RSA NETWITNESS® SUITE

Konfigurationsleitfaden für Broker und Concentrator

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

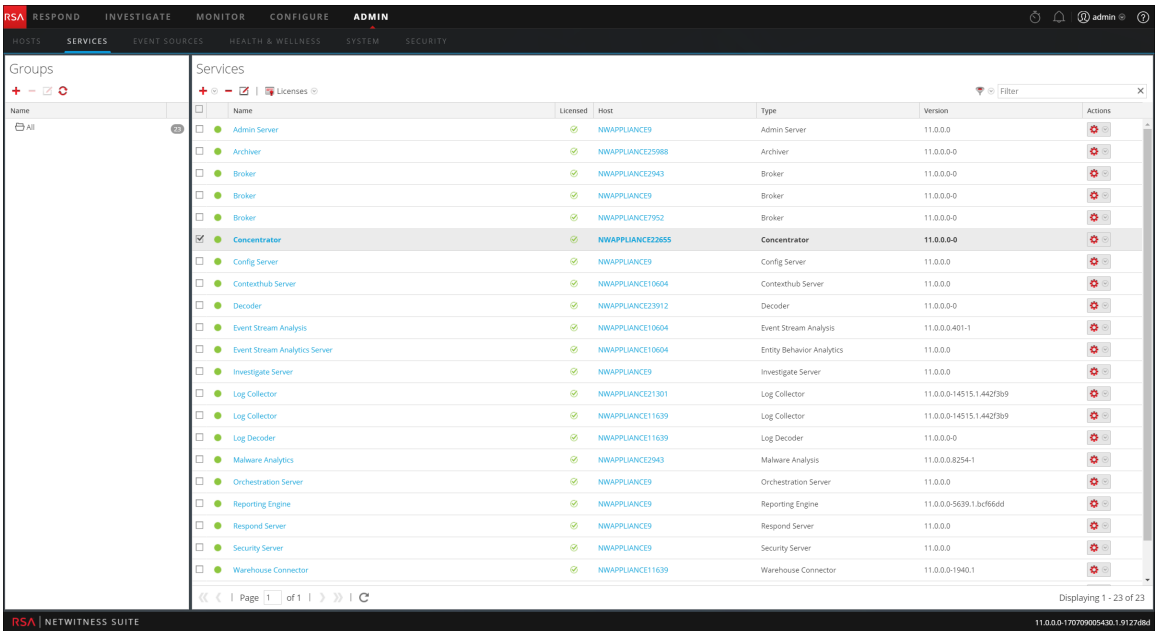
Grundlagen zu Broker und Concentrator

Im Gegensatz zu Decodern, die Daten erfassen, aggregieren Concentrators und Broker Daten, die von anderen Services erfasst oder aggregiert wurden.

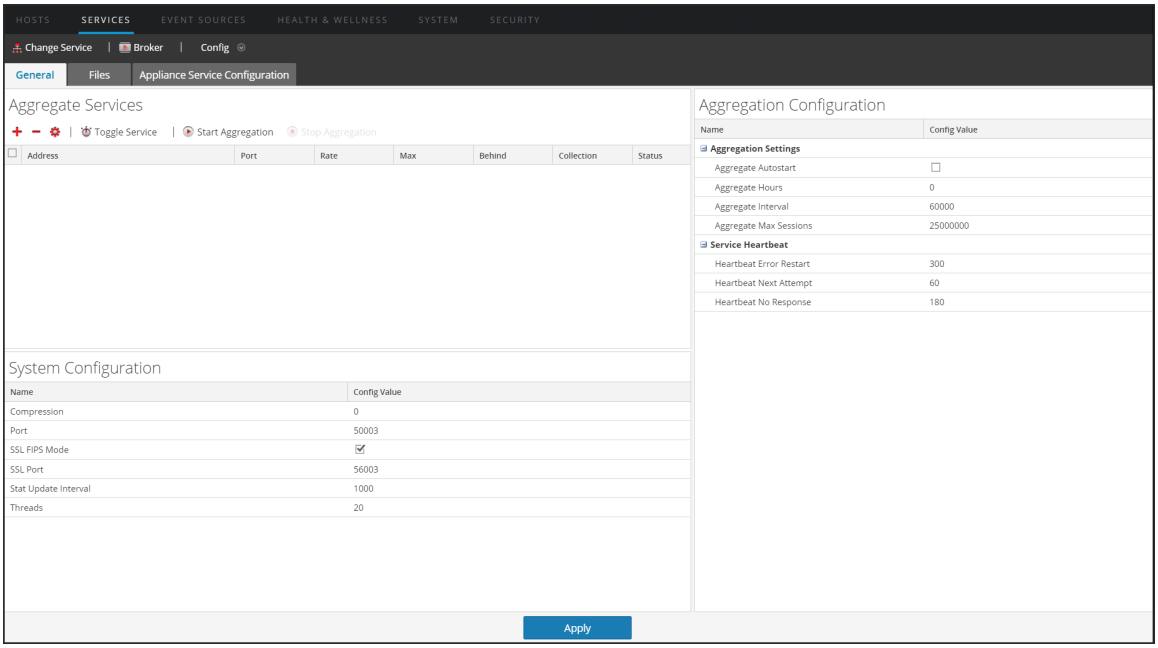
RSA NetWitness Suite unterstützt die Broker- und Concentrator-Services:

- Broker – sammeln Daten in der gesamten Infrastruktur von konfigurierten Concentrators. Sie können mehrere Concentrators in einem Broker zusammenfassen. Sie können ebenfalls mehrere Broker in einem einzigen Broker zusammenfassen.
- Concentrators – sammeln und analysieren Daten über mehrere Erfassungsorte von Decodern hinweg. Indexieren und leiten Abfragen.

Sie können verschiedene Broker und Concentrators zusammen in einem Broker konfigurieren. Broker können Daten schnell von den Concentrators abrufen, da sie nur Indexinformationen erhalten. Diese Konfiguration erfolgt mithilfe der RSA NetWitness Suite-Benutzeroberfläche. Der Großteil der Konfiguration erfolgt in der Ansicht „Administration > Services“.

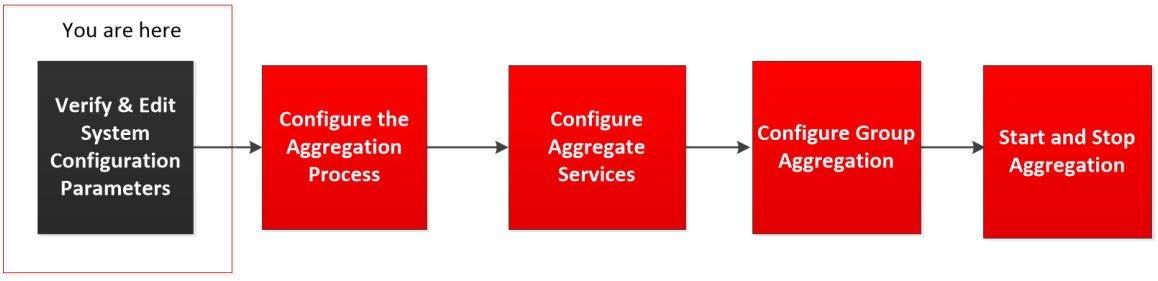


Sie können die Konfiguration der Aggregationsservices und den gesamten Aggregationsvorgang ebenfalls über die Ansicht „Services“ durchführen. Dies unterstützt die Einrichtung des automatischen Starts der Aggregation, der Timing- und Performanceparameter und der maximalen Anzahl von offenen Meta- und Sitzungsdaten. Zusätzlich können Sie die Versuche zeitlich so einstellen, dass sie einen nicht reagierenden Aggregationsservice neu starten, erneut verbinden oder offline nehmen. Die Konfiguration der Aggregationsservices umfasst das Management von Concentrators und Decodern als Aggregationsservices. Sie können ebenfalls mithilfe von Metafeldern und Filtern die durch den Aggregationsservice abgerufene Datenmenge begrenzen. Die Aggregationsaufgaben werden auf der Registerkarte „Allgemein“ der Ansicht „Administration > Services“ angezeigt.



Schritt 1. Überprüfen der Servicesystemkonfiguration

Wenn ein Service zum ersten Mal zu NetWitness Suite hinzugefügt wird, sind Standardwerte für die Systemkonfigurationsparameter wirksam. Sie können diese Werte bearbeiten, um die Performance zu verbessern.



In den meisten Fällen sind die Standardwerte für Komprimierung, Statistikaktualisierungsintervall und Anzahl der Threads im Threadpool auf einen geeigneten Wert für eine optimale Systemperformance festgelegt.

So bearbeiten Sie die Systemkonfigurationsparameter für einen Broker oder Concentrator:

1. Wählen Sie in der **Hauptmenü** ADMIN **> Services** aus.
2. Wählen Sie in der Ansicht **Services** einen Broker oder Concentrator aus und wählen Sie in der Spalte „Aktionen“  **> Ansicht > Konfiguration** aus.

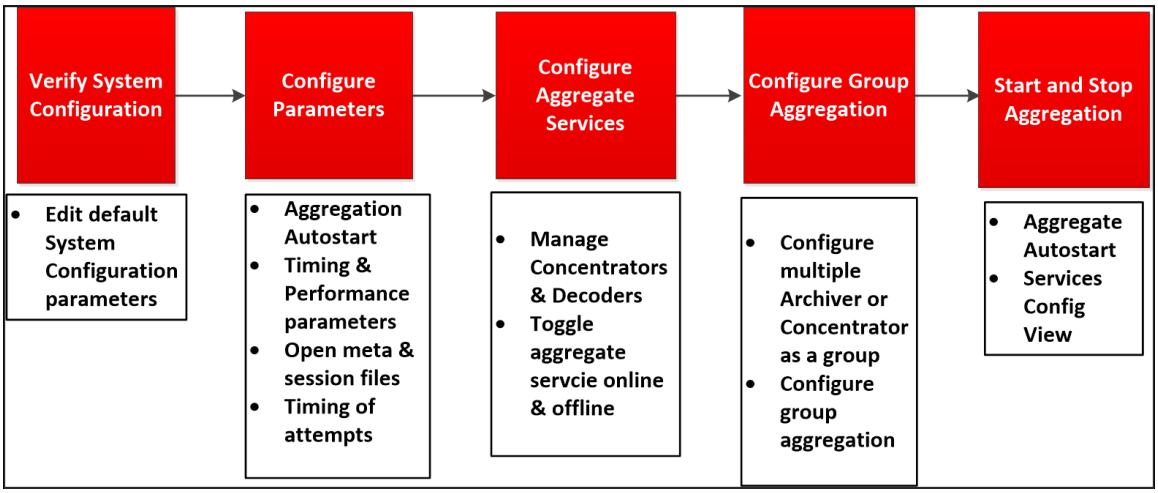
   Die Ansicht „Service-Konfiguration“ für den ausgewählten Service wird angezeigt.

3. Klicken Sie unter Systemkonfiguration in ein zu bearbeitendes Feld und geben Sie einen neuen Wert ein.
4. Klicken Sie nach dem Bearbeiten auf Anwenden.

Broker- und Concentrator-Konfiguration

Bei der Einrichtung eines Brokers oder Concentrators müssen die grundlegenden Serviceparameter, die Aggregationsservices sowie der Aggregationsprozess zwischen einem Broker oder Concentrator und den Aggregationsservices konfiguriert werden.

Dies sind die erforderlichen Schritte zur Konfiguration eines neuen Brokers oder Concentrators und zur Änderung der Konfiguration eines vorhandenen Brokers. Führen Sie die in diesem Abschnitt aufgezeigten Schritte in vorgegebener Reihenfolge aus.



Checkliste der grundlegenden Konfiguration

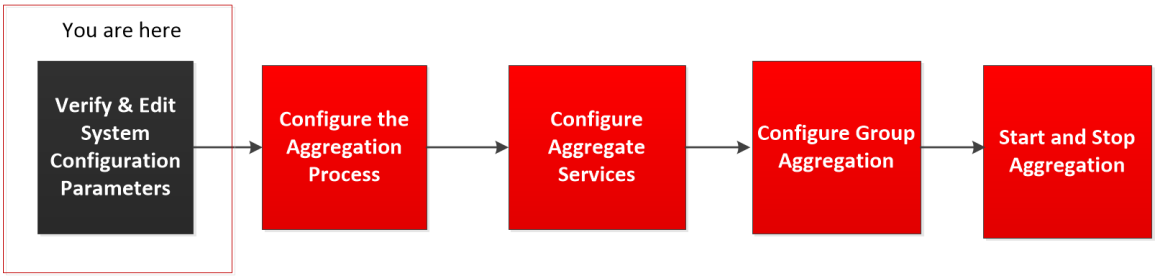
In der folgenden Checkliste sind die Aufgaben enthalten, die zur Konfiguration eines Brokers oder Concentrators erforderlich sind, der in Übereinstimmung mit dem *Leitfaden für die ersten Schritte mit Hosts und Services* zu RSA NetWitness Suite hinzugefügt wurde.

Konfigurationsschritt	Beschreibung
Schritt 1: Überprüfen der Systemkonfiguration	Überprüfen Sie, ob die Standardwerte der Systemkonfiguration für den Host und den Service geeignet sind, wie beschrieben in Schritt 1. Überprüfen der Servicesystemkonfiguration
Schritt 2: Konfigurieren von Parametern	Konfigurieren Sie Parameter zur Steuerung des gesamten Aggregationsprozesses, wie beschrieben in Schritt 2. Konfigurieren des Aggregationsprozesses

Konfigurationsschritt	Beschreibung
Schritt 3: Konfigurieren der Aggregationsservices	Konfigurieren Sie Aggregationsservices, wie beschrieben in Schritt 3. Konfigurieren der Aggregationsservices
Schritt 4: Konfiguration der Gruppenaggregation	(Optional) Konfigurieren Sie die Gruppenaggregation wie beschrieben in Schritt 4. (Optional) Konfigurieren der Gruppenaggregation
Schritt 5: Starten und Beenden der Aggregation	Starten und beenden Sie die Aggregation, wie beschrieben in Schritt 4. Starten und Beenden der Aggregation

Schritt 1. Überprüfen der Servicesystemkonfiguration

Wenn ein Service zum ersten Mal zu NetWitness Suite hinzugefügt wird, sind Standardwerte für die Systemkonfigurationsparameter wirksam. Sie können diese Werte bearbeiten, um die Performance zu verbessern.



In den meisten Fällen sind die Standardwerte für Komprimierung, Statistikaktualisierungsintervall und Anzahl der Threads im Threadpool auf einen geeigneten Wert für eine optimale Systemperformance festgelegt.

So bearbeiten Sie die Systemkonfigurationsparameter für einen Broker oder Concentrator:

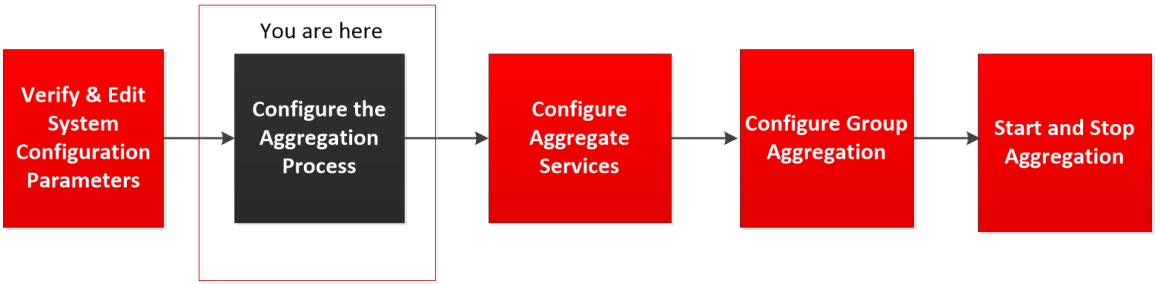
1. Wählen Sie in der **Hauptmenü** ADMIN > **Services** aus.
2. Wählen Sie in der Ansicht **Services** einen Broker oder Concentrator aus und wählen Sie in der Spalte „Aktionen“ > **Ansicht** > **Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ für den ausgewählten Service wird angezeigt.

3. Klicken Sie unter Systemkonfiguration in ein zu bearbeitendes Feld und geben Sie einen neuen Wert ein.
4. Klicken Sie nach dem Bearbeiten auf Anwenden.

Schritt 2. Konfigurieren des Aggregationsprozesses

Das Konfigurieren des Aggregationsprozesses für einen Broker oder Concentrator umfasst die Einstellung folgender Parameter:

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

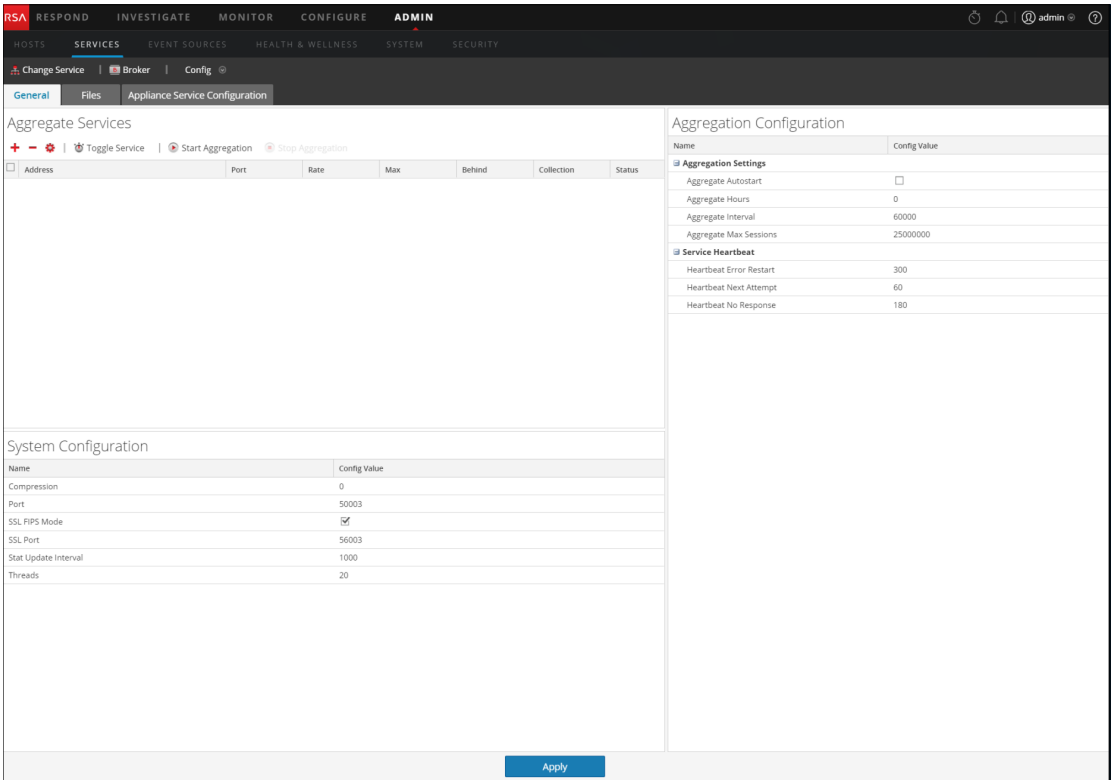


So konfigurieren Sie den Aggregationsprozess auf einem Broker oder Concentrator:

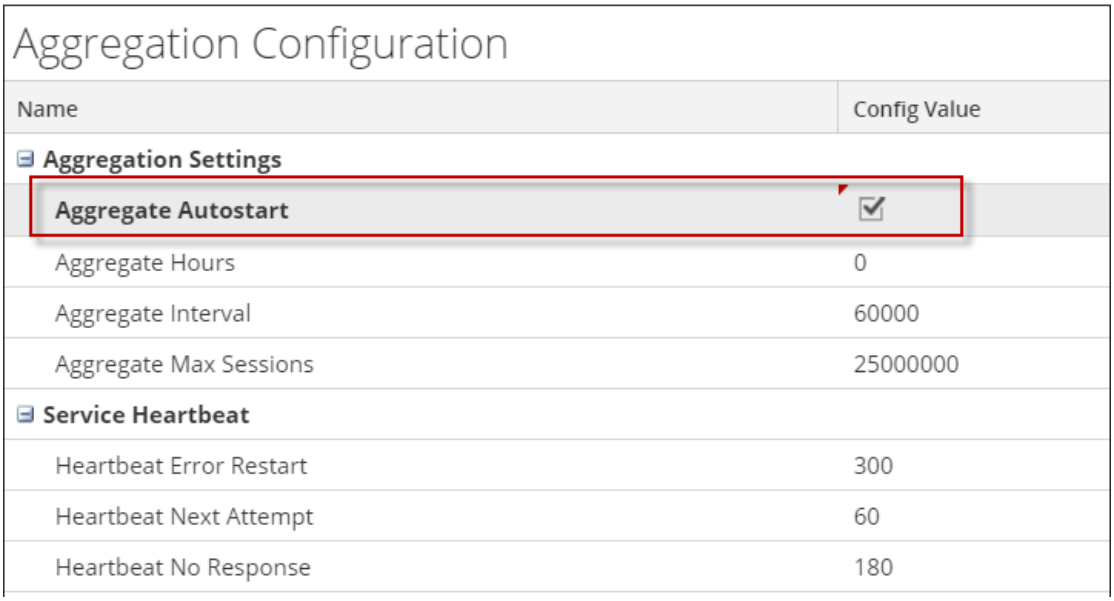
1. Wählen Sie im **Hauptmenü** die Optionen ADMIN > **Services** aus.
2. Wählen Sie in der Ansicht **Services** einen Broker oder Concentrator aus und wählen Sie  > **Ansicht** > **Konfiguration**.

   Die Ansicht „Services-Konfiguration“, die den Abschnitt „Aggregationskonfiguration“

enthält, wird angezeigt.



3. (Optional) Wählen Sie **Autom. Start der Aggregation**, um den automatischen Start der Aggregation zu aktivieren, wenn der Service online ist.



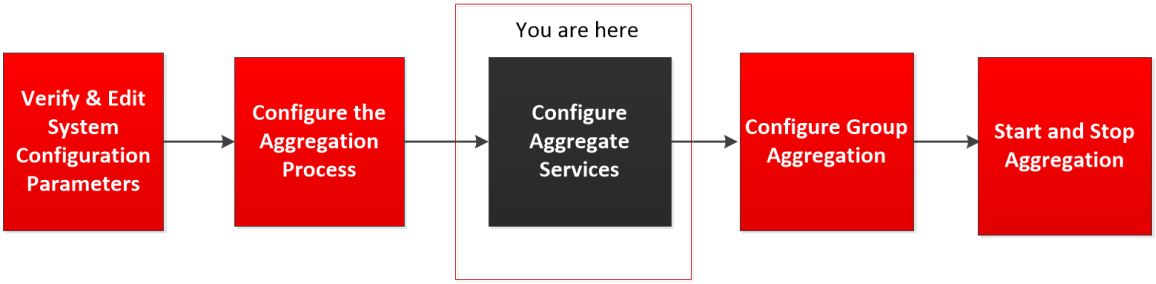
4. (Optional) Bearbeiten Sie beliebige Aggregationseinstellungen: die Stunden zurück zum Aggregationsbeginn, die Millisekunden zwischen Aggregationsrunden und maximale Anzahl der Sitzungen pro Aggregationsrunde.
5. (Optional) Bearbeiten Sie beliebige Einstellungen unter Service-Heartbeat, mit denen Sie das Timing des ersten Versuchs zum erneuten Verbinden des Services nach einem Fehler, des nächsten Versuchs zum erneuten Verbinden und das Offline-Nehmen des Services nach dem fehlgeschlagenen Versuch, die Verbindung widerherzustellen, festlegen können.
6. Klicken Sie nach dem Bearbeiten der Einstellungen auf **Anwenden**.
   Die Einstellungen werden sofort wirksam

Schritt 3. Konfigurieren der Aggregationsservices

In diesem Thema werden grundlegende Aufgaben bezüglich der Datenaggregation auf Broker und Concentrators beschrieben. Informationen zur optionalen Konfiguration der Gruppenaggregation finden Sie unter Schritt 4. (Optional) Konfigurieren der Gruppenaggregation.

Die Konfiguration der Aggregationsservices (dessen Daten gelesen und aggregiert werden) beinhaltet:

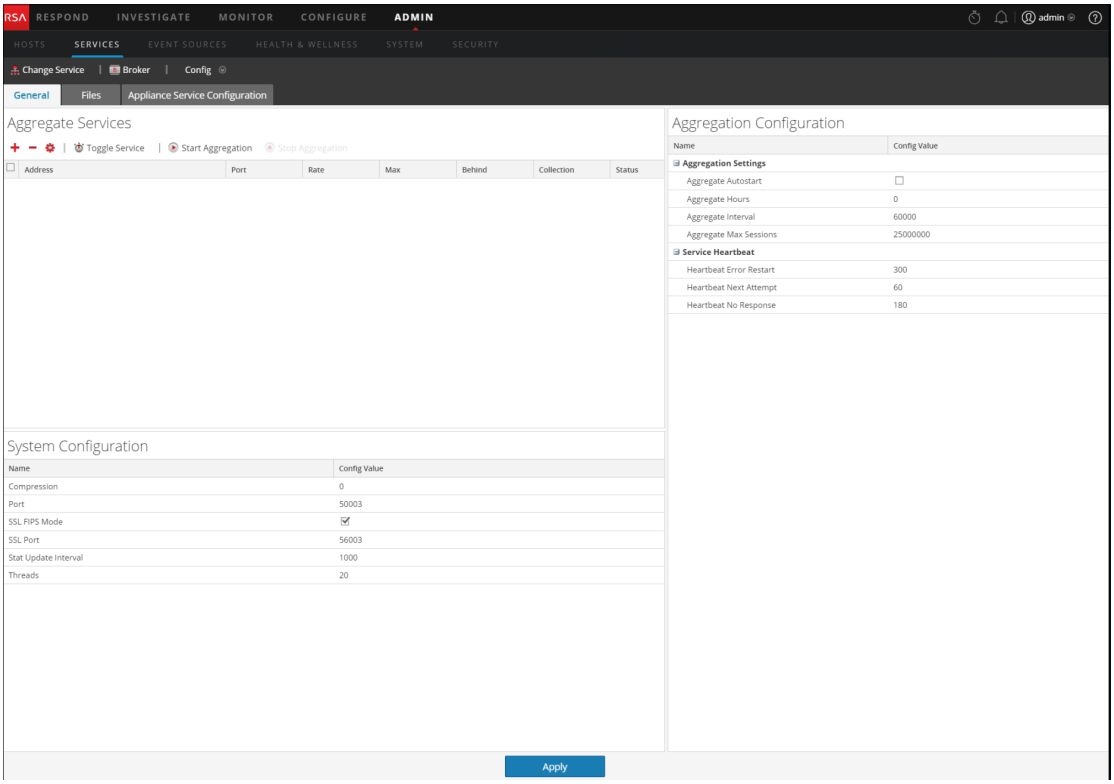
- Hinzufügen, Bearbeiten und Löschen von Concentrators und Decodern als Aggregationsservices
- Umschalten eines Aggregationsservices zwischen online und offline



Hinzufügen von Aggregationsservices zu einem Broker oder Concentrator

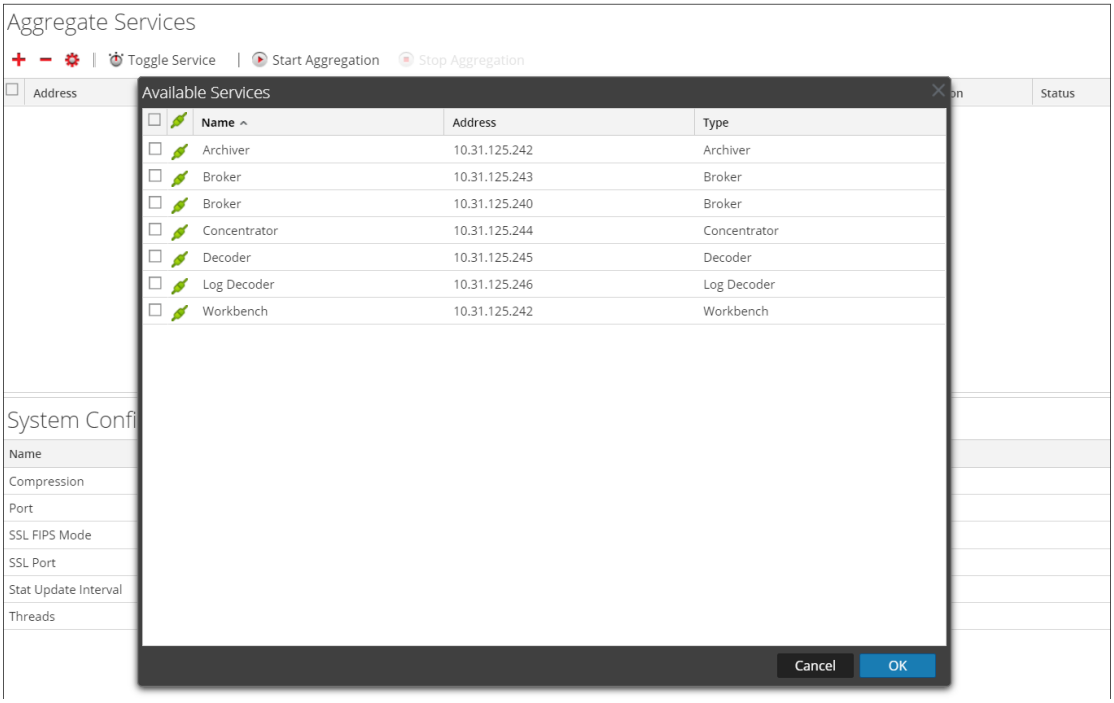
1. Wählen Sie im Menü **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie in der Ansicht **ADMIN Services** einen Broker oder Concentrator aus und wählen Sie  **> Ansicht > Konfiguration**

aus.Die Ansicht „Service-Konfiguration“ für den ausgewählten Service wird angezeigt.

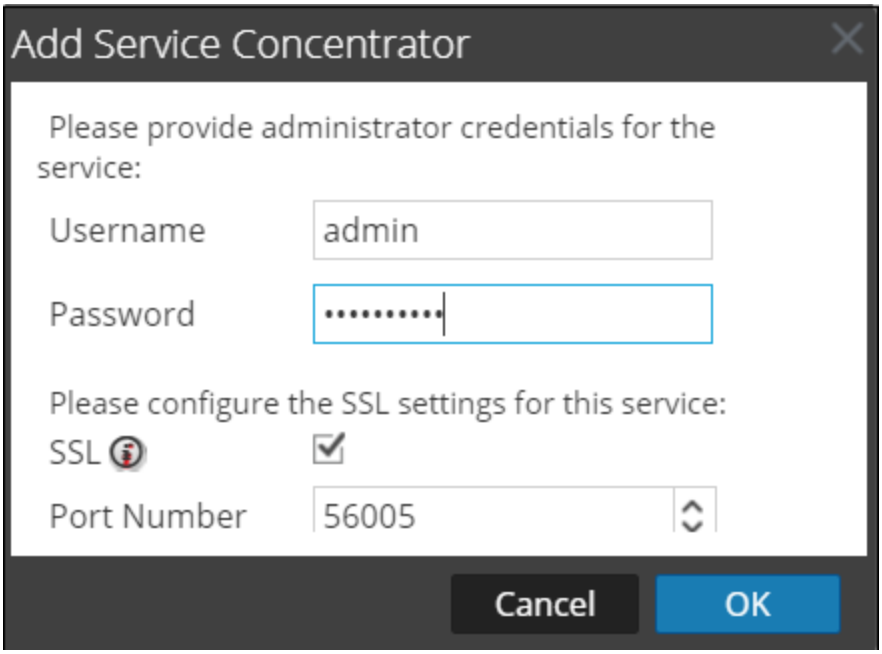


3. Klicken Sie auf + in der Symbolleiste **Services aggregieren**.

Das Dialogfeld „Verfügbare Services“ wird angezeigt.



4. Wählen Sie einen oder mehrere Services aus, die Sie hinzufügen möchten, und klicken Sie auf **OK**.
5. Geben Sie den Administrator-Benutzernamen und das Passwort ein, um sich zu authentifizieren, wenn Sie einen Service hinzufügen.



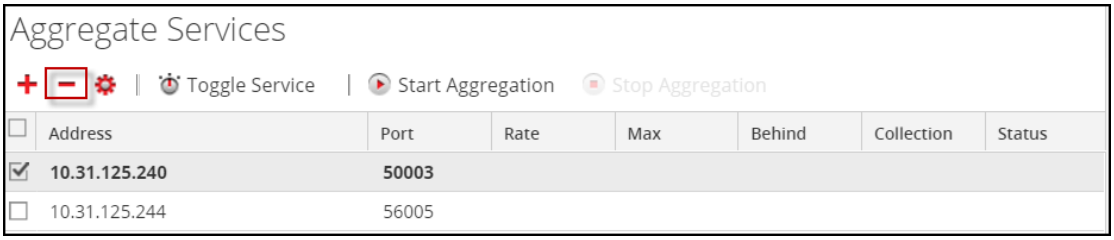
Die hinzugefügten Services werden in der Liste „Services aggregieren“ aufgeführt.

6. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.

Entfernen von Aggregationsservices aus einem Broker oder Concentrator

Hinweis: Diese Option gilt ausschließlich für Offlineservices. Ist der Aggregationsservice online, müssen Sie den Service zunächst in den Offlinestatus schalten.

1. Wählen Sie aus der Liste **Services aggregieren** einen oder mehrere Services aus.
2. Klicken Sie in der Symbolleiste auf − .



Der Service wurde aus der Liste „Services aggregieren“ entfernt.

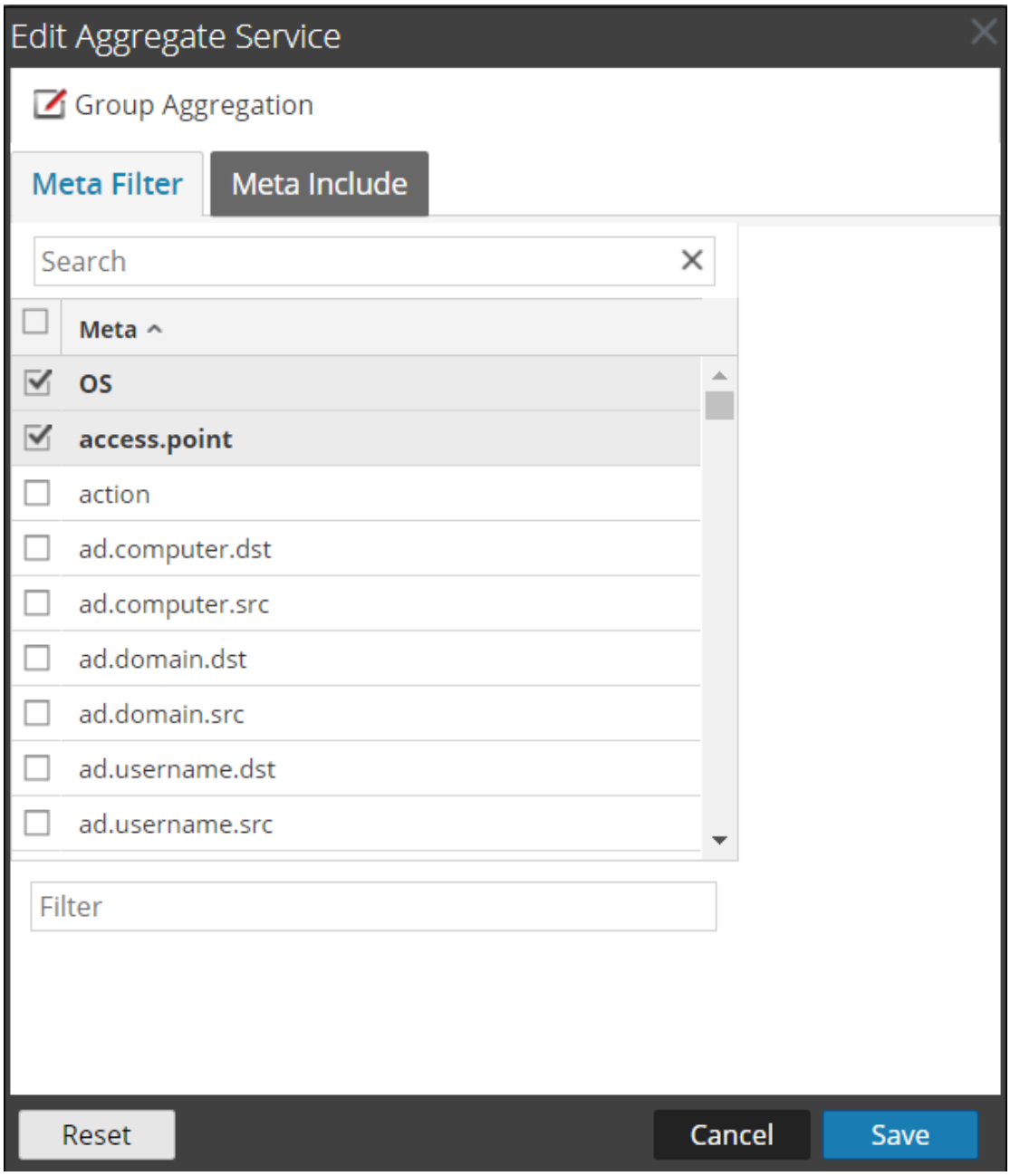
3. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.

Bearbeiten von Aggregationsservices in einem Concentrator

Hinweis: Diese Option gilt ausschließlich für Offlineservices. Ist der Aggregationsservice online, müssen Sie den Service zunächst in den Offlinestatus schalten. Sie können jeweils nur einen Service bearbeiten.

Sie können mithilfe von Metafeldern und Filtern die durch den Aggregationsservice abgerufene Datenmenge begrenzen. So konfigurieren Sie dies:

1. Klicken Sie auf **Service ändern**, um den Service für Concentrator zu ändern.
2. Wählen Sie aus der Liste **Services aggregieren** einen oder mehrere Services aus.
3. Klicken Sie in der Symbolleiste auf . Geben Sie die Authentifizierungsinformationen in das Pop-up-Dialogfeld ein.
   - Wurde der Service einer anderen Instanz von NetWitness Suite hinzugefügt, müssen Sie ihn zur Bearbeitung dieser Instanz von NetWitness Suite hinzufügen. In einem Warnmeldungsdialogfeld können Sie den Service hinzufügen. Wenn Sie auf **Ja** klicken, wird das Dialogfeld „Service hinzufügen“ angezeigt.
   - Wenn der Service online ist, weist Sie ein Dialogfeld darauf hin, dass der Service offline sein muss, und verlangt eine Bestätigung, dass Sie fortfahren möchten. Wenn Sie auf **Ja** klicken, wird der Service von NetWitness Suite offline genommen und das Dialogfeld Aggregierten Service bearbeiten wird angezeigt.
   - Befindet sich der Service im Offlinemodus, wird das Dialogfeld „Aggregierten Service bearbeiten“ mit den zu bearbeitenden Eigenschaften eines Aggregationsservices in einem Concentrator angezeigt.
4. Klicken Sie in der Registerkarte **Enthaltene Metadaten** auf einen Metadatentyp, um den Metadatentyp auszuwählen, den der Concentrator aus diesem Service abrufen soll. Klicken Sie auf **Speichern**.



5. Zum Aufstellen einer Regel für das Filtern der Daten, die der Concentrator aus diesem Service abruft, erstellen Sie auf der Registerkarte **Metafilter** eine Regel. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Schließen**.
   Das Dialogfeld „Aggregierten Service bearbeiten“ wird geschlossen und die Änderungen werden in der Liste „Services aggregieren“ angezeigt. In diesem Beispiel wurden zwei Metadaten auf der Registerkarte „Enthaltene Metadaten“ ausgewählt. Wenn Sie im Feld „Enthaltene Metadaten“ auf das Informationssymbol klicken, wird diese Auswahl angezeigt.

7. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.

Service an-/ausschalten

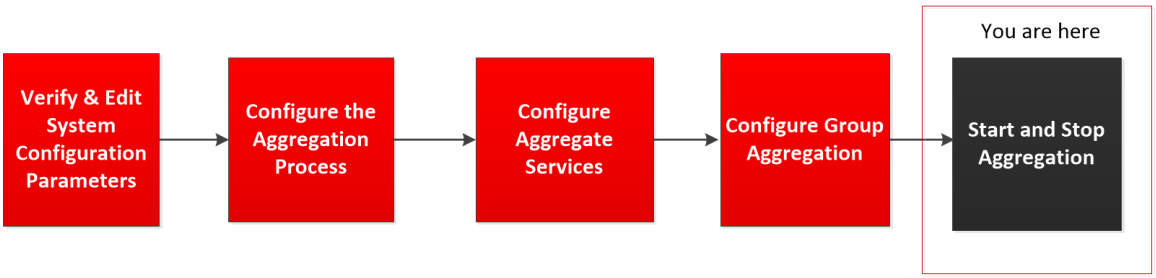
Wenn die Datenaggregation beginnt, rufen Broker und Concentrators die Daten aus den Aggregationsservices ab, die sich im Onlinemodus befinden. Beim Hinzufügen zu einem Broker oder Concentrator befinden sich die Aggregationsservices im Offlinemodus. So schalten Sie einen Service zwischen Online- und Offlinemodus hin und her.

1. Wählen Sie aus der Liste **Services aggregieren** einen Service aus.
2. Klicken Sie auf Toggle Service .

   Der Status ändert sich.

Schritt 4. Starten und Beenden der Aggregation

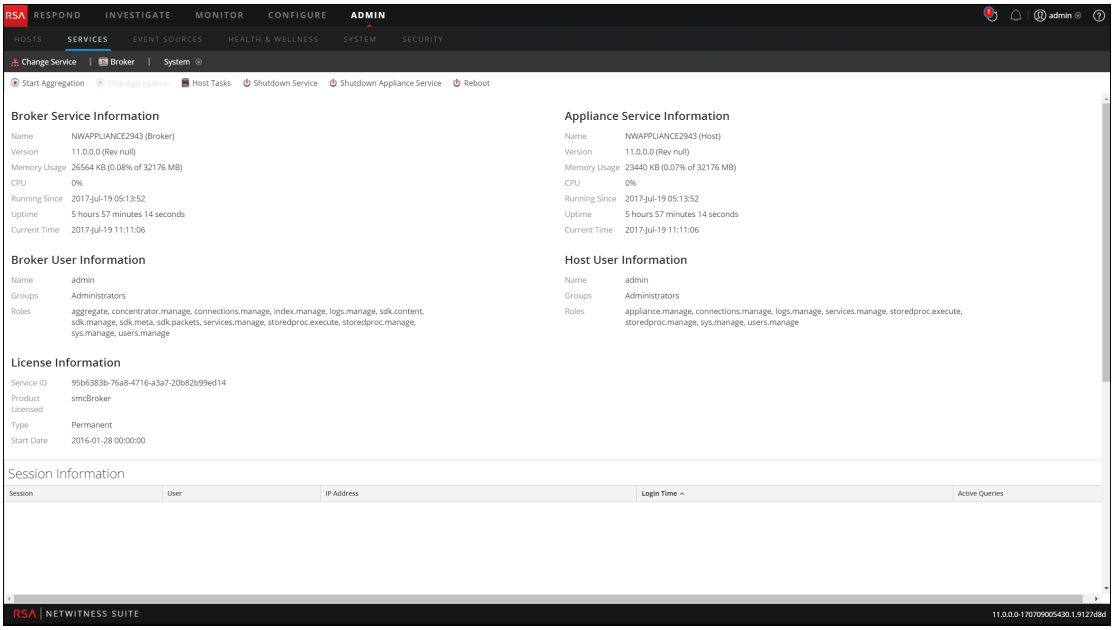
Wenn ein Broker oder Concentrator startet, beginnt er automatisch mit dem Aggregieren von Daten, wenn Automatischer Start der Aggregation aktiviert ist. Wenn der automatische Start nicht aktiviert ist, können Sie die Datenaggregation manuell starten und beenden.



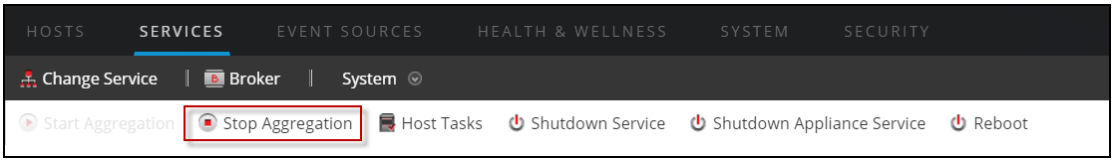
Hinweis: Die Aggregationskonfigurationseinstellungen in der Servicekonfigurationsansicht für einen Broker oder Concentrator legen fest, ob automatischer Start der Aggregation aktiviert ist, sowie die Größe einer Aggregationsrunde und den Zeitraum zwischen den Runden.

Starten und Beenden der Datenaggregation in der Ansicht „Services-System“

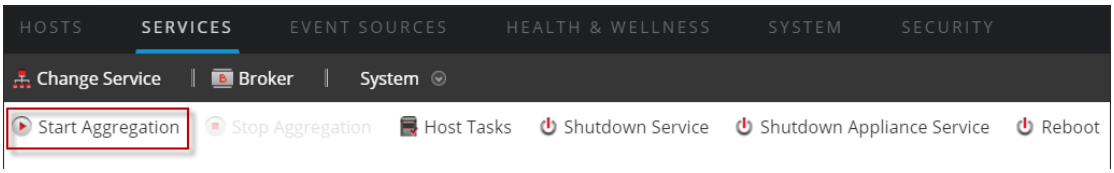
1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie in der Ansicht **ADMIN > Services** einen Broker oder einen Concentrator aus und wählen Sie  **> Ansicht > System** aus.



3. Klicken Sie zum Beenden eines Brokers oder Concentrators, der dabei ist, Daten zu erfassen, auf **Aggregation beenden** in der Symbolleiste.
   Der Service beendet die Datenaggregation und die Option **Aggregation beenden** in der Symbolleiste ist nicht verfügbar. Die Option **Aggregation starten** wird aktiv.

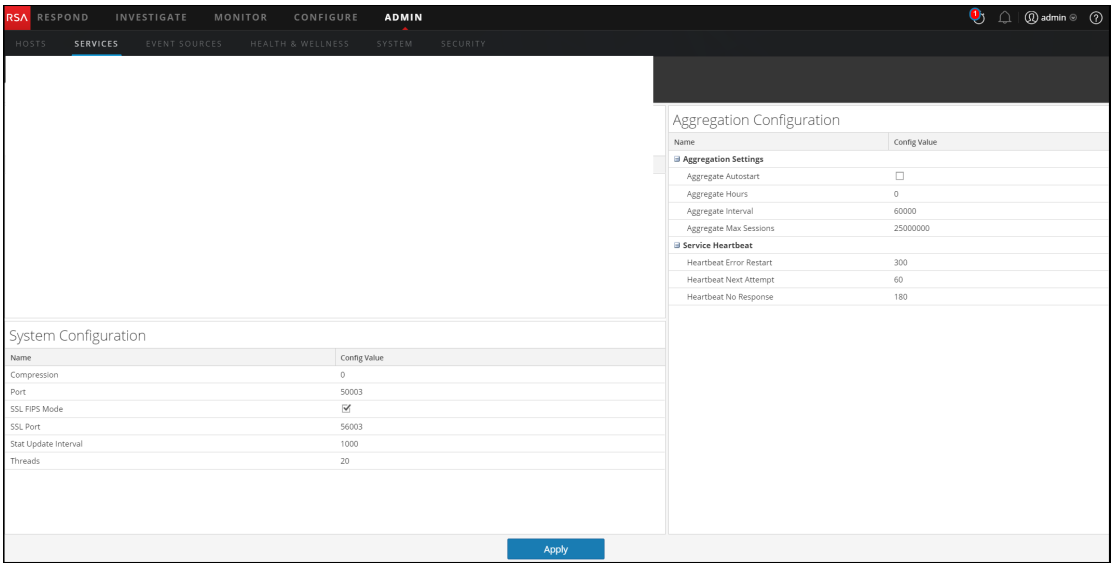


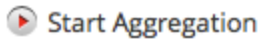
4. Wenn Sie möchten, dass der Service wieder beginnt, Daten zu aggregieren, klicken Sie auf **Aggregation starten**.
   Sie können jetzt die erfassten Daten im Modul Investigation ermitteln.



Starten und Beenden der Aggregation in der Ansicht „Service-Konfiguration“

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie in der Ansicht **Administrationsservices** einen Broker oder einen Concentrator aus und wählen Sie  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“, die den Abschnitt „Services aggregieren“ enthält, wird angezeigt.



3. Klicken Sie zum Starten der Aggregation auf dem ausgewählten Broker oder Concentrator auf 

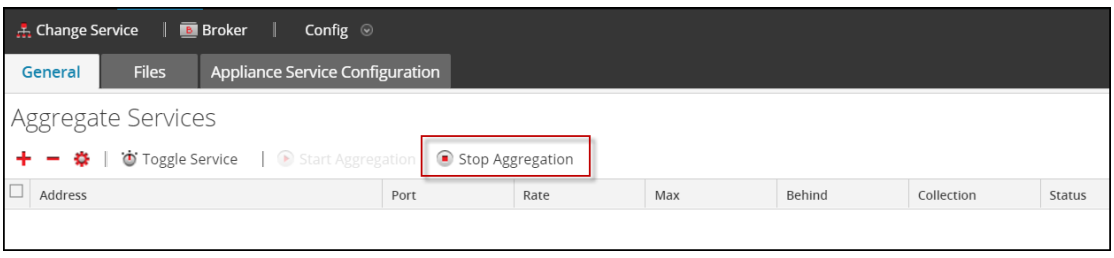
in der Systemleiste **Services aggregieren**.

   Wenn die Aggregation startet, ändert sich der Status aller Online-Aggregationsservices in **wird verarbeitet**. Die Schaltfläche „Aggregation starten“ ist deaktiviert und die Schaltfläche „Aggregation beenden“ ist aktiviert.

4. Klicken Sie zum Beenden der Aggregation auf 

in der Symbolleiste **Services aggregieren**.

   Wenn die Aggregation beendet wird, ändert sich der Status aller verarbeitenden Aggregationsservices in **online**. Die Schaltfläche „Aggregation beenden“ ist deaktiviert und die Schaltfläche „Aggregation starten“ ist aktiviert.



Broker- und Concentrator-Konfiguration – Referenzen

Sie können Broker und Concentrators mithilfe der NetWitness Suite-Benutzeroberfläche konfigurieren.

Zusätzlich zu den hier beschriebenen Ansichten können Sie die vollständigen Service-Nodes in einer Baumstruktur in der Ansicht „Durchsuchen“ zu einem Service anzeigen. Siehe das Thema „Ansicht Durchsuchen zu einem Service“ im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Themen

Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“ für Broker oder Concentrator

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

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

- Hinzufügen, Bearbeiten und Löschen von Concentrators und Brokern 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?

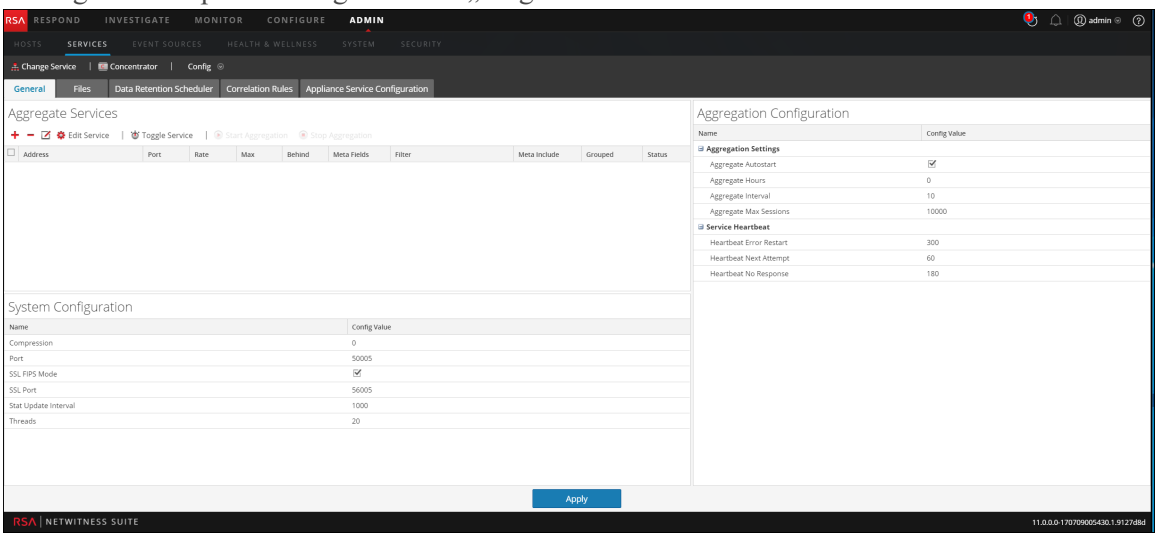
Rolle	Ziel	Siehe
Administrator	Starten und Beenden Sie die Aggregation Einen Aggregatservice hinzufügen, bearbeiten, löschen und umschalten	Abschnitt „Services aggregieren“
Administrator	Systemkonfiguration verwalten	Abschnitt „Systemkonfiguration“

Verwandte Themen

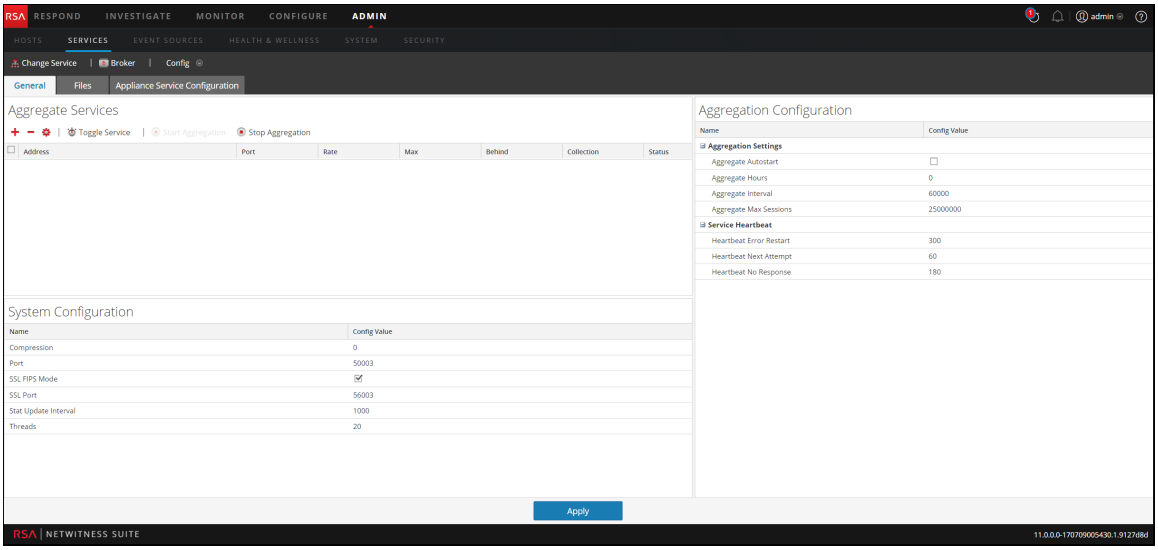
- Grundlagen zu Broker und Concentrator
- Broker- und Concentrator-Konfiguration

Registerkarte „Allgemein“

Es folgt ein Beispiel der Registerkarte „Allgemein“ für einen Concentrator.



Es folgt ein Beispiel der Registerkarte „Allgemein“ für einen Broker.



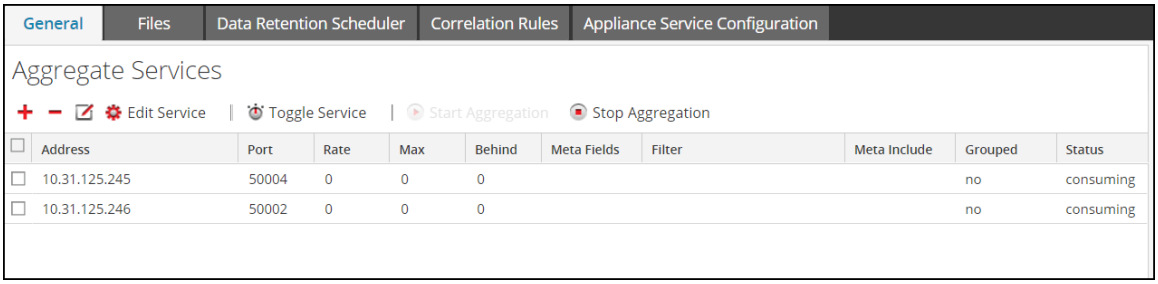
Es folgen die drei Hauptabschnitte der Registerkarte „Allgemein“ für Broker und Concentrators:

- 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.
	Nur für Concentrators: Öffnet ein Dialogfeld, in dem die Werte für **Metafelder** und **Filter** für den Concentrator bearbeitet werden können.
Edit Service	Hier können Sie die Administrator-Anmeldedaten des ausgewählten aggregierten Services eingeben, damit dieser mit dem Broker oder Concentrator kommunizieren kann.
Start Aggregation	Startet die Datenaggregation vom Onlineservice in der Liste durch die Verwendung der für den Service definierten Regeln, wenn Aggregation gestoppt oder nicht gestartet wurde.
Stop Aggregation	Stoppt die Aggregation des Broker oder Concentrator, wenn die Aggregation läuft. Beendet alle Services und

Option	Beschreibung
	löscht den Index. Der Abschluss dieses Vorgangs kann einige Minuten dauern. Aggregatservices müssen beendet werden, damit verschiedene Administrationsverfahren durchgeführt werden können.
Toggle Service	Wechselt den Servicestatus zwischen offline und online. Nur Daten des Onlineservices werden während der Aggregation abgerufen.

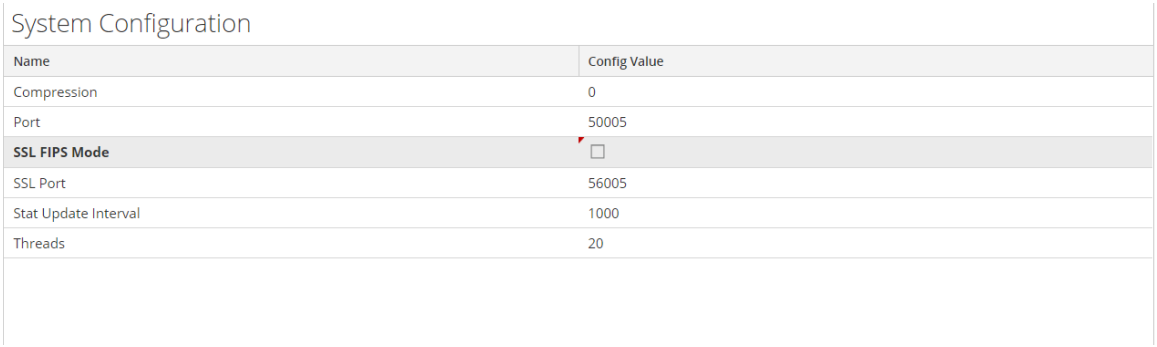
Die Abschnittsliste „Services aggregieren“ hat folgende Spalten.

Spalte	Beschreibung
Adresse	Gibt die Serviceadresse an.
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.

Spalte	Beschreibung
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.
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.



Der Abschnitt Systemkonfiguration enthält diese Parameter.

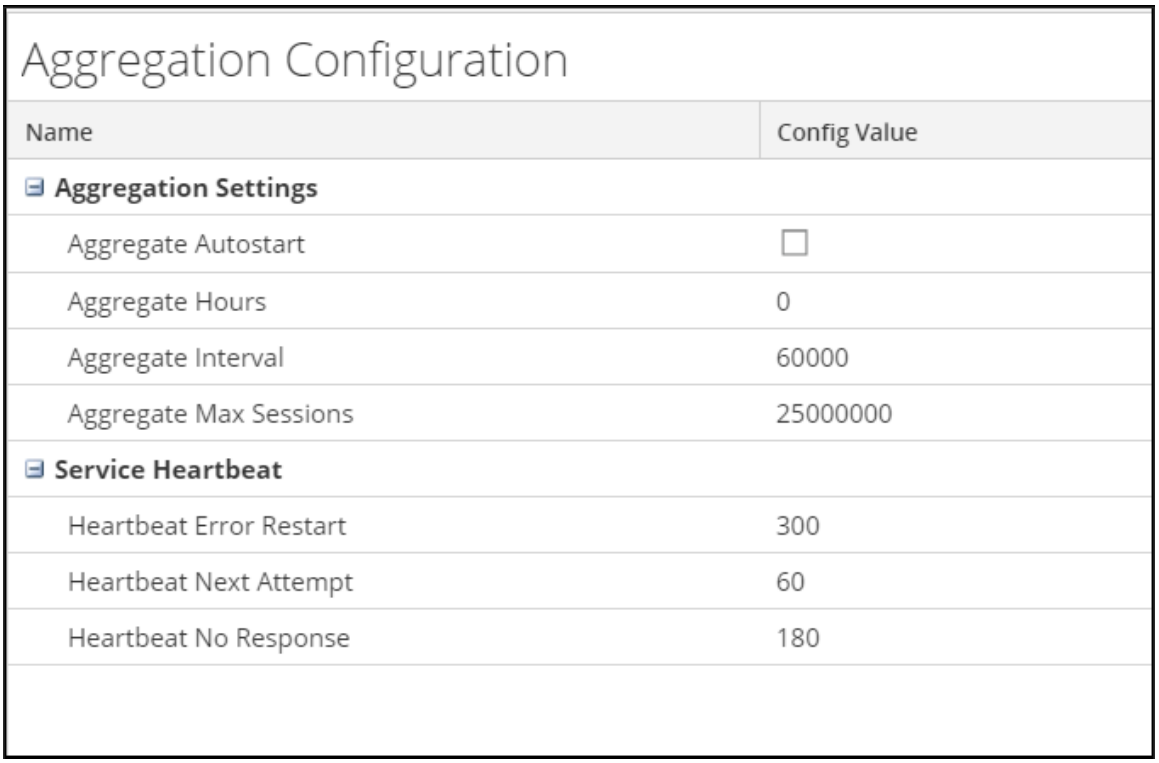
Parameter	Beschreibung
Komprimierung	Die Mindestanzahl Byte, die pro Antwort vor der Komprimierung übertragen werden muss. Die Einstellung **0** deaktiviert die Komprimierung. Der Standardwert ist **0**. Eine Veränderung des Werts ist sofort für alle nachfolgenden Verbindungen wirksam.
Port	Der Port,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

Parameter	Beschreibung
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: Ändern Sie keine dieser Einstellungen, wenn Sie nicht durch die Entwickler oder das Team des Kundensupports angeleitet werden. Wenden Sie sich bei Fragen an den Kundensupport, bevor Sie eine dieser Einstellungen bearbeiten.



Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	☐
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Aggregationseinstellungen

Einstellung	Beschreibung
Autom. Start der Aggregation	Option zum automatischen Start der Aggregation bei jedem Start des Broker oder Concentrator. Aktiviert bedeutet „ja“, deaktiviert bedeutet „nein“. Diese Änderung wird sofort wirksam.

Einstellung	Beschreibung
Stunden für Aggregation	Die Anzahl der zurückliegenden Stunden für alle Services, die der Concentrator oder Broker am Anfang der Aggregation wiederherzustellen versucht. Diese Änderung wird sofort wirksam. • Wenn der Wert auf 0 gesetzt ist, startet die Aggregation für jeden Service beim letzten Stoppzeitpunkt, unabhängig von der Anzahl der zurückliegenden Stunden. • Handelt es sich bei dem Wert um eine positive ganze Zahl, ruft der Concentrator oder Broker nur Sitzungen ab, die kürzer sind als die Anzahl der zurückliegenden Stunden sind. Wenn die aktuelle Sitzung eines Services beispielsweise mehr als 10 Stunden nach der letzten Sitzung stattfindet, geschieht bei diesen beiden Werten für „Stunden für Aggregation“ Folgendes: • Bei einem Wert von 12 beginnt der Concentrator oder Broker da an abzurufen, wo er aufgehört hatte. • Bei einem Wert von 4 werden alle Sitzungen mit zwischen 5 und 10 zurückliegende Stunden übersprungen und der Concentrator oder Broker nimmt das Abrufen jener Sitzung auf, die einen Wert von 4 zurückliegende Stunden hat.
Aggregationsintervall	Die Anzahl an Millisekunden zwischen Serviceaggregationsrunden. Alle vom Broker oder Concentrator verwalteten Services fordern zusätzliche Sitzungsrunden und zu aggregierende Metadaten an. Wenn ein Broker oder Concentrator noch beim Abrufen der vorherige Datenrunde ist, kann er bis zum Schluss keine weiteren Daten mehr anfordern. Die Änderung wird sofort wirksam.
Max. Sitzungen für Aggregation	Die maximale Anzahl an Sitzungen, die der Broker oder Concentrator in einer festgelegten Datenaggregationsrunde anfordert. Die Änderung wird nach einem Neustart wirksam.

Service-Heartbeat

Bei der Kommunikation mit jedem Aggregatservice überwachen Broker und Concentrators den Servicetakt. Diese Parameter legen das Timing des ersten Versuchs, nach einer Fehlermeldung erneut eine Verbindung zu einem Service herzustellen, des nächsten Versuchs zur Wiederherstellung einer Verbindung und des Offlinenehmens des Services nach einem Verbindungsfehler fest.

Einstellung	Beschreibung
Heartbeat-Fehler Neustart	Nachdem ein Heartbeat-Fehler bei einem Aggregationsservice erkannt wurde, wird die Anzahl der Sekunden angegeben, die ein Broker oder Concentrator warten muss, bevor ein Versuch zur Wiederherstellung der Verbindung mit dem Service unternommen wird.
Nächster Heartbeat-Versuch	Nach einem fehlgeschlagenen Versuch zur erneuten Herstellung einer Verbindung zu einem Aggregatservice wird die Anzahl der Sekunden angegeben, die ein Broker oder Concentrator warten muss, bevor ein weiterer Versuch zur Wiederherstellung der Verbindung mit dem Service unternommen wird. Die Änderung wird sofort wirksam.
Keine Heartbeat-Antwort	Wenn die Verbindung mit einem nicht reagierenden Service nicht wiederhergestellt werden kann, wird die Anzahl der Sekunden angegeben, die der Broker oder Concentrator warten muss, bevor er den nicht reagierenden Service offline setzt. Die Änderung wird sofort wirksam.

Klicken Sie beim Bearbeiten von Parametern in der Registerkarte Allgemein auf **Anwenden**, um die Änderungen zu speichern.

Ansicht „Services-System“ - Broker oder Concentrator

In der Ansicht „Services-System“ werden Informationen angezeigt, die für Broker und Concentrators spezifisch sind.

Die in dieser Ansicht angezeigten Informationen sind für alle Core-Servicetypen gleich, einige Optionen in der Symbolleiste sind jedoch nur für Broker und Concentrators relevant.

Was möchten Sie tun?

Rolle	Ziel	Siehe
Administrator	Starten und Beenden Sie die Aggregation Einen Aggregatservice hinzufügen, bearbeiten, löschen und umschalten	Ansicht „Services-System“ - Broker oder Concentrator
Administrator	Systemkonfiguration verwalten	Ansicht „Services-System“ - Broker oder Concentrator

Verwandte Themen

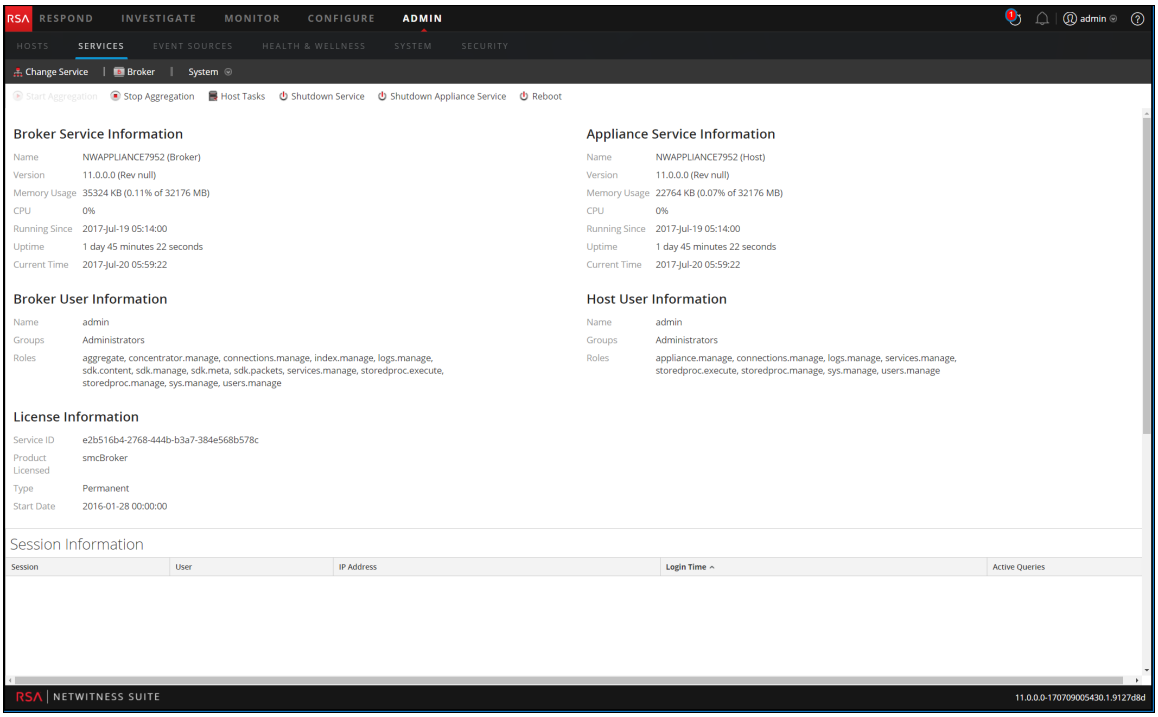
- Grundlagen zu Broker und Concentrator
- Broker- und Concentrator-Konfiguration

Ansicht „Services-System“

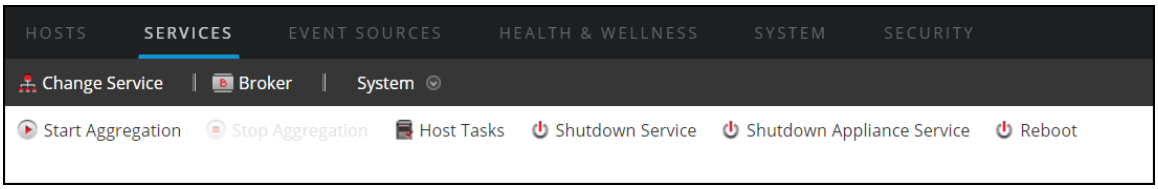
Sie können auf diese Ansicht zugreifen, indem Sie wie folgt vorgehen:

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Concentrator oder Broker aus und wählen Sie dann  **> Ansicht > System** aus.

   Die Ansicht „System“ für den ausgewählten Concentrator oder Broker wird angezeigt.



In der folgenden Abbildung ist ein Beispiel der Symbolleiste für einen Broker oder Concentrator gezeigt.



Die Optionen Hostaufgaben, Service herunterfahren, Appliance-Service herunterfahren (oder Appliance herunterfahren) und Neustart sind für alle Services verfügbar und werden unter **Ansicht Services-System** im *Leitfaden für die ersten Schritte mit Hosts und Services* beschrieben.

In dieser Tabelle werden die Symbolleistenoptionen beschrieben, die nur für einen a Concentrator oder Broker gelten. Beide Schaltflächen sind erst verfügbar, wenn Aggregatorservices konfiguriert wurden und Daten verarbeiten.

Aktion	Beschreibung
Aggregation starten	Startet die Aggregation von Daten, die auf einem Concentrator oder Decoder verarbeitet werden, der als Aggregationsservice für den ausgewählten Broker oder Concentrator konfiguriert wurde. Die Schaltfläche Aggregation starten ist nur verfügbar, wenn Aggregatorservices konfiguriert wurden und Daten verarbeiten.

Aktion	Beschreibung
Aggregation beenden	Beendet die Aggregation von Daten, die auf einem Concentrator oder Decoder verarbeitet werden, der als Aggregationsservice für den ausgewählten Broker oder Concentrator konfiguriert wurde. Die Schaltfläche Aggregation beenden ist nur verfügbar, wenn die Aggregation ausgeführt wird.