RSA NETWITNESS® SUITE

Konfigurationsleitfaden Archiver

für Version 11.0

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

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Februar 2018

Inhalt

Übersicht über Archiver

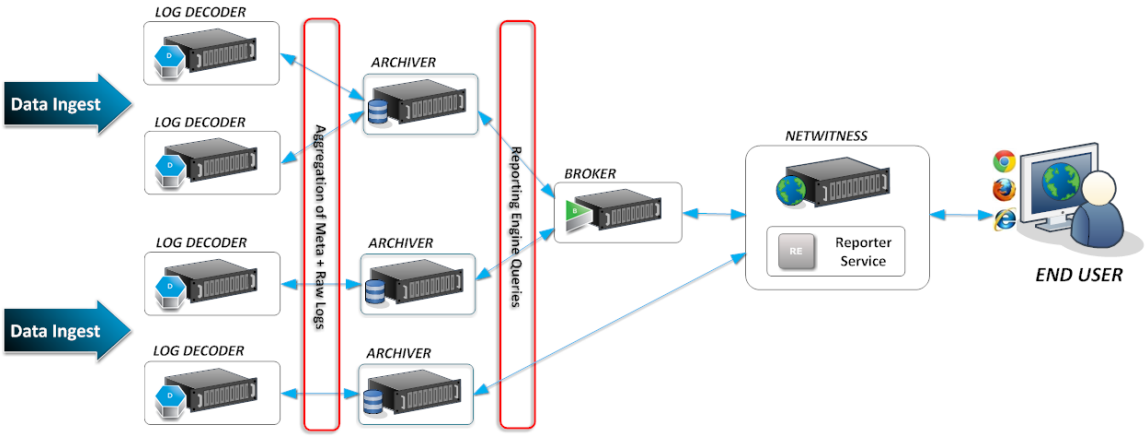
Dieser Leitfaden bietet detaillierte Anweisungen zur Konfiguration von Archiver in Ihrem Netzwerk. Außerdem enthält er Beschreibungen von zusätzlichen Verfahren, die zu anderen Zeitpunkten verwendet werden, sowie Referenzmaterial, das die Benutzeroberfläche für die Konfiguration von Archiver in Ihrem Netzwerk erläutert.

Der NetWitness Suite Archiver ist eine Appliance, die eine Langzeitarchivierung von Protokollen ermöglicht, indem Protokolldaten indiziert und komprimiert und dann an den Archivierungsspeicher gesendet werden. Der Archivierungsspeicher wird damit für die langfristige Datenaufbewahrung und das Compliance-Reporting optimiert.

Archiver speichert Rohdatenprotokolle und Protokollmetadaten von Log Decoder für eine langfristige Aufbewahrung. Zur Speicherung wird DAC (Direct-Attached Capacity) verwendet.

Hinweis: Rohdatenpakete und Paketmetadaten werden nicht im Archiver gespeichert.

Die folgende Abbildung zeigt die Architektur eines NetWitness Suite-Netzwerks, das den Archiver implementiert:



Konfigurieren eines Archivers

Der NetWitness Suite-Archiver ist eine Appliance, die eine Langzeitarchivierung von Protokollen ermöglicht, indem Protokolldaten indiziert und komprimiert und dann an den Archivierungsspeicher gesendet werden. Der Archivierungsspeicher wird damit für die langfristige Datenaufbewahrung und das Compliance-Reporting optimiert.

Archiver speichert Rohdatenprotokolle und Protokollmetadaten von Log Decoder für eine langfristige Aufbewahrung. Zur Speicherung wird DAC (Direct-Attached Capacity) verwendet.

Hinweis: Rohdatenpakete und Paketmetadaten werden nicht im Archiver gespeichert.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Sie haben den Archiver-Host in Ihrer Netzwerkumgebung installiert.
- Der Log Decoder Version 11.0.0.0 wurde in Ihrer Netzwerkumgebung installiert und konfiguriert.

Wenn Sie mehrere Archiver- oder Concentrator-Services als Gruppe konfigurieren und die Aggregationsaufgaben zwischen ihnen aufteilen möchten, lesen Sie dazu **Gruppenaggregation** im *Leitfaden zur Bereitstellung*.

Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver.

Die folgende Tabelle beschreibt die grundlegenden Schritte für die Konfiguration eines Archiver. Die Aufgaben müssen in der Reihenfolge abgeschlossen werden, in der sie aufgeführt sind.

Konfigurationsschritt	Beschreibung
Hinzufügen des Archiver-Services	In diesem Thema erfahren Sie, wie Sie den Archiver-Service auf dem Archiver-Host hinzufügen und eine Lizenz auf ihn anwenden.
Hinzufügen von Log Decoder als Datenquelle zu Archiver	In diesem Thema erhalten Sie Anweisungen zum Hinzufügen von Log Decoder zu einem Archiver.
Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung	Enthält Anweisungen zum Konfigurieren des Speichers und der Protokollaufbewahrung auf einem Archiver.
Hinzufügen von Archiver als Datenquelle zur Reporting Engine	Enthält Anweisungen zum Hinzufügen von Archiver als Datenquelle zu Reporting Engine für das Erzeugen eines Berichts zur Datensammlung durch die Archiver.
Konfigurieren der Archiver-Überwachung	Enthält Anweisungen zum Konfigurieren des Warnmeldungsmechanismus in Bezug auf den Archiver-Speicher.

Hinzufügen des Archiver-Services

Um einen Archiver-Srvice hinzuzufügen, stellen Sie sicher, dass Sie einen Archiver-Host installiert haben, auf dem Sie den Archiver-Service ausführen möchten. Siehe **Schritt 1: Hinzufügen oder Aktualisieren von Hosts** im *Leitfaden für die ersten Schritte mit Hosts und Services* für Informationen zum Hinzufügen eines Hosts.

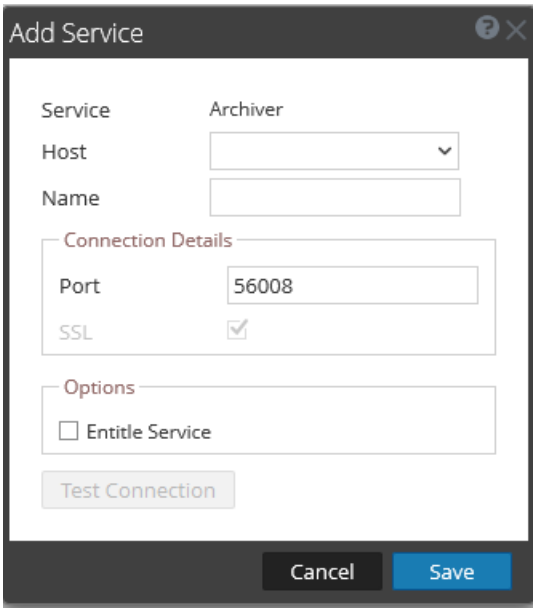
Nach der Installation eines Archiver-Hosts müssen Sie einen Archiver-Service hinzufügen und eine Lizenz darauf anwenden, wie im folgenden Verfahren beschrieben.

Hinweis: Dieses Verfahren ist nur erforderlich, wenn der Archiver-Service nicht installiert ist.

Führen Sie die folgenden Schritte aus, um den Archiver-Service hinzuzufügen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Symbolleiste im Bereich **Services** die Optionen + **> Archiver** aus.

   Das Dialogfeld „Service hinzufügen“ wird angezeigt.



3. Geben Sie die folgenden Details an.

Feld	Beschreibung
Host	Wählen Sie einen Host aus dem Drop-down-Menü aus.
Name	Geben Sie einen Namen für den Service ein.

Feld	Beschreibung
Port	Der Standardport ist 50008.
SSL	Wählen Sie **SSL** aus, wenn NetWitness Suite mithilfe von SSL mit dem Service kommunizieren soll. Die Sicherheit der Datenübertragung erfolgt durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten. **Hinweis:** Wenn Sie SSL auswählen, stellen Sie sicher, dass SSL im Bereich Systemkonfiguration aktiviert ist.
Benutzername	(Optional) Geben Sie den Benutzernamen für den Service ein.
Password	(Optional) Geben Sie das Passwort für den Service ein.
Service berechtigen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die gegenwärtig konfigurierten Ansprüche auf diesen Service anwenden möchten. Weitere Informationen finden Sie im Thema **Implementierung der Berechtigungsfunktion** im *Lizenzierungsleitfaden*.

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

   Der hinzugefügte Service wird jetzt im Bereich „Services“ angezeigt.

   Hinweis: Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Serviceinformationen und versuchen Sie es erneut.
6. Wenden Sie die Lizenz auf den Archiver-Service an.

   Einzelheiten zum Verfahren für die Aktivierung (Anwenden einer Lizenz) des Archiver-Services finden Sie im Thema **Synchronisieren des NetWitness-Server** im *Lizenzierungsleitfaden*.

Hinzufügen von Log Decoder als Datenquelle zu Archiver

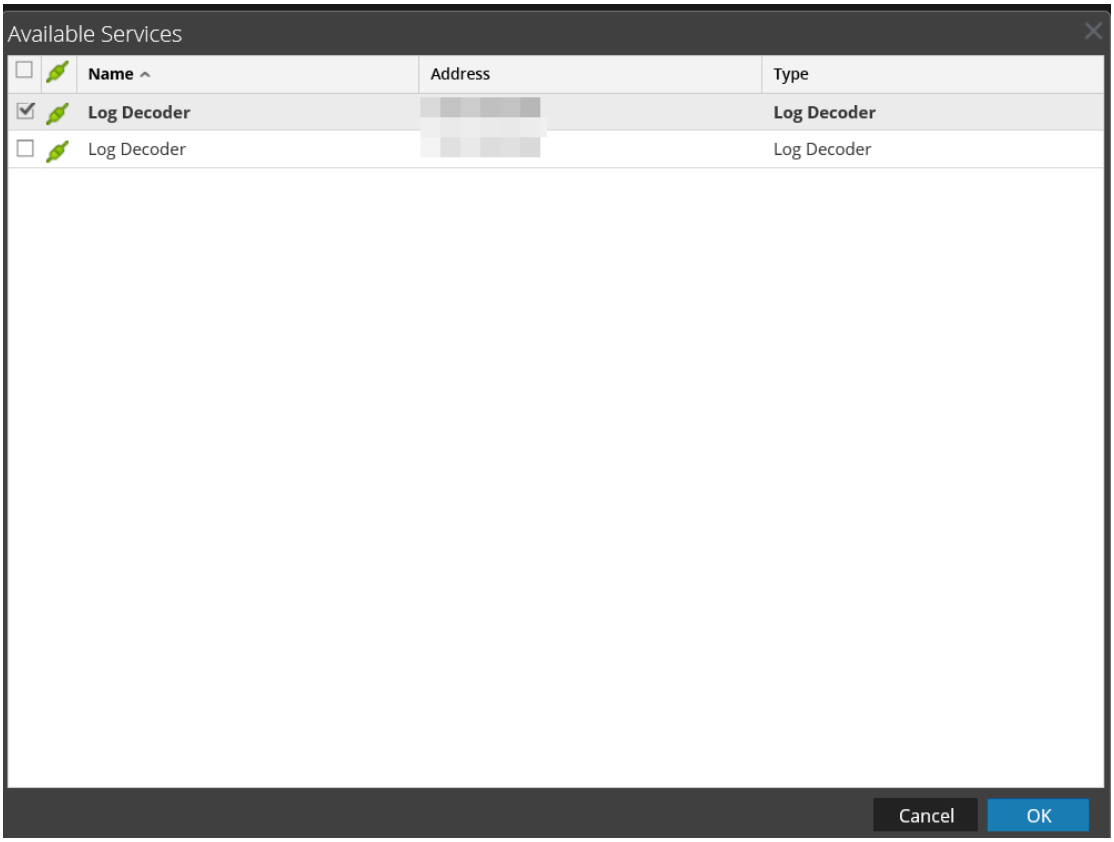
Um einen Log Decoder als Datenquelle zu Archiver hinzuzufügen, müssen Sie den Archiver-Host in Ihrer Netzwerkumgebung installiert, Log Decoder in Ihrer Netzwerkumgebung installiert und konfiguriert und den Archiver-Hosts zu NetWitness Suite hinzugefügt haben. Vergewissern Sie sich außerdem, dass der Archiver-Service aktiv und lizenziert ist.

Hinzufügen von Log Decoder als Datenquelle zu Archiver

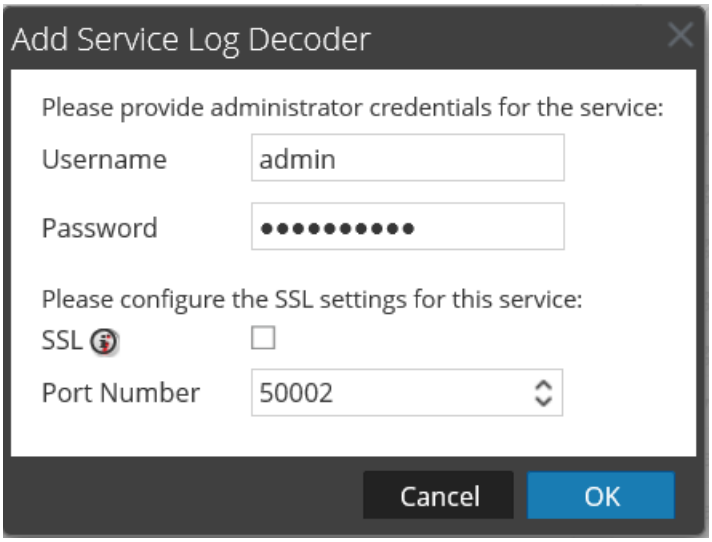
So fügen Sie einen Log Decoder als Datenquelle zu Archiver hinzu:

1. Navigieren Sie zu **ADMIN> Services.**
2. Wählen Sie den Archiver-Service aus.
3. Wählen Sie in der Spalte  **Aktionen** die Optionen **Ansicht > Konfiguration aus.**Die Ansicht „Services“ > „Konfiguration“ von Archiver wird angezeigt.
4. Klicken Sie auf der Registerkarte **Allgemein** im Bereich **Services aggregieren** auf  .

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



5. Wählen Sie den Log Decoder-Service aus, den Sie dem Archiver als Datenquelle hinzufügen möchten, und klicken Sie auf **OK**.
6. Wenn der Log Decoder ein Vertrauensmodell verwendet, wird das Dialogfeld „Service hinzufügen“ angezeigt:



7. Geben Sie den Benutzernamen und das Passwort für den Log Decoder ein und konfigurieren Sie die SSL-Einstellungen.
8. Klicken Sie auf **OK**.
   Der ausgewählte Log Decoder-Service wird im Bereich **Services aggregieren** aufgeführt.

Überlegungen zu Archiver-Metaeinstellungen

Zur Maximierung der Aufbewahrungszeit wurden die Metaelemente und der Index des Archiver reduziert (im Vergleich zum Concentrator), um typische Reportinganforderungen zu unterstützen. Das bedeutet, dass Sie standardmäßig möglicherweise nicht alle Berichte ausführen können, die Sie auf dem Concentrator auf dem Archiver ausführen. Sie können eine Liste der aktuell vom Archiver verwendeten Metadaten und Indexelemente an den folgenden Speicherorten anzeigen:

- **Ansicht Explorer:** Der Pfad **/archiver/devices/<logdecoder>/config/options** im Feld **metaInclude** zeigt die aktuelle Liste der Metaelemente an.
- Ansicht **Konfiguration > Registerkarte Dateien**: Die Datei **index-archiver.xml** zeigt die Standardindexkonfiguration an. Die Datei **index-archiver-custom.xml** zeigt alle Änderungen an.

Die Metaelemente und der Index des Archiver können zur Unterstützung von kundenspezifischen Reportinganforderungen angepasst werden. Dafür müssen jedoch zusätzlicher Speicher sowie zusätzliche CPU- und Arbeitsspeicherressourcen unterstützt werden. Zudem kann sich das auf die Aufbewahrungszeit auswirken. Wenn mehr Metaelemente zum Archiver hinzugefügt werden, reduziert sich die maximale Aggregationsrate und erhöht sich die Zeit zum Ausführen von Berichten.

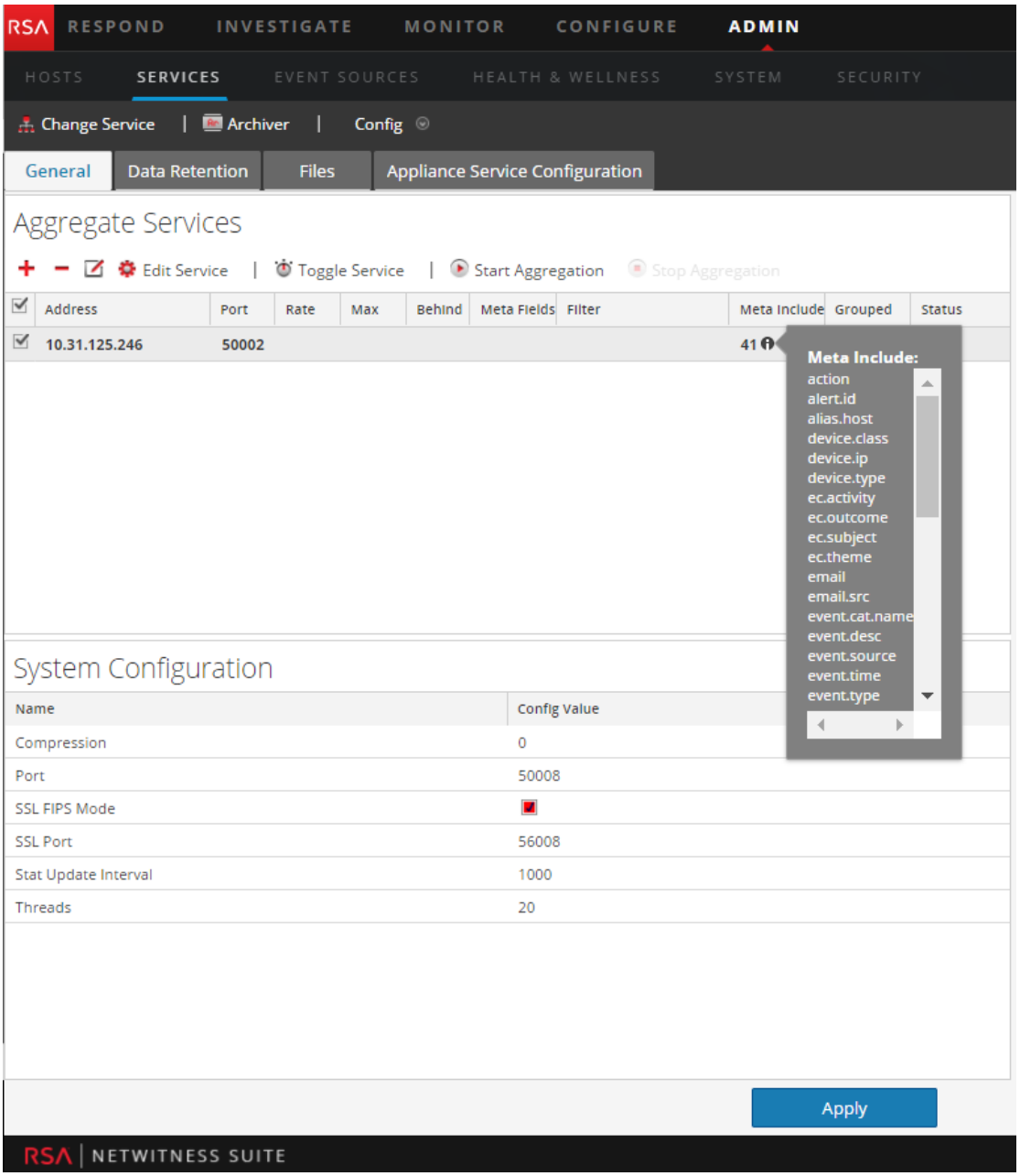
Unter (Optional) Konfigurieren von Metafiltern für Aggregation und (Optional) Hinzufügen von Indexeinträgen für Archiver Reporting finden Sie zusätzliche Details.

(Optional) Konfigurieren von Metafiltern für Aggregation

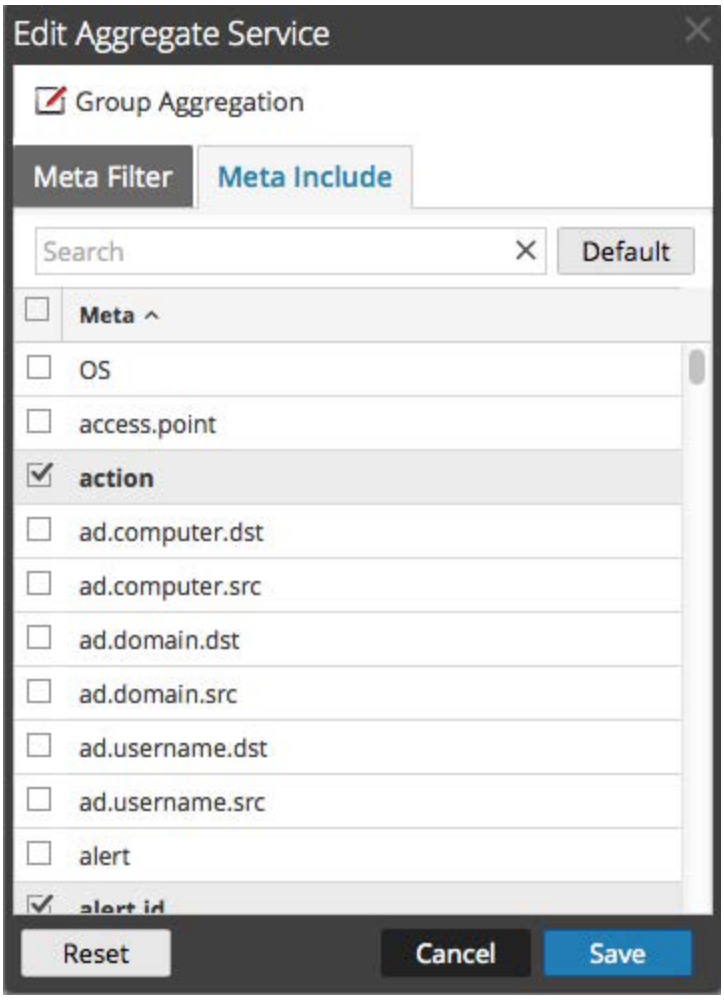
Gehen Sie folgendermaßen vor, um zusätzliche Metaelemente anzuzeigen und dem Archiver hinzuzufügen.

Achtung: Für das Hinzufügen von Metadaten oder Indizes müssen zusätzlicher Speicher sowie zusätzliche CPU- und Arbeitsspeicherressourcen unterstützt werden. Zudem kann sich das Hinzufügen auf die Aufbewahrungszeit auswirken. Wenn mehr Metaelemente zum Archiver hinzugefügt werden, reduziert sich die maximale Aggregationsrate und erhöht sich die Zeit zum Ausführen von Berichten.

1. Wählen Sie zum Anzeigen der aktuellen Metaelemente im Bereich **Services aggregieren** den Log Decoder-Service aus und klicken Sie im Feld **Enthaltene Metadaten** auf .



2. Wählen Sie zum Hinzufügen zusätzlicher Metaelemente den Log Decoder-Service aus und klicken Sie auf .



3. Wählen Sie im Dialogfeld „Aggregierten Service bearbeiten“ die Meta-Elemente aus, die in der Liste der enthaltenen Metadaten enthalten sein sollen. Sie können beispielsweise das Einschließen von „ip.srcport“, „tcp.srcport“, „udp.srcport“, „msg“, „url“, „query“, „bytes“, „alias.host“, „ip.dst“, „ip.dstport“, „ip.src“, „tcp.dstport“, „megabytes“, „time“, „event.desc“ und „word“ in Betracht ziehen.
4. Klicken Sie auf **Speichern** und dann auf **Schließen**.
5. Unter(Optional) Hinzufügen von Indexeinträgen für Archiver Reportingweiter unten finden Sie Informationen zum Indexieren der zusätzlichen Metaschlüssel.

(Optional) Hinzufügen von Indexeinträgen für Archiver Reporting

Achtung: Für das Hinzufügen von Metadaten oder Indizes müssen zusätzlicher Speicher sowie zusätzliche CPU- und Arbeitsspeicherressourcen unterstützt werden. Zudem kann sich das Hinzufügen auf die Aufbewahrungszeit auswirken. Wenn mehr Metaelemente zum Archiver hinzugefügt werden, reduziert sich die maximale Aggregationsrate und erhöht sich die Zeit zum Ausführen von Berichten.

Die Standardindexkonfiguration des Archiver enthält nur Wertindizes für die folgenden Schlüssel:

- time
- Decoder-Quelle (did)
- Zielbenutzerkonto(user.dst)
- Warnmeldungs-ID (alert.id)
- Device-IP-Adresse (device.ip)
- Quell-IP-Adresse (ip.src)
- Ziel-IP-Adresse (ip.dst)
- Beschreibung des Ereignisses (event.desc)
- Geräteklasse (device.class)
- medium
- Objektname (obj.name)
- Wort (word)

Informationen zur Anpassung dieser Liste finden Sie unter **Indexanpassung** im *Tuningleitfaden für die Core-Datenbank*.

Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung

Dieses Thema enthält Anweisungen für Administratoren zur Konfiguration des Speichers und der Protokollaufbewahrung auf einem Archiver.

Aus Gründen der Compliance ist es häufig erforderlich, einige Protokolle länger als andere aufzubewahren. Einige Protokolle sind rechtlich sensibel und dürfen nicht für einen langen Zeitraum aufbewahrt werden. Andere Protokollen müssen für viele Jahre aufbewahrt werden. Zusätzlich zur Compliance sind einige Protokolle nützlich für die Verlaufsforensik, während andere Protokolle wenig oder keinen sicherheits- oder betriebsbezogenen Wert haben und nach kurzer Zeit gelöscht werden können.

Da die geschäftlichen Anforderungen variieren, können Sie mit NetWitness Suite Sammlungen konfigurieren, die Protokollaufbewahrungssätze für das Speichern von Protokolldaten sind. Sie können für jede Sammlung angeben, wie viel des gesamten Speicherplatzes verwendet werden soll und für wie viele Tage die Protokolle in der Sammlung aufbewahrt werden. Zum Angeben des Protokolltyps für die Sammlung definieren Sie Aufbewahrungsregeln, die Sammlungen zugeordnet werden. Aufbewahrungsregeln für alle Sammlungen werden sequenziell in einer von Ihnen definierten Reihenfolge ausgeführt.

Dafür müssen Sie zunächst den gesamten physischen Speicherplatz für Ihre Sammlungen definieren. Mit NetWitness Suite können Sie drei Arten von Speicher definieren:

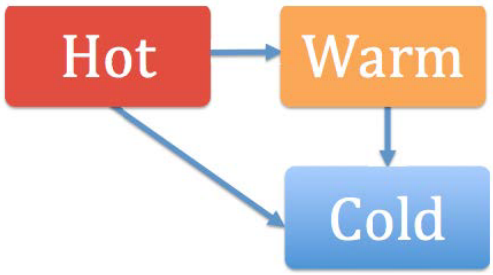
- **Hot-Tier-Speicher**: DieserSpeicher enthält Protokolldaten, die als Teil des Geschäftsprozesses aktiv verwendet werden. Benutzer können auf diese Protokolle schneller als auf andere Arten von Speicher zugreifen und sie können die Protokolle für Reporting- und andere Aufgaben verwenden. Hot-Speicher ist in der Regel SAN- oder DAC-Speicher (Direct Access Capacity).
- **Warm-Tier-Speicher**: (Optional) Dieser Speicher enthält ältere Protokolldaten, die von Archiver aggregiert werden. Der Zugriff auf Protokolldaten ist langsamer als beim Hot-Speicher. Benutzer können diese Protokolle ebenfalls für Reporting- und andere Aufgaben verwenden. Warm-Speicher ist in der Regel Network Attached Storage(NAS).
- **Cold-Tier-Speicher**: (Optional) Dieser Speicher enthält die ältesten Protokolldaten, die entweder für den Betrieb des Unternehmens benötigt werden oder gemäß behördlicher Auflagen erforderlich sind. Die Protokolle sind offline und Archiver kann auf diese Protokolle nicht für Reporting- oder andere Aufgaben zugreifen. Wenn Sie allerdings auf diese Protokolldaten zugreifen möchten, können Sie sie in den Sammlungen wiederherstellen, die im Archiver-Service erstellt wurden, und sie dann für das Reporting verwenden. Cold-Speicher ist in der Regel Offlinespeicher wie NAS oder temporärer Speicher vor der

Archivierung auf Band. Sobald die Daten an den Cold Tier verschoben wurden, werden diese Daten nicht mehr von Archiver verwaltet. Nach der Verschiebung sind externe Prozesse dafür zuständig, die Daten zu sichern oder diesen Cold-Tier-Speicherplatz so zu verwalten, dass die Kapazität nicht zu 100 % ausgelastet wird. Wenn die Kapazität erreicht ist, beendet Archiver die Aggregation, bis das Problem behoben ist.

Archivers verwenden per Vorkonfiguration verfügbaren Hot-Speicher und eine Standardprotokollsammlung. Das bedeutet, dass Sie Archiver-Speicher und die Protokollaufbewahrung nur dann konfigurieren müssen, wenn Sie komplexe Anforderungen an die Protokollaufbewahrung haben.

Protokolle können auf folgende Weise von einer Art von Speicher auf eine andere verschoben werden:

- Hot-Speicher > Cold-Speicher
- Hot-Speicher > Warm-Speicher > Cold-Speicher



Wenn eine Sammlung die Aufbewahrungsfristen für Hot- und Warm-Speicher erreicht hat, löscht NetWitness Suite die Protokolldaten aus diesen Speichern. Wenn ein Cold-Speicher konfiguriert wurde, wird eine Kopie darin abgelegt, bevor die Protokolle aus dem Hot- oder Warm-Speicher gelöscht werden. Wenn Sie beispielsweise eine Sammlung mit 1 TB Hot-Speicher, 1 TB Warm-Speicher und aktiviertem Cold-Speicher haben und die Protokolldaten 1 TB Hot-Speicher erreichen, werden die ältesten Protokolldaten in den Warm-Speicher verschoben. Wenn die Protokolldaten im Warm-Speicher 1 TB erreichen, werden die ältesten Protokolldaten vom Warm-Speicher in den Cold-Speicher kopiert, bevor sie aus dem Warm-Speicher entfernt werden.

Bei Hot- und Warm-Speicher können sich die Einstellungen für die Größe und Aufbewahrungsfrist für eine Sammlung gegenseitig außer Kraft setzen, je nachdem welches Kriterium (Größe oder Zeit) zuerst erfüllt ist. Wenn Sie beispielsweise eine Sammlung mit 1 TB Hot-Speicher, keinem Warm- oder Cold-Speicher und einer Aufbewahrungsfrist von 20 Tagen haben und die Protokolldaten nach 11 Tagen 1 TB überschreiten, werden die ältesten Protokolle über 1 TB gelöscht, obwohl die Sammlung eine Aufbewahrungsfrist von 20 Tagen hat.

Nach der Erstellung des Hot-, Warm- und Cold-Speichers konfigurieren Sie Ihre Speichersammlungen für die Protokollaufbewahrung. Sie können die maximale Größe des Hot- und Warm-Speichers für die Sammlung, eine eventuelle Verwendung von Cold-Speicher, die Anzahl der Tage, für die Protokolle in der Sammlung aufbewahrt werden, und die Datenkomprimierung angeben sowie festlegen, ob ein Hashalgorithmus verwendet werden soll, um die Datenintegrität der gespeicherten Dateien überprüfen zu können.

Nach der Konfiguration Ihrer Sammlungen definieren Sie Aufbewahrungsregeln für Ihre Sammlung. Diese Regeln geben den Typ der Protokolle an, die in der Sammlung gespeichert werden sollen. Jeder Sammlung muss mindestens eine Aufbewahrungsregel zugeordnet werden, damit sie Protokolldaten speichern kann.

Verfahren

Führen Sie die folgenden Aufgaben in der gezeigten Reihenfolge durch, um den Speicher und die Protokollaufbewahrung zu konfigurieren.

Aufgabe	Referenz
1. Konfigurieren Sie den Hot-, Warm- und Cold-Gesamtspeicher.	Weitere Informationen finden Sie unter Konfigurieren des Hot-, Warm- und Cold-Speichers.
2. Konfigurieren Sie die Speichersammlungen für die Protokollaufbewahrung.	Weitere Informationen finden Sie unter Konfigurieren von Protokollspeichersammlungen.
3. Definieren Sie Aufbewahrungsregeln für die Sammlungen und legen Sie die Reihenfolge der Ausführung der gesamten Liste von Aufbewahrungsregeln fest.	Weitere Informationen finden Sie unter Definieren der Aufbewahrungsregeln.

Konfigurieren des Hot-, Warm- und Cold-Speichers

Dieses Thema enthält Anweisungen für Administratoren zur Konfiguration des Hot-, Warm- und Cold-Gesamtspeichers auf einem Archiver.

Ein Archiver-Host verfügt über Hot-Speicher, der gemäß den Standardwerten vorkonfiguriert ist. Administratoren können den Hot-, Warm- und Cold-Gesamtspeicher konfigurieren, um ihre speziellen geschäftlichen Anforderungen zu erfüllen. Auf einem Archiver muss der Hot-Gesamtspeicher konfiguriert sein, dagegen sind Warm- und Cold-Speicherkonfigurationen optional. Der Cold-Speicher wird nicht von NetWitness Suite gemanagt.

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

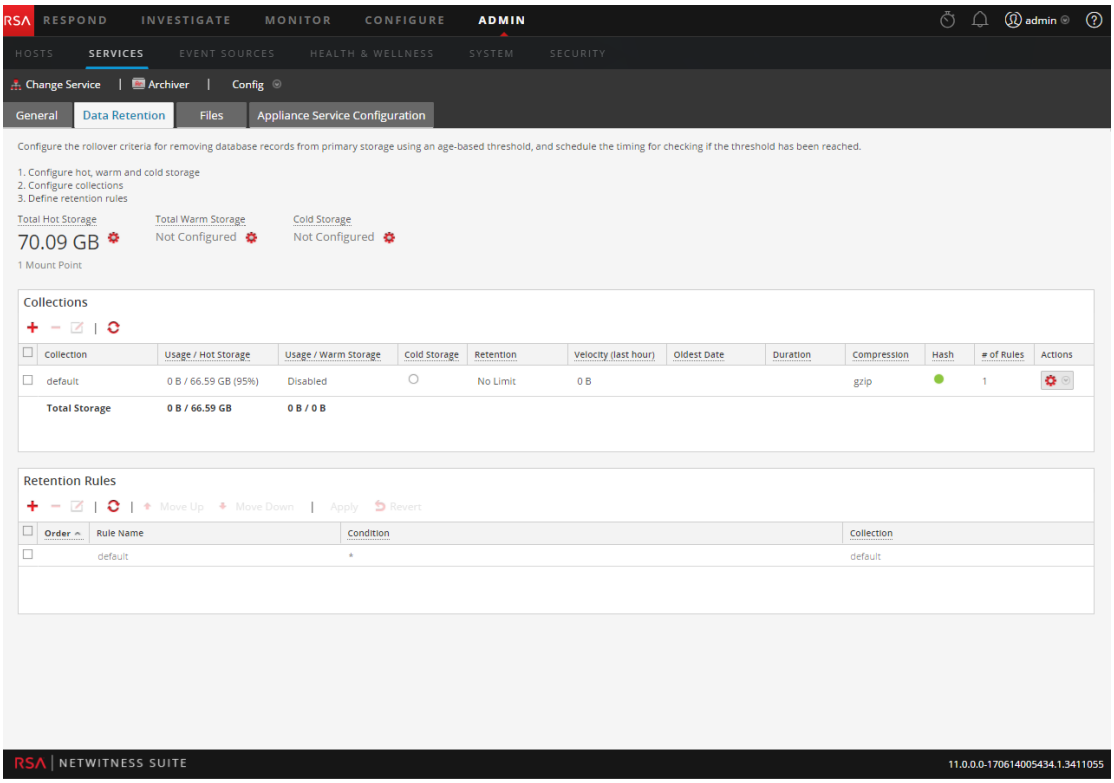
1. Sie haben den Archiver-Host in Ihrer Netzwerkumgebung installiert.
2. Der Log Decoder wurde in Ihrer Netzwerkumgebung installiert und konfiguriert.
3. Archiver wurde als Core-Service zu Ihrer NetWitness Suite-Bereitstellung hinzugefügt.
4. Log Decoder-Services wurden als Datenquelle für Archiver hinzugefügt.
5. DAC oder anderer physischer Speicher wurde in Ihrer Netzwerkumgebung installiert und konfiguriert.
6. Die Anforderungen an Protokollaufbewahrung und Speicher wurden ermittelt.

Methoden

Konfigurieren des Hot-Gesamtspeichers für einen Archiver

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Archiver-Service und dann  **>Ansicht > Konfiguration** aus.

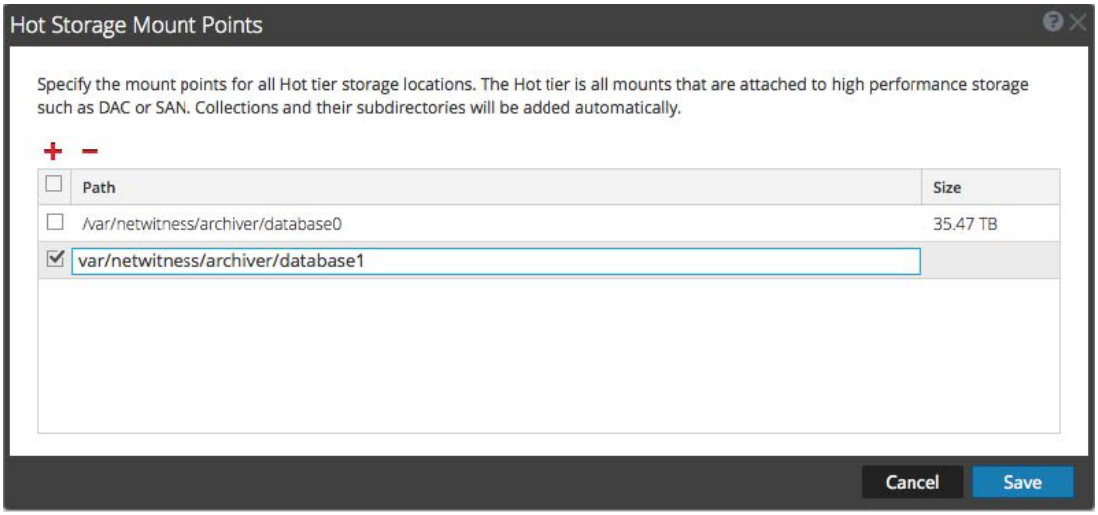
   Die Ansicht „Services“ > „Konfiguration“ von Archiver wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenaufbewahrung** im Bereich **Hot-Speicher gesamt** auf  , um den Hot-Gesamtspeicher zu konfigurieren.



4. Fügen Sie im Dialogfeld **Mount-Punkte für Hot-Speicher** die dem Archiver-Host angebundenen Mount-Punkte hinzu, die Sie in den Hot-Gesamtspeicher einschließen möchten.

   Dabei handelt es sich um die Pfade zum Speicher mit hoher Performance, wie DAC-Speicher und SAN. Fügen Sie keine Sammlungen oder Unterverzeichnisse zu den Mount-Punkten hinzu.

   Klicken Sie zum Hinzufügen eines Mount-Punkts auf + und geben Sie den Pfad zu dem Mount-Punkt ein.



5. Stellen Sie sicher, dass die Pfade er Mount-Punkt korrekt sind, und klicken Sie auf **Speichern**.
   NetWitness Suite erstellt automatisch die Verzeichnisse metadb, packetdb, sessiondb und index für jede auf dem Archiver definierte Sammlung:
   <storageLocation>/<CollectionName>/metadb
   <storageLocation>/<CollectionName>/packetdb
   <storageLocation>/<CollectionName>/sessiondb
   <storageLocation>/<CollectionName>/index

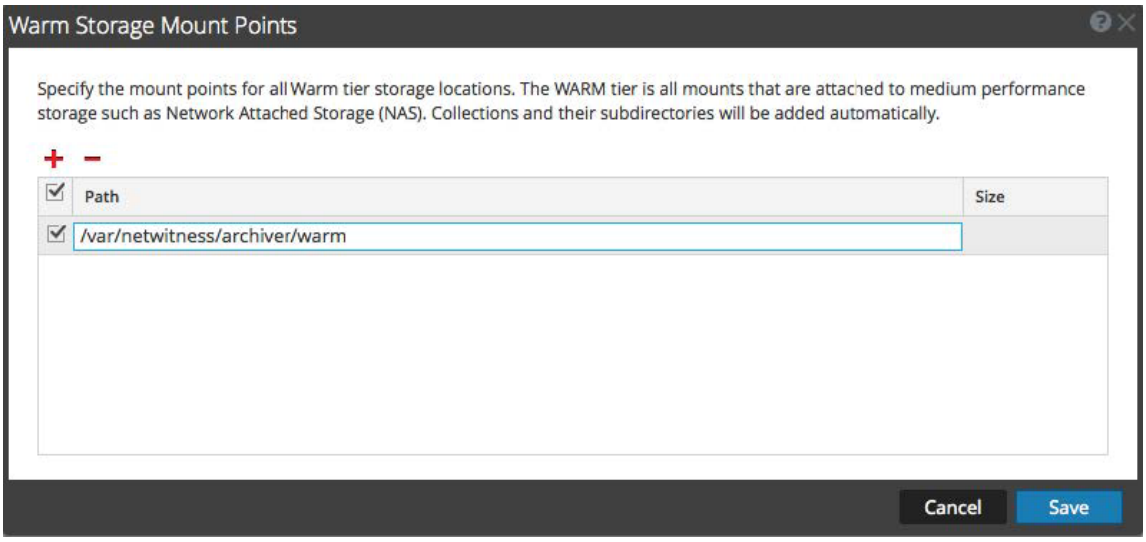
   Beispiel: Wenn Ihr Mount-Punkt /var/netwitness/archiver lautet, werden die folgenden Verzeichnisse für jede Ihrer Sammlungen erstellt:
   /var/netwitness/archiver/<CollectionName>/metadb
   /var/netwitness/archiver/<CollectionName>/packetdb
   /var/netwitness/archiver/<CollectionName>/sessiondb
   /var/netwitness/archiver/<CollectionName>/index

   Nach Neustart des Archiver-Services werden die Daten in den definierten Sammlungen gespeichert. Stellen Sie sicher, dass Ihre Protokollaufbewahrungssammlungen korrekt sind, bevor Sie den Archiver-Service neu starten.

Achtung: Nachdem die Daten an einen Mount-Punkt gespeichert wurden, können dieser nicht von der Benutzeroberfläche entfernt werden.

Konfigurieren des Warm-Gesamtspeichers für einen Archiver

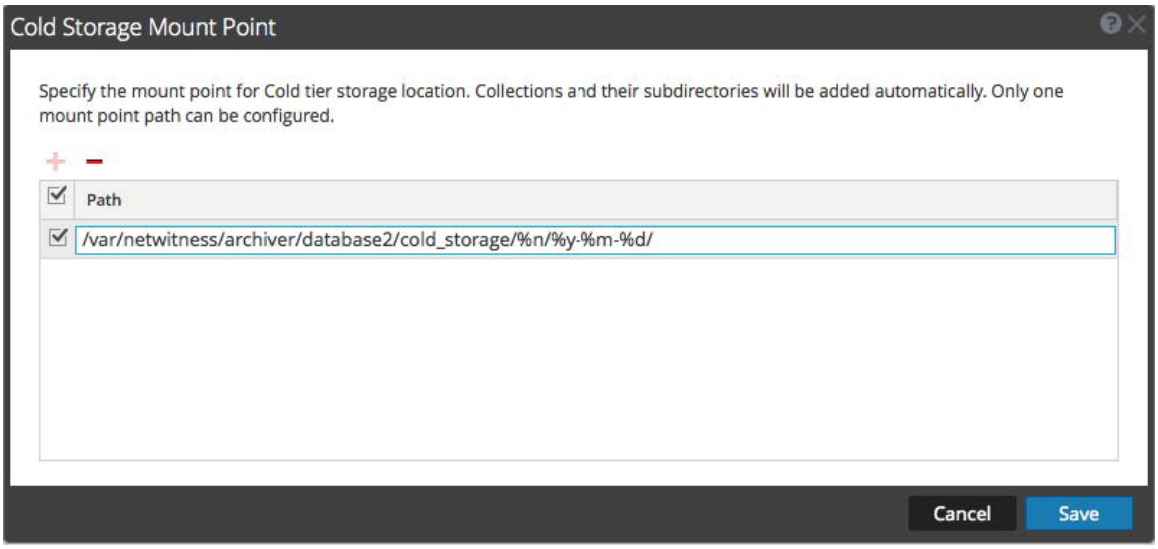
(Optional) Das Verfahren zum Konfigurieren von Warm-Gesamtspeichers für einen Archiver ist identisch mit dem Verfahren für den Hot-Gesamtspeicher, mit der Ausnahme, dass Sie im Bereich „Warm-Speicher gesamt“ auf  klicken und die Mount-Punkte hinzufügen, die Sie als Warm-Speicher verwenden möchten, d. h. die physischen Pfade zum Warm-Speicher, z. B. NAS (Network Attached Storage).



Konfigurieren des Cold-Gesamtspeichers für einen Archiver

(Optional) Das Verfahren zum Konfigurieren des Cold-Gesamtspeichers für einen Archiver ist identisch mit dem Verfahren für den Hot-Gesamtspeicher, mit der Ausnahme, dass Sie auf im Abschnitt „Cold-Speicher gesamt“ klicken und nur einen Mount-Punkt für Cold-Speicher hinzufügen. Cold-Speicher wird nicht von NetWitness Suite gemanagt.

Sie müssen an irgendeinem Punkt des Pfadnamens für den Cold-Speicher-Mount-Punkt die Formatspezifizierung `%n` für den Sammlungsnamen einschließen, um Dateinamenkonflikte zwischen Sammlungen zu vermeiden.



Die folgenden Formatspezifizierungen sind im Pfad zulässig:

Formatspezifizierung	Beschreibung
%n	Name der Sammlung (erforderlich)
%y	Jahr, in dem die Daten in den Cold-Speicher verschoben wurden
%m	Monat
%d	day
%h	Stunde
%##r	Block von Stunden für den aktuellen Tag. Beispiel: Wenn Sie beispielsweise drei 8-Stunden-Blöcke möchten, können Sie es auf %8r einstellen. Für die ersten 8 Stunden des Tages wird 0 zurückgeben, für die zweiten 8 Stunden 1 und die letzten 8 Stunden des Tages 2.

Die Änderungen werden sofort übernommen.

Beispiel: Wenn Sie eine Sammlung namens **Compliance** haben und den folgenden Cold-Speicherpfad erstellen:

```
/sa-cold-storage/%n/%y-%m-%d/
```

NetWitness Suite erstellt jeden Tag ein Verzeichnis mit dem folgenden Format:

/sa-cold-storage/compliance/2015-11-20/

Hot-, Warm- und Cold-Tier-Speicherfunktionen

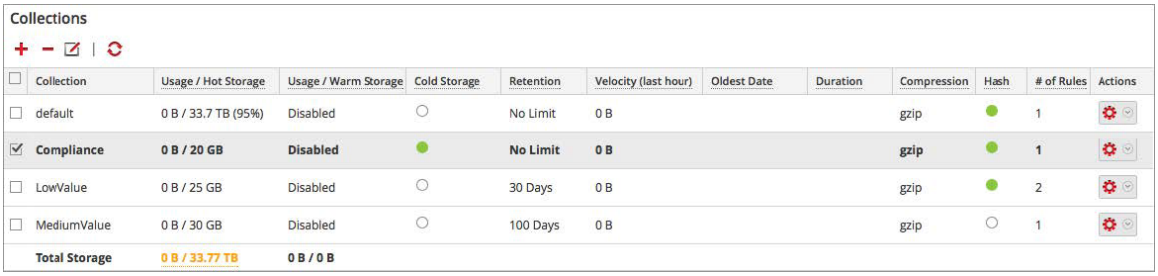
In der folgenden Tabelle sind die Funktionen der Dialogfelder für Hot-, Warm- und Cold-Tier-Speicher beschrieben.

Funktion	Beschreibung
+	Fügt einen Mount-Punkthinzu.
−	Entfernt einen Mount-Punkt. Sie können einen Mount-Punkt, der verwendet wird, nur löschen, wenn Sie die zugehörigen Sammlungen löschen.
☐	Wählen Sie die Mount-Punkte aus, die Sie dem Hot-, Warm- und Cold-Gesamtspeicher hinzufügen möchten. Sie können nur einen Mount-Punkt für Cold-Gesamtppeicherauswählen.

Funktion	Beschreibung
Mount-Punkt	Zeigt den Pfad zum verknüpften physischen Speicher an. Beispiel: **/var/netwitness/archiver/database0**, der Speicherort des Hot-Speicher-DAC. Fügen Sie den Mount-Punkten keine Sammlungen oder Unterverzeichnisse hinzu. NetWitness Suite erstellt automatisch die Verzeichnisse metadb, packetdb, sessiondb und index für jede auf dem Archiver definierte Sammlung: <storageLocation>/<CollectionName>/metadb <storageLocation>/<CollectionName>/packetdb <storageLocation>/<CollectionName>/sessiondb <storageLocation>/<CollectionName>/index Wenn z. B. Ihr Hot-Speicher-Mount-Punkt /var/netwitness/archiver ist, dann werden die folgenden Verzeichnisse für jede Ihrer Sammlungen erstellt: /var/netwitness/archiver/<CollectionName>/metadb /var/netwitness/archiver/<CollectionName>/packetdb /var/netwitness/archiver/<CollectionName>/sessiondb /var/netwitness/archiver/<CollectionName>/index Für Cpld-Speicher müssen Sie an irgendeinem Punkt des Pfadnamens für den Cold-Speicher-Mount-Punkt die Formatspezifizierung für den Sammlungsnamen `%n` einschließen, um Dateinamenkonflikte zwischen Sammlungen zu vermeiden.
Speichergröße	Zeigt die Größe des verknüpften Speichers an. Auf der Registerkarte „Datenaufbewahrung“ wird zu Referenzzwecken die Gesamtspeichermenge angezeigt.

Sammlungen

Im Abschnitt Sammlungen sind alle Speichersammlungen zusammen mit dem Gesamtspeicherplatz für Hot- und Warm-Speicher aufgeführt.



Funktionen von Sammlungen

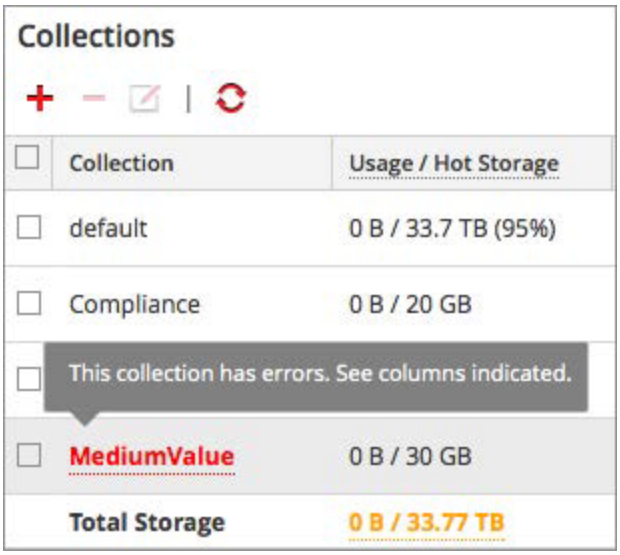
In der folgenden Tabelle werden die Symbole und Spalten des Abschnitts „Sammlungen“ beschrieben. Sie können einige der Spalten basierend auf Ihren Anforderungen ausblenden.

Funktion	Beschreibung
	Öffnet das Dialogfeld „Sammlungen“, in dem Sie eine Speichersammlung hinzufügen können.
	Entfernt die ausgewählte Sammlung. Beim Löschen der Sammlung werden alle gespeicherten Daten aus der Sammlung entfernt, die leeren Datenverzeichnisse bleiben jedoch erhalten.
	Öffnet das Dialogfeld „Sammlungen“, in dem Sie die ausgewählte Speichersammlung bearbeiten können.
	Aktualisiert Sammlungsinformationen.
	Wählt eine Sammlung aus. Sie können beispielsweise eine Sammlung zum Bearbeiten oder Entfernen auswählen.
Sammlung	Zeigt den Namen Ihrer Sammlung an, z. B. Standard, Compliance, MediumValue und LowValue. Sie können mehrere Sammlungen mit unterschiedlichen Kriterien für die Aufbewahrung von Protokollen erstellen. Wenn Sie keine Sammlungen erstellen, wird die Standardsammlung verwendet. Wenn eine Sammlung Fehler aufweist, werden der Name der Sammlung und die Spalten mit Fehlern in roter Schrift angezeigt.
Auslastung/Hot-Speicher	Zeigt die aktuelle Auslastung des Hot-Speichers und den maximalen Hot-Speicher für die Sammlung an. Wenn die Größe der Protokolle die maximale Hot-Speichermenge erreicht, werden die Protokolle entfernt oder auf den nächsten verfügbaren Storage Tier (Warm- oder Cold-Speicher) verschoben.

Funktion	Beschreibung
Auslastung/Warm-Speicher	Zeigt die aktuelle Auslastung des Warm-Speichers und den maximalen Hot-Speicher für die Sammlung an. Wenn die Größe der Protokolle die maximale Warm-Speichergröße erreicht, werden die Protokolle entfernt oder auf den verfügbaren Cold-Speicher verschoben.
Cold-Speicher	Zeigt an, ob Cold-Speicher aktiviert oder deaktiviert ist Ein vollfarbiger grüner Kreis zeigt an, dass der Cold-Speicher aktiviert ist ( ). Ein leerer weißer Kreis zeigt an, dass der Cold-Speicher deaktiviert ist.
Aufbewahrungszeitraum	Zeigt die Anzahl der Tage an, für die Protokolle aufbewahrt werden, bevor sie entfernt oder optional in Cold-Speicher verschoben werden. Keine Begrenzung gibt an, dass die Protokollaufbewahrung nicht durch eine angegebene Anzahl von Tagen eingeschränkt ist. Bei Hot- und Warm-Speicher können sich die Einstellungen für die Größe und Aufbewahrungsfrist für eine Sammlung gegenseitig außer Kraft setzen, je nachdem welches Kriterium (Größe oder Zeit) zuerst erfüllt ist.
Geschwindigkeit (letzte Stunde)	Zeigt die Anzahl der Protokolle an, die im Lauf der letzten Stunde erfasst wurden.
Ältestes Datum	Zeigt das Datum und Uhrzeit der letzten Protokollerfassung an.
Dauer	Zeigt an, vor wie vielen Tagen das letzte Protokoll erfasst wurde. Beispiel: 20 Tage
Komprimierung	Zeigt den für die Metadaten und Rohdaten in der Sammlung verwendeten Komprimierungstypan.

Funktion	Beschreibung
Hash	Zeigt an, ob Hash aktiviert oder deaktiviert ist. Bei Aktivierung wird der Hashalgorithmus verwendet, um die Datenintegrität der zu speichernden Dateien sicherzustellen. Standardmäßig werden nur Rohdatenprotokolle gehasht und die Hash-Dateien werden im selben Verzeichnis gespeichert wie die Daten.
Anzahl Regeln	Zeigt die Anzahl der Regeln an, die für die Sammlung angewendet werden. Definieren Sie mindestens eine Regel für jede Sammlung. Eine Sammlung ohne zugeordneten Regeln zeigt eine Null in roter Schrift als Warnung an: Der Name der Sammlung wird ebenfalls in roter Schrift dargestellt, was einen Fehler in der Sammlung anzeigt. **Achtung:** Wenn eine Sammlung keine Regel aufweist, werden in dieser Sammlung niemals Protokolle gespeichert.
Aktionen	Hier können Sie einer Sammlung zugeordneten Regeln im Abschnitt Aufbewahrungsregel anzeigen, wenn Sie <Aktionsschaltfläche> > **Regeln auswählen** auswählen. Im Abschnitt „Aufbewahrungsregel“ können Sie die allgemeine Priorität der Sammlungsregeln ändern.
Gesamtspeicherplatz	Zeigt die aktuelle Gesamtauslastung des Hot-Speichers und den maximalen Hot-Gesamtspeicher im unteren Bereich der Spalte **Auslastung/Hot-Speicher** an. Außerdem werden die aktuelle Gesamtauslastung des Warm-Speichers und der maximale Warm-Gesamtspeicher im unteren Bereich der Spalte **Auslastung/Warm-Speicher** angezeigt.

Fehler in der Sammlung werden in roter Schrift angezeigt. Eine gepunktete Unterstreichung gibt an, dass eine Kurzinformation mit Informationen zum Fehler verfügbar ist.



Sammlungen, bei denen die Bearbeitung deaktiviert (abgeblendet) ist, bieten ebenfalls Kurzinformationen, die Informationen über das Problem bereitstellen.

Aufbewahrungsregeln

Im Abschnitt Aufbewahrungsregeln werden alle Aufbewahrungsregeln für Ihre Speichersammlungen in der Reihenfolge der Regelausführung aufgeführt.

In der folgenden Tabelle werden die Funktionen des Abschnitts Aufbewahrungsregel beschrieben.

Funktion	Beschreibung
	Öffnet das Dialogfeld „Regeldefinition“, in dem Sie eine Aufbewahrungsregel für eine Speichersammlung hinzufügen können.
	Entfernt die ausgewählte Aufbewahrungsregel. Damit Ihre Protokollsammlungen Protokolldaten erfassen und speichern können, müssen Sie diese mit mindestens einer Aufbewahrungsregel verknüpfen.
	Öffnet das Dialogfeld „Regeldefinition“, in dem Sie die ausgewählte Aufbewahrungsregel bearbeiten können.

Funktion	Beschreibung
	Aktualisiert die Informationen zur Aufbewahrungsregel.
Nach oben	Verschiebt die ausgewählte Aufbewahrungsregel in der Prioritätenliste für Aufbewahrungsregeln nach oben. Die Reihenfolge der Aufbewahrungsregeln ist sehr wichtig. NetWitness Suite bewertet die Aufbewahrungsregeln für alle Sammlungen in numerischer Reihenfolge nach der in der Spalte Reihenfolge im Abschnitt Aufbewahrungsregel angegebenen Zahl. Sie können Aufbewahrungsregeln auch mithilfe von Drag-and-drop neusortieren.
Nach unten	Verschiebt die ausgewählte Aufbewahrungsregel in der Prioritätenliste für Aufbewahrungsregeln nach unten. Die Reihenfolge der Aufbewahrungsregeln ist sehr wichtig. NetWitness Suite führt die Aufbewahrungsregeln für alle Sammlungen in numerischer Reihenfolge nach der in der Spalte Reihenfolge im Abschnitt Aufbewahrungsregel angegebenen Zahl aus.
Anwenden	Speichert die Änderung der Regelreihenfolge.
Zurücksetzen	Setzt Änderungen an der Regelreihenfolge zurück.
	Wählt eine ausgewählte Aufbewahrungsregel aus oder zeigt sie an.
Reihenfolge	Zeigt die Reihenfolge einer Regel in der Gesamtliste der Aufbewahrungsregeln an.
Name der Regel	Zeigt den Namen der Regel an, z. B. ComplianceDevices und GeneralWindowsLogs.
Bedingung	Zeigt die Bedingungen für die Regel an. Diese Bedingungen geben Sie den Typ der Protokolle an, die in der Sammlung aufgenommen werden sollen. Unter Definieren der Aufbewahrungsregeln finden Sie die Richtlinien für alle Abfragen und Regelbedingungen in Core-Services.
Sammlung	Zeigt den Namen der Sammlung an und zeigt, für wie viele Tage die Sammlung aufbewahrt wird. Beispiel: MediumValue (30 Tage)

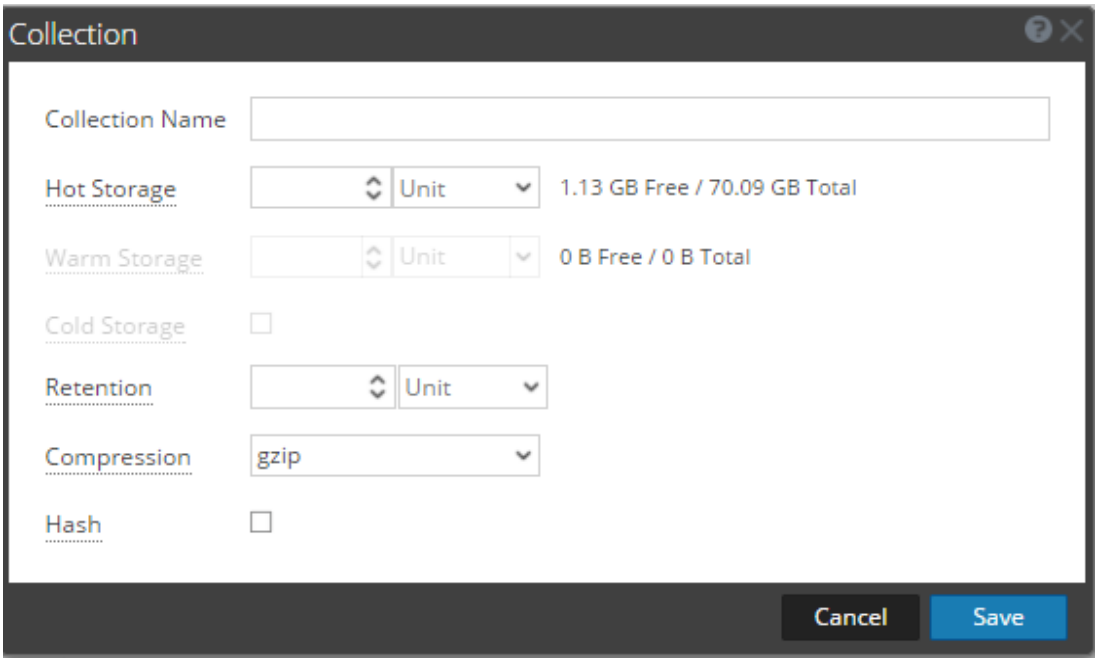
Dialogfeld „Sammlung“

Auf der Registerkarte „ADMIN > Services > Konfiguration > Datenaufbewahrung“ eines Archiver können Administratoren die Kriterien für die Protokollaufbewahrung und den Speicher definieren. Im Dialogfeld „Sammlung“, auf das Sie über den Abschnitt „Sammlungen“ zugreifen können, können Sie einzelne Sammlungen zur Verwendung mit verschiedenen Protokolltypen definieren. Sie können beispielsweise Sammlungen für Compliancezwecke oder die selektive Aufbewahrung kritischer Protokolle erstellen.

Verfahren im Zusammenhang mit diesem Dialogfeld sind unter Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung und Konfigurieren von Protokollspeichersammlungen beschrieben.

So greifen Sie auf das Dialogfeld „Sammlung“ zu:

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie einen Archiver-Service und dann **>Ansicht > Konfiguration** aus.
3. Klicken Sie in der Ansicht „Service-Konfiguration“ des Services auf die Registerkarte **Datenaufbewahrung**.
4. Klicken Sie im Abschnitt **Sammlungen** auf , um die Regel hinzuzufügen oder zu bearbeiten.
   Das Dialogfeld „Sammlung“ wird angezeigt.



In der folgenden Tabelle sind die Felder im Dialogfeld „Sammlung“ beschrieben.

Feld	Beschreibung
Name der Sammlung	Geben Sie einen Namen für Ihre Sammlung ein, z. B. Compliance, MediumValue oder LowValue.
Hot-Speicher	Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Hot-Speicher ein. Der freie Speicherplatz für den Hot-Speicher und der Hot-Gesamtspeicher werden neben diesem Feld angezeigt. Wenn die Größe der Protokolle die maximale Hot-Speichergröße erreicht, werden die Protokolle entfernt oder auf den nächsten verfügbaren Storage Tier (Warm- oder Cold-Speicher) verschoben.
Warm-Speicher	(Optional) Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Warm-Speicher ein. Der freie Speicherplatz für den Warm-Speicher und der Warm-Gesamtspeicher werden neben diesem Feld angezeigt. Wenn die Größe der Protokolle die maximale Warm-Speichergröße erreicht, werden die Protokolle entfernt oder auf den verfügbaren Cold-Speicher verschoben.
Cold-Speicher	(Optional) Geben Sie an, ob für diese Sammlung Cold-Speicher verwendet wird. Bei Verwendung von Cold-Speicher für die Sammlung werden Protokolle außerhalb der angegebenen Größe und Aufbewahrungsfristen auf Cold-Speicher übertragen. Wenn Sie keinen Cold-Speicher verwenden, werden Protokolle außerhalb der angegebenen Größe und Aufbewahrungsfristen entfernt.
Aufbewahrungszeitraum	(Optional) Geben Sie die Anzahl der Tage an, für die Protokolle aufbewahrt werden, bevor sie entfernt oder per Rollover in den Cold-Speicher verschoben werden.Bei Hot- und Warm-Speicher können sich die Einstellungen für die Größe und Aufbewahrungsfrist für eine Sammlung gegenseitig außer Kraft setzen, je nachdem welches Kriterium (Größe oder Zeit) zuerst erfüllt ist.

Feld	Beschreibung
Komprimierung	Geben Sie den Typ der Komprimierung für Metadaten und unverarbeitete Protokolle in der Sammlung an. Sie können die Metadaten und unverarbeiteten Protokolle mithilfe von GZIP oder LZMA komprimieren,um Speicherplatz zu sparen. GZIP ermöglicht eine sehr schnelle Komprimierung und Dekomprimierung, komprimiert jedoch nicht so gut sowie LZMA. LZMA bietet eine bessere Komprimierung auf Kosten derDekomprimierungsgeschwindigkeit (ca. dreimal langsamer als GZIP). Komprimierungsverhältnisse sind stark abhängig von Ihren Daten. Die Standardkomprimierung ist GZIP.
Hash	Geben Sie an, ob Hash aktiviert oder deaktiviert werden soll. Bei Aktivierung wird der Hashalgorithmus verwendet, um die Datenintegrität der zu speichernden Dateien zu gewährleisten. Standardmäßig werden nur Rohdatenprotokolle gehasht und die Hash-Dateien werden im selben Verzeichnis gespeichert wie

Hinweis: Wenn die Speicherzuweisungen für Sammlungen verringert werden oder die Aufbewahrungszeit verkürzt wird, kann es je nach Menge der zu verschiebenden (Rollout-)Daten mehrere Minuten bis Stunden dauern, bis die Daten verschoben wurden und Speicherplatz verfügbar wird. Die Standardzeiten sind alle 20 Minuten für ein Größen-Rollout und alle sechs Stunden für ein Zeit-Rollout.

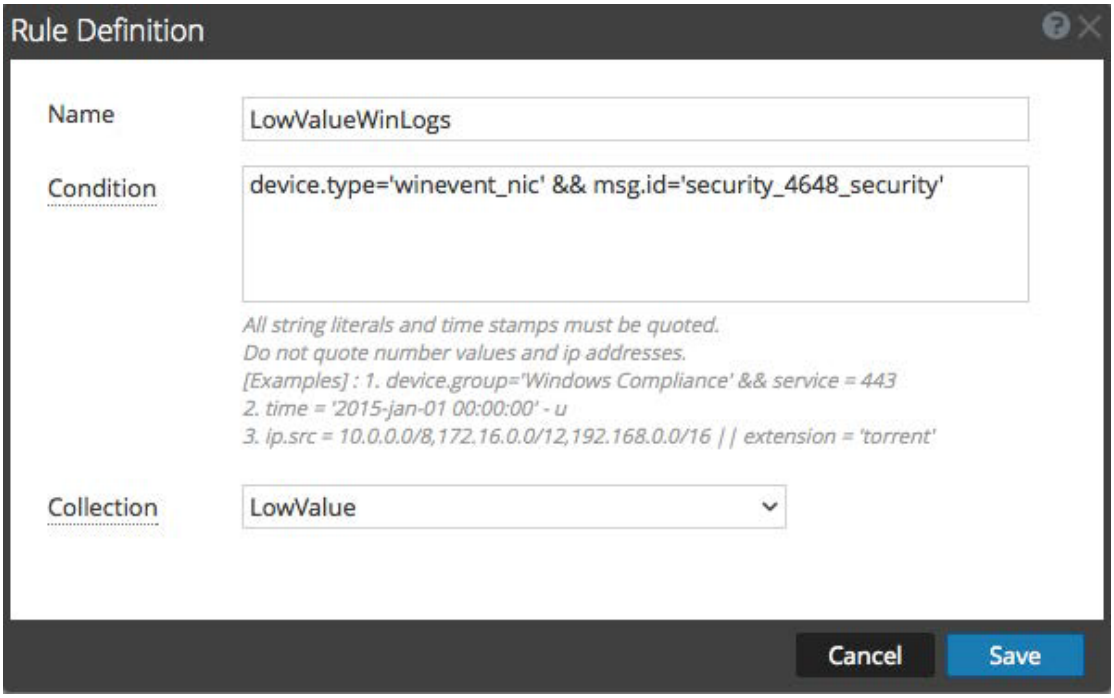
Dialogfeld „Regeldefinition“

Auf der Registerkarte „ADMIN > Services > Konfiguration > Datenaufbewahrung“ eines Archiver können Administratoren die Kriterien für die Protokollaufbewahrung und den Speicher definieren. Im Dialogfeld „Regeldefinition“, das über den Abschnitt „Aufbewahrungsregeln“ zugänglich ist, können Sie Aufbewahrungsregeln zur Verwendung für Ihre Speichersammlungen definieren.

Verfahren im Zusammenhang mit diesem Dialogfeld sind unter Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung und Definieren der Aufbewahrungsregeln beschrieben.

So greifen Sie auf das Dialogfeld „Regeldefinition“ zu:

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie einen Archiver-Service und dann >**Ansicht > Konfiguration** aus.
3. Klicken Sie in der Ansicht „Service-Konfiguration“ des Services auf die Registerkarte **Datenaufbewahrung**.
4. Klicken Sie im Abschnitt **Aufbewahrungsregel** auf + oder .
   Das Dialogfeld „Regeldefinition“ wird angezeigt.



In der folgenden Tabelle sind die Felder im Dialogfeld „Regeldefinition“ beschrieben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für Ihre Aufbewahrungsregel an. Beispiel: ComplianceDevices

Feld	Beschreibung
Bedingung	Geben Sie die Bedingungen für den Typ der Protokolle an, die Sie in die Sammlung einfügen möchten. Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Beispiel: `device.group='PCI Devices' || device.group='HIPPA Devices'`
Sammlung	Wählen Sie die Sammlung aus, für die Sie diese Regel anwenden möchten. Beispiel: Compliance

Nächster Schritt

Konfigurieren SieProtokollspeichersammlungen.

Konfigurieren von Protokollspeichersammlungen

Dieses Thema enthält Anweisungen für Administratoren zur Konfiguration von Protokollspeichersammlungen auf einem Archiver.

NetWitness Suite ermöglicht Ihnen, einzelne Speichersammlungen für verschiedene Protokolltypen zu definieren. Sie können die maximale Größe des von der Sammlung verwendeten Hot- und Warm-Speicherplatzes, eine eventuelle Verwendung von Offlinespeicher (Cold-Speicher), die Anzahl der Tage, für die Protokolle in der Sammlung aufbewahrt werden, und die Datenkomprimierung angeben sowie festlegen, ob ein Hashalgorithmus verwendet werden soll, um die Datenintegrität der gespeicherten Dateien überprüfen zu können. Sie sollten Sammlungen basierend auf Ihre Speicheranforderungen für die Protokollaufbewahrung erstellen. Jede erstellte Sammlung muss mindestens einer Aufbewahrungsregel zugeordnet werden.

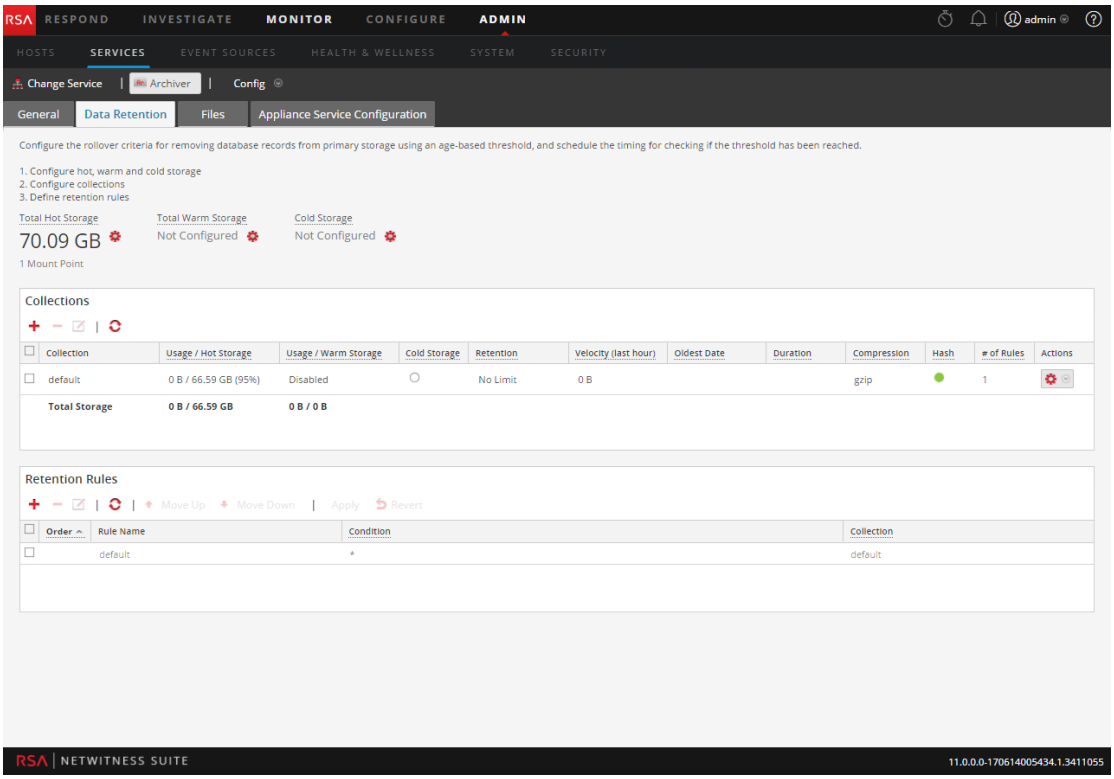
Voraussetzungen

Bevor Sie Ihre Speichersammlungen für die Protokollaufbewahrung konfigurieren, konfigurieren Sie den Hot-, Warm- und Cold-Gesamtspeicher.

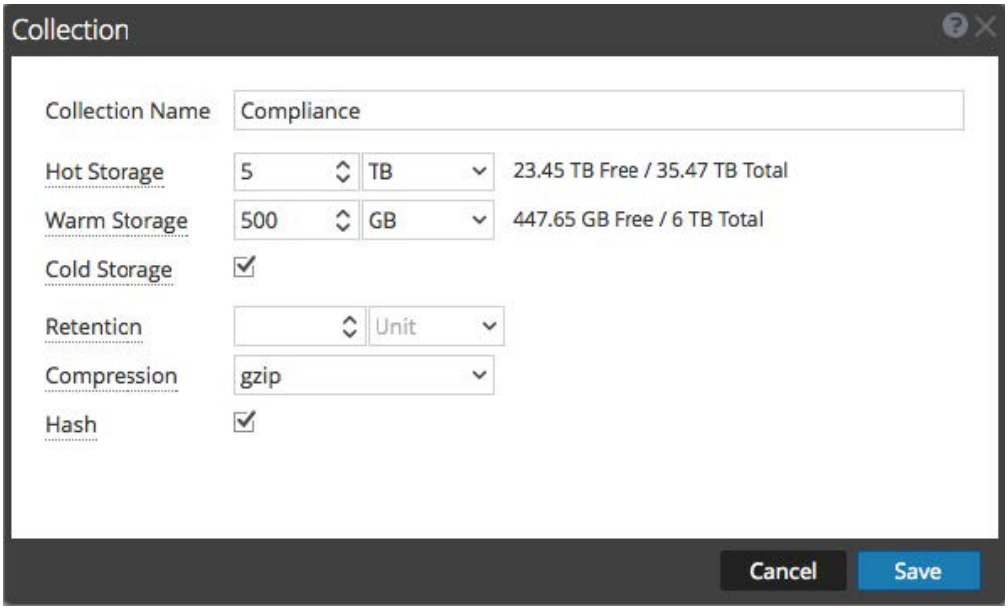
Konfigurieren einer Protokollspeichersammlung

So konfigurieren eine Speichersammlung für die Protokollaufbewahrung auf einem Archiver:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Archiver-Service und dann  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services“ > „Konfiguration“ von Archiver wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenaufbewahrung** im Bereich **Sammlungen** auf  , um eine Sammlung hinzufügen.
   (Wenn Sie Änderungen an einer vorhandenen Sammlung vornehmen möchten, können Sie die Sammlung auswählen und auf  klicken, um die Einstellungen zu ändern.)



Das Dialogfeld **Sammlung** wird angezeigt.



4. Konfigurieren Sie die Sammlung wie in der folgenden Tabelle beschrieben.

Feld	Beschreibung
Name der Sammlung	Geben Sie einen eindeutigen Namen für Ihre Sammlung ein, z. B. Compliance, MediumValue oder LowValue.
Hot-Speicher	Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Hot-Speicher ein. Der freie Speicherplatz für den Hot-Speicher und der Hot-Gesamtspeicher werden neben diesem Feld angezeigt.
Warm-Speicher	(Optional) Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Warm-Speicher ein. Der freie Speicherplatz für den Warm-Speicher und der Warm-Gesamtspeicher werdennebendiesem Feld angezeigt.
Cold-Speicher	(Optional) Geben Sie an, ob für diese Sammlung Cold-Speicher verwendet wird. Wenn Sie Cold-Speicher für die Sammlung verwenden, werden Protokolle außerhalb der Speichergrenzen in den Cold-Speicher kopiert, bevor sie aus dem Hot- oder Warm-Speicher gelöscht werden.
Aufbewahrung	(Optional) Geben Sie die Anzahl der Tage an, für die Protokolle aufbewahrt werden, bevor sie entfernt oder per Rollover in den Cold-Speicher verschoben werden. Bei Hot- und Warm-Speicher können sich die Einstellungen für die Größe und Aufbewahrungsfrist für eine Sammlung gegenseitig außer Kraft setzen, je nachdem welches Kriterium (Größe oder Zeit) zuerst erfüllt ist.
Komprimierung	Geben Sie den Typ der Komprimierung für Metadaten und unverarbeitete Protokolle in derSammlung an. Sie können die Metadaten und unverarbeiteten Protokolle mithilfe von GZIP oder LZMA komprimieren,um Speicherplatz zu sparen. GZIP ermöglicht eine sehr schnelle Komprimierung und Dekomprimierung, komprimiert jedochnicht so gut sowie LZMA. LZMA bietet eine bessere Komprimierung auf Kosten derDekomprimierungsgeschwindigkeit (ca. dreimal langsamer als GZIP). Komprimierungsverhältnisse sind stark abhängig von Ihren Daten. Die Standardkomprimierung ist GZIP.

Feld	Beschreibung
Hash	Geben Sie an, ob Hash aktiviert oder deaktiviert werden soll. Bei Aktivierung wird der Hashalgorithmus verwendet, um die Datenintegrität der zu speichernden Dateien zu gewährleisten. Standardmäßig werden nur Rohdatenprotokolle gehasht und die Hash-Dateien werden im selben Verzeichnis gespeichert wie die Daten.

5. Klicken Sie auf **Speichern**.
   Fehler in der Sammlung werden in roter Schrift angezeigt. Eine gepunktete Unterstreichung gibt an, dass eine Kurzinformation mit Informationen zum Fehler verfügbar ist. Der Name Ihrer Sammlung wird in roter Schrift angezeigt, bis mindestens eine Aufbewahrungsregel für Ihre Sammlung definiert ist.
   Wenn Sie eine Sammlung haben, bei der das Bearbeiten deaktiviert (abgeblendet) ist, sehen Sie sich die zugehörige Kurzinformation für weitere Informationen an.

Hinweis: Wenn die Speicherzuweisungen für Sammlungen verringert werden oder die Aufbewahrungszeit verkürzt wird, kann es je nach Menge der zu verschiebenden (Rollout-)Daten mehrere Minuten bis Stunden dauern, bis die Daten verschoben wurden und Speicherplatz verfügbar wird. Die Standardzeiten sind alle 20 Minuten für ein Größen-Rollout und alle sechs Stunden für ein Zeit-Rollout.

Nächster Schritt

Definieren Sie Aufbewahrungsregeln für Ihre Sammlungen.

Definieren der Aufbewahrungsregeln

Administratoren können Aufbewahrungsregeln für Protokollspeichersammlungen auf einem Archiver definieren und sortieren. Diese Aufbewahrungsregeln geben den Typ der Protokolle an, die in der Sammlung gespeichert werden sollen. Damit Ihre Protokollsammlungen Protokolldaten erfassen und speichern können, müssen Sie diese mit mindestens einer Aufbewahrungsregel verknüpfen. Wenn Sie eine Aufbewahrungsregel konfigurieren, geben Sie eine Bedingung und eine Sammlung für die Regel an. Die Bedingung (Regeldefinition) bestimmt den Typ der Protokolle, die in der Sammlung gespeichert werden.

Als Bedingung können Sie alles verwenden, das in eine regulären Abfrage-`where`-Klausel funktioniert.

Zum Abrufen von Protokollen von Compliance Services können Sie beispielsweise die folgende Bedingung verwenden:

```
device.group='PCI Devices' || device.group='HIPPA Devices'
```

Nachdem Sie die Aufbewahrungsregeln für Ihre Sammlungen definiert haben, ist es wichtig, dass Sie die Reihenfolge der Aufbewahrungsregeln angeben. NetWitness Suite bewertet die Aufbewahrungsregeln für alle Sammlungen in numerischer Reihenfolge nach der Anzahl in der Spalte „Reihenfolge“ im Abschnitt „Aufbewahrungsregel“ der Registerkarte Datenaufbewahrung des Archiver (ADMIN > Ansicht „Services-Konfiguration“).

Achtung: Die Regelreihenfolge ist sehr wichtig. Sie bestimmt die Priorität für die Bewertung der Protokolldaten für die Speicheraufbewahrung.

Voraussetzungen

Führen Sie vor dem Konfigurieren Ihrer Aufbewahrungsregeln Folgendes durch:

- Konfigurieren des Hot-, Warm- und Cold-Gesamtspeichers
- Konfigurieren von Protokollspeichersammlungen

Methoden

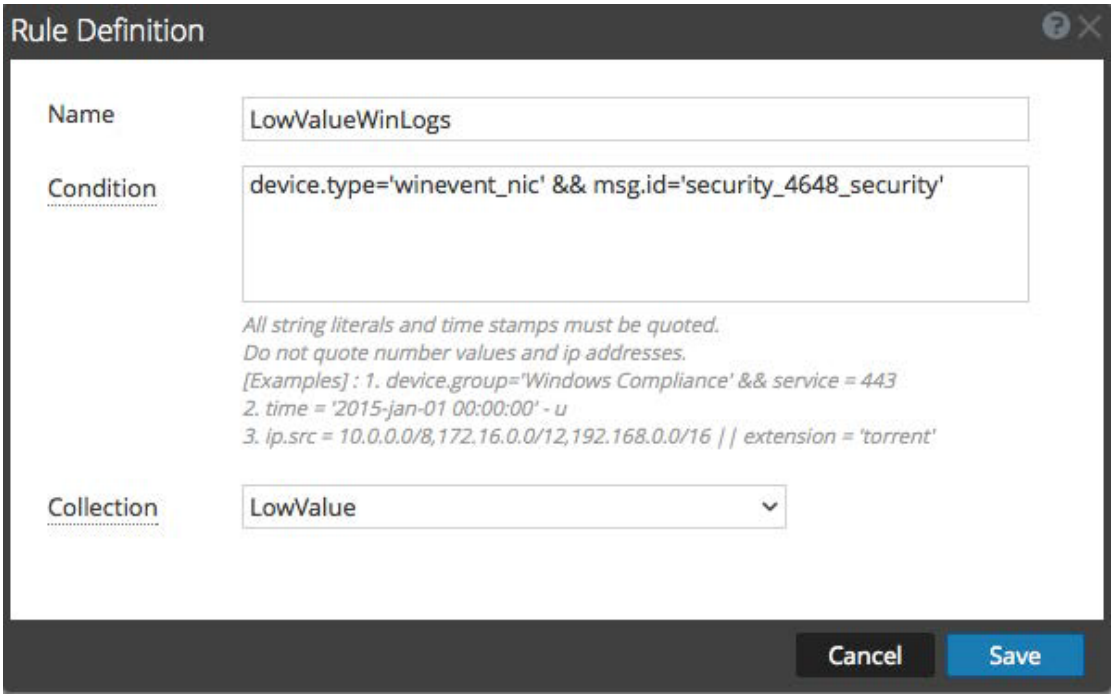
Definieren einer Aufbewahrungsregel für eine Sammlung

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Archiver-Service und dann  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Services“ > „Konfiguration“ von Archiver wird angezeigt.

3. Klicken Sie auf der Registerkarte **Datenaufbewahrung** im Abschnitt **Aufbewahrungsregel** auf +.

   Das Dialogfeld **Regeldefinition** wird angezeigt.

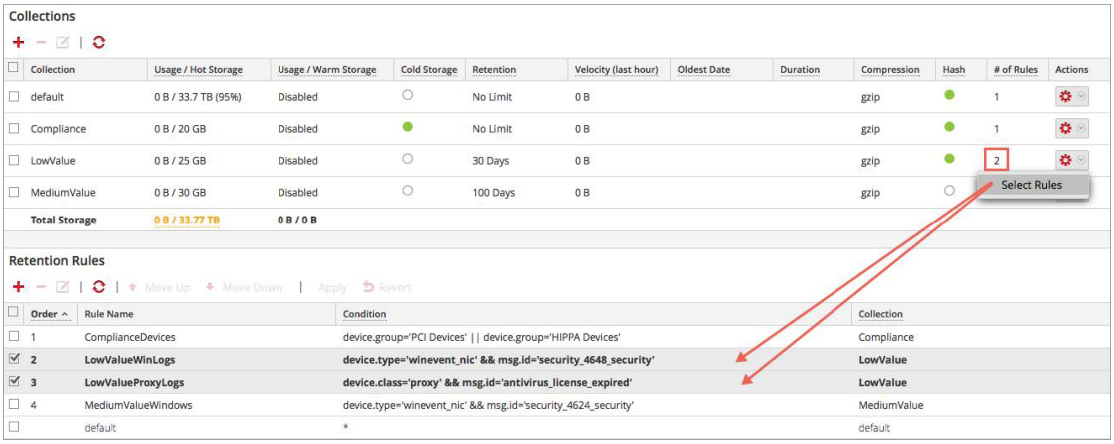


4. Konfigurieren Sie die Felder im Dialogfeld Regeldefinition wie in der folgenden Tabelle beschrieben:

Feld	Beschreibung
Name der Regel	Geben Sie einen eindeutigen Namen für Ihre Aufbewahrungsregel an. Er darf keine Leerzeichen enthalten. Beispiel: LowValueWinLogs
Bedingung	Geben Sie die Bedingungen für den Typ der Protokolle an, die Sie in die Sammlung einfügen möchten. Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Beispiel: `device.type='winevent_nic' && msg.id='security_4648_security'`

Feld	Beschreibung
Sammlung	Wählen Sie die Sammlung aus, für die Sie diese Regel anwenden möchten. Beispiel: LowValue.

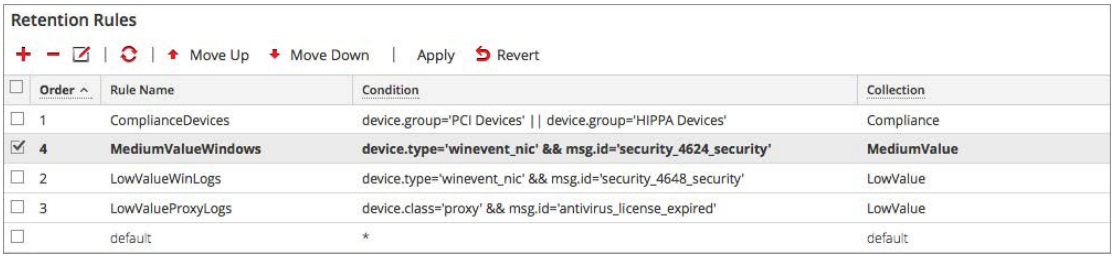
5. Klicken Sie auf **Speichern**.
   Die von Ihnen definierte Aufbewahrungsregel wird der ausgewählten Sammlung zugeordnet. Auf der Registerkarte **Datenaufbewahrung** können Sie im Abschnitt **Sammlungen** auf  > **Regeln auswählen** in der Spalte **Aktionen** für die ausgewählte Sammlung klicken, um die mit der Sammlung verknüpften Aufbewahrungsregeln im Abschnitt **Aufbewahrungsregel** anzuzeigen.



Angeben der Reihenfolge Ihrer Aufbewahrungsregeln

So priorisieren Sie die vollständige Liste aller Aufbewahrungsregeln:

1. Wählen Sie im Bereich **Aufbewahrungsregel** der Registerkarte **Datenaufbewahrung** eine Aufbewahrungsregel aus und verwenden Sie Drag-and-drop (oder wählen Sie **Nach oben verschieben** und **Nach unten verschieben** aus), um die Reihenfolge in der Prioritätenliste zu ändern.



2. Klicken Sie auf **Anwenden**, um die Reihenfolge der Aufbewahrungsregeln zu speichern.

Achtung: Die Regelreihenfolge ist sehr wichtig. Sie bestimmt die Priorität für die Bewertung der Protokolldaten für die Speicheraufbewahrung.

Nächster Schritt

Fügen Sie Archiver als Datenquelle zur Reporting Engine hinzu.

Hinzufügen von Archiver als Datenquelle zur Reporting Engine

In diesem Thema erhalten Sie Anweisungen zum Hinzufügen von Archiver Archiver als Datenquelle zur Reporting Engine für das Erzeugen eines Berichts zur Datensammlung durch Archiver.

Voraussetzungen

Stellen Sie sicher, dass Folgendes zutrifft:

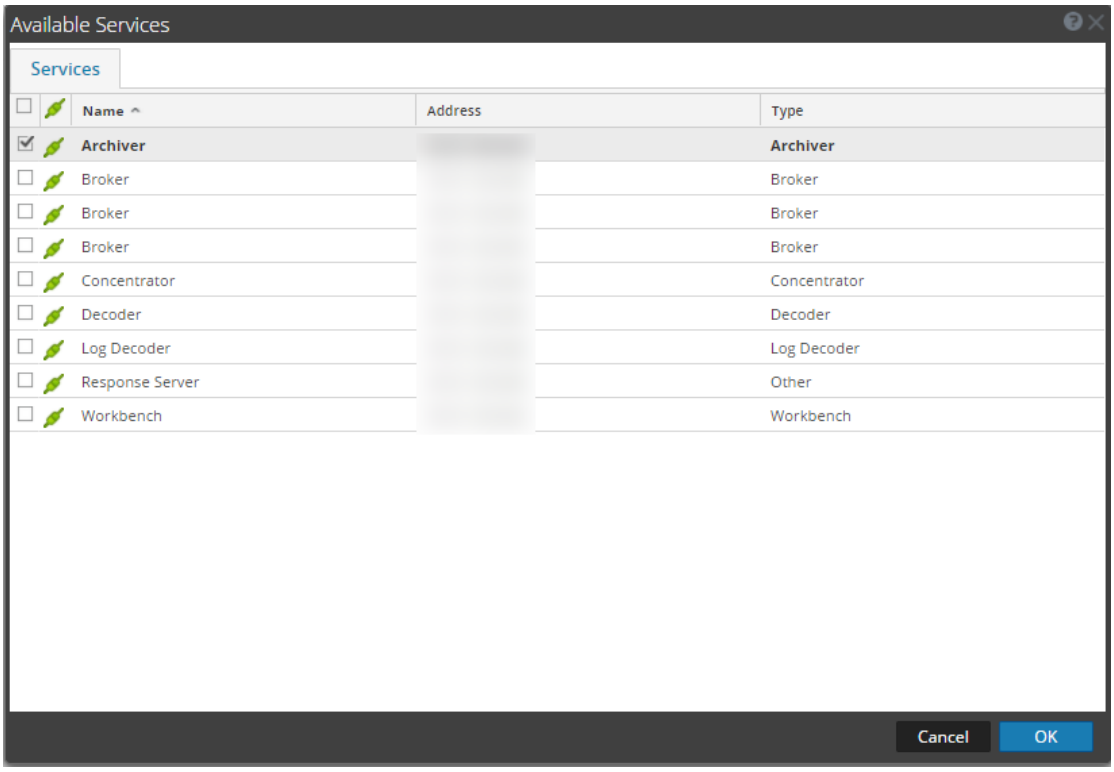
1. Der Archiver-Host wurde in Ihrer Netzwerkumgebung installiert.
2. Der Log Decoder Decoder wurde in Ihrer Netzwerkumgebung installiert und konfiguriert.
3. Sie haben überprüft, ob Reporting Engine und Archiver-Services aktiv sind.

Verfahren

So verknüpfen Sie eine Archiver-Datenquelle mit Reporting Engine:

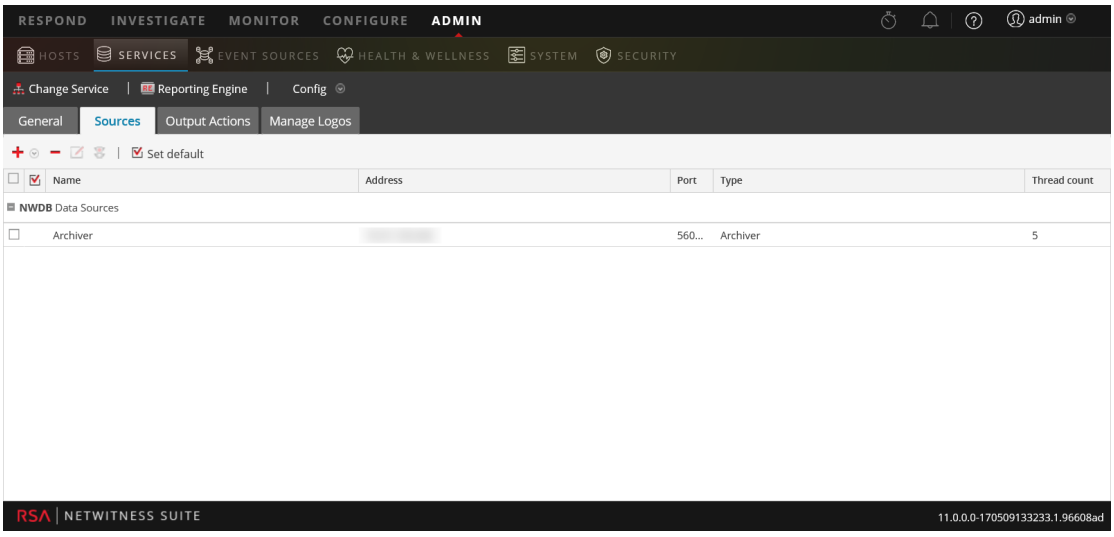
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Bereich **Services** einen **Reporting Engine**-Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
4. Wählen Sie die Registerkarte **Quellen** aus.
5. Klicken Sie auf + und wählen Sie **Verfügbare Services** aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



6. Wählen Sie den Archiver, den Sie als Datenquelle zur Reporting Engine hinzufügen möchten, und klicken Sie auf **OK**.
7. Geben Sie im Dialogfeld „Serviceinformationen“ den Benutzernamen und das Passwort für den Archiver ein.
8. Klicken Sie auf **OK**.

   Der ausgewählte Archiver wird in der Kategorie „NWDB-Datenquellen“ aufgeführt.



Sie können jetzt Berichte über die von Archiver erfassten Daten erstellen.

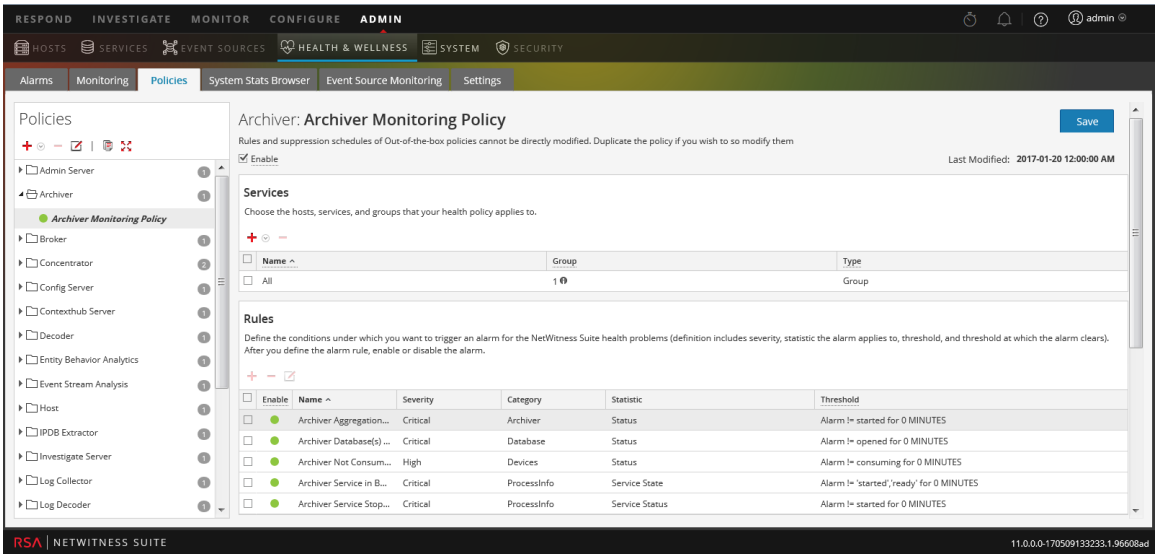
Nächster Schritt

Konfigurieren Sie Warnmeldungen für Archivspeicher.

Konfigurieren der Archiver-Überwachung

Über „Integrität“ und „Zustand“ können Sie automatisch Benachrichtigungen erzeugen, wenn kritische Schwellenwerte erreicht werden.

Überprüfen Sie die Policies für Integrität und Zustand für den Archiver und Host im Bereich „Policies für Integrität und Zustand“. Führen Sie bei Bedarf Aktualisierungen durch.



Detaillierte Informationen finden Sie unter **Policies managen** im *Leitfaden Systemwartung*.

Zusätzliche Archiver-Konfiguration

Dieses Thema ist eine Sammlung einzelner Verfahren, die ein Administrator jederzeit durchführen kann, und es ist nicht erforderlich, dass sie die anfängliche Einrichtung von Archiver abschließen. Diese Verfahren sind in alphabetischer Reihenfolge aufgeführt.

Verwenden Sie diesen Abschnitt, wenn Sie nach Anweisungen suchen, um eine bestimmte Aufgabe nach der anfänglichen Einrichtung von Archiver durchzuführen.

Themen

Konfigurieren von Backup und Wiederherstellung der Daten

In diesem Thema finden Sie Informationen zur Datensicherungs- und Wiederherstellungsfunktion für einen Archiver. Mit dieser Funktion können Sie Archiver-Daten sichern und die gesicherten Daten abrufen.

Sie können die Daten auf folgende Weisen sichern:

- Dateien mithilfe von Skripts aus Cold-Speicher-Backupordnern in einen Offlinespeicher kopieren
- Dateien mithilfe von Backupsoftware aus Cold-Speicher-Backupordnern in einen Offlinespeicher kopieren
- EMC Networker oder eine andere Backupsoftware auf dem Archiver ausführen und täglich inkrementelle Backups der Datenbankdateien ausführen

Hinweis: Details zu den Verfahren zum Sichern von Daten mit Networker finden Sie im *Administrationshandbuch für Networker*.

Wenn das Datenbackup vorliegt, müssen Sie folgende Aufgaben ausführen, um die gesicherten Daten wiederherzustellen, die auf dem Archiver installiert sind.

Aktion	Beschreibung
1. Stellen Sie Ihre Daten an einem Speicherort wieder her, der für Archiver zugänglich ist.	Siehe Erstellen einer Sammlung.
2. Erstellen Sie eine Sammlung in Archiver, die diesem Standort verwendet.	Weitere Informationen finden Sie im Thema **Managen von Sammlungen** im *Konfigurationsleitfaden Workbench*.
3. Fügen Sie den Archiver-Service als Datenquelle für die Reporting Engine hinzu, um einen Bericht für die Daten zu erzeugen, die im Archiver-Service wiederhergestellt wurden.	Weitere Informationen erhalten Sie unter Hinzufügen von Archiver als Datenquelle zur Reporting Engine

Hinzufügen des Archiver-Services

Mit dem NetWitness Suite Archiver-Service können Sie Sammlungen mit wiederhergestellten Daten aus Archiver-Offlinespeicher (Cold-Speicher) erstellen. Dieses Verfahren ist nur erforderlich, wenn bei Ihnen der Archiver-Service nicht installiert ist.

Voraussetzungen

Vergewissern Sie sich, dass Sie einen Archiver-Host hinzugefügt und eine Lizenz darauf angewendet haben.

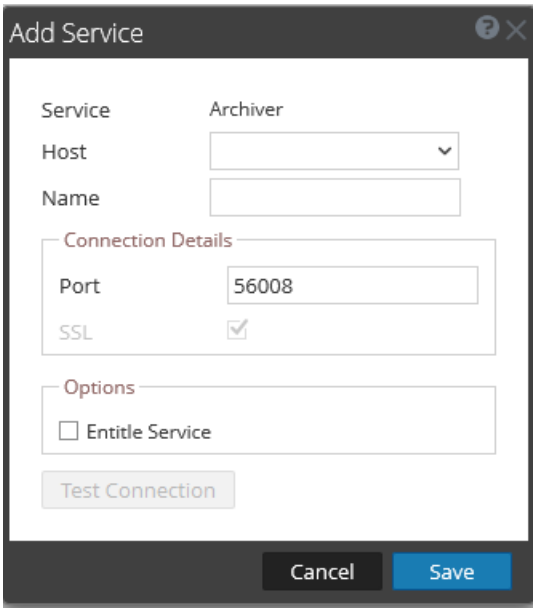
Verfahren

Hinweis: Dieses Verfahren ist nur erforderlich, wenn bei Ihnen der Archiver-Service nicht installiert ist.

Führen Sie die folgenden Schritte aus, um den Archiver-Service hinzuzufügen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Bereich **Services** die Optionen + **>Archiver** aus.

   Das Dialogfeld „Service hinzufügen“ wird angezeigt, wie unten dargestellt.



3. Geben Sie die folgenden Details an.

Feld	Beschreibung
Host	Wählen Sie einen Archiver-Host aus dem Drop-down-Menü aus.
Name	Geben Sie einen Namen für den Service ein.
Port	Der Standardport ist 50007.
SSL	Wählen Sie **SSL** aus, wenn NetWitness Suite mithilfe von SSL mit dem Service kommunizieren soll. Die Sicherheit der Datenübertragung erfolgt durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten. **Hinweis:** Wenn Sie SSL auswählen, stellen Sie sicher, dass SSL im Bereich Systemkonfiguration aktiviert ist.
Benutzername	(Optional) Geben Sie den Benutzernamen für den Service ein.
Passwort	(Optional) Geben Sie das Passwort für den Service ein.

4. Klicken Sie auf **Überprüfen der Verbindung**, um festzustellen, ob NetWitness Suite sich mit dem Service verbindet.
5. Wenn das Ergebnis erfolgreich ist, klicken Sie auf **Speichern**.
   Der hinzugefügte Service wird jetzt im Bereich „Services“ angezeigt.

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

Erstellen einer Sammlung

Dieses Thema enthält Informationen über das Erstellen einer Sammlung auf einem Archiver-Service.

Sie können eine Sammlung mithilfe von Daten erstellen, die aus den gesicherten Daten oder einer bestehenden Teilmenge der Daten wiederhergestellt wurden. Wenn Sie die gesicherten Daten wiederherstellen, müssen Sie sie in dem Sammlungsordner ablegen, der auf dem Archiver-Service erstellt wurde, damit Sie die erforderlichen Berichte für die abgerufenen Daten erzeugen können. Zum Beispiel, wenn Sie die Daten mithilfe von EMC Networker unter <*Speicherort*> gesichert haben, können Sie die Wiederherstellungsoptionen in Networker verwenden, um die gesicherten Daten in dem Sammlungsordner wiederherzustellen, der auf dem Archiver-Service erstellt wurde. Informationen über das Wiederherstellungsverfahren mithilfe von EMC Networker finden Sie im *Administrationsleitfaden für Networker*.

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Auf einem Archiver-Host installierter Archiver-Service
- Stellen Sie sicher, dass der Archiver-Service ausreichend Speicherplatz für die Sammlung hat.
- Die gesicherten Daten an einem bekannten Speicherort auf Ihrem lokalen Host, wenn Sie eine Sammlung mithilfe der Daten erstellen, die aus gesicherten Daten wiederhergestellt wurden

Verfahren

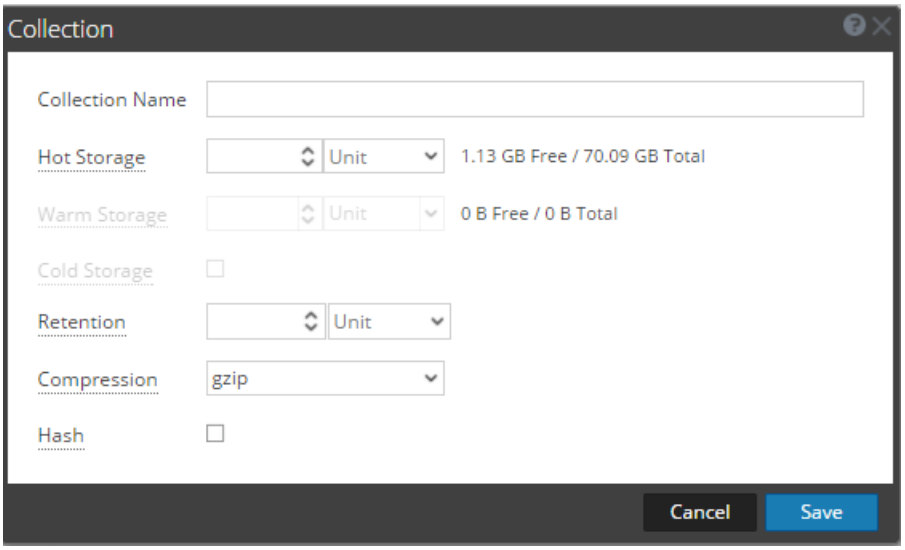
Auf der Registerkarte „Datenaufbewahrung“ können Administratoren Daten wiederherstellen und speichern, die von einem Backup oder einem vorhandenen Datensatz wiedergestellt wurden.

Hinweis: Als Quellpfad gibt der Administrator den Speicherort der Datenbankdateien an. Mit dem Befehl zum Wiederherstellen werden diese dann auf die Archiver kopiert. Bevor eine Wiederherstellungssammlung erstellt werden kann, muss der Administrator diese Verzeichnisse auf den Archiver mounten.

So erstellen Sie eine Sammlung mithilfe von Daten, die aus den gesicherten Daten oder einer bestehenden Teilmenge der Daten wiederhergestellt wurden:

1. Navigieren Sie zu **ADMIN > ServicesArchiver**.
2. Wählen Sie im Raster **Services** die Optionen  **> Ansicht > Konfiguration** aus.
   Die Registerkarte **Allgemein** wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenaufbewahrung** im Bereich **Sammlungen** auf  , um eine Sammlung hinzufügen.

Das Dialogfeld **Sammlung** wird angezeigt.



4. Stellen Sie folgende Informationen bereit:

   - **Name der Sammlung:** Der Name der Archiver-Sammlung, die Sie wiederherstellen möchten.
   - **Hot-Speicher:**Geben Sie die Anzahl der Archiver-Datenbankdateien und die Einheitengröße (Gigabyte oder Terabyte) an, die aus dem Cold-Speicher verschoben wurden.
   - **Aufbewahrungszeitraum:** Wählen Sie die Anzahl der Tage oder Stunden, für die Sie die Sammlung speichern möchten.
   - **Komprimierung:** Wählen Sie den Komprimierungstyp für die Sammlung.

6. Klicken Sie auf **Speichern**, um die Sammlung wiederherzustellen.

   Hinweis: Ziel ist der Speicherort, an dem die Sammlung erstellt wird.

   Hinweis: Wenn der Quellpfad, der für die Erstellung der Wiederherstellungssammlung angegeben wurde, nicht vorhanden ist, wird die folgende Fehlermeldung angezeigt:
   „Der Quellpfad '/xxx/xxx/' ist nicht vorhanden.“
   Wenn nicht genügend Speicherplatz vorhanden ist, um Ihre Sammlung wiederherzustellen, wird die folgende Fehlermeldung angezeigt:
   „Fehler bei der Überprüfung des Speicherplatzes. An Speicherort '/xxx/xxx/' ist nicht ausreichend Speicherplatz vorhanden.“

   Das Dialogfeld „Job planen“ wird mit der folgenden Meldung angezeigt:
   „Die Daten werden in einer neuen Sammlung wiederhergestellt. Überprüfen Sie den

Fortschritt auf der Seite „Jobs“.

7. Klicken Sie auf das Symbol **Jobs**  oben rechts in Hauptmenü, um die Liste der Jobs zur Wiederherstellungssammlung mit dem jeweiligen aktuellen Status anzuzeigen.

Hinweis: Bei der Wiederherstellung einer Sammlung dauert die Wiederherstellung umso länger, je größer das wiederherzustellende Dataset ist. Wenn Sie eine Sammlung mit Hunderten von Gigabyte oder mehr wiederherstellen, kann die Wiederherstellung mehrere Stunden dauern.

Hinzufügen eines Archiver-Service als Datenquelle zu Reporting Engine

In diesem Thema erfahren Sie, wie Sie den Archiver-Service als Datenquelle zur Reporting Engine hinzufügen, um Berichte zur Datenwiederherstellung auf dem Archiver zu erzeugen.

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

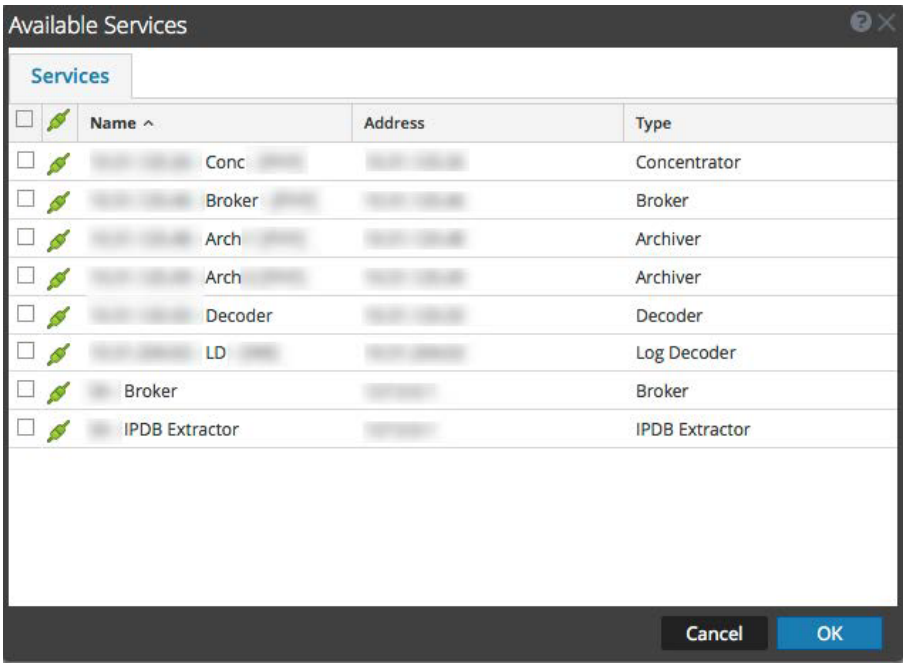
- Auf dem Archiver-Host installierter Archiver-Service
- Eine Sammlung wurde zum Archiver-Service hinzugefügt.

Verfahren

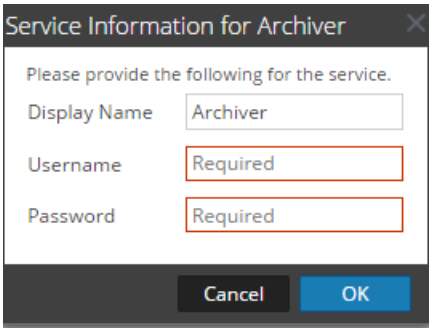
Führen Sie die folgenden Schritte aus, um den Archiver-Service als Datenquelle zur Reporting Engine hinzuzufügen:

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie im Bereich **Services** einen Reporting Engine-Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
4. Wählen Sie die Registerkarte **Quellen** aus.

5. Klicken Sie auf + und wählen Sie **Verfügbare Services** aus.
   Das Dialogfeld „Verfügbare Services“ wird angezeigt.

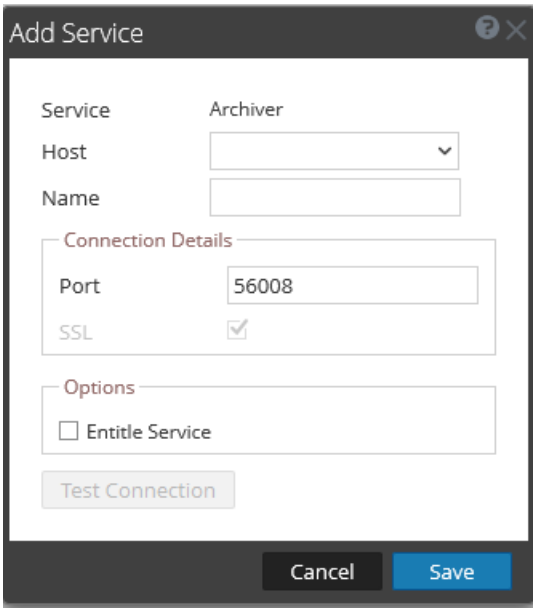


6. Wählen Sie den Archiver-Service aus und klicken Sie auf **OK**.
   Wenn der Archiver-Service ein Vertrauensmodell verwendet, wird das Dialogfeld „Serviceinformationen“ für den ausgewählten Service angezeigt, welches den erforderlichen Benutzernamen und das Passwort enthält. Wenn der Service kein Vertrauensmodell verwendet, sind diese Felder optional.



7. Geben Sie den Benutzernamen und das Passwort der Administratorzugangsdaten für den Service ein.

8. Klicken Sie auf **OK**.
   Das Dialogfeld „Service hinzufügen“ wird angezeigt.



9. Wählen Sie in der Drop-down-Liste einen Host aus und klicken Sie dann auf **Speichern**.
   Der Archiver-Service wird nun als Datenquelle zur Reporting Engine hinzugefügt und in der Liste „NWDB-Datenquellen“ aufgeführt.

Hinweis: Dieses Verfahren muss für jede Sammlung durchgeführt werden.

Administratoren können Workbench-Sammlungen erstellen und löschen und Workbench-Statistiken und -Protokolle anzeigen. Dieses Thema enthält alle diese Verfahren und ein Beispiel für die Vorgehensweise zum Wiederherstellen einer Sammlung für Reporting und Investigation.

- Mounten von Archiver-Verzeichnissen
- Erstellen einer Sammlung
- Löschen einer Sammlung
- Untersuchen einer Sammlung
- Anzeigen von Workbench-Sammlungsstatistiken
- Anzeigen von Workbench-Protokollen

Mounten von Archiver-Verzeichnissen

Wenn sich Daten in einem Offlinespeicher oder Cold-Tier-Speicher befinden, müssen Sie die Archiver-Verzeichnisse mounten, um die Daten für Berichts- und Ermittlungszwecke wiederherzustellen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ einen **Archiver** aus und wählen Sie  **> Ansicht > Durchsuchen** aus.
   Die Ansicht „Explorer“ für den Archiver wird angezeigt.
3. Klicken Sie im linken Strukturbaum mit der rechten Maustaste auf den Node **Datenbank** und wählen Sie **Datenbankeigenschaften** aus, um diese im rechten Bereich zu öffnen.
4. Führen Sie den Befehl **manifest** für einen Zeitraum aus, z. B. vom 1. April 2015 bis 10. April 2015.
   Die Suche gibt alle Dateien zurück, die für die ausgewählte Abfrage wiederhergestellt werden müssen.

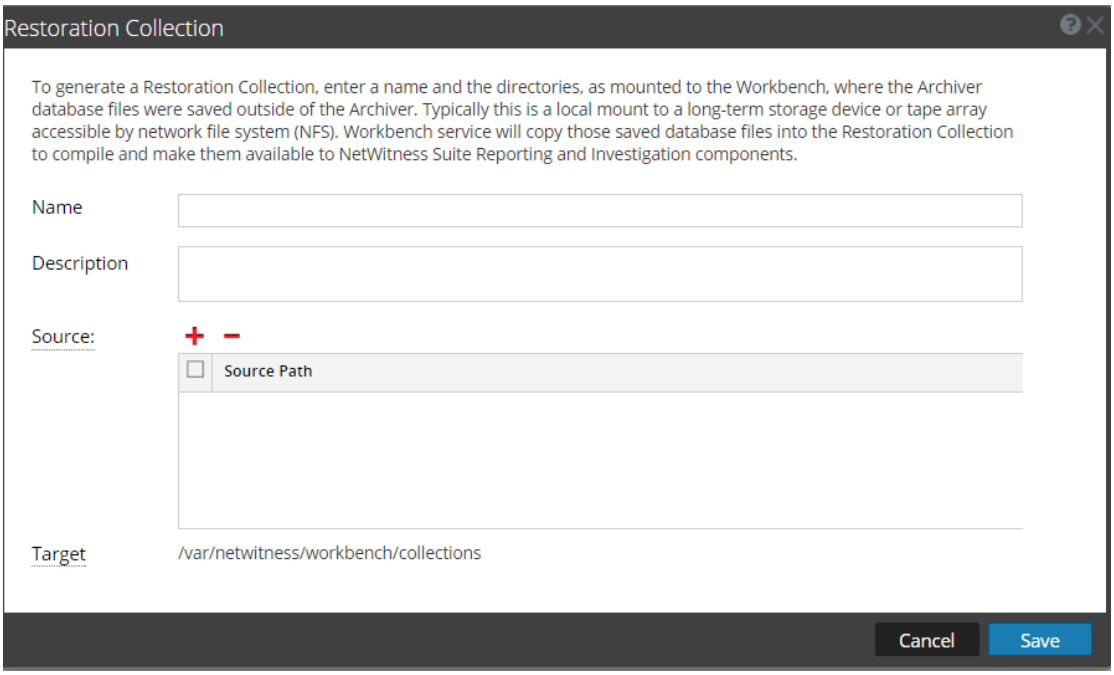
Erstellen einer Sammlung

Administratoren können Sammlungen aus wiederhergestellten Daten aus einem Backup oder einem vorhandenen Datensatz erstellen.

Hinweis: Als Quellpfad können Sie den Speicherort der Datenbankdateien angeben. Mit dem Befehl zum Wiederherstellen werden diese dann auf die Archiver kopiert. Bevor eine Wiederherstellungssammlung erstellt werden kann, müssen Sie diese Verzeichnisse in dem Archiver mounten, in dem die Workbench installiert ist.

So erstellen Sie eine Sammlung mithilfe von Daten, die aus den gesicherten Daten oder einer bestehenden Teilmenge der Daten wiederhergestellt wurden:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ eine **Workbench**, und wählen Sie dann  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services“ > „Konfiguration“ wird mit geöffneter Registerkarte Allgemein angezeigt.
3. Klicken Sie auf die Registerkarte **Sammlungen**.
   Das Raster „Sammlungen“ wird angezeigt.
4. Klicken Sie in der Symbolleiste auf  .
   Das Dialogfeld „Wiederherstellungssammlung“ wird angezeigt.



5. Stellen Sie folgende Informationen bereit:
   - **Name:** Der Name der Workbench-Sammlung, die Sie wiederherstellen möchten.
   - **Quelle:** Der Speicherort, an den die Archiver-Datenbankdateien aus dem Cold-Speicher verschoben wurden.

   Hinweis: Ziel ist der Speicherort, an dem die Sammlung erstellt wird.

6. Klicken Sie auf **Speichern**, um die Sammlung wiederherzustellen.

   Hinweis: Wenn der Quellpfad, der für die Erstellung der Wiederherstellungssammlung angegeben wurde, nicht vorhanden ist, wird die folgende Fehlermeldung angezeigt:
   `The source path does not exist '/xxx/xxx/'.`

   Wenn nicht genügend Speicherplatz vorhanden ist, um Ihre Sammlung wiederherzustellen, wird die folgende Fehlermeldung angezeigt:
   `Error during disk space checking. Insufficient disk space in location '/xxx/xxx'.`

   Das Dialogfeld „Job planen“ wird mit der folgenden Meldung angezeigt:
   `Restoring data into a new collection. Check the jobs page for progress.`

7. Klicken Sie auf das Symbol **Jobs**  in der NetWitness Suite-Symbolleiste, um die Liste der Jobs zur Wiederherstellungssammlung mit dem jeweiligen aktuellen Status anzuzeigen.

Hinweis: Das Wiederherstellen einer Sammlung, die größer als 550 GB ist, kann mehrere Stunden dauern.

Löschen einer Sammlung

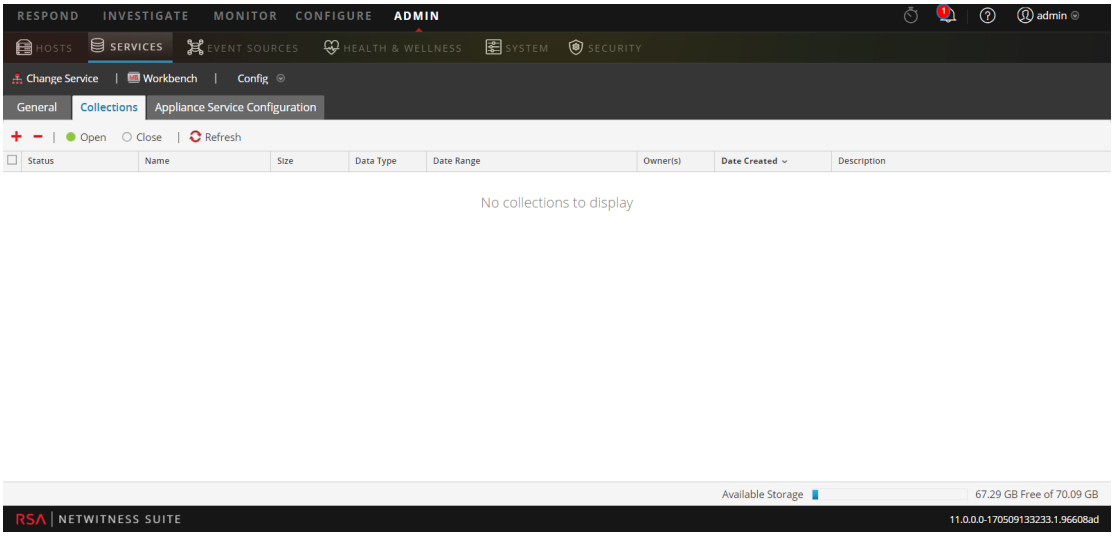
Administratoren können Sammlungen aus dem Workbench-Service löschen.

Führen Sie die folgenden Schritte aus, um eine Sammlung zu löschen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht Services eine **Workbench** aus und klicken Sie auf  > **Ansicht > Konfiguration**.

   Die Ansicht „Services“ > „Konfiguration“ wird mit geöffneter Registerkarte Allgemein angezeigt.
3. Wählen Sie die Registerkarte **Sammlungen** aus.

   Das Raster „Sammlungen“ wird angezeigt.



4. Wählen Sie im Raster „Sammlungen“ die Sammlung aus, die Sie löschen möchten.
5. Klicken Sie in der Symbolleiste auf .

   In einem Warnmeldungsdialogfeld werden Sie zur Bestätigung aufgefordert.
6. Wenn Sie die Sammlung löschen möchten, klicken Sie auf **Ja**.

   Die Sammlung wird aus dem Workbench-Service gelöscht.

Beispiel für die Vorgehensweise: Wiederherstellung einer Sammlung für Berichts- und Ermittlungszwecke

Die folgenden Schritte veranschaulichen, wie Daten, die sich in einem Offlinespeicher oder einem Cold-Tier-Speicher befinden, für Berichts- und Ermittlungszwecke wiederhergestellt werden können. Im folgenden Beispiel werden Daten für den Zeitraum zwischen dem 1. April 2015 und dem 10. April 2015 wiederhergestellt.

So stellen Sie Daten für Berichts- und Ermittlungszwecke wieder her:

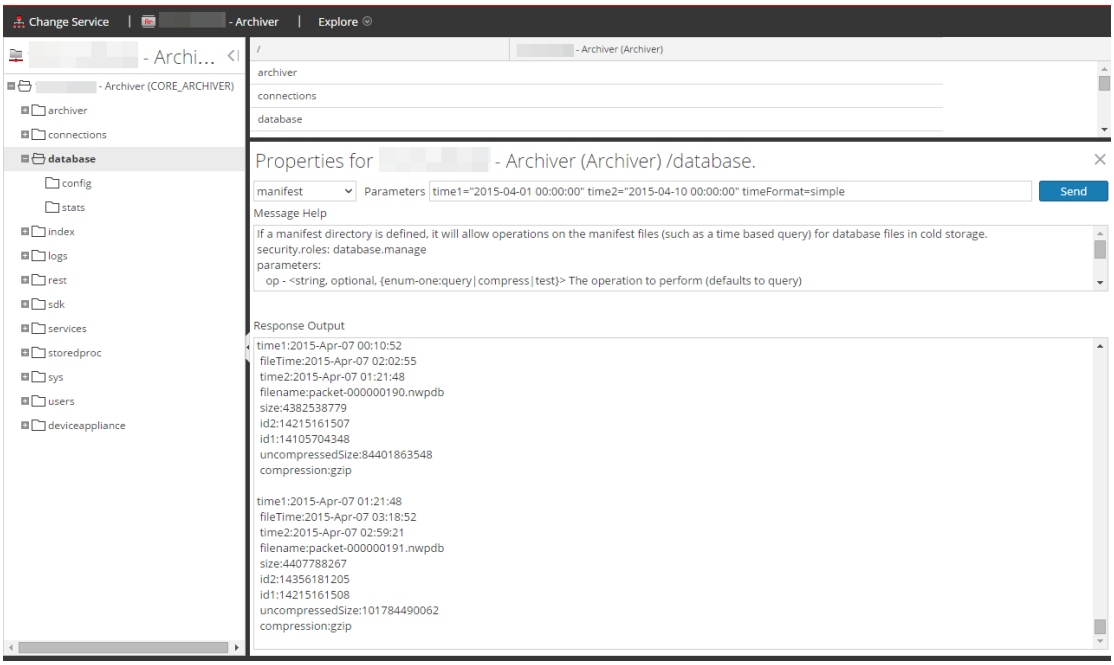
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ den **Archiver** aus.
3. Navigieren Sie zur Ansicht Explorer einer Archiver-Appliance, indem Sie  **> Ansicht > Durchsuchen** auswählen.

   Die Ansicht „Explorer“ für den Archiver wird angezeigt.
4. Klicken Sie im linken Strukturbaum mit der rechten Maustaste auf den Node **Datenbank** und wählen Sie **Datenbankeigenschaften** aus, um diese im rechten Bereich zu öffnen.
5. Führen Sie den Befehl **manifest** für den ausgewählten Zeitraum vom 1. April 2015 bis 10. April 2015 aus.

   Die Suche gibt alle Dateien zurück, die für die ausgewählte Abfrage wiederhergestellt werden müssen.

   Suchbeispiel:

   ```
   time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
   timeFormat=simple
   ```



6. Navigieren Sie zu **ADMIN > Services**.
7. Wählen Sie in der Ansicht „Services“ eine **Archiver** und wählen Sie dann  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Services“ > „Konfiguration“ wird mit geöffneter Registerkarte Allgemein angezeigt.
8. Wählen Sie die **Registerkarte Sammlungen**aus.
9. Erstellen Sie eine Wiederherstellungssammlung mit dem Quellpfad, der auf die in der Ausgabe des Befehls „manifest“ aufgeführten Dateien verweist.
10. Speichern Sie die Sammlung.
    Nach der erfolgreichen Erstellung einer Sammlung können Sie diese für Berichts- und Ermittlungszwecke verwenden.

Untersuchen einer Sammlung

So führen Sie eine Untersuchung an einer Archiver-Sammlung durch:

1. Wählen Sie **Untersuchen** aus.
   Das Dialogfeld „Untersuchen“ wird angezeigt.
2. Klicken Sie im Dialogfeld „Untersuchen“ auf die Registerkarte **Sammlungen**.
3. Wählen Sie im linken Bereich einen Archiver-Service aus.

4. Wählen Sie im rechten Bereich die Sammlung aus, die Sie untersuchen möchten.
5. Klicken Sie auf **Navigieren**.

Die Ansicht „Navigieren“ wird mit Daten in Bezug auf die ausgewählte Archiver-Sammlung angezeigt.

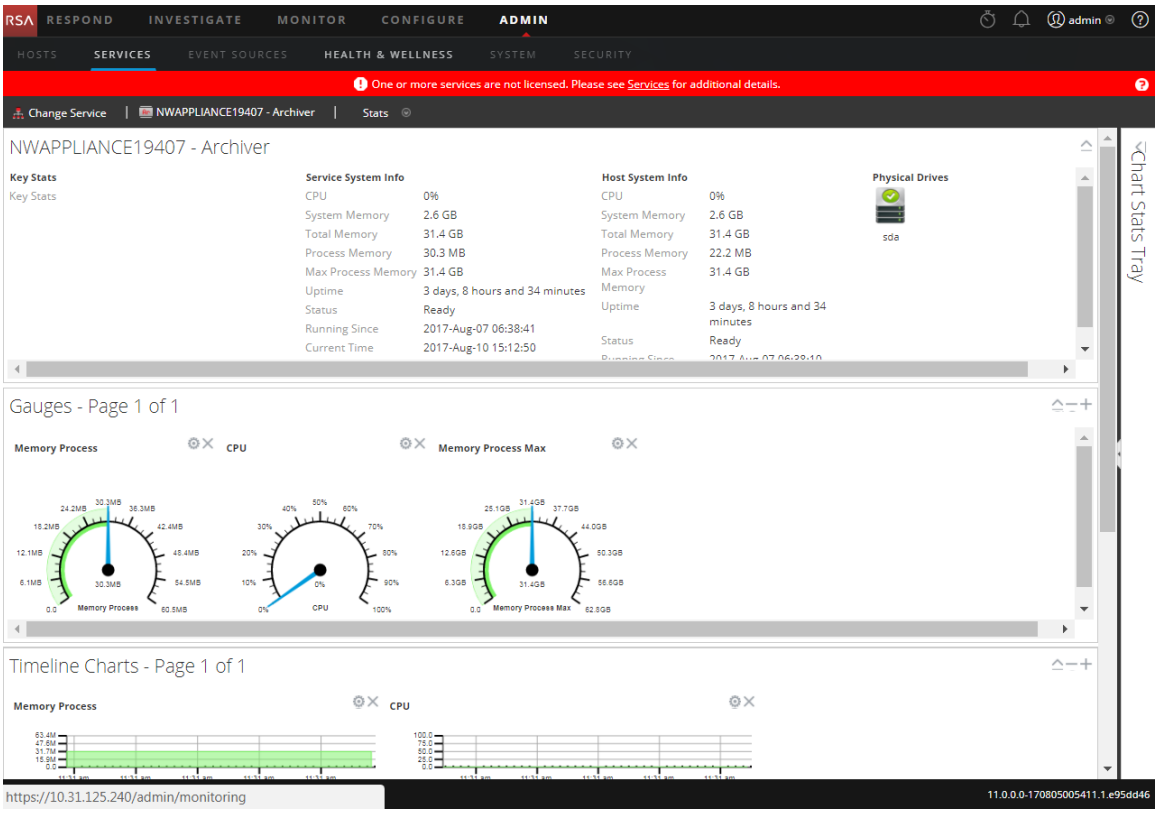
Hinweis: Detaillierte Informationen zur Verwendung von Investigation finden Sie unter *Investigation und Malware Analysis*.

Anzeigen von Archiver-Sammlungsstatistiken

Für den Archiver-Service sind dieselben Statistiken verfügbar wie für andere Services. In der Ansicht „Services“ > „Statistik“ werden wichtige Statistiken und Systeminformationen im Zusammenhang mit dem ausgewählten Archiver-Service angezeigt. Die Informationen werden in mehreren verschiedenen Abschnitten innerhalb der Ansicht „Statistik“ angezeigt: Archiver, Messdiagramme, Zeitachsendiagramm und Diagrammstatistikbereich. Im Diagrammstatistikbereich werden alle verfügbaren Statistiken für die Archiver aufgelistet. Jede Statistik im Diagrammstatistikbereich kann in einem Messdiagramm oder in einem Zeitplandiagramm angezeigt werden.

Führen Sie zum Anzeigen von Archiver-Statistiken folgende Schritte durch:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ eine Archiver und wählen Sie dann  **> Ansicht > Statistiken** aus.
   Die Ansicht „Services-Statistik“ wird angezeigt.



Hinweis: Weitere Informationen über Archiver-Statistiken finden Sie im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Anzeigen von Archiver-Protokollen

Führen Sie zum Anzeigen von Protokollen zu einem Archiver-Service folgende Schritte durch:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ eine **Archiver** und wählen Sie dann  > **Ansicht > Protokolle** aus.
   Das Raster „Serviceprotokolle“ wird angezeigt.

Hinweis: Weitere Informationen zum Anzeigen und Konfigurieren von Auditprotokollen erhalten Sie in den Themen **Konfigurieren der globalen Auditprotokollierung** im *Systemkonfigurationsleitfaden.*

Hinzufügen von Archiver-Service als eine Datenquelle zu Broker

Das Hinzufügen des Archiver-Services als Datenquelle zu Broker ist hilfreich, wenn Sie mehr als eine Sammlung haben und einen Bericht über die archivierten Daten erstellen möchten. Hierzu können Sie einem Broker mehr als eine Sammlung als Downstreamservice hinzufügen und dann einen Bericht dazu erzeugen.

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

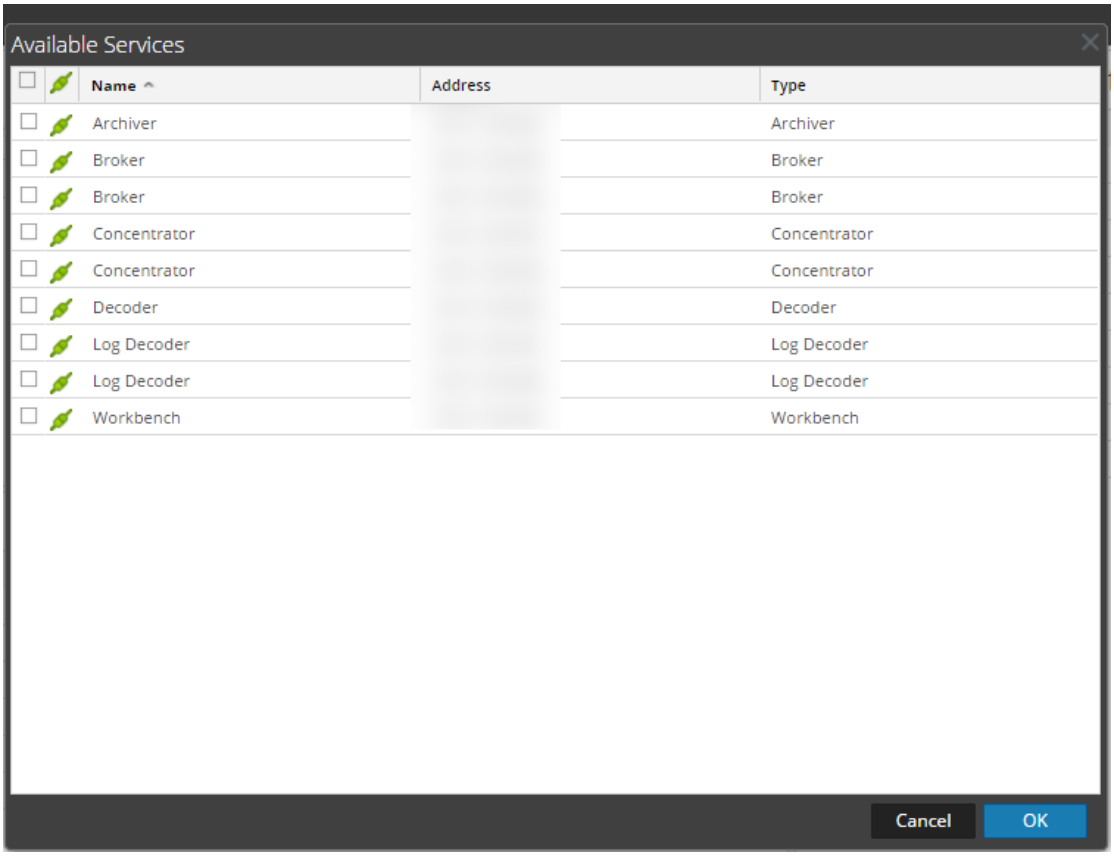
- Auf dem Archiver-Host installierter Archiver-Service
- Eine Sammlung wurde zum Archiver-Service hinzugefügt.

Verfahren

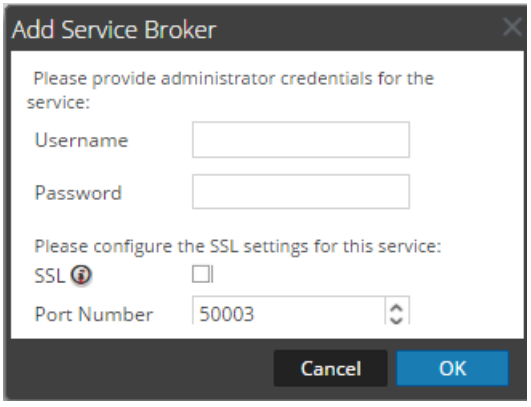
So fügen Sie einen Archiver-Service als Datenquelle auf dem Broker hinzu:

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie im Bereich **Services** einen Broker-Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Konfiguration“ wird mit geöffneter Registerkarte „Allgemein“ angezeigt.

4. Klicken Sie im Abschnitt **Aggregationsservices** auf +.
   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



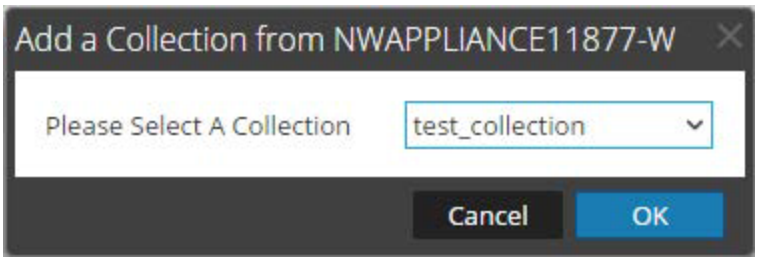
6. Wählen Sie den Broker-Service aus und klicken Sie auf **OK**.
7. Wenn der Archiver-Service ein Vertrauensmodell verwendet, wird ein Dialogfeld „Serviceinformationen“ für den ausgewählten Service angezeigt.



8. Geben Sie den Benutzernamen und das Passwort der Administratorzugangsdaten für den Service ein.

9. Klicken Sie auf **OK**.

   Das Dialogfeld „Sammlung hinzufügen“ wird angezeigt.



10. Wählen Sie eine Sammlung aus der Drop-down-Liste aus und klicken Sie auf **OK**.

    Der Archiver-Service wird nun als Datenquelle dem Broker hinzugefügt.

Hinweis: Dieses Verfahren muss für jede Sammlung durchgeführt werden.

Abrufen von Hash-Informationen

Archiver enthält den Befehl **hashInfo**, mit dem Sie Hash-Informationen für jede Sitzungs-, Meta-, und Paketdatenbank abrufen können, die die Kriterien der Sitzungsliste oder des Datumsbereichs erfüllt. Die Hash-Informationen werden in Form einer Liste von Parametern für Zeichenketten abgerufen, wobei jeder Parameter für Zeichenketten der Hash-Informationen einer einzelnen Datenbankdatei entspricht. Sie können Hash-Informationen von Datenbankdateien mithilfe der Ansicht „Durchsuchen“ des Archiver-Services oder der REST-Benutzeroberfläche des Archiver-Services abrufen. Die dadurch abgerufenen Hash-Informationen werden verwendet, um die Datenbankdateien im ursprünglichen Speicherort und im Exportspeicherort zur Prüfung der Datenintegrität zu vergleichen.

In der folgenden Tabelle werden die Kriterien aufgelistet, die Sie zum Abrufen der Hash-Dateien aus der Datenbank verwenden können.

Kriterien	Beschreibung
Sitzungen	Sie können die Hash-Informationen von Datenbankdateien abrufen, indem Sie die vorhandenen Sitzungen oder Sitzungen, die aus der Sitzungsdatenbank ausgelesen werden, angeben, um die zugehörige Meta- und Paket-ID zu bestimmen. Diese werden benötigt, um festzulegen, welche Meta- und Paketdatenbankdateien benötigt werden, um Hash-Informationen abzurufen. **Beispiel:** sessions=100 – ruft die Hash-Informationen aller Datenbankdateien ab, die die Bestandteile (Sitzung, Meta, Inhalt) von Sitzung 100 beinhalten. sessions=100,500000 – Ruft die Hash-Informationen aller Datenbankdateien ab, welche die Bestandteile (Sitzung, Meta, Inhalt) der Sitzung 100 und 500.000 beinhalten.
beginDate	Sie können ein Anfangsdatum als Filter für die Datenbankdateien angeben. So werden Hash-Informationen der Dateien angezeigt, die nach diesem bestimmten Datum erstellt wurden. Das angegebene Anfangsdatum muss folgendem Format entsprechen: YYYY-MM-DD HH:MM:SS.

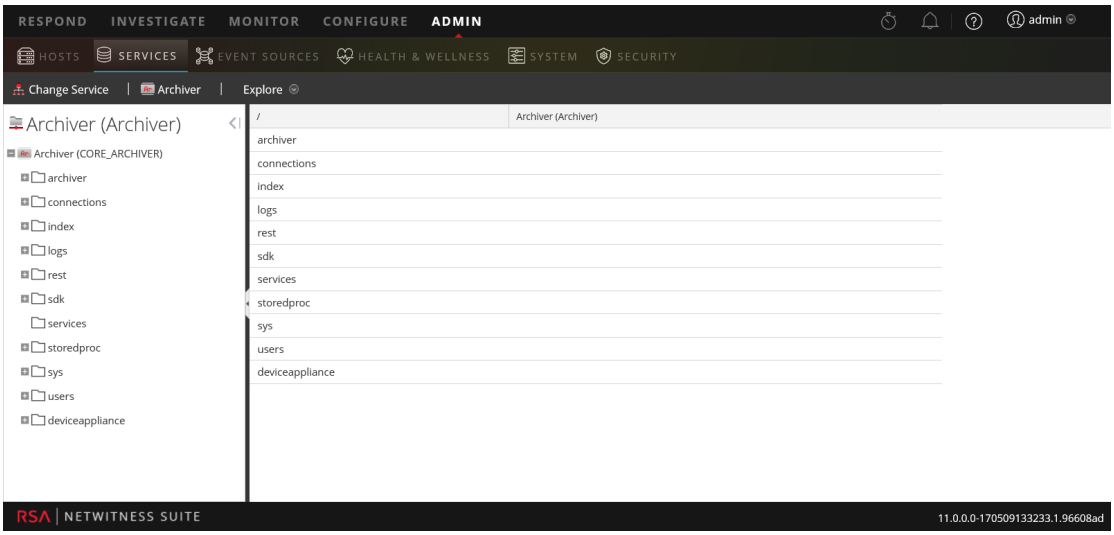
Kriterien	Beschreibung
endDate	Sie können ein Enddatum als Filter für die Datenbankdateien angeben. So werden Hash-Informationen der Dateien angezeigt, die vor diesem bestimmten Datum erstellt wurden. Das angegebene Enddatum muss folgendem Format entsprechen: JJJJ-MM-TT HH:MM:SS. **Beispiel:** beginDate: "2014-Mar-25 05:52:00" endDate="2014-Mar-27 05:52:00" – Ruft die Hash-Informationen aller Datenbankdateien ab, die zwischen dem 25. März 2014 und dem 27. März 2014 im angegebenen Zeitraum erstellt wurden.
Verzeichnisse	Die Hash-Informationsdateien werden standardmäßig zusammen mit den Datenbankdateien gespeichert, für die sie erstellt wurden. Sie können die Hash-Informationsdatei auch an einem anderen Ort speichern. Hierfür müssen Sie mehrere Speicherorte im Konfigurationsparameter hash.dir angeben. Sie können den Speicherort als Filter setzen und nur die Hash-Informationsdateien für diesen konfigurierten Speicherort anzeigen. **Beispiel:** directories="/home/hash" – ruft Hash-Informationen der Datenbankdateien des Speicherorts /home/hash ab

Verfahren

So rufen Sie Hash-Informationen aus den Datenbankdateien ab:

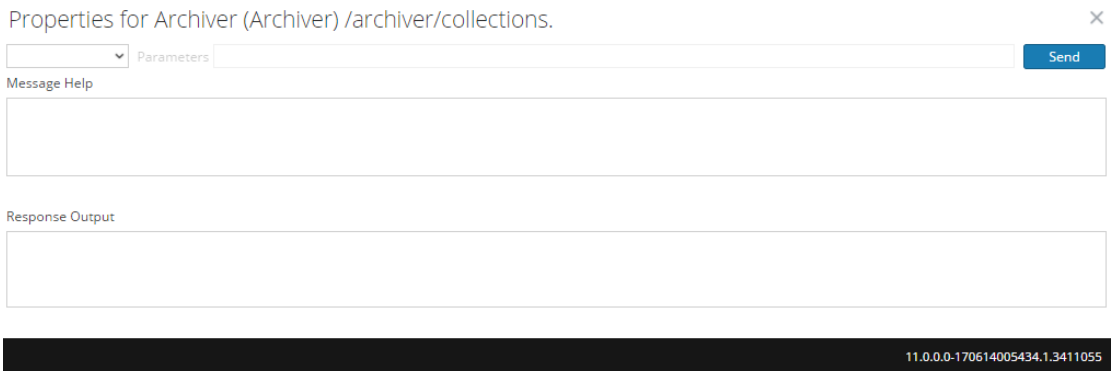
1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie einen Archiver-Service.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Durchsuchen** aus.

   Die Ansicht „Durchsuchen“ des Archiver-Services wird angezeigt.



4. Klicken Sie in der Node-Struktur mit der rechten Maustaste auf **Archiver** und wählen Sie **Eigenschaften**.

   Das Dialogfeld „Eigenschaften“ wird angezeigt.



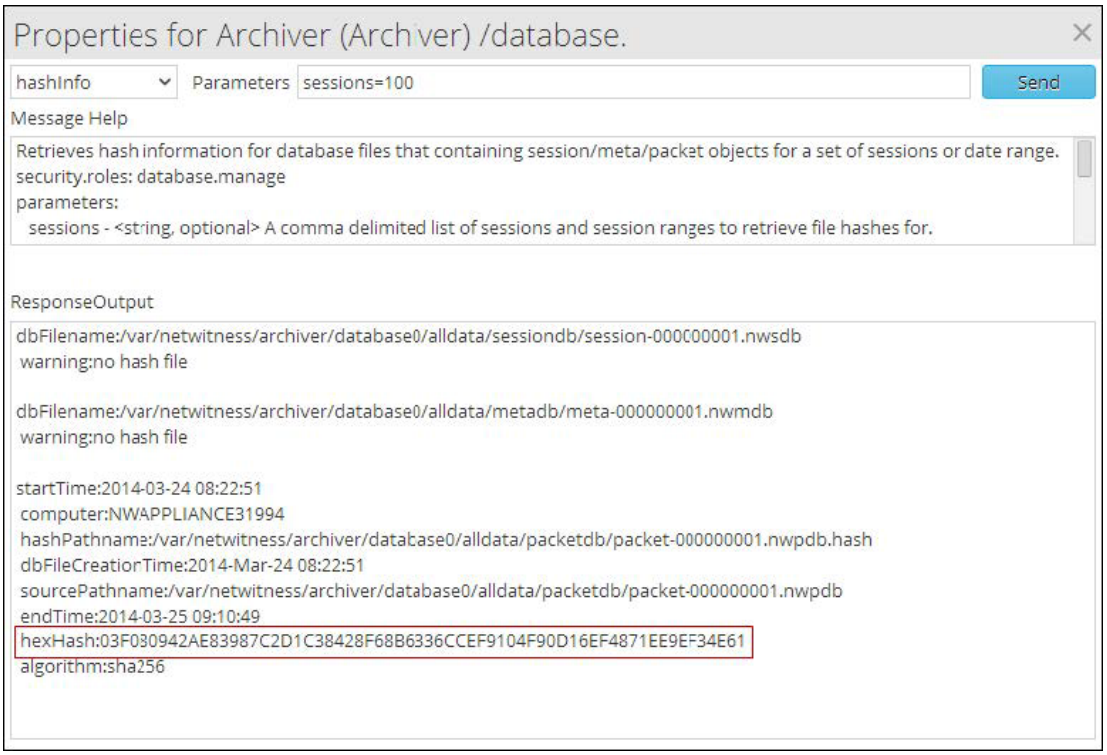
5. Wählen Sie im Drop-down-Menü die Option **hashInfo** aus.
6. Geben Sie im Feld **Parameter** die Kriterien an, die Sie zum Abrufen von Hash-Informationen aus der Datenbank verwenden möchten
7. Klicken Sie auf **Senden**.

   Die Befehlsausgabe wird im Textfeld „ResponseOutput“ angezeigt. In der Ausgabe wird die Hash-Information im Parameter hexHash angezeigt. Sie können diese Hash-Information verwenden, um die Datenintegrität manuell zu überprüfen.

Beispiele

Abrufen der Hash-Informationen der Datenbankdateien für die bestehende Sitzung.
Criteria: sessions=100

Ausgabe

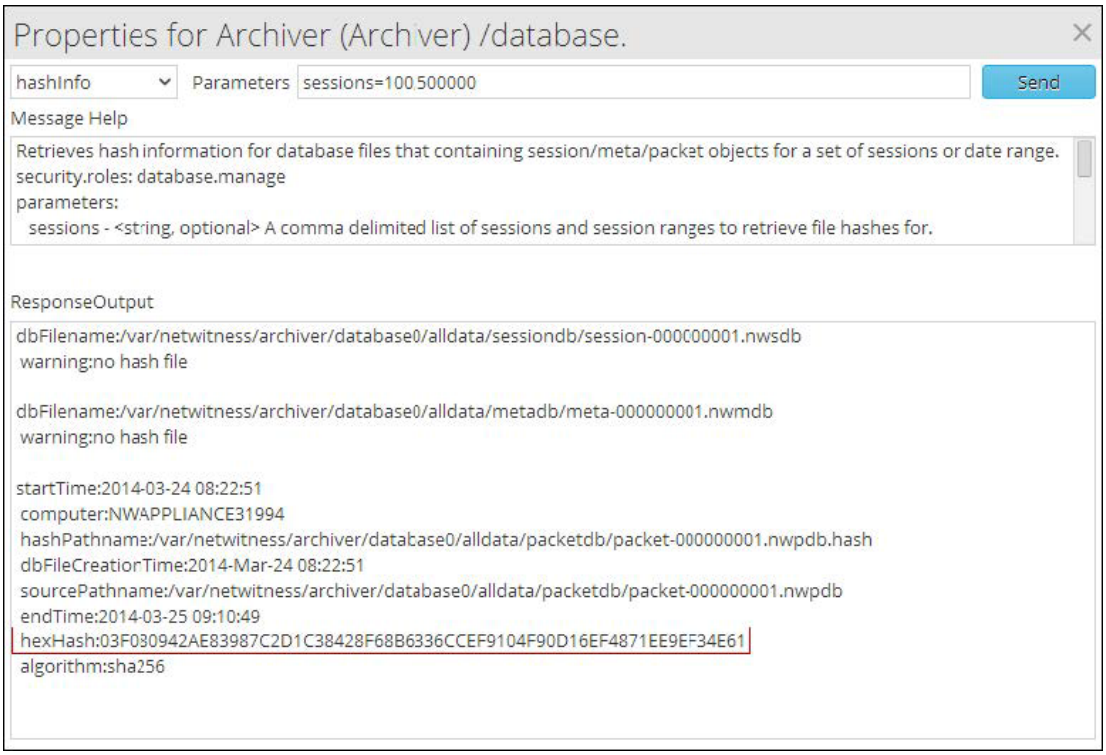


Die Hash-Informationen, die im Parameter hexHash angezeigt werden, werden abgerufen und Sie können diese zur manuellen Überprüfung der Datenintegrität von Sitzung 100 verwenden.

Abrufen der Hash-Informationen der Datenbankdateien für den bestehenden Sitzungsbereich.

Criteria: sessions=100,500000

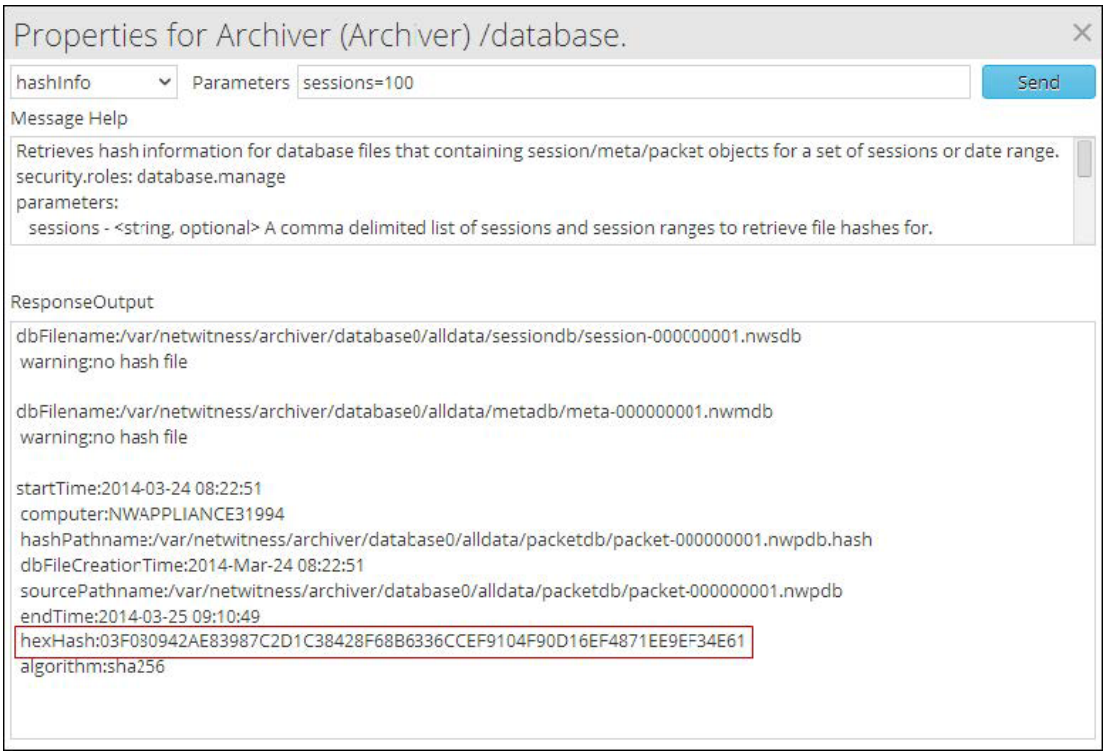
Ausgabe



Die Hash-Informationen, die im hexHash-Parameter angezeigt werden, werden abgerufen und Sie können diese zur manuellen Überprüfung der Datenintegrität des Sitzungsbereichs 100 bis 500.000 verwenden.

Abrufen der Hash-Informationen der Datenbankdateien, die in einem bestimmten Zeitraum erstellt wurden
Criteria: beginDate="2017-Mar-25 05:52:15" endDate="2017-Mar-27 05:52:15"

Ausgabe



Die Hash-Informationen, die im hexHash-Parameter angezeigt werden, werden abgerufen und Sie können diese zur manuellen Überprüfung der Datenintegrität für diesen angegebenen Zeitraum verwenden.

Referenzen

Dieses Thema besteht aus einer Sammlung verschiedener Referenzen, in denen die Benutzeroberfläche für Archiver in NetWitness Suite beschrieben wird.

Themen

Dialogfeld „Archiver-Sammlung“

Unter der Ansicht „Administration > Services > Konfiguration“ > Registerkarte „Datenaufbewahrung“ eines Archiver können Administratoren die Kriterien für die Protokollaufbewahrung und den Speicher definieren. Im Dialogfeld „Sammlung“, auf das Sie über den Abschnitt „Sammlungen“ zugreifen können, können Sie einzelne Sammlungen zur Verwendung mit verschiedenen Protokolltypen definieren. Sie können beispielsweise Sammlungen für Compliancezwecke oder die selektive Aufbewahrung kritischer Protokolle erstellen.

Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Archiver-Sammlungen konfigurieren	Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung

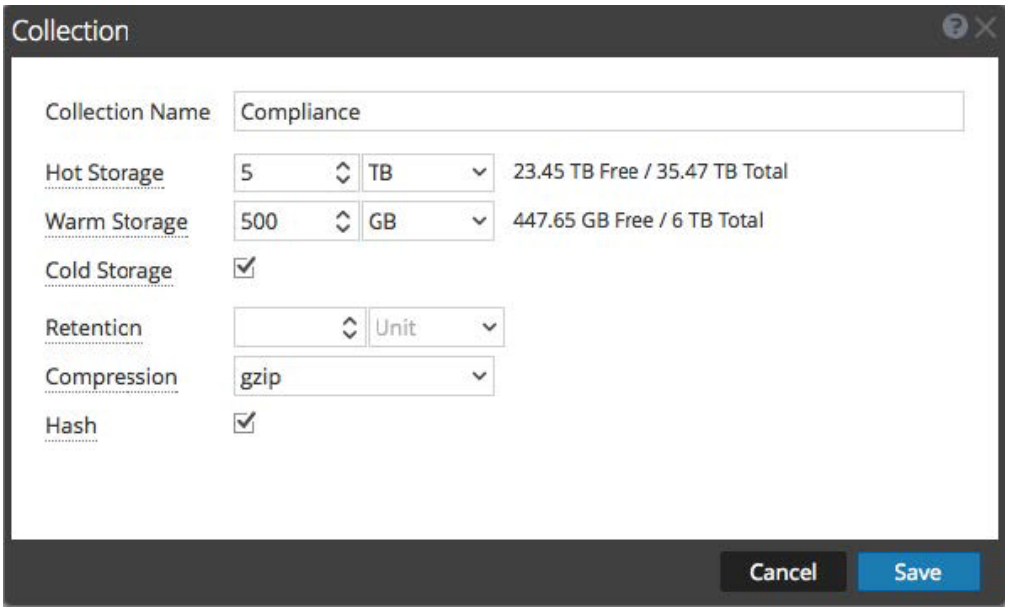
Verwandte Themen

Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung

Überblick

So greifen Sie auf das Dialogfeld „Sammlung“ zu:

1. Navigieren Sie zu ADMIN > Services.
2. Wählen Sie einen Archiver-Service und >  Ansicht > Konfiguration aus.
3. Klicken Sie in der Ansicht „Service-Konfiguration“ des Services auf die Registerkarte Datenaufbewahrung.
4. Klicken Sie im Abschnitt „Sammlungen auf  .
   Das Dialogfeld „Sammlung“ wird angezeigt.



Hinweis: Wenn die Speicherzuweisungen für Sammlungen verringert werden oder die Aufbewahrungszeit verkürzt wird, kann es je nach Menge der zu verschiebenden (Rollout-)Daten mehrere Minuten bis Stunden dauern, bis die Daten verschoben wurden und Speicherplatz verfügbar wird. Die Standardzeiten sind alle 20 Minuten für ein Größen-Rollout und alle sechs Stunden für ein Zeit-Rollout.

In der folgenden Tabelle sind die Felder im Dialogfeld „Sammlung“ beschrieben.

Feld	Beschreibung
Name der Sammlung	Geben Sie einen Namen für Ihre Sammlung ein, z. B. Compliance, MediumValue oder LowValue.
Hot-Speicher	Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Hot-Speicher ein. Der freie Speicherplatz für den Hot-Speicher und der Hot-Gesamtspeicher werden neben diesem Feld angezeigt. Wenn die Größe der Protokolle die maximale Hot-Speichergröße erreicht, werden die Protokolle entfernt oder auf den nächsten verfügbaren Storage Tier (Warm- oder Cold-Speicher) verschoben.

Feld	Beschreibung
Warm-Speicher	(Optional) Geben Sie die maximale Größe oder den Prozentsatz für den in dieser Sammlung zu verwendenden Warm-Speicher ein. Der freie Speicherplatz für den Warm-Speicher und der Warm-Gesamtspeicher werden neben diesem Feld angezeigt. Wenn die Größe der Protokolle die maximale Warm-Speichergröße erreicht, werden die Protokolle entfernt oder auf den verfügbaren Cold-Speicher verschoben.
Cold-Speicher	(Optional) Geben Sie an, ob für diese Sammlung Cold-Speicher verwendet wird. Bei Verwendung von Cold-Speicher für die Sammlung werden Protokolle außerhalb der angegebenen Größe und Aufbewahrungs fristen auf Cold-Speicher übertragen. Wenn Sie keinen Cold-Speicher verwenden, werden Protokolle außerhalb der angegebenen Größe und Aufbewahrungsfristen entfernt.
Aufbewahrung	(Optional) Geben Sie die Anzahl der Tage an, für die Protokolle aufbewahrt werden, bevor sie entfernt oder per Rollover in den Cold-Speicher verschobenwerden. Bei Hot- und Warm-Speicher können sich die Einstellungen für die Größe und Aufbewahrungsfrist für eine Sammlung gegenseitig außer Kraft setzen, je nachdem welches Kriterium (Größe oder Zeit) zuerst erfüllt ist.

Feld	Beschreibung
Komprimierung	Geben Sie den Typ der Komprimierung für Metadaten und unverarbeitete Protokolle in der Sammlung an. Sie können die Metadaten und unverarbeiteten Protokolle mithilfe von GZIP oder LZMA komprimieren, um Speicherplatz zu sparen. GZIP ermöglicht eine sehr schnelle Komprimierung und Dekomprimierung, komprimiert jedoch nicht so gut sowie LZMA. LZMA bietet eine bessere Komprimierung auf Kosten der Dekomprimierungsgeschwindigkeit (ca. dreimal langsamer als GZIP). Komprimierungs verhältnisse sind stark abhängig von Ihren Daten. Die Standardkomprimierung ist GZIP.
Hash	Geben Sie an, ob Hash aktiviert oder deaktiviert werden soll. Bei Aktivierung wird der Hashalgorithmus verwendet, um die Datenintegrität der zu speichernden Dateien zu überprüfen.

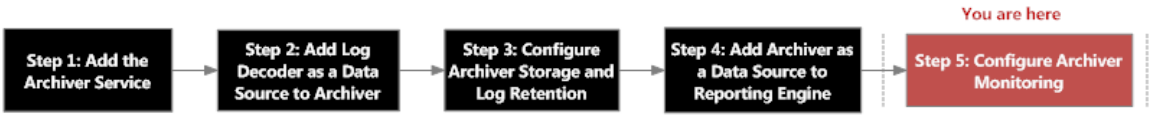
Ansicht „Archiver-Services-Konfiguration“ – Registerkarte „Allgemein“

Die Registerkarte „Allgemein“ für einen Archiver in der Ansicht „Services-Konfiguration“ hilft, die Basis-Servicekonfiguration zu verwalten, den Aggregationservice zu konfigurieren und den Aggregationsprozess zwischen einem Archiver und dem Aggregationsservice zu konfigurieren.

Um auf die Registerkarte „Allgemein“ zuzugreifen, gehen Sie zu „ADMIN > Services“, wählen Sie einen Archiver-Service und dann „Ansicht > Konfiguration“ aus.

Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver.



Die Konfiguration des Aggregationsservices (dessen Daten abgerufen und aggregiert werden) beinhaltet folgende Schritte:

- Hinzufügen, Bearbeiten und Löschen von Archivers als Aggregationsservices.
- Umschalten eines Aggregationsservices zwischen online und offline
- Monitoring von Statistiken für Aggregationsservices
- Starten und Stoppen einer Aggregation

Das Konfigurieren des Aggregationsprozesses umfasst die Einstellung folgender Parameter:

- Automatischer Start der Aggregation
- Timing- und Performanceparameter, wie die Anzahl der Sitzungen pro Aggregationsrunde und die Zeit zwischen Runden
- Das Timing der Versuche, einen nicht reagierenden Aggregationsservice neu zu starten, erneut zu verbinden oder offline zu nehmen

Was möchten Sie tun?

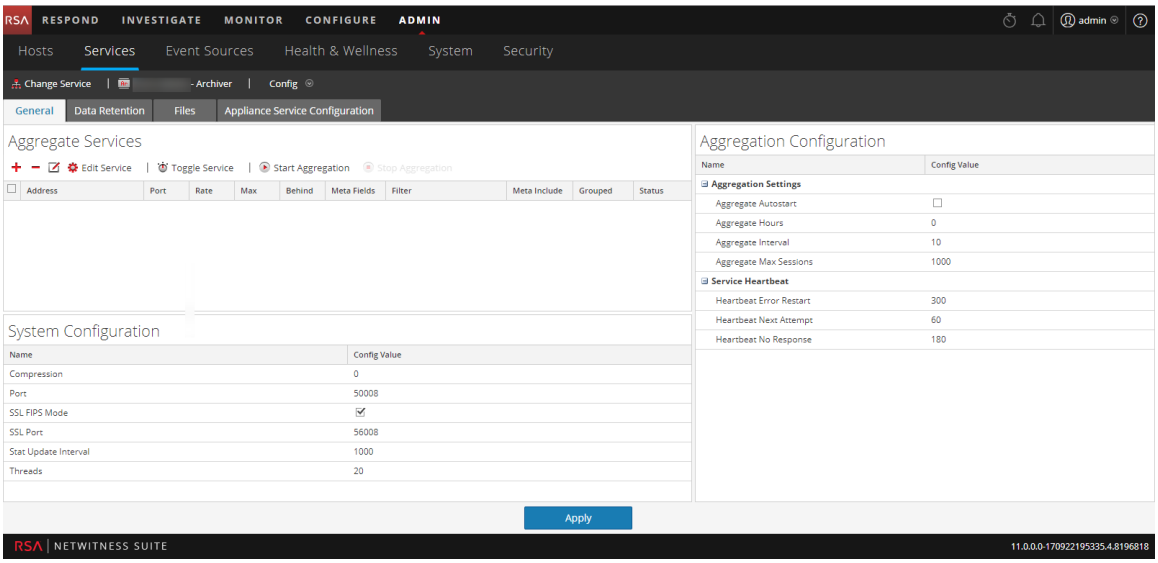
Rolle	Ziel	Details anzeigen
Administrator	Starten und Beenden Sie die Aggregation Einen Aggregatservice hinzufügen, bearbeiten, löschen und umschalten	Abschnitt „Services aggregieren“
Administrator	Systemkonfiguration verwalten	Abschnitt „Systemkonfiguration“

Verwandte Themen

Konfigurieren der Archiver-Überwachung

Überblick

Dies ist ein Beispiel für die Registerkarte „Allgemein“.



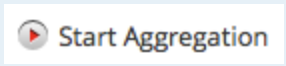
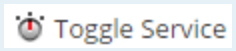
Es folgen die drei Hauptabschnitte der Registerkarte „Allgemein“ für Archivers:

- Services aggregieren
- Systemkonfiguration
- Aggregationskonfiguration

Abschnitt „Services aggregieren“

Der Abschnitt „Services aggregieren“ bietet eine Möglichkeit zum Starten und Stoppen von Aggregation sowie zum Hinzufügen, Bearbeiten, Löschen und Umschalten eines Aggregatservices. Es folgt ein Beispiel des Abschnitts „Services aggregieren“ für einen Concentrator.

Diese Optionen finden Sie in der Symbolleiste des Abschnitts „Services aggregieren“.

Option	Beschreibung
	Öffnet ein Dialogfeld, in dem Sie einen Concentrator einen Decoder oder Log Decoder als einen Aggregatservice hinzufügen können.
	Entfernt den ausgewählten Aggregatservice.
	Öffnet ein Dialogfeld zum Bearbeiten von **Metafeldern** und **Filterwerten**.
	Startet die Datenaggregation vom Onlineservice in der Liste durch die Verwendung der für den Service definierten Regeln, wenn Aggregation gestoppt oder nicht gestartet wurde.
	Stoppt die Aggregation des Broker oder Concentrator, wenn die Aggregation läuft. Beendet alle Services und löscht den Index. Der Abschluss dieses Vorgangs kann einige Minuten dauern. Aggregatservices müssen beendet werden, damit verschiedene Administrationsverfahren durchgeführt werden können.
	Wechselt den Servicestatus zwischen offline und online. Nur Daten des Onlineservices werden während der Aggregation abgerufen.

Die Abschnittsliste „Services aggregieren“ hat folgende Spalten.

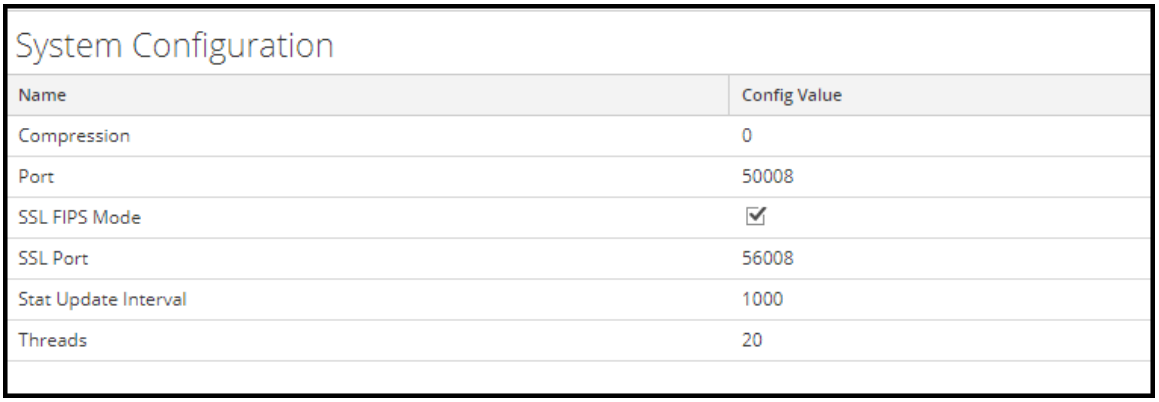
Spalte	Beschreibung
Adresse	Gibt die Serviceadresse an.

Spalte	Beschreibung
Port	Gibt den Port, den der Service abhört, an. Die Standardports sind: • 50001 für Protokollsammlung • 50002 für Log Decoder • 50003 für Broker • 50004 für Decoder • 50005 für Concentrators • 50007 für andere Services
Rate	Gibt die Anzahl der Metadatenobjekte an, die pro Sekunde in die Datenbank geschrieben werden. Werte sind gleitende Durchschnittswerte für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Erfassung beendet wurde, wird dieser Wert auf **0** zurückgesetzt.
Max	Gibt die maximale Anzahl der Metadatenobjekte an, die seit Beginn der Erfassung pro Sekunde in die Datenbank geschrieben wurden. Werte sind gleitende Durchschnittswerte für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Erfassung beendet wurde, zeigt **Max.** weiterhin den Maximalwert während der Erfassung an.
Hinter	Gibt die Anzahl der Sitzungen für den Service an, die aggregiert werden müssen.
Sammlung	Nur für Broker: Gibt die Sammlung an, die ausgewählt wurde, als der Archiver-Workbench-Service dem Abschnitt Services aggregieren hinzugefügt wurde.
Metafelder	Nur für Concentrators: Gibt die Metadatentypen an, die vom Aggregatservice abgerufen werden.
Filter	Nur für Concentrators: Gibt alle Filter an, die auf Metadaten, die vom Aggregatservice abgerufen werden, angewandt werden.
Enthaltene Metadaten	Nur für Concentrators: Gibt die Anzahl der Metadatentypen an, die der Aggregationsservice umfasst.

Spalte	Beschreibung
Gruppiert	Gibt an, ob ein Aggregatservice Teil einer Gruppe ist.
Status	Zeigt den aktuellen Servicestatus an. • online = verfügbar zur Bereitstellung von Daten, für das Abrufen durch einen Broker oder Concentrator • offline = nicht verfügbar zur Bereitstellung von Daten für das Abrufen durch einen Broker oder Concentrator • beim Abrufen = Daten werden für das Abrufen durch einen Broker oder Concentrator bereitgestellt

Abschnitt „Systemkonfiguration“

Im Abschnitt „Systemkonfiguration“ wird die Servicekonfiguration eines Services verwaltet. Wenn ein Service zum ersten Mal hinzugefügt wird, sind Standardwerte wirksam. Sie können diese Werte bearbeiten, um die Performance zu verbessern.


System Configuration

Name	Config Value
Compression	0
Port	50008
SSL FIPS Mode	☑
SSL Port	56008
Stat Update Interval	1000
Threads	20

Der Abschnitt Systemkonfiguration enthält diese Parameter.

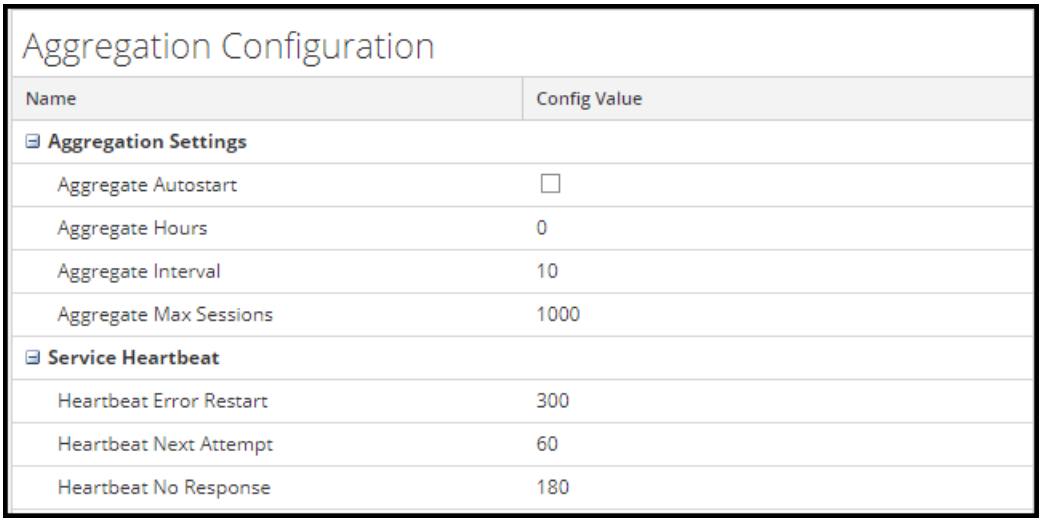
Parameter	Beschreibung
Komprimierung	Die Mindestanzahl Byte, die pro Antwort vor der Komprimierung übertragen werden muss. Die Einstellung **0** deaktiviert die Komprimierung. Der Standardwert ist **0**. Eine Veränderung des Werts ist sofort für alle nachfolgenden Verbindungen wirksam.

Parameter	Beschreibung
Port	Der Port, den der Service überwacht. Die Standardports sind: • 50001 für Protokollsammlung • 50002 für Log Decoder • 50003 für Broker • 50004 für Decoder • 50005 für Concentrators • 50007 für andere Services
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**.
SSL-Port	Gibt den SSL-Port an.
Statistikaktualisierungsintervall	Die Anzahl der Millisekunden zwischen Statistikaktualisierungen auf dem System. Niedrigere Zahlen führen zu häufigeren Aktualisierungen und können andere Prozesse verlangsamen. Der Standardwert ist **1000**. Eine Änderung des Werts ist sofort wirksam.
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.

Abschnitt Aggregationskonfiguration

Der Abschnitt „Aggregationskonfiguration“ enthält Konfigurationseinstellungen, die verschiedene Aspekte des Aggregatprozesses beeinflussen. Wenn Sie auf **Anwenden** klicken, werden die Änderungen gespeichert, jedoch werden nicht alle Einstellungen sofort wirksam. Die Tabellen für Aggregationseinstellungen und Service-Heartbeat liefern weitere Details.

Achtung: Bearbeiten Sie diese Einstellungen nicht ohne Anleitung des Kundensupports.



Aggregation Configuration

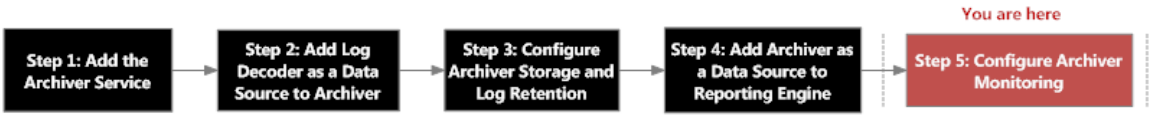
Name	Config Value
Aggregation Settings	
Aggregate Autostart	☐
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	1000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Archiver-Servicekonfiguration

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

Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver



Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Archiver-Einstellungen konfigurieren	/archiver/config
Administrator	Datenbankeinstellungen konfigurieren	/database/config
Administrator	Indexeinstellungen konfigurieren	/index/config
Administrator	Protokolleinstellungen konfigurieren	/logs/config
Administrator	REST-Einstellungen konfigurieren	/rest/config
Administrator	SDK-Einstellungen konfigurieren	/sdk/config
Administrator	Services-Einstellungen konfigurieren	/services/<Servicename>/config
Administrator	Systemeinstellungen konfigurieren	/sys/config

Verwandte Themen

- Weitere Informationen zum Konfigurieren von Datenbankeinstellungen finden Sie im Thema „Datenbankkonfigurations-Nodes“ im *RSA NetWitness Core-Datenbank-Tuning-Leitfaden)*.
- Weitere Informationen zum Konfigurieren von Indexeinstellungen finden Sie im Thema „Indexkonfigurations-Nodes“ im *RSA NetWitness Core-Datenbank-Tuning-Leitfaden)*.
- Weitere Informationen zum Konfigurieren von SDK-Einstellungen finden Sie im Thema „SDK-Konfigurations-Nodes“ im *RSA NetWitness Core-Datenbank-Tuning-Leitfaden)*.

Registerkarte „Datenaufbewahrung“ – Archiver

Unter der Ansicht „Admin > Services > Konfiguration“ > Registerkarte „Datenaufbewahrung“ eines Archiver können Administratoren die Kriterien für die Protokollaufbewahrung und den Speicher definieren.

Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver. Über die Registerkarte „Datenaufbewahrung“ können Sie Hot-, Warm- und Cold-Speicher zusammen mit mehreren Speichersammlungen für die Datenaufbewahrung konfigurieren.

Was möchten Sie tun?

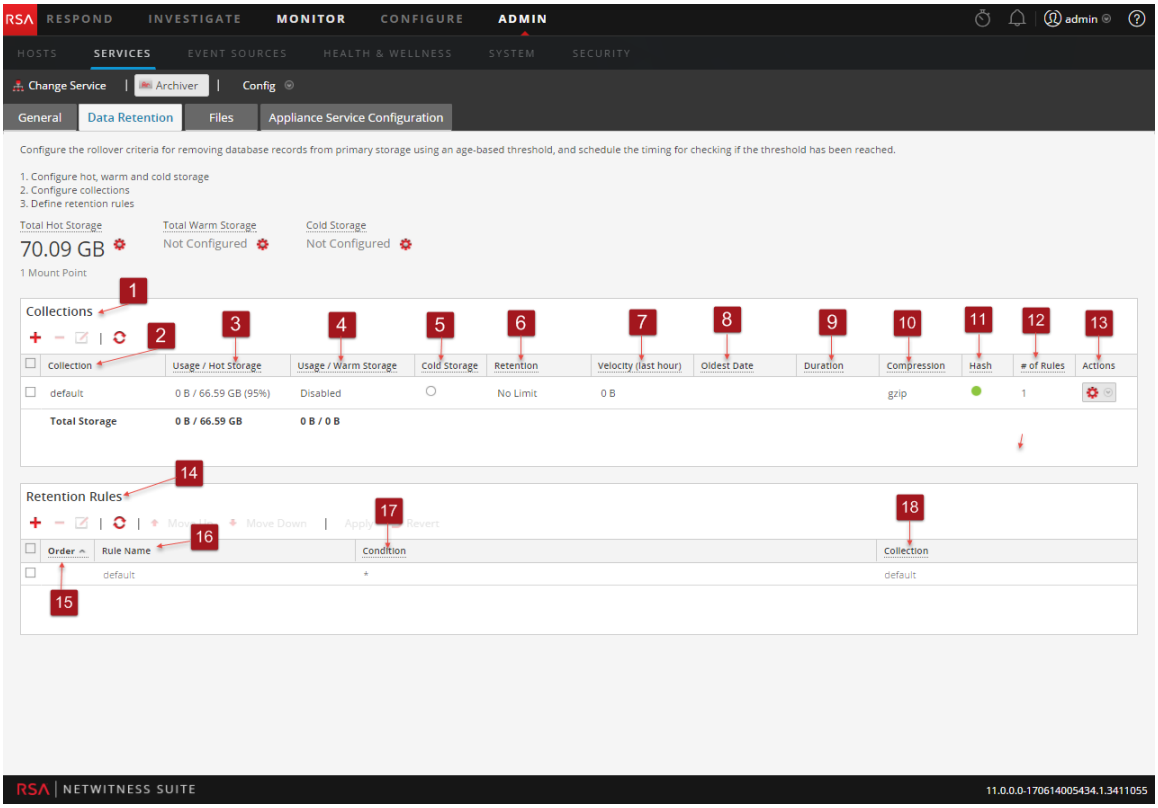
Rolle	Ziel	Details anzeigen
Administrator	Hot-Gesamtspeicher konfigurieren	Konfigurieren des Hot-, Warm- und Cold-Speichers
Administrator	Warm-Gesamtspeicher konfigurieren (optional)	Konfigurieren des Hot-, Warm- und Cold-Speichers
Administrator	Cold-Gesamtspeicher konfigurieren (optional)	Konfigurieren des Hot-, Warm- und Cold-Speichers
Administrator	Sammlungen konfigurieren	Konfigurieren von Protokollspeichersammlungen
Administrator	Aufbewahrungsregeln konfigurieren	Definieren der Aufbewahrungsregeln

Verwandte Themen

- Konfigurieren des Hot-, Warm- und Cold-Speichers
- Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung
- Definieren der Aufbewahrungsregeln

Überblick

Als Administrator können Sie Hot-, Warm- und Cold-Speicher sowie mehrere Speichersammlungen mit verschiedenen Speicherorten und Kriterien für die Aufbewahrung von Protokollen konfigurieren. Sie können beispielsweise eine Compliancesammlung erstellen, in der Protokolle für einen bestimmten Zeitraum in Übereinstimmung mit behördlichen Vorschriften gespeichert werden. Sie können eine andere Sammlung erstellen, in der Protokolle mit geringem Wert in Hot-Speicher mit einer deutlich kürzeren Aufbewahrungsfrist gespeichert werden. Durch die Flexibilität dieser Sammlungen sind Ihre Gesamtspeicheranforderungen wesentlich geringer.



1	Zeigt den Bereich „Sammlungen“ mit geöffneter Registerkarte „Datenaufbewahrung“ an.
2	Ermöglicht Ihnen, die Sammlungen in aufsteigender oder absteigender Reihenfolge zu sortieren.
3	Zeigt den zugewiesenen Hot-Speicherplatz für die Sammlung sowie die ungefähre aktuelle Auslastung an.
4	Zeigt den zugewiesenen Warm-Speicherplatz für die Sammlung sowie die ungefähre aktuelle Auslastung an.
5	Zeigt an, ob die Sammlung Cold-Speicher für die langfristige Datensicherung verwendet.
6	Zeigt den Zeitbereich an, mit dem festgelegt wird, wann Daten in den Cold-Speicher verschoben oder verworfen werden.

7	Zeigt die Menge an Daten an, die innerhalb der letzten Stunde in die Sammlung geschrieben wurden.
8	Zeigt das Datum der ältesten Daten an, die in der Sammlung gespeichert sind.
9	Zeigt das ungefähre Alter der ältesten Daten an, die in der Sammlung gespeichert sind.
10	Zeigt den in der Sammlung verwendeten Komprimierungstyp an.
11	Zeigt an, ob beim Speichern von Daten in der Sammlung Hash-Werte verwendet werden.
12	Zeigt die Anzahl der Aufbewahrungsregeln an, deren Daten in dieser Sammlung gespeichert werden.
13	Zeigt das Drop-down-Menü „Aktionen“ an.
14	Zeigt den Bereich „Aufbewahrungsregeln“ an.
15	Zeigt die Reihenfolge an, in der Aufbewahrungsregeln in der Ausführungskette bewertet werden.
16	Zeigt den Namen der Aufbewahrungsregel an.
17	Daten, die diese Bedingung erfüllen, werden in der zugehörigen Sammlung gespeichert.
18	Zeigt die Sammlung an, in der die Daten gespeichert werden, die diese bestimmte Regelbedingung erfüllen.

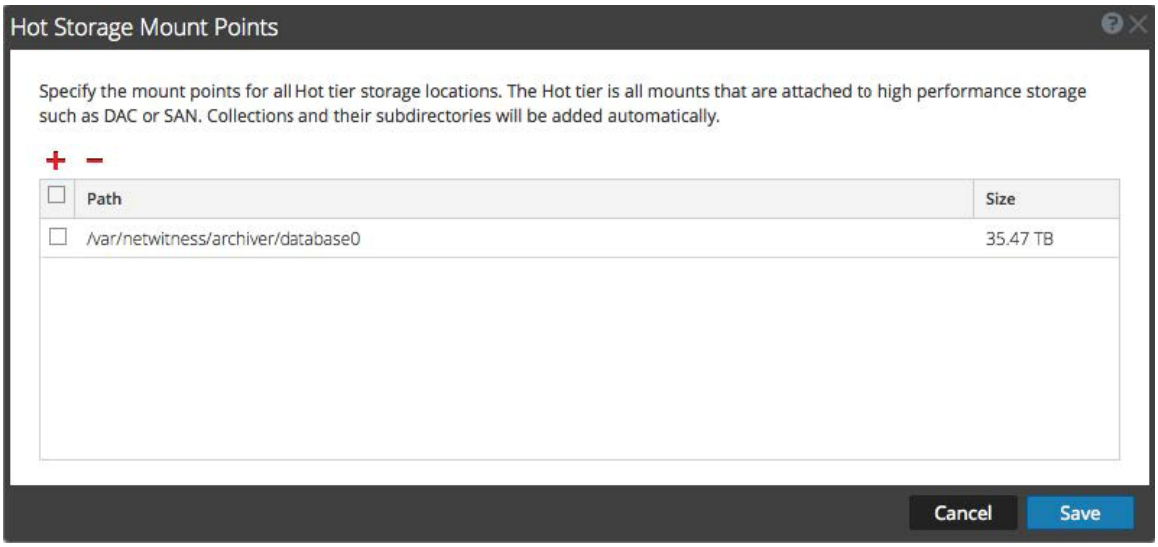
Hot-, Warm- und Cold-Gesamtspeicher

Im Abschnitt „Hot-Gesamtspeicher“ wird die Gesamtmenge des verfügbaren Hot-Speichers und die Anzahl der Mount-Punkte für Hot-Speicher angezeigt. Im Abschnitt „Warm-Gesamtspeicher“ wird die Gesamtmenge des verfügbaren Warm-Speichers und die Anzahl der Warm-Speicher-Mount-Punkte angezeigt. Im Abschnitt „Cold-Gesamtspeicher“ wird die Gesamtmenge des Cold-Speichers und der verbleibende freie Speicherplatz im Cold-Speicher angezeigt.

Dialogfelder für die Hot-, Warm- und Cold-Speicher-Mount-Punkte

In den Dialogfeldern für die Hot-, Warm- und Cold-Speicher-Mount-Punkte können Sie die Mount-Punkte für Ihre Speicherorte angeben. Sie können Teile dieses Speichers zur Verwendung für Ihre Protokollspeichersammlungen angeben.

Klicken Sie zum Zugreifen auf die Dialogfelder für die Hot-, Warm- und Cold-Speicher-Mount-Punkte auf das -Symbol neben dem jeweiligen Abschnitt.

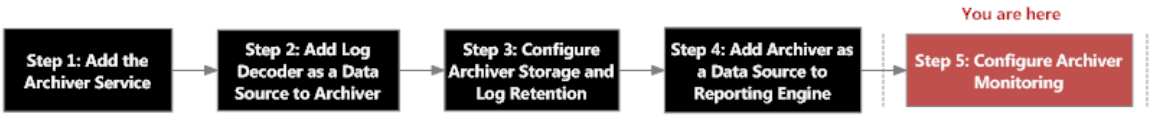


Ansicht „Service-Konfiguration“ – Archiver

Über die Ansicht „Services-Konfiguration“ (ADMIN > Services > Archiver-Service > > Ansicht > Konfiguration) können Sie grundlegende Servicekonfigurationen managen, Aggregatservices, Protokollaufbewahrung und Speicher konfigurieren, Servicekonfigurationsdateien bearbeiten und den Appliance-Service für einen Archiver konfigurieren.

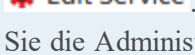
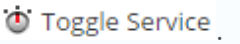
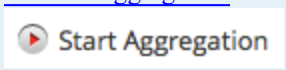
Workflow

Dieser Workflow zeigt den End-to-End-Installations- und Konfigurationsprozess für einen Archiver.



Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	*Einen Log Decoder als Aggregatservice hinzufügen.	Klicken Sie im Abschnitt Services aggregieren auf +.
Administrator	*Den ausgewählten Aggregatservice entfernen.	Klicken Sie im Abschnitt Services aggregieren auf −.
Administrator	*Metafelder und Filterwerte des Aggregatservices bearbeiten.	Klicken Sie im Abschnitt Services aggregieren auf . Sie können den Typ der Metadaten angeben, die der Archiver über diesen Service nutzt. Sie können auch eine Regel zum Filtern von Daten angeben, die der Archiver über diesen Service nutzt.

Rolle	Ziel	Details anzeigen
Administrator	*Mit dem Archiver kommunizieren.	Klicken Sie im Abschnitt Services aggregieren auf  . Hier können Sie die Administrator-Anmeldedaten des ausgewählten Aggregatservices eingeben, damit dieser mit dem Archiver kommunizieren kann.
Administrator	*Wechselt den Servicestatus zwischen offline und online.	Klicken Sie im Abschnitt Services aggregieren auf  .
Administrator	*Daten mithilfe der für den Service definierten Regeln aggregieren.	Klicken Sie im Abschnitt Services aggregieren auf  . Die Aggregatservices müssen nach dem Beenden der Aggregation erneut gestartet werden.
Administrator	*Aggregation auf dem Archiver beenden.	Klicken Sie im Abschnitt Services aggregieren auf  . Beendet alle Services und löscht den Index. Der Abschluss dieses Vorgangs kann einige Minuten dauern. Aggregatservices müssen gestoppt werden, damit verschiedene Administrationsverfahren durchgeführt werden können.

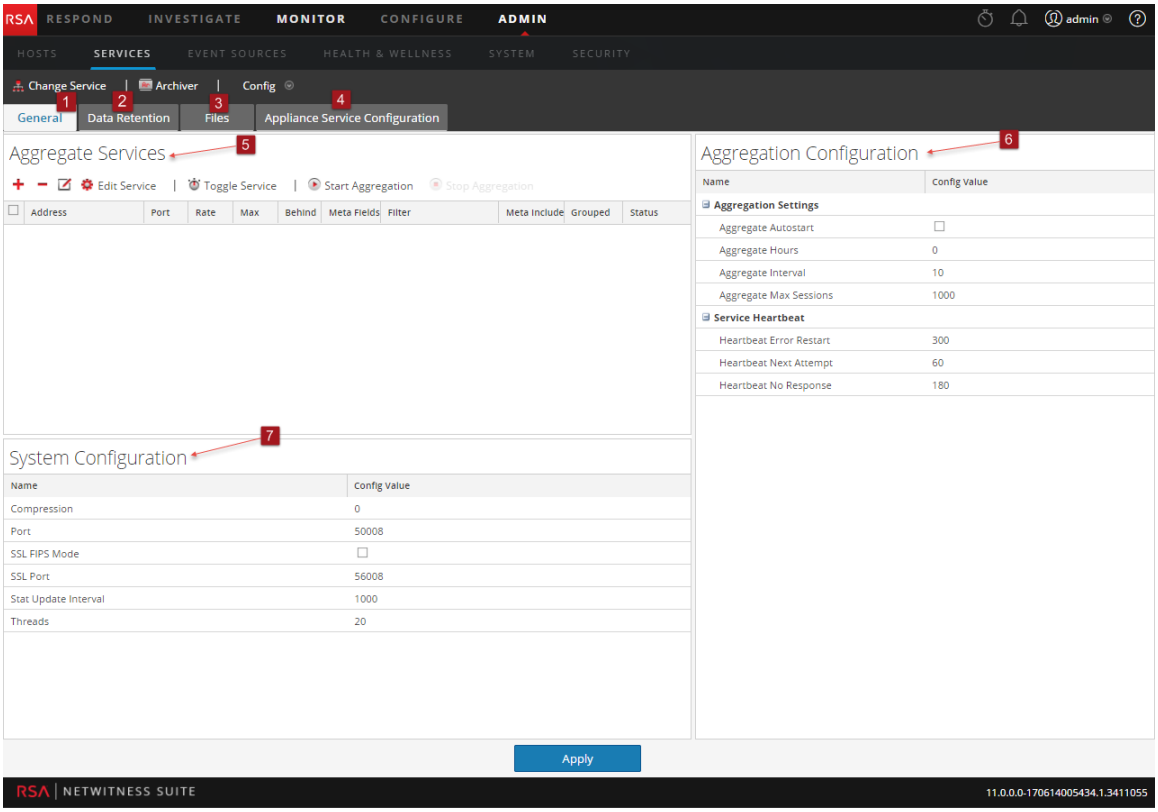
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Hinzufügen von Log Decoder als Datenquelle zu Archiver
- Konfigurieren der Archiver-Überwachung
- Konfigurieren von Protokollspeichersammlungen

Überblick

Die Ansicht „Services-Konfiguration“ verfügt über vier Registerkarten und drei Bereiche.



1	Die Registerkarte „Allgemein“ bietet eine Möglichkeit für das Management der grundlegenden Archiver-Servicekonfiguration.
2	Die Registerkarte „Datenaufbewahrung“ bietet eine Möglichkeit zum Anzeigen und Bearbeiten von Sammlungen und Aufbewahrungsregeln.
3	Die Registerkarte „Dateien“ ermöglicht Ihnen das Bearbeiten der Service-Konfigurationsdateien für den Archiver als Textdateien.
4	Die Registerkarte „Appliance-Servicekonfiguration“ bietet eine Möglichkeit zum Konfigurieren eines Archiver-Services.
5	Der Bereich „Services aggregieren“ bietet eine Möglichkeit zum Starten und Stoppen von Aggregation sowie zum Hinzufügen, Bearbeiten, Löschen und Umschalten eines

Aggregatservices.

6 Der Bereich „Aggregationskonfiguration“ enthält Konfigurationseinstellungen, die verschiedene Aspekte des Aggregationsprozesses beeinflussen.

7 Der Bereich „Systemkonfiguration“ bietet eine Möglichkeit zum Managen der Servicekonfiguration für einen Archiver-Service.

Allgemein

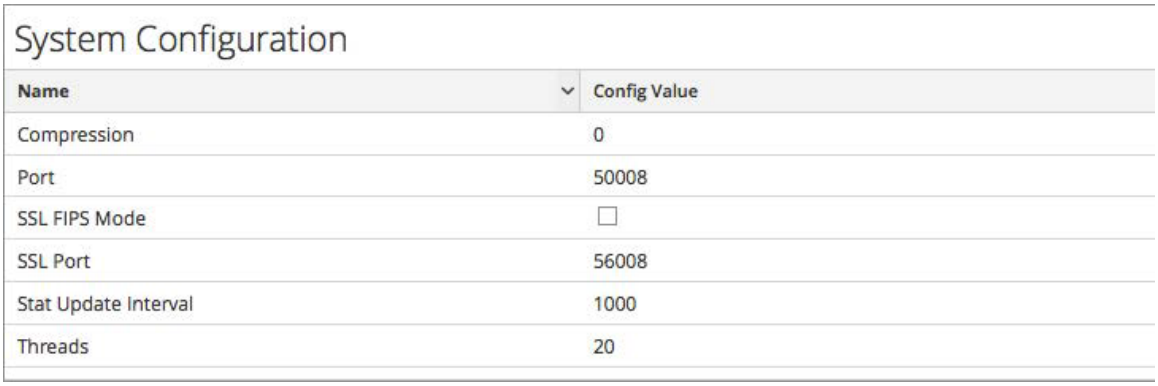
Die Registerkarte Allgemein enthält die folgenden Abschnitte:

- Services aggregieren
- Systemkonfiguration
- Aggregationskonfiguration

Services aggregieren

Der Abschnitt „Services aggregieren“ bietet eine Möglichkeit zum Starten und Stoppen von Aggregation sowie zum Hinzufügen, Bearbeiten, Löschen und Umschalten eines Aggregatservices.

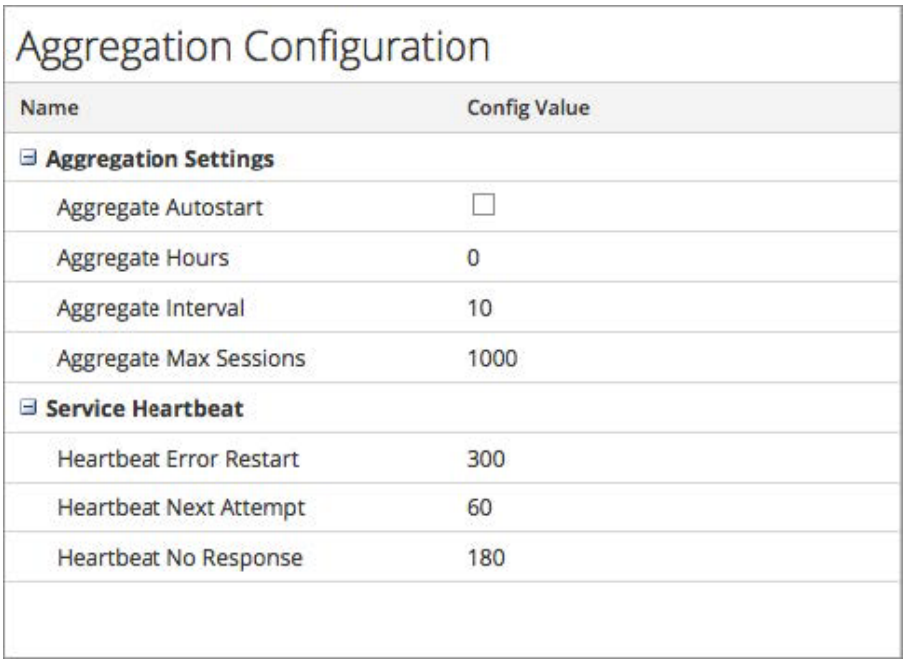
Systemkonfiguration



Wenn Sie einen Archiver-Service hinzufügen, gelten die Standardwerte. RSA hat die Standardwerte so ausgelegt, dass sie die meisten Umgebungen unterstützen, und empfiehlt, diese Werte nicht zu bearbeiten, da dies negative Auswirkungen auf die Performance haben kann. In der folgenden Tabelle werden die Systemkonfigurationsparameter beschrieben.

Aufgabe	Beschreibung
Komprimierung	Bestimmt die Mindestanzahl an Byte bevor eine Meldung komprimiert wird. Bei einem Wert von null werden Meldungen nicht komprimiert.
Port	Bestimmt den Port, den der Service verwendet. **Hinweis:** Wenn Sie die Portnummer ändern, müssen Sie den Service neu starten.
SSL FIPS-Modus	Wenn diese Option aktiviert ist, werden alle Daten, die in das Netzwerk übertragen werden, mithilfe von SSL verschlüsselt.
SSL-Port	Gibt den Port an, der zur Verschlüsselung mithilfe von SSL verwendet wird.
Statistikaktualisierungsintervall	Legt fest, wie oft (in Millisekunden) Statistik-Nodes im System aktualisiert werden
Threads	Bestimmt die Anzahl der Threads im Thread-Pool für die Verarbeitung eingehender Anforderungen.

Aggregationskonfiguration



Der Bereich „Aggregationskonfiguration“ enthält die folgenden Abschnitte:

- Aggregationseinstellungen
- Service-Heartbeat

Aggregationseinstellungen

Der Abschnitt Aggregationseinstellungen enthält die folgenden Parameter:

Parameter	Beschreibung
Autom. Start der Aggregation	Wenn diese Option aktiviert ist, wird die Datenaggregation nach einem Serviceneustart automatisch neu gestartet.
Stunden für Aggregation	Legt die maximale Anzahl der Stunden fest, für die ein Service die Aggregation starten kann.
Aggregationsintervall	Legt die Mindestanzahl von Millisekunden fest, bevor eine andere Aggregationsrunde angefordert wird
Max. Sitzungen für Aggregation	Legt die Anzahl der in jeder Runde zu aggregierenden Sitzungen fest

Service-Heartbeat

Der Abschnitt „Service-Heartbeat“ enthält die folgenden Parameter:

Parameter	Beschreibung
Heartbeat-Fehler Neustart	Gibt die Anzahl der Sekunden an, die nach einem Servicefehler gewartet werden soll, bevor eine erneute Serviceverbindung versucht wird.
Nächster Heartbeat-Versuch	Legt die Anzahl von Sekunden fest, die gewartet werden soll, bevor versucht wird, erneut eine Verbindung zum Service herzustellen.
Keine Heartbeat-Antwort	Legt die Anzahl von Sekunden fest, die gewartet werden soll, bevor der nicht reagierende Service offline gesetzt wird.

Dateien

Die Registerkarte **Dateien** in der Ansicht „Services-Konfiguration“ ermöglicht Ihnen das Bearbeiten der Servicekonfigurationsdateien für den Archiver als Textdateien. Die für die Bearbeitung verfügbaren Dateien sind abhängig von dem Servicetyp, der konfiguriert wird.

Die folgenden Dateien sind für alle Core-Services verfügbar:

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

Weitere Informationen über die Registerkarte **Dateien** finden Sie unter „Registerkarte Dateien“ im *Leitfaden für die ersten Schritte mit Hosts und Services*.