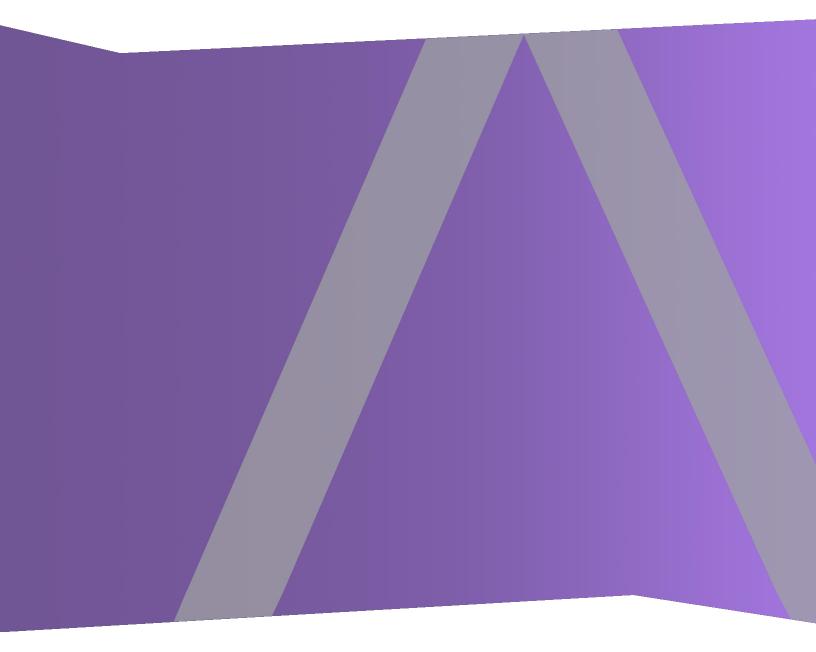


Broker and Concentrator Configuration Guide

for Version 11.2



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

September 2018

Contents

Broker and Concentrator Basics	4
Overview of Broker and Concentrator	6
Broker and Concentrator Configuration	7
Basic Configuration Checklist	7
Step 1. Verify Service System Configuration	8
Step 2. Configure the Aggregation Process	10
Step 3. Configure Aggregate Services	12
Toggle a Service	
Step 4. (Optional) Configuring Group Aggregation	16
RSA Group Aggregation Deployment Recommendations	
Configure Group Aggregation	
Step 5. Start and Stop Aggregation	
Broker and Concentrator Configuration References	
Services Config View - Broker or Concentrator General Tab	
What do you want to do?	
Related Topics	
General tab	
Aggregate Services Section	
Services System View - Broker or Concentrator	
What do you want to do?	
Related Topics	
Services System View	

Broker and Concentrator Basics

Concentrators and Brokers aggregate data captured or aggregated by other services unlike Decoders, which capture data.

NetWitness Platform supports the following Broker and Concentrator services:

- Brokers aggregate data across entire infrastructure from configured Concentrators. You can have multiple concentrators aggregating into one broker. You can also have multiple brokers aggregating into a single broker.
- Concentrators aggregates and analyzes data across multiple capture locations from decoders, indexes and directs queries.

You can configure various Brokers and Concentrators together under a Broker. Brokers are able to pull in data quickly from the Concentrators because they acquire index information only. This configuration is done using the NetWitness Platform user interface. Most of the configuration is performed in the Administration Services view (ADMIN > Services).

RSA RESPOND II	NVESTIGA	TE N	IONITOR	CONFIGURE	ADMIN				Ō	
Hosts Services	Event S	ources	Health &	Wellness	System	Security				
Groups		Servi	ces							
+ - 🛛 O		- 🗷							Filter	×
Name			Name			Licensed	Host	Туре	Version	Actions
🗄 All	20		adminserver - A	dmin Server		0	adminserver	Admin Server	11.2.0.0	•
		1	adminserver - E	Broker		S	adminserver	Broker	11.2.0.0	
			adminserver - Co	onfig Server		ø	adminserver	Config Server	11.2.0.0	♦ ⊙
			adminserver - Co	ontent Server		ø	adminserver	Content Server	11.2.0.0	♦ ⊙
			adminserver - In	tegration Server		ø	adminserver	Integration Server	11.2.0.0	♦ ⊙
			adminserver - In	vestigate Server		ø	adminserver	Investigate Server	11.2.0.0	♦ ⊙
			adminserver - O	rchestration Serve	r	ø	adminserver	Orchestration Server	11.2.0.0	♦ ⊙
			adminserver - Re	eporting Engine		ø	adminserver	Reporting Engine	11.2.0.0	♦ ⊙
			adminserver - Re	espond Server		ø	adminserver	Respond Server	11.2.0.0	♦ ⊙
			adminserver - Se	ecurity Server		ø	adminserver	Security Server	11.2.0.0	♦ ⊙
			adminserver - So	ource Server		ø	adminserver	Source Server	11.2.0.0	♦ ⊙
			endpointloghybr	rid - Concentrator		ø	endpointloghybrid	Concentrator	11.2.0.0	♦ ⊙
			endpointloghybr	rid - Endpoint Serv	er	ø	endpointloghybrid	Endpoint Server	11.2.0.0	♦ ⊙
			endpointloghybr	rid - Log Collector		ø	endpointloghybrid	Log Collector	11.2.0.0	♦ ⊙
			endpointloghybr	rid - Log Decoder		ø	endpointloghybrid	Log Decoder	11.2.0.0	♦ ⊙
			esaprimary - Cor	ntexthub Server		ø	esaprimary	Contexthub Server	11.2.0.0	♦ ⊙
		4								► F
		« ‹	Page 1	of1 🔪 渊	l C					Displaying 1 - 20 of 20
	ORM									11.2.0

You can also configure the aggregate services and perform the whole aggregation process using the Services view. This helps setup aggregation autostart, timing and performance parameters, maximum number of open meta and session files. In addition to this, you can also time the attempts to restart, reconnect, or take a non-responsive aggregate service offline. Configuring Aggregate services includes managing Concentrators and Decoders as aggregate services. You can also limit the data being consumed from an aggregate service using meta fields and filters. The aggregation tasks are performed in the General tab of Administration Services view (ADMIN > Services).

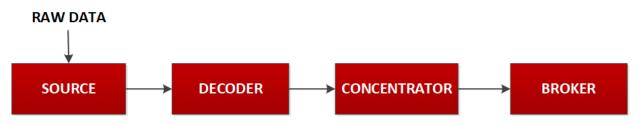
Overview of Broker and Concentrator

Brokers and Concentrators work in conjunction with Decoders and Log Decoders in the NetWitness Platform network. Unlike the two types of Decoders, which capture packets and logs, Concentrators and Brokers aggregate the data captured or aggregated by other services. Brokers aggregate data from configured Concentrators; Concentrators aggregate data from Decoders. A complete overview of the NetWitness Platform is provided in the *NetWitness Platform Getting Started Guide*.

Note: Go to the Master Table of Contents in RSA Link to find and view referenced documents.

As raw data is entered in the system from the source for analysis, it has to be collected and parsed. This raw data is collected, parsed, and stored using a Decoder. The packet data is then indexed, stored, and parsed by the Concentrator. Parsed packet data is also provided as an endpoint for queries. Eventually, the Broker routes queries across multiple Decoder and Concentrator appliances. Here is how information flows to a Concentrator and Broker.

In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance.

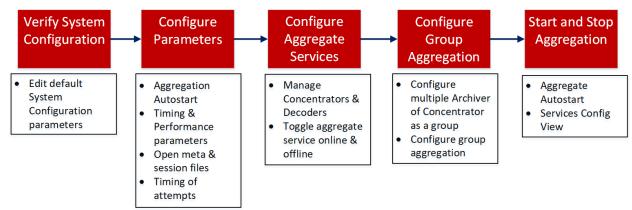


- Concentrator: is required for any large environment to store the Meta data that is generated by the parsers and feeds being triggered by packets and logs ingested into the decoders.
- Broker: The Broker service is similar to the Concentrator service except that it indexes the collected information. It performs virtual mapping of indices on all connected concentrators. Due to the less internal processing performed, the response time is fast. To allow investigation, multiple brokers and/or concentrators report data into a broker.

Broker and Concentrator Configuration

Setting up a Broker or Concentrator involves configuring the basic system parameters, the aggregate services, and the aggregation process between a Broker or Concentrator and the aggregate services.

These are the required configuration steps for a new Broker or Concentrator, and also for changing the configuration of an existing Broker. Perform the steps in the section in the sequence they are given.



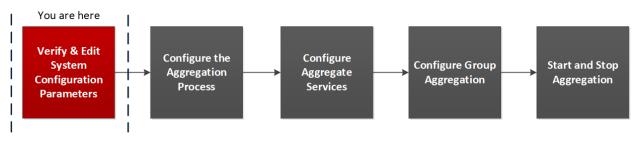
Basic Configuration Checklist

The following checklist provides the sequence for tasks that are required to configure a Broker or Concentrator that has been added to NetWitness Platform in accordance with the *Hosts and Services Guide*.

Configuration Step	Description
Step 1 - Verify System Configuration	Verify system configuration default values for the host and service are appropriate as described in <u>Step 1. Verify Service System Configuration</u>
Step 2 - Configure Parameters	Configure parameters that govern the overall aggregation process as described in <u>Step 2. Configure the Aggregation Process</u>
Step 3 - Configure Aggregate Services	Configure aggregate services as described in <u>Step 3. Configure Aggregate</u> <u>Services</u>
Step 4 - Configure Group Aggregation	(Optional) Configure group aggregation as described in <u>Step 4. (Optional)</u> <u>Configuring Group Aggregation</u>
Step 5 - Start and Stop Aggregation	Start and stop aggregation as described in Step 5. Start and Stop Aggregation

Step 1. Verify Service System Configuration

When a service is first added to NetWitness Platform, default values for the system configuration parameters are in effect. You can edit these values to tune performance.



In most cases, the default values for compression, statistics update interval, and number of threads in the thread pool are set at a good point for optimal system performance.

To edit system configuration parameters for a Broker or Concentrator:

- 1. Go to **ADMIN** > Services.
- 2. In the Services view, select a Broker or Concentrator, and in the Actions column, select [♀] ≥ View > Config.

The Services Config view for the selected service is displayed.

Hosts Services Event	Sources Health & '	Wellness S	system S	ecurity					
A Change Service 🗈 adminser	ver-Broker Config ⊚								
General Files Applian	ce Service Configuration								
Aggregate Services							Aggregation Configuratio	n	
	Start Aggregation I Start Aggregation						Name	Config Value	
Address	Port	Rate	Max	Behind	Collection	Status	Aggregation Settings		
- Address	Port	Rate	IVIAX	bennu	collection	status	Aggregate Autostart		
							Aggregate Hours	0	
							Aggregate Interval	60000	
							Aggregate Max Sessions	2500000	
							∃ Service Heartbeat		
							Heartbeat Error Restart	300	
System Configuration							Heartbeat Next Attempt	60	
							Heartbeat No Response	180	
Name		Config Va	alue						
Compression		50003							
SSL FIPS Mode		50003							
SSL Pirs Mode		56003							
Stat Update Interval		1000							
Threads		20							
		20							

3. Under System Configuration, click a field that you want to edit, and type a new value.

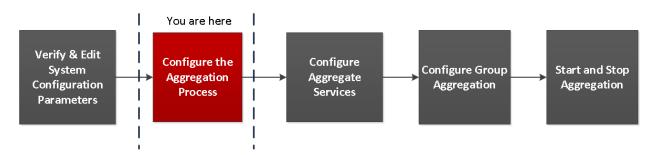
RSA RESPOND INVEST	IGATE MONITOR	CONFIGURE	ADMIN					ỗ ậ 🕼 admin ⊗ 🤇
Hosts Services Even	t Sources Health &	Wellness	System S	Security				
🏯 Change Service 🛛 📧 adminse	erver - Broker Config @							
General Files Applia	ince Service Configuration							
Aggregate Services							Aggregation Configuration	on
	Start Aggregation 📧 🖲						Name	Config Value
Address	Port	Rate	Max	Behind	Collection	Status		
- Address	Tore	hate	in the second se	benna	concetion	Status	Aggregate Autostart	
							Aggregate Hours	0
							Aggregate Interval	60000
							Aggregate Max Sessions	25000000
							∃ Service Heartbeat	
							Heartbeat Error Restart	300
System Configuration							Heartbeat Next Attempt	60
, ,							Heartbeat No Response	180
Name		Config \	ratue					
Port		50003	0					
SSL FIPS Mode		<u>5000s</u>	V					
SSL Port		56003						
Stat Update Interval		1000						
Threads		20						
		20						
					Apply			
					- 4490			

4. When finished editing, click **Apply**.

Step 2. Configure the Aggregation Process

Configuring the aggregation process for a Broker or Concentrator includes setting:

- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- Maximum number of open meta and session files
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service



To configure the aggregation process on a Broker or Concentrator:

- 1. Go to **ADMIN** > **Services**.
- 2. In the Services view, select a Broker or Concentrator, and select 🔅 🖻 > View > Config.

The Services Config view, which includes the Aggregation Configuration section, is displayed.

🛔 Change Service 🛛 📔 adminserver - Broke	r Config ⊚								
General Files Appliance Service									
Aggregate Services							Aggregation Configuratio	n	
							Name	Config Value	
+ - 🌣 🕲 Toggle Service 💽 Start.							Aggregation Settings	Coning value	
Address	Port	Rate	Max	Behind	Collection	Status	Aggregate Autostart		
							Aggregate Hours	0	
							Aggregate Interval	60000	
							Aggregate Max Sessions	25000000	
							■ Service Heartbeat		
							Heartbeat Error Restart	300	
System Configuration							Heartbeat Next Attempt	60	
							Heartbeat No Response	180	
Name		Config Va	ilue						
Compression Port		0							
SSL FIPS Mode		50003							
SSL Port		56003							
Stat Update Interval		1000							
		20							
Threads									

3. (Optional) Select Aggregate Autostart to enable automatic start of aggregation when a service is online.

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						

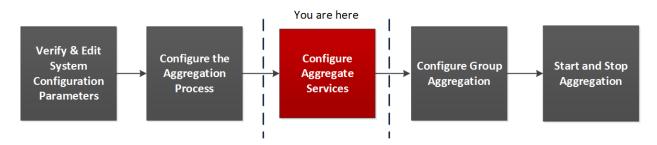
- 4. (Optional) Edit any of the aggregation settings: the hours back to begin aggregation, the milliseconds between rounds of aggregation, and maximum number of sessions per aggregation round.
- 5. (Optional) Edit any of the Service Heartbeat settings, which specify the timing of the first attempt to reconnect to a service after an error, the next attempt to reconnect, and taking the service offline after failure to reconnect.
- 6. When finished editing the settings, click **Apply**. The settings become effective immediately.

Step 3. Configure Aggregate Services

This topic introduces basic tasks related to data aggregation on Brokers and Concentrators. For information on the optional setup of group aggregation, see <u>Step 4. (Optional) Configuring Group</u> Aggregation.

Configuring the aggregate services (whose data is consumed and aggregated) includes:

- Adding, editing, and deleting Concentrators and Decoders as aggregate services
- Toggling an aggregate service online and offline



To configure aggregate services to a Broker or Concentrator:

- 1. Go to **ADMIN > Services**.
- In the ADMIN Services view, select a Broker or Concentrator, and select >View > Config. The Services Config view for the selected service is displayed.

A Change Service 💿 adminserver - Broke	er Config ⊙									
General Files Appliance Service	Configuration									
Aggregate Services							Aggregation Configuratio	Aggregation Configuration		
+ - 🌣 🍈 Toggle Service 💽 Start.	Aggregation 💿 Sh						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		
System Configuration							Heartbeat Next Attempt	60		
							Heartbeat No Response	180		
Name		Config Va	lue							
e		50003								
		50003								
Port		•								
Port SSL FIPS Mode		56002								
Port SSL FIPS Mode SSL Port		56003								
Compression Port SSL FIPS Mode SSL Port Stat Update Interval Transfit		1000								
Port SSL FIPS Mode SSL Port										

 Click + in the Aggregate Services toolbar. The Available Services dialog is displayed.

RSA RESPOND INVESTIGATE MONITOR	CONFIGURE ADMIN				
Hosts Services Event Sources Health					
🚠 Change Service 💽 adminserver - Broker Config	Available Services				
General Files Appliance Service Configuration	🗆 💋 Name ^	Address	Туре		
	🗌 💋 endpointloghybrid - Concentrator	1101110	Concentrator		
Aggregate Services	🗌 💋 endpointloghybrid - Log Decoder	1100100	Log Decoder	on	
🕂 🗕 🔅 🍎 Toggle Service 💽 Start Aggregation 🖗	🗆 💋 packethybrid - Concentrator	110110	Concentrator		Config Value
Address Port	🗌 💋 packethybrid - Decoder	1110111110	Decoder		
Address					
					0
					60000
					25000000
					300
System Configuration					60
Name					180
Compression				I	
Port				I	
SSL FIPS Mode				I	
SSL Port				I	
Stat Update Interval				I	
Threads					
			Cancel OK		
		Apply		-	
RSA NETWITNESS" PLATFORM					11.2.0.0

- 4. Select one or more services to be added and click **OK**.
- 5. Enter the Administrator username and password to authenticate adding a service.

Add Service Con	centrator	×
Please provide adr service:	ninistrator credentials for the	2
Username	admin]
Password	•••••]
Please configure th SSL 🔞	ne SSL settings for this service ☑	<u>;</u>
Port Number	56005	
	Cancel	ОК

The added services are listed in the Aggregate Services list.

6. To save the changes, click **Apply**.

To remove aggregate services from a Broker or Concentrator:

Note: This option applies only to offline services. If the aggregate service is online, you must first toggle the service offline.

- 1. In the Aggregate Services list, select one or more services.
- 2. Click in the toolbar.

A٤	Aggregate Services							
+ 🔁 🔅 🛛 🐨 Toggle Service 🔰 🕟 Start Aggregation 💿 Stop Aggregation								
	Address	Port	Rate	Max	Behind	Collection	Status	
	50003							
	10.011100.000	56005						

The service is removed from Aggregate Services list.

3. To save the change, click **Apply**.

To edit aggregate services on a Concentrator:

Note: This option applies only to offline services. If the aggregate service is online, you must first toggle the service offline. You can edit only one service at a time.

You can limit the data being consumed from an aggregate service using meta fields and filters.

- 1. Click **Change Service** to change the service to Concentrator.
- 2. In the Aggregate Services list, select one or more services.
- 3. Click \square in the toolbar. Enter the authentication information in the pop up dialog box.
 - If the service was added on a different instance of NetWitness Platform, you must add it to this instance of NetWitness Platform in order to edit. A warning dialog allows you to add the service. If you click **Yes**, the Add Service dialog is displayed.
 - If the service is online, a dialog notifies that the service must be offline and requests confirmation that you want to continue. If you click **Yes**, NetWitness Platform takes the service offline and the Edit Aggregate Service dialog is displayed.
 - If the service is offline, the Edit Aggregate Service dialog is displayed with the editable properties for an aggregate service on a Concentrator.
- 4. Click a type of metadata in the **Meta Include** tab to select the type of metadata for the Concentrator to consume from this service. Click **Save**.

Edit	Aggregate Service		×
	Group Aggregation		
Me	ta Filter Meta Include		
Se	arch	×	
	Meta ^		
\blacksquare	OS	•	
\blacksquare	access.point		
	action		
	ad.computer.dst		
	ad.computer.src		
	ad.domain.dst		
	ad.domain.src		
	ad.username.dst		
	ad.username.src	-	
Fil	er		
F	Reset	Cancel	Save

- 5. To specify a rule to filter data that the Concentrator consumes from this service, compose a rule in the **Meta Filter** tab. Click **Save**.
- 6. Click Close.

The Edit Aggregate Service dialog closes and the changes are shown in the Aggregate Services list. In this example, two meta were selected on the Meta Include tab. When you click the information icon in the Meta Include field, it shows the selections.

7. To save the changes, click **Apply**.

Toggle a Service

When data aggregation starts, Brokers and Concentrators consume data from aggregate services that are online. When first added to a Broker or Concentrator, aggregate services are offline.

To toggle a service between online and offline:

- 1. Select a service in the Aggregate Services list.
- 2. Click Toggle Service .

The status is changed.

Step 4. (Optional) Configuring Group Aggregation

You use Group Aggregation to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them. You can configure multiple Archiver services or Concentrator services to efficiently aggregate from multiple Log Decoder services to improve query performance on the data:

- Stored in the Archiver.
- Processed through the Concentrator.

RSA Group Aggregation Deployment Recommendations

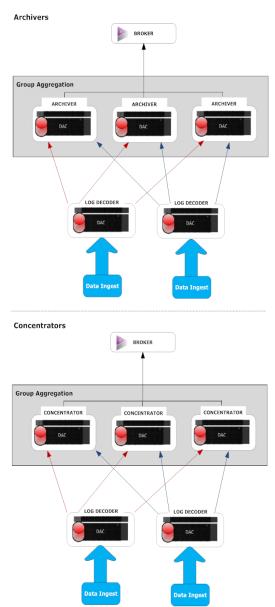
RSA recommends the following deployment for Group Aggregation:

- 1 2 Log Decoders
- 3 5 Archivers or Concentrators

Advantages of Using Group Aggregation

- Increases the speed of RSA NetWitness® Platform queries.
- Improves the performance of aggregate queries (Count and Sum) on the environment.
- Enhances investigation service performance.
- Gives you the option of storing data for a longer duration for investigation purposes.

The following diagram illustrates Group Aggregation.



You can have any number of Archivers or Concentrators grouped together and form an aggregation group. The Archiver or Concentrator services in the group divide all the aggregated session between them based on the number of sessions defined in the Aggregate Max Sessions parameter.

For example, in an aggregation group containing two Archiver services or two Concentrator services with the Aggregate Max Sessions parameter, set to 10000 the services would divide the session between themselves as illustrated in the following table.

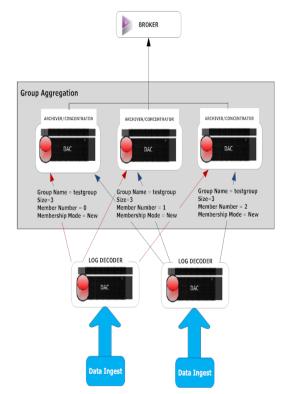
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

Configure Group Aggregation

Complete this procedure to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them.

Prerequisites

Plan the network design for group aggregation. The following figure is an example of a group aggregation setup.



Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

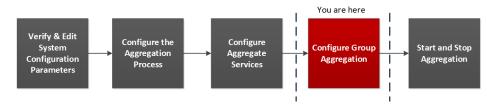
Parameter	Description
Group Name	It determines the group to which the Archiver or Concentrator belongs. You can add any number of groups aggregating data from a Log Decoder. The Group Name parameter is used by the Log Decoder to identify which Archiver or Concentrator services are working together. All Archiver or Concentrator services in the group should have the same group name.
Size	It determines the number of Archiver or Concentrator services in the aggregation group.

Parameter	Description
Member Number	It determines the position of the Archiver or Concentrator in the aggregation group. For a group of size N, member number from 0 to N-1 must be set on each of the Archiver or Concentrators services in the aggregation group. For example: If the size of the aggregation group is 2, the member number of one of the Archiver or Concentrator service should be set to 0 and the member number of the other Archiver or Concentrator should be set to 1.
Membership Mode	 There are two membership modes: New: Adding a new Archiver or Concentrator service as a member to the existing aggregation group or creating an aggregation group. The Archiver or Concentrator service does not aggregate any existing sessions from the service as other members of the group would have already aggregated all the sessions on the service. This Archiver or Concentrator service will only aggregate new sessions as they appear on the service.
	• Replace: Replacing an existing aggregation group member. The Archiver or Concentrator will begin aggregation from the oldest session available on the service it is aggregating from.
	it is aggregating from.

Note: Membership mode parameter has an effect only when no sessions have been aggregated from the service. After some sessions are aggregated, this parameter has no effect.

Set up Group Aggregation

This workflow shows the procedures you complete to configure group aggregation.



To set up group aggregation:

- 1. Configure multiple Archiver or Concentrator services in your environment. Make sure that you add the same Log Decoder as data source to all the services.
- 2. Perform the following on all the Archiver or Concentrator services that you want to be part of aggregation group:
 - a. Go to **ADMIN > Services**.
 - b. Select the Archiver or Concentrator service, and in the Actions column, select View > Config. The Service Config view of the Archiver or Concentrator is displayed.
 - c. In the Aggregate Services section, select Log Decoder.
 - d. Click **Toggle Service** to change the status of the Log Decoder to offline if it is online.
 - e. Click 🗹.

The Edit Aggregate Service dialog is displayed.

Edit	Aggregate Service									
	Group Aggregation									
M	eta Filter Meta Include									
Se	earch X									
	Meta ^									
	OS 🔺									
	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									

f. Click Group Aggregation

The Edit Group Aggregation dialog is displayed.

Edit Group Aggregation								
Enabled	\checkmark							
Group Name	testgroup							
Size	3	\$						
Member Number	0	\$						
Membership Mode	New	~						
	_							
Reset	Cancel	Save						

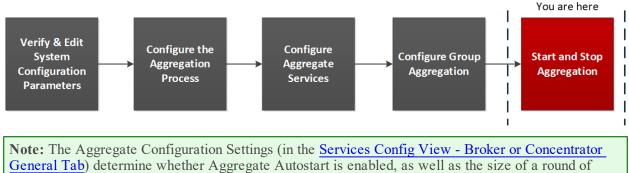
- g. Select the **Enabled** checkbox and set the following parameters:
 - In the Group Name field, type the group name.
 - In the **Size** field, select the number of Archiver or Concentrator services in the aggregation group.
 - In the **Member Number** field, select the position of the Archiver or Concentrator in the aggregation group.
 - In the Membership Mode drop-down menu, select the mode.
- h. Click Save.
- i. In the Service Config View page, click Apply.
- j. Perform **Step b** to **Step i** on all other Archiver or Concentrator services that need to be part of group aggregation.

3. In the Aggregation Configuration section, set the Aggregate Max Sessions parameter set to 10000.

RSA RESPOND INV	ESTIGATE	. мо	DNITOR	CONF	IGURE	ADMIN					9 (〕 ① admin ◎ ?
🛔 Change Service 🛛 📧 Cor	ncentrator	Confi	g 😔									
General Files Da	ata Retentio	n Schedule	er Corre	elation Rules	Appliance	Service Configuration						
Aggregate Services										Aggregation Configuration	I	
+ - Z 🌣 Edit Service	🖄 Toggle	Service	Start /		Stop Age	regation				Name	Config Value	
Address	Port	Rate	Max	Behind		Filter	Meta Include	Grouped	Status	Aggregation Settings		
10.31.125.245	50004	0	0	0	meta rieius	Flicer	wieta include	no	consuming	Aggregate Autostart	×	
10.31.125.246	50002	0	0	0				yes @	offline	Aggregate Hours	0	
	50002	÷	•	v				yes	onnic	Aggregate Interval	10	
										Aggregate Max Sessions	10000	
										∃ Service Heartbeat		
										Heartbeat Error Restart	300	
										Heartbeat Next Attempt	60	
										Heartbeat No Response	180	
System Configuratic	on				Config Va	line						
Compression					0	lide						
Port					50005							
SSL FIPS Mode					⊻							
SSL Port					56005							
Stat Update Interval					1000							
Threads					20							
							A	pply				

Step 5. Start and Stop Aggregation

When a Broker or Concentrator starts up, it automatically begins aggregating data if Aggregate Autostart is enabled. When autostart is not enabled, you can start and stop data aggregation manually.



aggregation and time between rounds.

To start and stop data aggregation in the services system view:

- 1. Go to **ADMIN** > **Services**.
- 2. In the ADMIN Services view, select a Broker or Concentrator, and select 🕸 💿 > View > System.

RSA RESPO	OND INVESTIG	ATE MONITOR CON	FIGURE ADMIN						
Hosts Se	ervices Event	Sources Health & Wel	lness System Security						
📥 Change Serv	vice 💽 adminserv	ver - Broker System 🏾							
Start Aggreg	ation 💿 Stop Aggre	gation 📕 Host Tasks 🖞 Shutd	lown Service 🖞 Shutdown Appliance Service	😃 Reboot					
Broker Se	rvice Informati	on		Appliance	Service Information				
Name	adminserver (Broker)		Name	adminserver (Host)				
Version	11.2.0.0 (Rev null)			Version	11.2.0.0 (Rev null)				
Memory Usage	14268 KB (0.04% of 3	2176 MB)		Memory Usage	9220 KB (0.03% of 32176 MB)				
CPU	5%				10%				
Running Since	2018-Jul-05 13:23:46			Running Since	ce 2018-jul-05 13:23:46				
Uptime	3 weeks 3 days 16 ho	ours 40 minutes 53 seconds		Uptime	3 weeks 3 days 16 hours 40 minutes 54 seconds				
Current Time	2018-Jul-30 06:04:39			Current Time	e 2018-Jul-30 06:04:40				
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, dok.content. sdk.manage. sdk.meta. sdk.packets. services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage			Roles	Roles appliance.manage.connections.manage.logs.manage.sen/ces.manage. storedproc.execute.storedproc.manage.sys.manage.users.manage				
Session In	formation								
Session	1	Jser	IP Address		Login Time ^	Active Queries			
2486		admin	127.0.0.1:49298		2018-Jul-06 07:16:03	0			
2660	i	admin	127.0.0.1:52184		2018-Jul-06 08:26:46	0			

3. To stop a Broker or Concentrator that is capturing data, click **Stop Aggregation** in the toolbar. The service stops aggregating data and the **Stop Aggregation** option in the toolbar is unavailable. The **Start Aggregation** option becomes active.

HOSTS	SERVICES				
🚠 Change Ser	vice 🕴 甅 Brok	xer ∥ System ⊚			
🕟 Start Aggre	gation 💽 Stop	Aggregation 📕 Host Ta	sks 🖞 Shutdown Service	😃 Shutdown Appliance Service	也 Reboot

4. If you want the service to start aggregating data again, click Start Aggregation.

You can now investigate the captured data in the Investigation module.

HOSTS	SERVICES						
🕂 Change Se	rvice 📗 🗾 Bro	ker Sys	tem Θ				
● Start Aggre	egation 🖲 Stop	Aggregation	层 Host Tasks	😃 Shutdown Servi	ce 🖞 Shutdown Ap	pliance Service	也 Reboot

To start and stop aggregation in the services config view:

- 1. Go to **ADMIN** > Services.
- In the Admin Services view, select a Broker or Concentrator, and select Services Config.
 The Services Config view, which includes the Aggregate Services section, is displayed.

	rces Health &	wenness a	system s	ecunty				
🙏 Change Service 🔰 🔟 adminserver - Br	oker Config ©							
General Files Appliance Serv	vice Configuration							
Aggregate Services							Aggregation Configuration	n
	art Aggregation 🛛 🖲 S						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
System Configuration							Heartbeat Next Attempt	60
							Heartbeat No Response	180
Name		Config Va	aiue					
Port		50003						
SSL FIPS Mode								
SSL Port		56003						
Stat Update Interval		1000						
		20						
Threads								

3. To start aggregation on the selected Broker or Concentrator, click Start Aggregation in the Aggregate Services toolbar.

When aggregation starts, the status of all online aggregate services changes to **consuming**. The Start Aggregation button is disabled and the Stop Aggregation button is enabled.

HOSTS SERVICES EVEN									
A Change Service 🖻 Broker Config \odot									
General Files Appliance Service Configuration									
Aggregate Services	Aggregate Services								
🕂 🗕 🌞 🛛 🍅 Toggle Service	🛨 🗕 🏟 🍎 Toggle Service 💽 Start Aggregation 💿 Stop Aggregation								
Address	Port	Rate	Max	Behind	Collection	Status			

4. To stop aggregation, click



When aggregation stops, the status of all consuming aggregate services changes to **online**. The Stop Aggregation button is unavailable and the Start Aggregation button is available.

A Change Service 🔤 Broker Config 🐵								
General Files Appliance Service Config	guration							
Aggregate Services	Aggregate Services							
🕂 🗕 🌞 🛛 谢 Toggle Service 🛛 🕞 Start Aggrega	ation 💿 Stop Agg	gregation						
□ Address	Port	Rate	Max	Behind	Collection	Status		

Broker and Concentrator Configuration References

You can configure Brokers and Concentrators using the NetWitness Platform user interface.

In addition to the views described here, you can view the complete service nodes in a tree form in the Services Explore view, see the "Services Explore View" topic in the *Hosts and Services Getting Started Guide*.

Related Topics

- Services Config View Broker or Concentrator General Tab
- Services System View Broker or Concentrator

Services Config View - Broker or Concentrator General Tab

The General tab for a Broker or Concentrator in the Services Config helps manage basic service configuration, configure the aggregate service, and configure the aggregation process between a Broker or Concentrator and the aggregate service.

Configuring the aggregate service (whose data is consumed and aggregated) includes:

- Adding, editing, and deleting Concentrators and Brokers as aggregate services
- Toggling an aggregate service online and offline
- Monitoring statistics for aggregate services
- Starting and stopping aggregation

Configuring the aggregation process includes setting:

- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service

What do you want to do?

Role	I want to	Refer to
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Aggregate Services Section
Administrator	Manage System Configuration	System Configuration Section

Related Topics

- Broker and Concentrator Basics
- Broker and Concentrator Configuration

General tab

This is an example of the General tab for a Concentrator.

Hosts Services	Event S	ources	Heal	lth & W	ellness	System Security						
📩 Change Service 🛛 🖻					Config ⊚							
General Files	Data Rete	ntion Sche	duler	Correlatio	on Rules Ap	pliance Service Configura	ation			И		
Aggregate Servic	es									Aggregation Configurati	on	
🕂 🗕 🗹 🌞 Edit Servic	e 🕲 Top	gle Service			egation 💿 S	top Aggregation				Name	Config Value	
Address	Port	Rate	Max	Behind	Meta Fields		Meta Include	Grouped	Status	Aggregation Settings		
-	56002	0	10	0				no	offline	Aggregate Autostart		
										Aggregate Hours	0	
										Aggregate Interval	10	
										Aggregate Max Sessions	2000	
										■ Service Heartbeat		
										Heartbeat Error Restart	300	
System Configura	ation									Heartbeat Next Attempt	60	
, 0										Heartbeat No Response	180	
Name					Config	alue						
Port					50005	0						
SSL FIPS Mode					50005							
SSL FIPS Mode					56005							
Stat Update Interval					1000							
Threads					20							
					20							
								pply				

This is an example of the General tab for a Broker.

Hosts Services Event Sources Health & Wellness System Security								
📩 Change Service 🛛 🔟 adminserver - Broke	er Config ⊙							
General Files Appliance Service	Configuration							
Aggregate Services							Aggregation Configuration	on
+ - 🌣 ΰ Toggle Service 🖲 Start.	Aggregation Stor						Name	Config Value
Address		Rate	Max	Behind	Collection	Status	G Aggregation Settings	
Address	POR	Note	WIGA	Dennia	conection	Status	Aggregate Autostart	
							Aggregate Hours	0
							Aggregate Interval	60000
							Aggregate Max Sessions	25000000
							∃ Service Heartbeat	
							Heartbeat Error Restart	300
System Configuration							Heartbeat Next Attempt	60
Name							Heartbeat No Response	180
Compression		0	Config Value					
Port		50003						
SSI EIPS Mode								
SSL Port		56003						
Stat Update Interval			1000					
	Threads							

These are the three major sections in the General tab for Brokers and Concentrators:

- Aggregate Services
- System Configuration
- Aggregation Configuration

Aggregate Services Section

The Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service. This is an example of the Aggregate Services section for a Concentrator.

General	Files	Data Retenti	on Schedul	ler Co	orrelation Rul	es Appliar	ce Service Configura	ation			
Aggregat	Aggregate Services										
+ - 🗵	😫 Edit Service	谢 Toggle	e Service	🕞 💽 Sta		n 💿 Stop A	ggregation				
Address		Port	Rate	Max	Behind	Meta Fields	Filter	Meta	Include	Grouped	Status
10.31.125	245	50004	0	0	0					no	consuming
10.31.125	246	50002	0	0	0					no	consuming

The Aggregate Services section toolbar offers these options.

Option	Description
+	Opens a dialog in which you can add a Concentrator, Decoder, or Log Decoder as an aggregate service.
-	Removes the selected aggregate service.
Z	For Concentrators only, opens a dialog to edit Meta Fields and Filter values for the Concentrator.
🔅 Edit Service	Enables you to enter the administrator credentials of the selected aggregate service so that it can communicate with the Broker or Concentrator.
● Start Aggregation	When aggregation has been stopped or has not started, starts aggregating data from the online service in the list using the rules defined for the service.
Stop Aggregation	When aggregation is in progress, stops aggregation on the Broker or Concentrator. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.
🕲 Toggle Service	Toggles the state of a service between offline and online. Only data from online service is consumed during aggregation.

The Aggregate Services section list has these columns.

Column	Description
Address	Lists the address of the service.

Column	Description
Port	Lists the port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
Rate	Lists the number of metadata objects being written to the database per second. Values are rolling average samples over a short time period (10 seconds). After capture stops, the rate is reset to 0 .
Max	Lists the maximum number of metadata objects written to the database per second since capture started. Values are rolling average samples over a short time period (10 seconds). After capture stops, Max continues to show the maximum value during capture.
Behind	Lists the number of sessions on the service that need to be aggregated.
Collection	For Brokers only, indicates the collection that was selected when the Analyst Workbench service was added to the Aggregate Services section.
Meta Fields	For Concentrators only, lists the types of metadata being consumed by the aggregate service.
Filter	For Concentrators only, a rule expression (as used in a 'where' clause) can be used to filter the results. You must add a meta key along with an operator and a value, for example ip.src !=127.0.0.1 && word exists
Meta Include	For Concentrators only, lists the number of types of meta included in the aggregate service.
Grouped	Whether or not the aggregate service is part of a group.
Status	 Lists the current status of the service: online = available to provide data for consumption by the Broker or Concentrator offline = not available to provide data for consumption by the Broker or Concentrator consuming = providing data for consumption by the Broker or Concentrator

System Configuration Section

The System Configuration section manages service configuration for a service. When a service is first added, default values are in effect. You can edit these values to tune performance.

System Configuration	
Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	
SSL Port	56005
Stat Update Interval	1000
Threads	20

The System Configuration section has these parameters.

Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is 0 . A change in value is effective immediately for all subsequent connections.
Port	 The port on which the service listens. The default ports are: 50001 for Log Collectors 50002 for Log Decoders 50003 for Brokers 50004 for Decoders 50005 for Concentrators 50007 for other services
SSL FIPS Mode	When enabled (on), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is off .
SSL Port	Indicates the SSL port.
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is 1000 . A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of 0 lets the system decide. The default value is 15. A change takes effect on service restart.

Aggregation Configuration Section

The Aggregation Configuration section provides configuration settings that affect various aspects of the aggregation process. When you click **Apply**, the changes are saved; however, not all settings take effect immediately. The tables for Aggregation Settings and Service Heartbeat provide details.

Caution: Do not change any of these settings unless guided by the Developers or the Customer Support team. Contact the Customer Support for any questions before editing any of these settings.

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			

The following table describes the aggregation settings

Setting	Description
Aggregate Autostart	Option to start aggregation automatically each time the Broker or Concentrator is started. Checked means yes, unchecked means no. This change takes effect immediately.
Aggregate Hours	 The number of hours back for each service that the Concentrator or Broker attempts to recover at the beginning of aggregation. This change takes effect immediately. If the value is set to 0, aggregation for each service starts where it last left off, no matter the number of hours behind. If the value is any positive integer, the Concentrator or Broker only consumes sessions less than that number of hours back. For example, if a service's most current session is +10 hours from the last session, this is what happens with two different Aggregate Hours values: With a value of 12, the Concentrator or Broker starts consuming where it left off. With a value of 4, all sessions between 5 and 10 hours back are skipped and the Concentrator or Broker starts consuming the session that started 4 hours back.
Aggregate Interval	The number of milliseconds between rounds of service aggregation. All services managed by the Broker or Concentrator request additional rounds of session and metadata to be aggregated. If a Broker or Concentrator is still consuming the previous round of data, it cannot request more until it finishes. Change takes effect immediately.
Aggregate Max Sessions	The maximum number of sessions that the Broker or Concentrator requests in a given round of data aggregation. Change takes effect after restart.

Service Heartbeat

In communicating with each aggregate service, Brokers and Concentrators monitor the heartbeat of the service. These parameters specify the timing of the first attempt to reconnect to a service after an error, the next attempt to reconnect, and taking the service offline after failure to reconnect.

Setting	Description
Heartbeat Error Restart	After a heartbeat error is detected on an aggregate service, specifies the number of seconds for a Broker or Concentrator to wait before attempting a service reconnect.
Heartbeat Next Attempt	After a failed attempt to reconnect to an aggregate service, specifies the number of seconds for a Broker or Concentrator to wait before attempting another service reconnect. Change takes effect immediately.
Heartbeat No Response	After failing to reconnect to an unresponsive service, specifies the number of seconds for the Broker or Concentrator to wait before taking the unresponsive service offline. Change takes effect immediately.

When editing parameters in the General tab, you must click **Apply** to save changes.

Services System View - Broker or Concentrator

The Services System view displays information specific to specific to Brokers and Concentrators.

While information displayed in this view is the same for all types of Core services, several options in the toolbar are relevant only for Brokers and Concentrators.

Role	I want to	Refer to
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Services System View - Broker or Concentrator
Administrator	Manage System Configuration	Services System View - Broker or Concentrator

What do you want to do?

Related Topics

- Broker and Concentrator Basics
- Broker and Concentrator Configuration

Services System View

You can access this view by doing the following:

- 1. Go to **ADMIN** > **Services.**
- Select a Concentrator or Broker, and select System > View > System.
 The System view for the selected Concentrator or Broker is displayed.

RSA RESPO	OND INVEST	IGATE MONITOR COI	NFIGURE ADMIN			Ö û (D) admin ⊚	
Hosts S	ervices Ever	nt Sources Health & We	llness System Security				
🛔 Change Ser	vice 🖻 admins	erver - Broker System 👳					
Start Aggre	gation 🔋 Stop Agg	regation 📑 Host Tasks 🖞 Shut	down Service 🖞 Shutdown Appliance Servic	e 😃 Reboot			
Broker Se	rvice Informa	tion		Appliance	e Service Information		
Name	adminserver (Brol	er)		Name	adminserver (Host)		
/ersion	11.2.0.0 (Rev null)			Version	11.2.0.0 (Rev null)		
Memory Usage	14268 KB (0.04% c	f 32176 MB)		Memory Usag	e 9588 KB (0.03% of 32176 MB)		
CPU	16%			CPU	12%		
Running Since	e 2018-Jul-05 13:23:46			Running Since	ce 2018-Jul-05 13:23:46		
Jptime	3 weeks 3 days 17	hours 29 minutes 48 seconds		Uptime	3 weeks 3 days 17 hours 29 minutes 48 seconds		
Current Time	2018-Jul-30 06:53:	34		Current Time	2018-Jul-30 06:53:34		
Broker Us	er Informatio	n		Host Use	r Information		
Name	admin				admin		
Groups	Administrators			Groups	Administrators		
Roles	aggregate, concentrator.manage, connections.manage, index.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage			Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage		
Session Ir	nformation						
Session		User	IP Address		Login Time ^	Active Queries	
2486		admin	1271001100120		2018-Jul-06 07:16:03	0	
2660		admin	1.7 million (1.1.2.3.4 Mar		2018-Jul-06 08:26:46	0	

The following figure is an example of the toolbar for a Broker or Concentrator.

hosts s	SERVICES						
🛔 Change Servio	ce 🕴 🖪 Brok	er Sy	stem 👳				
🕟 Start Aggrega	tion 💿 Stop /		📕 Host Task	s 😃 Shutdown Service	也 Shutdown Appli	ance Service	也 Reboot

Host Tasks, Shutdown Service, Shutdown Appliance Service or (Shutdown Appliance), and Reboot are common to all services and are described in the "Services System view" topic in the *Host and Services Getting Started Guide*.

This table describes toolbar options that apply only to a Concentrator or Broker. Both buttons are unavailable until aggregator services are configured and consuming data.

Action	Description
Start Aggregation	Starts aggregation of data being consumed on a Concentrator or Decoder configured as an aggregation service for the selected Broker or Concentrator. The Start Aggregation button is available only when aggregator services are configured and consuming data.
Stop Aggregation	Stops aggregation of data being consumed on a Concentrator or Decoder configured as an aggregation service for the selected Broker or Concentrator. The Stop Aggregation button is available only when aggregation is occurring.