



Konfigurationsleitfaden für Broker und Concentrator

für Version 11.0

Copyright © 1994-2017 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

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

5
6
9
9
0
2
5
5
7
8
0
1
1
2
4
5
5
6
6
7
1
5
5
5
5

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".

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE ADMIN				ŏΩI	® admin ⊗ ? ?
HOSTS SERVICES EVENT SOUR						
Groups	Services					
+ - 🗵 O	+ 🛛 🗕 🗹 🐺 Licenses 🕅				· Filter	×
Name	Name	Licensed	Host	Туре	Version	Actions
🕀 A I	Admin Server	8	NWAPPLIANCE9	Admin Server	11.0.0.0	^ ا
	Archiver	8	NWAPPLIANCE25988	Archiver	11.0.0.0-0	۵ 🛛
	Broker	8	NWAPPLIANCE2943	Broker	11.0.0.0-0	۰ د
	Broker	8	NWAPPLIANCE9	Broker	11.0.0.0-0	۰ د
	Broker	8	NWAPPLIANCE7952	Broker	11.0.0.0-0	۰ د
	Concentrator	0	NWAPPLIANCE22655	Concentrator	11.0.0.0-0	۰ و
	Config Server	8	NWAPPLIANCE9	Config Server	11.0.0.0	⇔ ⊙
	Contexthub Server	8	NWAPPLIANCE10604	Contexthub Server	11.0.0.0	⇔ ⊙
	Decoder	8	NWAPPLIANCE23912	Decoder	11.0.0.0-0	\$ ©
	 Event Stream Analysis 	8	NWAPPLIANCE10604	Event Stream Analysis	11.0.0.0.401-1	\$ ©
	 Event Stream Analytics Server 	8	NWAPPLIANCE10604	Entity Behavior Analytics	11.0.0.0	⇔ ⊙
	 Investigate Server 	0	NWAPPLIANCE9	Investigate Server	11.0.0.0	۰ د
	Log Collector	8	NWAPPLIANCE21301	Log Collector	11.0.0.0-14515.1.442f3b9	\$ \odot
	Log Collector	8	NWAPPLIANCE11639	Log Collector	11.0.0.0-14515.1.442/3b9	⇔ ⊙
	Log Decoder	8	NWAPPLIANCE11639	Log Decoder	11.0.0.0-0	⇔ ⊙
	Malware Analytics	8	NWAPPLIANCE2943	Malware Analysis	11.0.0.0.8254-1	⇔ ⊙
	Orchestration Server	8	NWAPPLIANCE9	Orchestration Server	11.0.0.0	⇔ ⊙
	Reporting Engine	8	NWAPPLIANCE9	Reporting Engine	11.0.0.0-5639.1.bcf66dd	⇔ ⊙
	Respond Server	8	NWAPPLIANCE9	Respond Server	11.0.0.0	⇔ ⊙
	Security Server	8	NWAPPLIANCE9	Security Server	11.0.0.0	⇔ ⊙
	Warehouse Connector	0	NWAPPLIANCE11639	Warehouse Connector	11.0.0.0-1940.1	. ♦
	<pre><< < Page 1 of 1 > >> C</pre>				Displa	aying 1 - 23 of 23
RSA NETWITNESS SUITE					11.0.0.0-1707	09005430.1.9127d8d

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.

HOSTS SERVICES EVENT SOURCES HEALTH & WELLNESS SYSTEM SECURITY								
te Change Service ■ Broker Config ⊙								
General Files Appliance Service Configuration								
Aggrogate Septises	<u> </u>						Aggregation Configuration	
Aggregate services							Aggregation Configuration	
🕂 🗕 🔅 🍅 Toggle Service 🕞 Start Aggr	regation 🛛 🛞 Stop /						Name	Config Value
Address	Port Ri	ate	Max	Behind	Collection	Status	∃ 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
System Configuration								
Name		Config Val	ue					
Compression		0						
Port		50003						
SSL FIPS Mode		\checkmark						
SSL Port		56003						
Stat Update Interval		1000						
Threads		20						
					Apply			

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.
- Wählen Sie in der Ansicht Services einen Broker oder Concentrator aus und wählen Sie in der Spalte "Aktionen" Services > 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 <u>Schritt 1. Überprüfen</u> <u>der Servicesystemkonfiguration</u>
Schritt 2: Konfigurieren von Parametern	Konfigurieren Sie Parameter zur Steuerung des gesamten Aggregationsprozesses, wie beschrieben in <u>Schritt 2. Konfigurieren des Aggregationsprozesses</u>

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

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.
- Wählen Sie in der Ansicht Services einen Broker oder Concentrator aus und wählen Sie in der Spalte "Aktionen" Salte > 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.
- 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.

RSA RESPOND INVESTIGATE MONITOR	CONFIGURE ADMIN					Ö _ Û @ admin ⊚ _ ?)
HOSTS SERVICES EVENT SOURCES HEA						
A Change Service Broker Config ©						
General Files Appliance Service Configuration						
					Aggregation Configuration	
Aggregate services					Aggregation Configuration	
+ - 🌣 🕲 Toggle Service 💽 Start Aggregation 💿					Name	Config Value
Address Port	Rate Max	Behind	Collection	Status	Aggregation Settings	
					Aggregate House	
					Aggregate Interval	60000
					Aggregate Max Serriopr	2500000
					Service Heartheat	2300000
					Heartbeat Error Restart	300
					Heartbeat Next Attempt	60
					Heartbeat No Response	180
System Configuration						
Name	Config Value					
Compression	0					
Port	50003					
SSL FIPS Mode	\checkmark					
SSL Port	56003					
Stat Update Interval	1000					
Threads	20					
			Apply			

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

Aggregation Configuration						
Name	Config Value					
□ Aggregation Settings						
Aggregate Autostart						
Aggregate Hours	0					
Aggregate Interval	60000					
Aggregate Max Sessions	2500000					
∃ Service Heartbeat						
Heartbeat Error Restart	300					
Heartbeat Next Attempt	60					
Heartbeat No Response	180					

- 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.
- 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 <u>Schritt 4. (Optional) Konfigurieren der Gruppenaggregation</u>.

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.
- Wählen Sie in der Ansicht ADMIN Services einen Broker oder Concentrator aus und wählen Sie Services > Ansicht > Konfiguration

STATUES EVENT SOURCES INTER A DUILLANSES STATUE A DUILLANSES Aggregation Configuration Aggregates Cenvices Image: Statue Aggregation Image: Statue Aggregation Statue Aggregation Configuration Aggregation Statue Aggregation Statue <th>RSA RESPOND</th> <th>INVESTIGATE</th> <th>MONITOR</th> <th>CONFIG</th> <th>URE ADMIN</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>ġΩI</th> <th>()) admin ⊚</th> <th>0</th>	RSA RESPOND	INVESTIGATE	MONITOR	CONFIG	URE ADMIN						ġΩI	()) admin ⊚	0
• Configuration Configuration Aggregate Services • Start Aggregation • Origonal • Start Aggregation • Origonal • Start Aggregation • Origonal • Nate • Nate • Origonal • Nate • Nate • Nate • Origonal • Nate • Nate • Nate • Nate • Origonal • Origonal • Nate • Nate • Nate • Origonal • Origonal • Nate • Nate • Origonal • Origonal System Configuration Nate Origonal Origonal Origonal Origonal System Configuration Origonal Origonal Origonal Origonal St. Nate Origonal	HOSTS SERVICE												
Conversion System Configuration Name Startes Name Configuration Name	A Change Service	🔤 Broker 🕴 Confi	g⊚										
Aggregate Services Aggregate Service Start Aggregation Stop Aggregation Vot Not Beind Collectorn Starts Address Vot Not Collectorn Starts Address Vot Not Collectorn Starts Aggregate Association Collectorn Starts Collectorn Aggregate Kanceloue Collectorn Collectorn Aggregate Kanceloue Aggregate Kanceloue Collectorn Collectorn Aggregate Kanceloue Aggregate Kanceloue Collectorn Collectorn Aggregate Kanceloue System Configuration Congreated Collectorn Collectorn Name Congregation Collectorn Collectorn System Configuration Congregation Collectorn Collectorn Name Congregation Congregation Collectorn System Configuration Congregation Collectorn Collectorn Name Congregation Collectorn Collectorn System Configuration Congregation Collectorn Name Congregation Collectorn Collectorn System Configuration Collectorn Collectorn Name Congregation Collectorn System Configuration Collectorn Collectorn System Configuration Collectorn Collectorn System Configuration Collectorn Collectorn System Configuration Collectorn Collectorn System Conf	General Files	Appliance Service	Configuration										
Address Not Start Aggregation Start Aggregation Address Not Rate Ordecosin Starts Address Not Rate Collecosin Starts Aggregation Collecosin Starts Aggregation 0 Aggregation Collecosin Starts Aggregation 0 Aggregation Collecosin Starts Starts Starts System Configuration Starts Starts Starts Name Configuration Configuration Starts Starts System Configuration Starts Starts Starts Starts Starts Starts Starts Star	Aggregate Servi	ces							Aggregation Configuration				
Address Not Mate Max Related Collection Statistic Aggregate Advisant	+ - 😄 🕲 Toggle	e Service 🕞 Start /	Aggregation	Stop Aggregation					Name	Config Value			
Name	Address		Port	Pate	May	Behind	Collection	Status	G Aggregation Settings				
Aggregate Hours 0000 Aggregate Hours 0000 Aggregate MacSestions 250000 Bernheit Foreit 00 Hernheit Foreit Kteringt 00 Hernheit Nork Attempt 00 Bartheit NorReparts 00 System Configuration 0 Name Centy Male Compression 0 Start Johann Martheit NorReparts Start Stafe Martheit NorReparts Start Stafe 0 Port 50003 Start Stafe Martheit NorReparts Start Stafe Martheit NorReparts Start Stafe Martheit NorReparts	- 1001055								Aggregate Autostart				
Aggregate interval 0000 Bargergate interval 0000 Barches Harof, Kannya 00 Heartheat Iron Restant 00 Heartheat Hori, Altomya 00 Starter Hori, Starter Hori, Altomya 00 Starter Hori, Start									Aggregate Hours	0			
Agregat May Sensions 200000 Intertheat Error Retart 30 Heartheat Keit Attempt 0 Heartheat Keit Attempt 0 Heartheat Keit Attempt 0 Reartheat Keit Attempt 0 System Configuration Intertheat No Reporce Sin Point 5003 Sin Profile 5003 Sin Rode 5003 Sin Rofe 30									Aggregate Interval	60000			
System Configuration Configuration Number Configura									Aggregate Max Sessions	25000000			
Hearings from Restart 300 Hearing from Restart 60 Hearing from Restart 60 Hearing from Restart 10 System Configuration Name Compression 0 Star Part 5003 Star Part 5003 Star Update Interval 100 Threads 20									Service Heartbeat				
Heartbeart Not Attempt 0 Heartbeart Not Response 180 System Configuration Compression 0 Port 5003 SSL PR5 Mode 5003 Start Part Notes 5004 Start Part No									Heartbeat Error Restart	300			
Heartback No Response 180 System Configuration Congression 0 Congression 0 0 Part 5003 0 Star Port Social Signer Social 0 Treeds 20 0 0									Heartbeat Next Attempt	60			
System Configuration Name Config Value Compresion 0 Pot 5003 SSL PPS Mode 9 SSL Update Interval 50003 Threads 20									Heartbeat No Response	180			
Name Configuation Compression 0 Port 50003 SSL Port 50003 SSL Port 50003 Stat Update Interval 1000 Threads 20	System Configu	ration											
Compension 0 Port 5003 SSI, PSP Mode Pf SSI, PSP Mode 5603 SSI, Update Interval 1000 Threads 20	Name			Co	onfig Value								
Trial 2003 SS, IPS Mode M SS, Port 5003 Sat Update Interval 1000 Threads 20	Compression			50	1003								
Sa Nort 5603 Sa Nort 1000 Threads 20	SSL FIPS Mode				/.								
Sac Update Interval 000 Threads 20	SSL Port			54	5003								
Threads 20	Stat Update Interval			10	00								
	Threads			20)								
							Annki						

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.

Address	Available Services			× on Status
	🗆 💋 Name 🔿	Address	Туре	
	🗌 🥖 Archiver	10.31.125.242	Archiver	
	🗌 🕖 Broker	10.31.125.243	Broker	
	🗌 💋 Broker	10.31.125.240	Broker	
	🗌 🥖 Concentrator	10.31.125.244	Concentrator	
	🗆 🥖 Decoder	10.31.125.245	Decoder	
	🗆 🥖 Log Decoder	10.31.125.246	Log Decoder	
	🗆 💋 Workbench	10.31.125.242	Workbench	
System Cor	nfi			
Name				
Compression				
Port				
SSL FIPS Mode	-			
SSL Port	-			
Stat Update Interval				
Threads	1			

- 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.

Add Service Con	centrator						
Please provide administrator credentials for the service:							
Username	admin						
Password	••••••						
Please configure th SSL 🕥	e SSL settings for this service	:					
Port Number	56005						
	Cancel	ОК					

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 —.

A٤	Aggregate Services								
+	🕂 든 🔅 谢 Toggle Service 🕟 Start Aggregation 💿 Stop Aggregation								
	Address	Port	Rate	Max	Behind	Collection	Status		
	10.31.125.240	50003							
	10.31.125.244	56005							

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 ^{III}. 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.
- 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.

Edit	Aggregate Service		×						
	Group Aggregation								
M	eta Filter Meta Include								
Se	earch	×							
	Meta ^								
\mathbf{Z}	OS	A							
\mathbf{V}	access.point								
	action								
	ad.computer.dst								
	ad.computer.src								
	ad.domain.dst								
	ad.domain.src								
	ad.username.dst								
	ad.username.src	-							
Fi	ter								
	Reset	Cancel	Save						

- Zum Aufstellen einer Regel f
 ür 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 ^O 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 <u>Servicekonfigurationsansicht</u> 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.
- Wählen Sie in der Ansicht ADMIN > Services einen Broker oder einen Concentrator aus und wählen Sie > Ansicht > System aus.

<mark>RS∧</mark> RESPO	ND INVESTIGA	TE MONITOR	CONFIGURE	ADMIN					🤨 🔔 (0) admin ⊗ (?)
HOSTS									
🙏 Change Serv	vice 📧 Broker	System ⊚							
Start Aggreg	gation 🛛 🖲 Stop Aggregati	on 🛛 🗮 Host Tasks 🖞 S	hutdown Service	Shutdown Appliance	Service 😃 F	Reboot			
Broker Se	rvice Information						Appliance	Service Information	
Name	NWAPPLIANCE2943 (Bro	iker)					Name	NWAPPLIANCE2943 (Host)	
Version	11.0.0.0 (Rev null)						Version	11.0.0.0 (Rev null)	
Memory Usage	26564 KB (0.08% of 3217	76 MB)					Memory Usage	23440 KB (0.07% of 32176 MB)	
CPU	0%						CPU	0%	
Running Since	2017-Jul-19 05:13:52						Running Since	2017-Jul-19 05:13:52	
Uptime	5 hours 57 minutes 14 s	econds					Uptime	5 hours 57 minutes 14 seconds	
Current Time	2017-Jul-19 11:11:06						Current Time	2017-jul-19 11:11:06	
Broker Us	er Information						Host User	Information	
Name	admin						Name	admin	
Groups	Administrators						Groups	Administrators	
Roles	aggregate, concentrator sdk.manage, sdk.meta, s sys.manage, users.mana	.manage, connections.man. idk.packets, services.manag ige	age, index.manage, je, storedproc.execi	logs.manage, sdk.conte ute, storedproc.manage	ent,		Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	
License In	formation								
Service ID	95b6383b-76a8-4716-a3	a7-20b82b99ed14							
Product Licensed	smcBroker								
Туре	Permanent								
Start Date	2016-01-28 00:00:00								
Session In	formation								
Carrier	lioimadon	User		D Address				tank Time -	- Cruster
50550011		user		F AUULESS				Logar time ~ Activ	e querres
<.									•
RSA NET	WITNESS SUITE								11.0.0.0-170709005430.1.9127d8d

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.

HOSTS	SERVICES						
🛔 Change Ser	vice 甅 Brok	er Sys	tem 👳				
● Start Aggre	gation 💿 Stop /	Aggregation	📕 Host Tasks	😃 Shutdown Service	也 Shutdown App	liance Service	😃 Reboot

Starten und Beenden der Aggregation in der Ansicht "Service-

Konfiguration"

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

Die Ansicht "Services-Konfiguration", die den Abschnitt "Services aggregieren" enthält, wird angezeigt.

RSA RESPOND INVESTIGATE MONITOR CONFIG	GURE ADMIN		🎐 🇘 🔯 admin ⊚ 🕐
HOSTS SERVICES EVENT SOURCES HEALTH & WELLN			
		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
System Configuration			
Name	Config Value		
Compression	0		
Port	50003		
SSL FIPS Mode	R		
SSL Port	56003		
Stat Update Interval	1000		
Threads	20		
	Apply		

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

auf **Start Aggregation** 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.

HOSTS SERVICES EV	ENT SOURCES	HEALTH & V	VELLNESS S	YSTEM SEC	URITY		
🚠 Change Service 🛛 🗈 Broker	Config 😔						
General Files Applian	nce Service Configur	ration					
Aggregate Services							
+ - 🔅 🝅 Toggle Service 💽 Start Aggregation							
Address	P	ort	Rate	Max	Behind	Collection	Status

4. Klicken Sie zum Beenden der Aggregation auf **Stop Aggregation** 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.

🚠 Change Service 🔟 Broker Config 🐵								
General Files Appliance Service Conf	iguration							
Aggregate Services								
🕂 🗕 🌞 🍎 Toggle Service 🕟 Start Aggre	+ - 🔅 🖄 Toggle Service 🕑 Start Aggregation 💿 Stop Aggregation							
Address	Port	Rate	Max	Behind	Collection	Status		

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/Concentrator
- Ansicht Services-System Broker

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	Abschnitt "Services aggregieren"
	Einen Aggregatservice hinzufügen, bearbeiten, löschen und umschalten	
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.

HOSTS SERVICES EVENT SOURCES HEALTH & WELLNESS SYSTEM SECURITY		
🚣 Change Service 🔤 Concentrator Config 🐵		
General Files Data Retention Scheduler Correlation Rules Appliance Service Configuration		
Aggregate Services	Aggregation Configuration	
- C A full famile - M Tente famile - Oper Association - Oper Association	Name	Config Value
T - C T CUIL Service @ 1020/e service @ said Aggregation @ solp Aggregation	Aggregation Settings	
Address Port Rate Max Behind Meta Filter Meta Include Grouped Statu	Aggregate Autostart	×
	Aggregate Hours	0
	Aggregate Interval	10
	Aggregate Max Sessions	10000
	Service Heartbeat	
	Heartbeat Error Restart	300
	Heartbeat Next Attempt	60
	Heartbeat No Response	180
System Configuration		
Name Config Value		
Compression 0		
Port 50005		
SSL FIPS Mode		
SSL Port 56005		
Stat Update Interval 1000		
Threads 20		
Арру		
RSA NETWITNESS SUITE		11.0.0.0-170709005430.1.9127d8d

Es folgt ein Beispiel der Registerkarte "Allgemein" für einen Broker.

RSA RESPOND INVESTIGATE MONI		IRE ADMIN						🖲 💭 🔍 🔍 🔍
HOSTS SERVICES EVENT SOURCES								
A Change Service B Broker Config @								
Constall Film Appliance Configurat	i							
General Piles Appliance Service Computat	lion							
Aggregate Services							Aggregation Configuration	
🕂 🗕 🔅 🍯 Toggle Service 🛞 Start Aggregation	Stop Aggregation						Name	Config Value
Address	Port	Rate	Max	Behind	Collection	Status	■ 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
System Configuration								
Name		Config Value						
Compression		0						
Port		50003						
SSL FIPS Mode		1						
SSL Port		56003						
Stat Update Interval		1000						
Threads		20						
					Apply			
RSA NETWITNESS SUITE								11.0.0.0-170709005430.1.9127d8d

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.

General	Files	Data Retenti	on Schedu	ler Co	orrelation Rule	es Appliar	ce Service Configuration			
Aggrega	Aggregate Services									
+ - 🗷	🔅 Edit Service	💧 谢 Toggle	e Service	🕞 💽 Sta		🖲 Stop A	ggregation			
Address		Port	Rate	Мах	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
10.31.12	5.245	50004	0	0	0				no	consuming
10.31.12	5.246	50002	0	0	0				no	consuming

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.					
	Startet die Datenaggregation vom Onlineservice in der					
Start Aggregation	Liste durch die Verwendung der für den Service					
	definierten Regeln, wenn Aggregation gestoppt oder					
	nicht gestartet wurde.					
	Stoppt die Aggregation des Broker oder Concentrator,					
- oroh voglegarion	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.

System Configuration		
Name	Config Value	
Compression	0	
Port	50005	
SSL FIPS Mode		
SSL Port	56005	
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.		
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.

RolleZielSieheAdministratorStarten und Beenden Sie die
Aggregation
Einen Aggregatservice hinzufügen,
bearbeiten, löschen und umschaltenAnsicht "Services-System" -
Broker oder ConcentratorAdministratorSystemkonfiguration verwaltenAnsicht "Services-System" -
Broker oder Concentrator

Was möchten Sie tun?

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 ^{Sie} ≥ Ansicht > System aus.

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

RSA RESPO	ND INVESTI	GATE MONITOR CON	FIGURE ADMIN			🎐 🔔 இ admin ⊚ 👩
HOSTS						
Å Change Sen	vice 📧 Broker	System ⊚				
🕞 Start Aggreg	gation 💿 Stop Aggre	egation 📲 Host Tasks 🖞 Shutdown	service 🖞 Shutdown Appliance Service 🖞 Reb	oot		
Duchan				A	Consider to former them	A
Broker Se	rvice informati	on		Appliance	Service Information	
Name	NWAPPLIANCE7952	(Broker)		Name	NWAPPLIANCE7952 (Host)	
Version	11.0.0.0 (Rev null)			Version	11.0.0.0 (Rev null)	
Memory Usage	35324 KB (0.11% of 3	32176 MB)		Memory Usage	22764 KB (0.07% of 32176 MB)	
CPU	0%			CPU	0%	
Running Since	2017-Jul-19 05:14:00			Running Since	2017-Jul-19 05:14:00	
Uptime	1 day 45 minutes 22	seconds		Uptime	1 day 45 minutes 22 seconds	
Current Time	2017-Jul-20 05:59:22			Current Time	2017-Jul-20 05:59:22	
Broker Us	er Information			Host User	Information	
Name	admin			Name	admin	
Groups	Administrators			Groups	Administrators	
Roles aggregate concentrator manage, connections manage, index manage, logs manage, subcontent, sids manage, sube mata, sub-packets, services manage, storedproc.execute, storedproc.manage, syx.manage, users.manage		Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage			
License In	formation					
Service ID	e2b516b4-2768-444	b-b3a7-384e568b578c				
Product Licensed	smcBroker					
Туре	Permanent					
Start Date	2016-01-28 00:00:00					
Session Ir	nformation					
Session		User	IP Address		Login Time ~	Active Queries
4						-
RSA NET	WITNESS SUITE					11.0.0.0-170709005430.1.9127d8d

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

HOSTS SERV	VICES EVENT SO					
🚠 Change Service	🗈 Broker Sys	tem 🍥				
• Start Aggregation	Stop Aggregation	层 Host Tasks	😃 Shutdown Service	😃 Shutdown Appli	ance Service	😃 Reboot

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