfeld eingegebenen Änderungen ab.
Speichern	Fügt das DSN und seine Namen-Wert-Paare hinzu oder speichert Änderungen an den Namen-Wert-Paaren.

Funktion	Beschreibung
Schließen	Schließt das Dialogfeld, ohne das DSN und seine Namen-Wert-Paare hinzuzufügen oder Änderungen an den Namen-Wert-Paaren zu speichern.

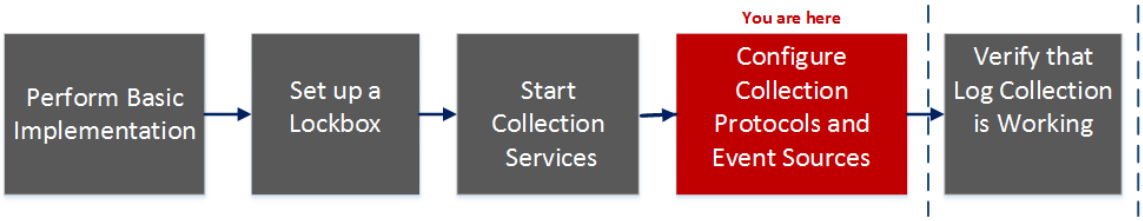
Konfigurationsparameter für Remote/Local Collectors

Wenn Sie die Protokollsammlung bereitstellen, müssen Sie die Log Collectors so konfigurieren, dass diese die Protokollereignisse von unterschiedlichen Ereignisquellen erfassen und diese Ereignisse verlässlich und sicher an den Log Decoder-Host weitergeben. Dort werden die Ereignisse dann analysiert und für weitere Analysen gespeichert.

In diesem Thema werden die Funktionen der Ansicht Services-Konfiguration > Registerkarte Remote-Collectors/Local Collectors erläutert.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Provisioning von Local Collectors und Remote Collectors
- Konfigurieren von Local und Remote Collectors

Ansicht „Service-Konfiguration“

In der Ansicht „Service-Konfiguration“ pflegen Sie alle Parameter für die Protokollsammlung. Die in diesem Leitfaden behandelten Bereitstellungsparameter werden auf der Registerkarte **Remote/Local Collectors** verwaltet:

- Wenn Sie einen Local Collector konfigurieren, zeigt NetWitness Suite die Registerkarte **Remote Collectors** an, auf der Sie den Local Collector zum Abrufen von Ereignissen aus Remote Collectors konfigurieren können.
- Wenn Sie einen Remote Collector konfigurieren, zeigt NetWitness Suite die Registerkarte **Local Collectors** an, auf der Sie den Remote Collector zum Übertragen von Ereignissen an einen Local Collector konfigurieren können.

Registerkarte „Remote Collectors“

Bei einem Local Collector bietet der Bereich „Remote Collectors“ die Möglichkeit, Remote Collectors hinzuzufügen oder zu löschen, aus denen der Local Collector Ereignisse abrufen soll.

Spalte	Beschreibung
+	Das Dialogfeld **Quelle hinzufügen** wird angezeigt. Hier können Sie die Remote Collectors auswählen, von denen der Local Collector Ereignisse abfragen soll.
−	Löscht den Remote Collector aus dem Local Collector Remote Controllers-Bereich.
	Zeigt das Dialogfeld **Quelle bearbeiten** für den ausgewählten Remote Collector an.
	Wählt Remote Collectors aus.
Name	Namen der Remote Collectors, von denen der Local Collector aktuell Ereignisse abfragt.

Spalte	Beschreibung
Adresse	IP-Adressen der Remote Collectors, von denen der Local Collector aktuell Ereignisse abfragt.
Sammlungen	Wählen Sie die Sammlungsprotokolle aus, die der Remote Collector an einen Local Collector überträgt. Sie können eine beliebige Kombination von Protokollen auswählen. Wenn Sie kein Protokoll auswählen, wählt NetWitness Suite alle Protokolle aus.

Registerkarte „Local Collector“

Bei einem Remote Collector können Sie im Local Collector-Bereich die Local Collectors hinzufügen oder löschen, an die der Remote Collector Ereignisse übertragen soll.

Wählen Sie im Drop-down-Menü **Konfiguration auswählen** die Option **Ziel** oder **Quelle** aus.

- Wenn Sie **Ziel** auswählen, wird das Dialogfeld **Remoteziel hinzufügen** angezeigt.
- Wenn Sie „Quelle“ auswählen, wird das Dialogfeld **Quelle hinzufügen** angezeigt.

In der folgenden Tabelle wird das Dialogfeld „Quelle hinzufügen“ beschrieben.

Spalte	Beschreibung
	Das Dialogfeld **Quelle hinzufügen** wird angezeigt. Hier können Sie die Remote Collectors auswählen, von denen der Local Collector Ereignisse abfragen soll.
	Löscht den Remote Collector aus dem Local Collector Remote Controllers-Bereich.
	Zeigt das Dialogfeld **Quelle bearbeiten** für den ausgewählten Remote Collector an.
	Wählt Remote Collectors aus.
Name	Namen der Remote Collectors, von denen der Local Collector aktuell Ereignisse abfragt.
Adresse	IP-Adressen der Remote Collectors, von denen der Local Collector aktuell Ereignisse abfragt.

In der folgenden Tabelle wird der Bereich „Local Collectors“ beschrieben.

Spalte	Beschreibung
	Zeigt das Dialogfeld **Remoteziel hinzufügen** für die ausgewählte Gruppe an. Für diese Gruppe fügen Sie die Local Collectors als Ziele hinzu, an die der Remote Collector Ereignisse übertragen soll.
	Löscht den als Ziel ausgewählten Log Collector aus der Gruppe.
	Zeigt das Dialogfeld **Remoteziel bearbeiten** für den als Ziel ausgewählten Local Collector an.
	Wählt einen als Ziel ausgewählten Local Collector aus.
Zielname	Zeigt den Namen des als Ziel ausgewählten Local Collector an.
Adresse	Zeigt die IP-Adresse des als Ziel ausgewählten Local Collector an.
Sammlungen	Wählen Sie die Sammlungsprotokolle aus, die der Local Collector aus einem Remote Collector abrufen soll. Sie können eine beliebige Kombination von Protokollen auswählen. Wenn Sie kein Protokoll auswählen, wählt NetWitness Suite alle Protokolle aus.

Registerkarten der Protokollsammlung

In diesem Thema werden die in der Ansicht „Protokollsammlung“ verfügbaren Registerkarten beschrieben.

Zugang zur Ansicht „Protokollsammlung“

1. Navigieren Sie zu **ADMIN > Services** im Menü NetWitness Suite.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Wählen Sie unter „Aktionen“ **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.

   Die Ansicht **Services > Konfiguration** wird mit geöffneter Registerkarte **Allgemein** des Log Collector angezeigt.
4. Wählen Sie eine der verfügbaren Registerkarten aus, um die entsprechenden Parameter anzuzeigen oder zu aktualisieren.

Verfügbare Registerkarten

Verwenden Sie die Ansicht „Administration“ > „Services“, um Protokollsammlungsparameter zu verwalten. Sie enthält die folgenden Registerkarten:

- **Allgemein**: enthält allgemeine Parameter, die den Betrieb des Log Collector-Services und die jeweiligen Sammlungsprotokolle steuern. Nähere Informationen finden Sie unter Protokollsammlung – Registerkarte „Allgemein“.
- **Remote Collectors**: Verwenden Sie diese Registerkarte zum Einrichten von Remote Collectors. Nähere Informationen finden Sie unter Konfigurieren von Local und Remote Collectors.
- **Dateien**: bietet eine Benutzeroberfläche für die Bearbeitung der Konfigurationsdateien für Log Collector.
- **Ereignisquellen**: Verwenden Sie diese Registerkarte zum Konfigurieren der Sammlung für Ihre Ereignisquellen. Nähere Informationen finden Sie unter Protokollsammlung – Registerkarte „Ereignisquellen“.
- **Ereignisziele**: Auf der Registerkarte „Ereignisziele“ der Ansicht „Konfiguration“ des Protokollsammlungsservices konfigurieren Sie das Ziel für die vom Log Collector erfassten Ereignisdaten. Nähere Informationen finden Sie unter Protokollsammlung – Registerkarte „Ereignisziele“.
- **Einstellungen**: enthält Parameter für die Lockbox-Sicherheitseinrichtung und Zertifikatmanagement.
- **Appliance-Servicekonfiguration**: enthält Konfigurationsparameter für den RSA NetWitness Suite Core Appliance-Service.

Informationen zu den Konfigurationsparametern für die Registerkarten **Dateien** und **Appliance-Servicekonfiguration** finden Sie in den Abschnitten zu den jeweiligen Registerkarten im *Konfigurationsleitfaden für Hosts und Services*.

Protokollsammlung – Registerkarte „Allgemein“

In diesem Thema werden Funktionen in der Ansicht „Services“ >-„Konfiguration“ > Registerkarte „Allgemein“ vorgestellt, die speziell für Log Collector gelten.

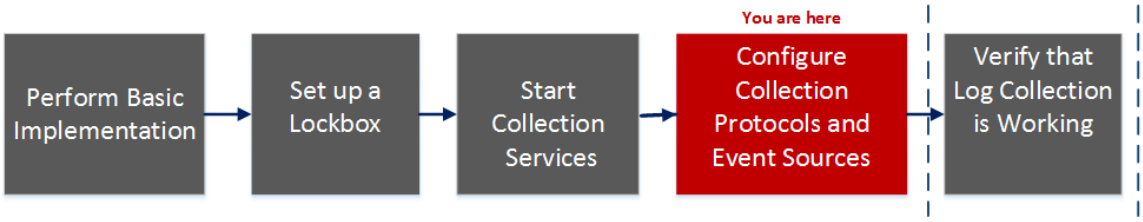
So rufen Sie die Registerkarte „Allgemein“ der Protokollsammlung auf:

1. Navigieren Sie im Menü NetWitness Suite zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.
3. Klicken Sie unter „Aktionen“ auf  und wählen Sie **Ansicht > Konfiguration** aus.

   Die Ansicht **Services > Konfiguration** wird mit geöffneter Registerkarte **Allgemein** des Log Collector angezeigt.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen

Rolle	Ziel	Dokumentation
Administrator	*Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

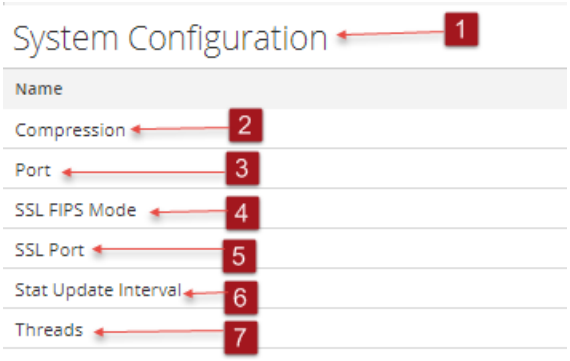
- Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite
- Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite
- Konfigurieren von Dateiereignisquellen in NetWitness Suite
- Konfigurieren Sie Netflow-Ereignisquellen in NetWitness Suite
- Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite
- Konfigurieren von SDEE-Ereignisquellen in NetWitness Suite
- Konfigurieren von SNMP-Ereignisquellen in NetWitness Suite
- Konfigurieren der Syslog-Ereignisquellen für Remote Collector
- Konfigurieren von VMware-Ereignisquellen in NetWitness Suite
- Konfigurieren Sie Windows-Ereignisquellen in NetWitness Suite
- Konfiguration für Windows-Legacy- und NetApp-Sammlung

Überblick

Der RSA NetWitness Suite-Administrator muss Ereignisquellen konfigurieren, um Protokolle an die Collectors zu senden. Wenn Ereignisquellen konfiguriert sind, fragen sie Ereignisquellen ab, rufen Protokolle ab und senden die Ereignisdaten an NetWitness Suite.

Bereich „Systemkonfiguration“

Im Bereich „Systemkonfiguration“ wird die Servicekonfiguration für einen NetWitness Suite-Service gemanagt. Wenn ein Service zum ersten Mal hinzugefügt wird, sind Standardwerte wirksam. Sie können diese Werte bearbeiten, um die Performance zu verbessern. Eine Beschreibung dieser Parameter finden Sie auf der Registerkarte **Allgemein**.

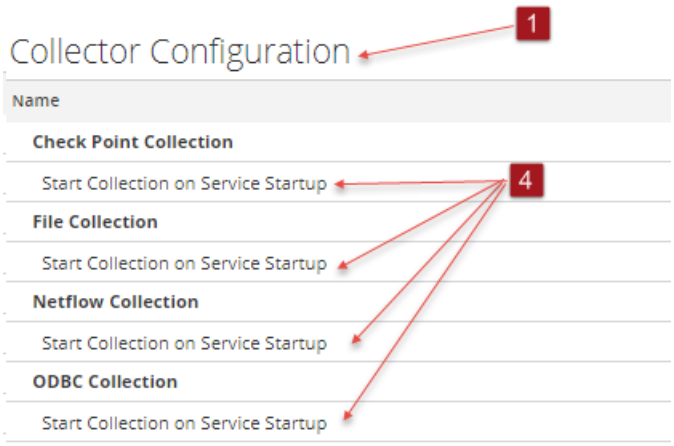


1	Im Bereich „Systemkonfiguration“ wird die Servicekonfiguration für einen NetWitness Suite-Service gemanagt.
2	Komprimierung: Die Mindestanzahl Byte, die pro Antwort vor der Komprimierung übertragen werden muss. Die Einstellung 0 deaktiviert die Komprimierung. Der Standardwert ist **0**. Eine Veränderung des Werts ist sofort für alle nachfolgenden Verbindungen wirksam.
3	Port: Der Port, den der Service überwacht. Folgende Ports sind verfügbar: • 50001 für Protokollsammlung • 50002 für Log Decoder • 50003 für Broker • 50004 für Decoder • 50005 für Concentrators • 50007 für andere Services
4	SSL FIPS-Modus: Sofern aktiviert (**ein**), wird die Sicherheit der Datenübertragung durch Verschlüsselung der Informationen und Bereitstellen der Authentifizierung mit SSL-Zertifikaten gemanagt. Der Standardwert ist **Aus**.
5	SSL-Port: Der NetWitness Suite-Core-SSL-Port, den der Service überwacht. Folgende Ports sind verfügbar: • 56001 für Protokollsammlung • 56002 für Log Decoder • 56003 für Broker • 56004 für Decoder • 56005 für Concentrators

	• 56007 für andere Services
6	Statistikaktualisierungsintervall: Die Anzahl der Millisekunden zwischen Statistikaktualisierungen auf dem System. Niedrigere Zahlen führen zu häufigeren Aktualisierungen und können andere Prozesse verlangsamen. Der Standardwert ist **1.000**. Eine Änderung des Werts ist sofort wirksam.
7	Threads: Die Anzahl der Threads im Threadpool für die Verarbeitung eingehender Anforderungen. Bei der Einstellung 0 wird es vom System entschieden. Der Standardwert ist 15. Die Änderung wirkt sich beim Serviceneustart aus.

Collector-Konfigurationsbereich

Der Bereich „Collector-Konfiguration“ bietet eine Methode zum Aktivieren des automatischen Starts der Protokollsammlung nach Ereignisquelltyp.



1	Der Bereich „Collector-Konfiguration“ bietet eine Methode zum Aktivieren des automatischen Starts der Protokollsammlung nach Ereignisquelltyp.
2	„Alle aktivieren“ aktiviert die automatische Sammlung für alle Ereignistypen. **Alle aktivieren** = Ereignisse werden empfangen und Protokolle werden für alle Ereignistypen gesammelt, wenn der Log Collector-Service gestartet wird.
3	„Alle deaktivieren“ deaktiviert die automatische Sammlung für alle Ereignistypen. **Alle deaktivieren** = (Standardeinstellung) Es werden so lange keine Ereignisdaten für die Ereignistypen empfangen, bis die Erfassung explizit gestartet wird.
4	„Sammlung bei Start des Services starten“ aktiviert den automatischen Start der Protokollsammlung gemäß Ereignisquelltyp, wenn der Log Collector-Service gestartet wird. Gültige Werte:

- Ausgewählt = Die Protokollsammlung wird beim Start des Log Collector-Services gestartet.
- Nicht ausgewählt = (Standardeinstellung) Es werden so lange keine Ereignisdaten erfasst, bis die Erfassung explizit gestartet wird.

5 **Anwenden**: Klicken Sie auf **Anwenden**, um die Änderungen der Parameterwerte zu speichern.

Protokollsammlung – Registerkarte „Ereignisziele“

Auf der Registerkarte „Ereignisziele“ der Konfigurationsansicht für den Protokollsammlungsservice konfigurieren Sie das Ziel für die von Log Collector gesammelten Ereignisdaten:

- Log Decoder
- Identitätsfeed

Voraussetzungen

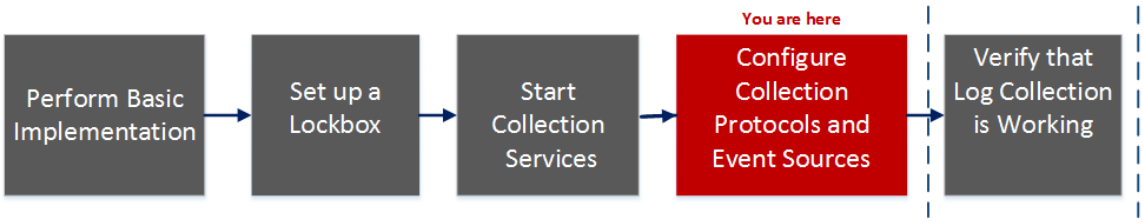
Sie müssen die folgende Konfiguration implementieren, um einen Identitätsfeed zu erstellen:

- Einen Log Collector-Service mit einem Identitätsfeed-Ereignisprozessor
- Einen Log Collector-Service mit konfigurierter und aktivierter Windows-Sammlung

Hinweis: Weitere Informationen zum Erstellen und Untersuchen eines Identitätsfeeds finden Sie im Thema „Erstellen von Identitätsfeeds“ im *Leitfaden „Live-Ressourcenmanagement“*.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	Eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices

Rolle	Ziel	Dokumentation
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

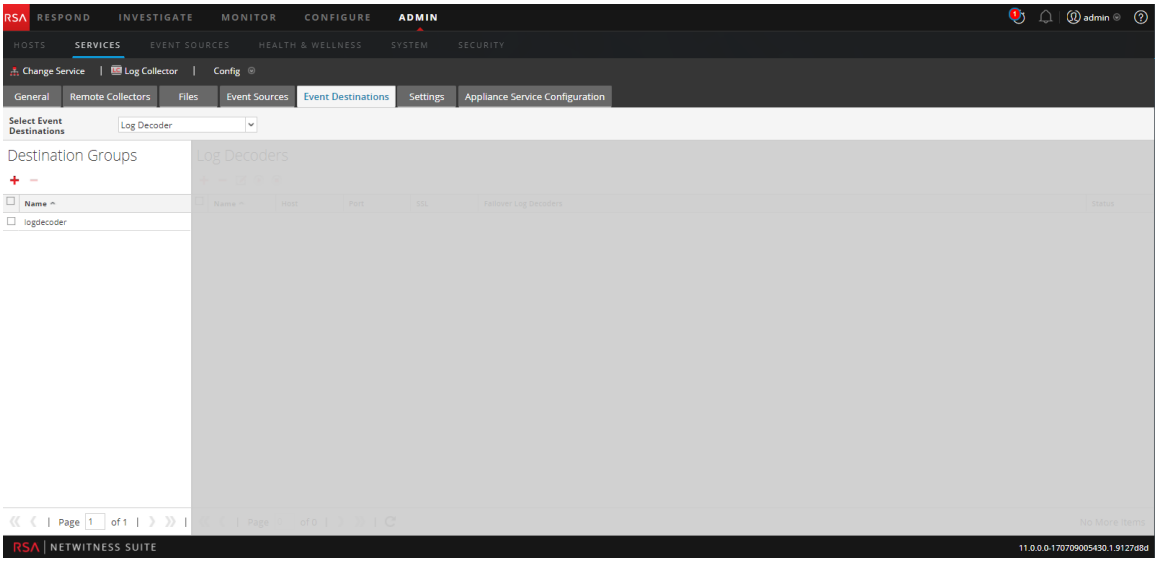
*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Weitere Informationen finden Sie im Thema **Erstellen von Identitätsfeeds** im *Leitfaden „Live-Ressourcenmanagement“*.

Überblick

Auf der Registerkarte „Ereignisziele“ der Konfigurationsansicht für den Protokollsammlungsservice konfigurieren Sie das Ziel für die von Log Collector gesammelten Ereignisdaten.

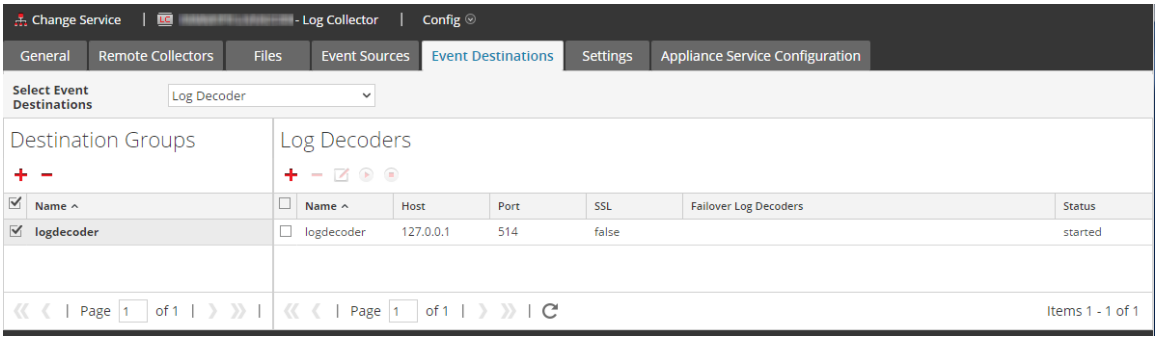


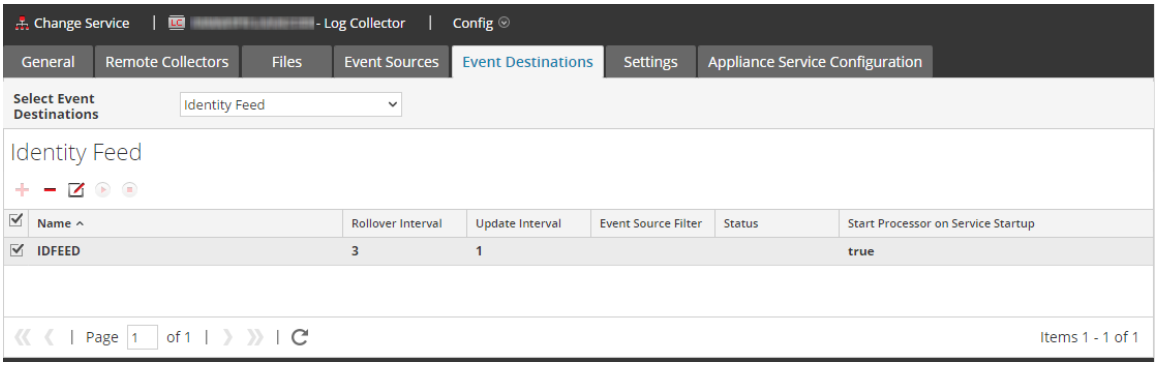
Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist Services managen.

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Protokollsammlungsservice aus.

3. Wählen Sie unter „Aktionen“  > **Ansicht > Konfiguration** aus, um die Registerkarte mit den Konfigurationsparametern für die Protokollsammlung anzuzeigen.
4. Klicken Sie auf die Registerkarte **Ereignisziele**.
5. Führen Sie im Drop-down-Menü **Ereignisziele auswählen** folgende Schritte aus:
   - Wählen Sie **Log Decoder** aus, um Log Decoder-Ziele für Ereignisdaten zu konfigurieren, die von Log Collector gesammelt werden.

     Hinweis: Sie müssen einen Log Decoder-Service im Dialogfeld „Log Decoder-Ziel hinzufügen“ auswählen, der Rest der Konfiguration wird aber automatisch durchgeführt.
   - Wählen Sie **Identitätsfeed** aus, um ein Identitätsfeedziel für die von Log CollectorLog Collector gesammelten Ereignisdaten zu konfigurieren.





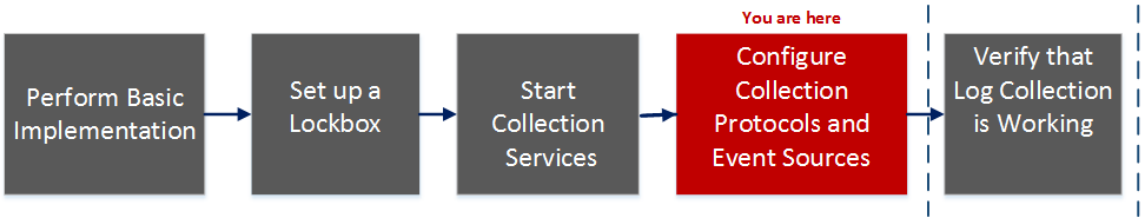
Protokollsammlung – Registerkarte „Ereignisquellen“

Verwenden Sie die Registerkarte „Ereignisquellen“, um die Ereignisquellen AWS (CloudTrail), Kontrollpunkt, Datei, ODBC, SDEE, SNMP, Syslog, SNMP, VMware, Windows und Windows-Legacy zu konfigurieren.

Um auf die Registerkarte „Ereignisquellen“ zuzugreifen, navigieren Sie zu ADMIN > „Services“ > wählen „Protokollsammlungsservice“ > „Ansicht“ > „Konfiguration“ > Ereignisquellen).

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	eine Lockbox zum Verwalten der Lockbox-Einstellungen einrichten.	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices
Administrator	*Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

*Sie können diese Aufgabe hier durchführen.

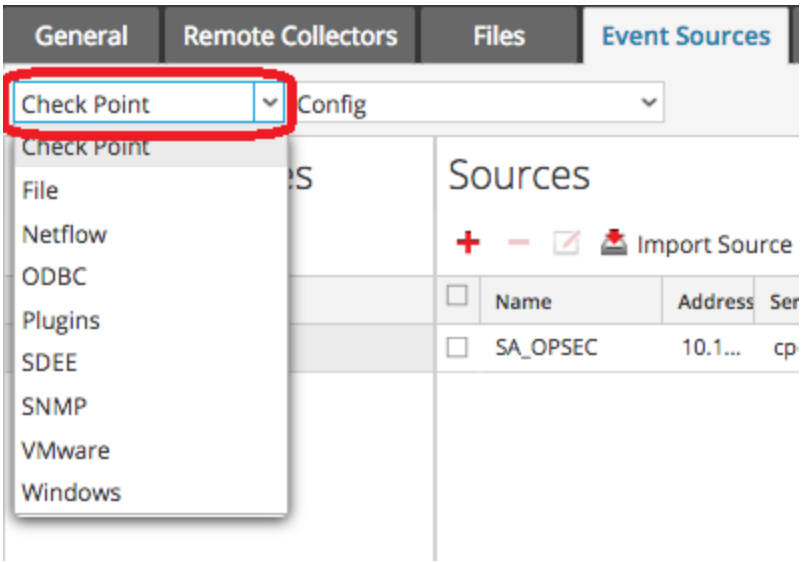
Verwandte Themen

- Konfigurieren der AWS (CloudTrail)-Ereignisquellen in NetWitness Suite
- Konfigurieren von Kontrollpunkt-Ereignisquellen in NetWitness Suite
- Konfigurieren von Dateiereignisquellen in NetWitness Suite
- Konfigurieren von ODBC-Ereignisquellen in NetWitness Suite
- Konfigurieren von SDEE-Ereignisquellen in NetWitness Suite
- Konfigurieren von SNMP-Ereignisquellen in NetWitness Suite
- Konfigurieren der Syslog-Ereignisquellen für Remote Collector
- Konfigurieren von VMware-Ereignisquellen in NetWitness Suite
- Konfigurieren Sie Windows-Ereignisquellen in NetWitness Suite
- Konfiguration für Windows-Legacy- und NetApp-Sammlung

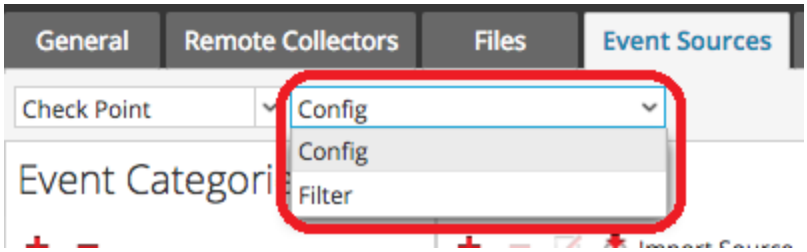
Überblick

Die Ansicht „Konfiguration“ hat zwei Drop-Down-Menüs:

- Das linke Menü enthält eine Liste aller verfügbaren Sammlungsprotokolle.



- Das rechte Menü hat zwei Optionen: **Konfigurieren** und **Filter**.



Die Ansicht „Konfiguration“ der Registerkarte „Ereignisquellen“ enthält zwei Bereiche: „Ereigniskategorien“ und „Quellen“.

Hinweis: Weitere Informationen über das Menüelement „Filter“ finden Sie unter Konfigurieren von Ereignisfiltern für einen Collector.

Menü Ereignisquelltypen

Die Log Collector-Registerkarte „Ereignisquellen“ enthält ein Drop-down-Menü mit zwei Feldern, in dem Sie das Sammlungsprotokoll und jegliche anderen unterstützenden Parameter für dieses Protokoll auswählen.

Im linken Feld wählen Sie eines der folgenden Protokolle aus: Kontrollpunkt, Datei, ODBC, Plug-Ins, SDEE, SNMP, VMware, Windows, und Windows-Legacy.

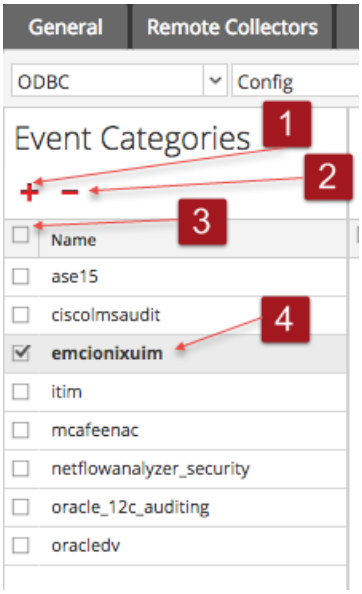
Im rechten Feld wählen Sie Folgendes aus:

- Konfiguration zur Konfiguration der allgemeinen Ereignisquellparameter für den Typ, den Sie im linken Kästchen ausgewählt haben. Allgemeine Konfig -Bereiche haben eine Registerkarte mit den folgenden Optionen:
  - Hinzufügen, Bearbeiten und Löschen
  - Importieren (auch Quelle importieren, DSN importieren)
  - Exportieren (auch Quelle exportieren, DSN exportieren)
- Nur für ODBC, SNMP, und Windows:
  - Für ODBC wählen Sie zur Konfiguration DSNs.
  - Für SNMP wählen Sie SNMPv3-Benutzer-Manager.
  - Für Windows wählen Sie Kerberos-Bereichsnamenkonfiguration.

Durch das Auswählen einer Option wird ein Konfigurationsbereich angezeigt, in dem Sie die Sammlungsparameter für die Ereignisquelle konfigurieren. Die Konfigurationsbereiche unterscheiden sich je nach Ereignisquelle leicht voneinander und werden separat beschrieben.

Bereich Ereigniskategorien

Sobald Sie ein Sammlungsprotokoll auswählen, wird der Bereich „Ereigniskategorien“ mit allen Ereignisquellen ausgefüllt, die Sie für dieses Sammlungsprotokoll konfiguriert haben. Die folgende Abbildung zeigt beispielsweise ODBC-Ereignisquellen, die konfiguriert wurden:



Im Bereich Ereigniskategorien besteht die Möglichkeit, Ereignisquelltypen hinzuzufügen oder zu löschen.

1	Zeigt das Dialogfeld Verfügbare Ereignisquelltypen an, in dem Sie den Typ der Ereignisquelle auswählen, für den Sie Parameter definieren möchten
2	Löscht den ausgewählten Ereignisquelltyp aus dem Bereich Ereigniskategorien
3	Wählt Ereignisquelltypen aus
4	Zeigt die Namen der Ereignisquelltypen an, die Sie hinzugefügt haben.

Bereich „Quellen“

Im Bereich „Quellen“ sind die Werte der Parameter für den ausgewählten Ereignisquelltyp aufgeführt. Weitere Informationen finden Sie in den Themen zu den einzelnen Sammlungsprotokollen.

Protokollsammlung – Registerkarte „Einstellungen“

Verwenden Sie die Registerkarte „Einstellungen“ für folgende Aufgaben:

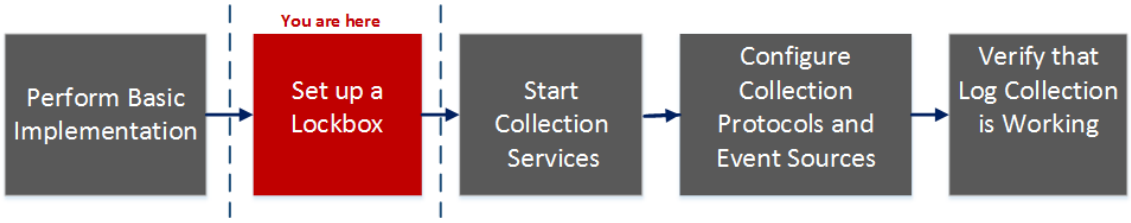
- Einrichten einer Lockbox
- Systemstabilitätswert zurücksetzen
- Managen von Zertifikaten

Achtung: Wenn der Name des Hosts, auf dem der Log Collector installiert ist, nach der Installation geändert wird, erfasst der Log Collector keine Ereignisse aus der Ereignisquelle. Sie müssen stabile Systemwerte zurücksetzen, wenn der Hostname geändert wird.

Um auf die Registerkarte „Einstellungen der Protokollsammlung“ zuzugreifen. navigieren Sie zu ADMIN > „Services“. Wählen Sie im Raster Services einen Log Collector-Service aus. Klicken Sie unter „Aktionen“ auf das Menü „Aktionen“ und wählen Sie „Ansicht“ > „Konfiguration“ aus.

Workflow

Dieser Workflow beschreibt die grundlegenden Aufgaben, die zum Starten der Erfassung von Ereignissen durch die Protokollsammlung durchgeführt werden müssen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Führen Sie die grundlegende Implementierung der Protokollsammlung durch.	Grundlegende Implementierung
Administrator	*Einrichten einer Lockbox zum Verwalten der Lockbox-Einstellungen	Einrichten einer Lockbox
Administrator	Starten von Protokollsammlungsservices	Starten von Sammlungsservices

Rolle	Ziel	Dokumentation
Administrator	Konfigurieren Sie Protokollsammlungsprotokolle und Ereignisquellen.	Konfigurieren von Sammlungsprotokollen und Ereignisquellen
Administrator	Überprüfen Sie, ob die Protokollsammlung funktioniert.	Überprüfen der ordnungsgemäßen Funktion der Protokollsammlung

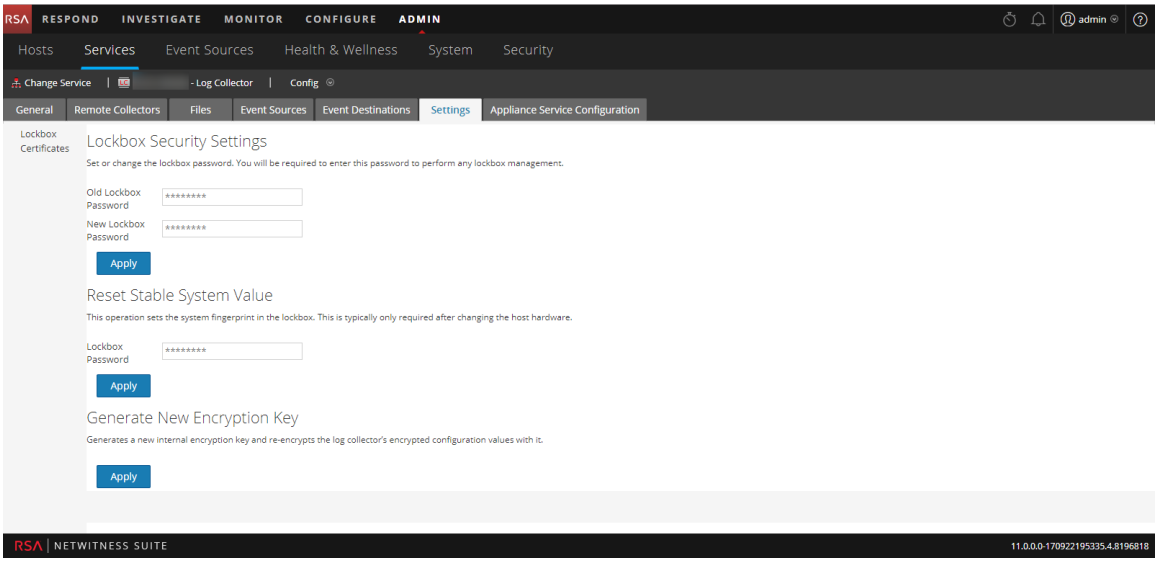
*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

- Weitere Informationen finden Sie im Thema „Erstellen von Identitätsfeeds“ im *Leitfaden „Live-Ressourcenmanagement“*.

Überblick

Dies ist ein Beispiel für die Registerkarte „Einstellungen“.



Troubleshooting der Protokollsammlung

In diesem Thema werden Format und Inhalt des Troubleshootings der Protokollsammlung beschrieben. NetWitness Suite informiert Sie auf die folgenden beiden Arten über Probleme oder potenzielle Probleme mit Log Collector.

- Protokolldateien
- Ansichten zur Überwachung der Integrität und des Zustands

Protokolldateien

Wenn Sie ein Problem mit einem bestimmten Ereignisquellen-Sammlungsprotokoll haben, können Sie Debugging-Protokolle überprüfen, um dieses Problem zu untersuchen. Jede Ereignisquelle verfügt über einen Debug-Parameter, den Sie aktivieren können (stellen Sie den Parameter auf Ein oder Detailliert), um diese Protokolle zu erfassen.

Achtung: Aktivieren Sie das Debugging nur, wenn Sie ein Problem mit dieser Ereignisquelle haben und Sie dieses Problem untersuchen müssen. Wenn Sie das Debugging ständig aktiviert haben, wirkt sich dies negativ auf die Performance des Log Collector aus.

Überwachung der von Integrität und Zustand

Die Überwachung von Integrität und Zustand macht Sie rechtzeitig auf mögliche Hardware- und Softwareprobleme aufmerksam, sodass Sie Ausfälle vermeiden können. RSA empfiehlt Ihnen, die statistischen Felder des Log Collector zu überwachen, um sicherzugehen, dass der Service effizient funktioniert und nicht an oder nahe den Maximalwerten ist, die Sie konfiguriert haben. Sie können die folgenden Statistiken (Stats) überwachen, die in der Ansicht **Admin > Integrität und Zustand** beschrieben sind.

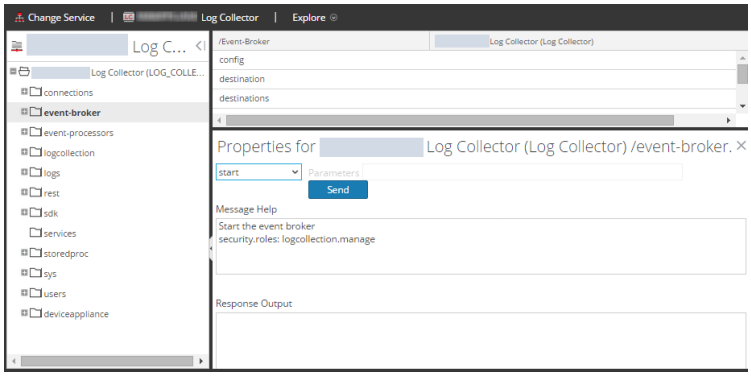
Beispiel für das Troubleshooting-Format

RSA NetWitness Suite gibt folgende Arten von Fehlermeldungen in den Protokolldateien zurück.

Protokollmeldungen	`timestamp failure (LogCollection) Message-Broker Statistics:...`
	`timestamp failure (AMQPClientBaseLogCollection):...`
	`timestamp failure (MessageBrokerLogReceiver):...`

Mögliche Ursache	Der Log Collector kann den Message Broker nicht erreichen, da der Message Broker:

	• nicht mehr ausgeführt wird. • fehlerhafte Verbindungseinstellungen hat.

Lösungen	1. <use the="the" systemctl="systemctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>
	`prompt$ systemctl status rabbitmq-server`
	`rabbitmq start/running, process 10916`
	2. Starten Sie den RabbitMQ Message Broker am Ereignis-Broker-Node in der Ansicht „Durchsuchen“:
	 

Troubleshooting: Windows-Protokollsammlung mit einem Endpunkt-Agent

Die folgenden Themen helfen Ihnen beim Troubleshooting von Problemen, die bei Verwendung der Windows-Protokollsammlung auf einem Agent von Endpoint Insights auftreten können.

Erläuterung des Formats der Windows-Protokollkonfigurationsdatei

Achtung: Bearbeiten Sie die generierte Konfigurationsdatei nicht. Wenn Sie Änderungen vornehmen, kann der Agent die Informationen aus der Datei nicht lesen.

Die Protokollkonfigurationsdatei enthält Informationen, die für die Analyse von Ereignisprotokollen nützlich sind. Es folgt ein Beispiel:

```
#### Warning: Do not modify this system generated file.
{
  "enabled" : true,
  "configName" : "FE",
  "servers" : [ "tcp://[redacted]" ],
  "filter" : "<QueryList><Query Id='0'> <Select
  Path='ForwardedEvents'>*</Select> </Query></QueryList>",
  "testLogOnLoad" : true
}

q5yrOSY6qkdediE9XUI361926LOF2ZyU7JU2sklntgMWeV3KWFekwqJqhZ8XmPr6vbeOTK6wiYb
uW6zDL0WB/PPo+x5bErzvjoALA7zwAu61HVk4R4sYP4MRgGCsuiikC2pMB667P5bFg0+sUESsxZ
eFN91cjFPUjIIujuUdd0uMhnyur4tt+4F/WGJsBl57pTow2D8NRHvb9hKBjE1lo7/nZ0WpSO0Fq
yHx90NuS42d0OhjrC3oDyucwdAjqKkxm7VtsAJQwwxZTlwUbmDRPoiIyTG7egERVDDyqGcu2Ii+
fkijkFhuxTta8kWIeleQiBts1BAk+JZNfDSNYdYqUg==
```

Die erzeugte Konfigurationsdatei enthält Folgendes:

- **config_name**: Der Name der Konfigurationsdatei.
- **Server**: Eine Reihe von Server-URLs mit Beschreibungen von Adresse und Protokoll zur Verwendung bei der Weiterleitung der Protokolle. Der Agent wird versuchen, sie der Reihe nach zu erreichen.
- **Filter**: Eine mit der Windows-Ereignisanzeige kompatible XML-Datei, in der die zu überwachenden Kanäle und jegliche Ereignis-ID-Ausschlüsse beschrieben sind. Ein Standard-XML-Filter zur Erfassung von Anwendung und System aus dem Kanal, wobei für beide eine Ereignis-ID-ausgeschlossen ist, würde wie folgt aussehen:

```
<QueryList>
    <Query Id="0" Path="Application">
        <Select Path="Application">*</Select>
        <Select Path="System">*</Select>
        <Suppress Path="Application">*[System[(EventID=3366)]]</Suppress>
        <Suppress Path="System">*[System[(EventID=3366)]]</Suppress>
    </Query>
</QueryList>
```

- **Enabled**: Ermöglicht das Deaktivieren der Erfassung, wobei immer noch ein Testprotokoll gesendet wird, sofern diese Funktion aktiviert ist.
- **TestLogOnLoad**: Sendet beim Laden einer Konfiguration selbst dann eine Protokollnachricht, wenn die Ereignisweiterleitung nicht aktiviert ist. Dies hilft Analysten beim Testen einer Konfiguration vor dem Aktivieren der Erfassung. Im Windows-Ereignisprotokoll wird diese Meldung nicht lokal eingetragen.

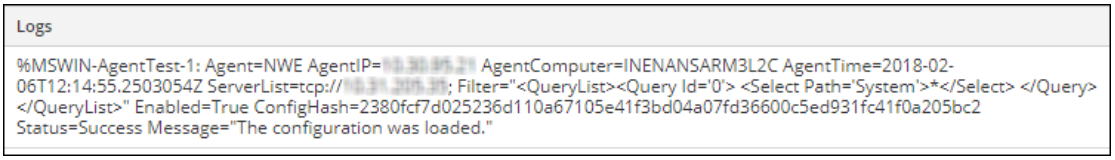
Lesen des Testprotokolls

Eine Testprotokollmeldung wird immer dann gesendet, wenn ein Endpunkt-Agent mit Windows-Protokollsammlungsdatei zum ersten Mal auf einem Endpunkt-Agent installiert wird oder wenn die Protokollkonfigurationsdatei aktualisiert wird. Bei erfolgreicher Installation oder Aktualisierung der Windows-Protokollsammlung: In der Testprotokolldatei werden drei Abschnitte angezeigt.

1	Typ der Testprotokollmeldung, IP-Adresse des Agent, Hostname des Agent und Zeitpunkt der Erzeugung des Testprotokolls
2	Konfiguration, die während der Erstellung des Agent bereitgestellt wurde
3	Status und die zugeordnete Meldung

Es gibt drei Szenarien.

1. Erfolgreiche Bereitstellung einer Protokollsammmlungskonfiguration: Die Testprotokollnachricht wird als -1 angezeigt und der Status als erfolgreich.



2. Manipulation der Protokollsammlungs-Konfigurationsdatei: Die Agent-Testnachricht wird als -2 angezeigt und eine Nachricht zeigt an, dass die Konfigurationsdatei manipuliert wurde. Falls Sie die Änderungen erneut anwenden möchten, erzeugen Sie die Protokollsammlungsdatei erneut.

3. Bei einem falschen benutzerdefinierten Kanalnamen: Eine Fehlerstatusnachricht wird angezeigt. Erzeugen Sie die Protokollsammlung erneut mit dem richtigen Kanalnamen.