

NetWitness[®] Platform XDR

Version 12.1.0.0

Broker and Concentrator Configuration Guide

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

October, 2022

Contents

Broker and Concentrator Basics	4
Overview of Broker and Concentrator	5
Broker and Concentrator Configuration	6
Basic Configuration Checklist	6
Step 1. Verify Service System Configuration	6
Step 2. Configure the Aggregation Process	9
Step 3. Configure Aggregate Services	11
Step 4. (Optional) Configuring Group Aggregation	15
RSA Group Aggregation Deployment Recommendations	15
Advantages of Using Group Aggregation	15
Configure Group Aggregation	17
Prerequisites	17
Set up Group Aggregation	18
Step 5. Start and Stop Aggregation	21
Broker and Concentrator Configuration References	24
Services Config View - Broker or Concentrator General Tab	25
What do you want to do?	25
Related Topics	25
General tab	25
Aggregate Services Section	27
System Configuration Section	28
Aggregation Configuration Section	29
Service Heartbeat	31
Services System View - Broker or Concentrator	32
What do you want to do?	32
Related Topics	32
Services System View	32


Broker and Concentrator Basics

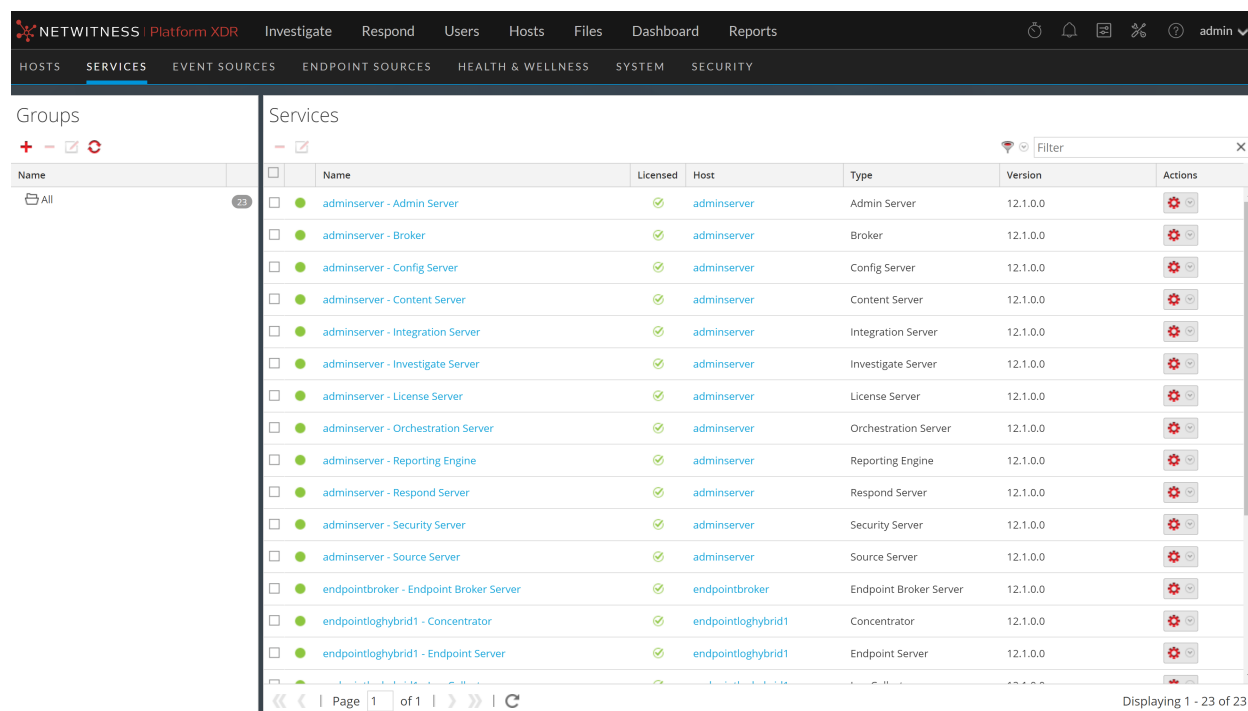
Concentrators and Brokers aggregate data captured or aggregated by other services unlike Decoders, which capture data.

NetWitness 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 user interface. Most of the configuration is performed in the

Administration Services view ( (Admin) > Services).



Name	Licensed	Host	Type	Version	Actions
adminserver - Admin Server	✓	adminserver	Admin Server	12.1.0.0	
adminserver - Broker	✓	adminserver	Broker	12.1.0.0	
adminserver - Config Server	✓	adminserver	Config Server	12.1.0.0	
adminserver - Content Server	✓	adminserver	Content Server	12.1.0.0	
adminserver - Integration Server	✓	adminserver	Integration Server	12.1.0.0	
adminserver - Investigate Server	✓	adminserver	Investigate Server	12.1.0.0	
adminserver - License Server	✓	adminserver	License Server	12.1.0.0	
adminserver - Orchestration Server	✓	adminserver	Orchestration Server	12.1.0.0	
adminserver - Reporting Engine	✓	adminserver	Reporting Engine	12.1.0.0	
adminserver - Respond Server	✓	adminserver	Respond Server	12.1.0.0	
adminserver - Security Server	✓	adminserver	Security Server	12.1.0.0	
adminserver - Source Server	✓	adminserver	Source Server	12.1.0.0	
endpointbroker - Endpoint Broker Server	✓	endpointbroker	Endpoint Broker Server	12.1.0.0	
endpointloghybrid1 - Concentrator	✓	endpointloghybrid1	Concentrator	12.1.0.0	
endpointloghybrid1 - Endpoint Server	✓	endpointloghybrid1	Endpoint Server	12.1.0.0	

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).

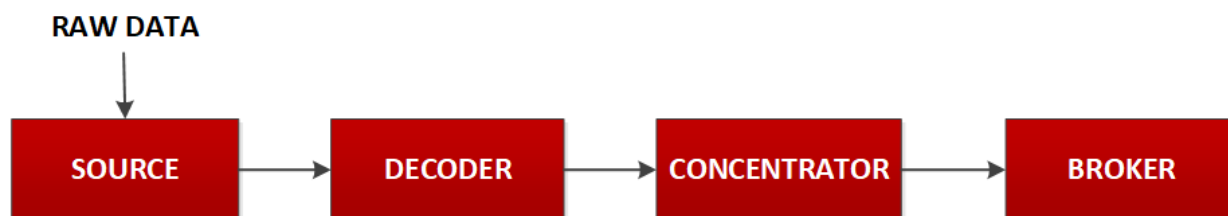
Overview of Broker and Concentrator

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 NetWitness community portal 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.

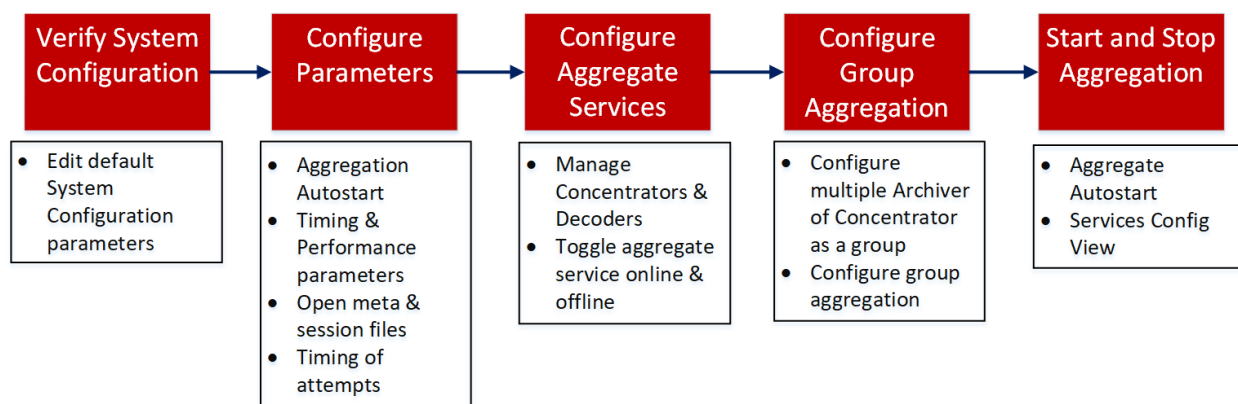


- Concentrator: is required for any large environment to store the Meta data that is generated by the parsers and feeds being triggered by packets and logs ingested into the decoders.
- Broker: The Broker service is similar to the Concentrator service except that it indexes the collected information. 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.



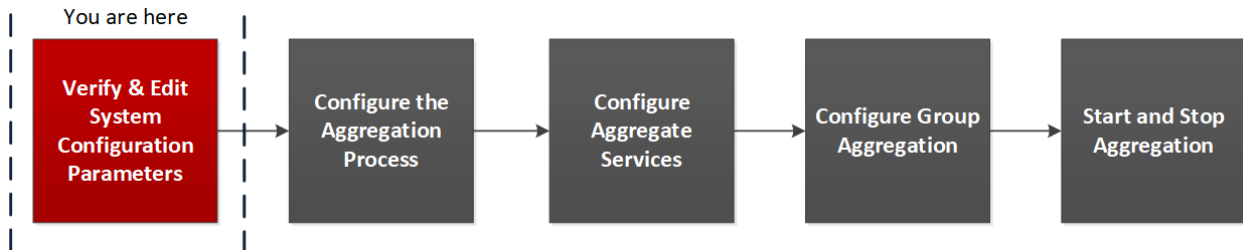
Basic Configuration Checklist

The following checklist provides the sequence for tasks that are required to configure a Broker or Concentrator that has been added to NetWitness 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 Step 1. Verify Service System Configuration
Step 2 - Configure Parameters	Configure parameters that govern the overall aggregation process as described in Step 2. Configure the Aggregation Process
Step 3 - Configure Aggregate Services	Configure aggregate services as described in Step 3. Configure Aggregate Services
Step 4 - Configure Group Aggregation	(Optional) Configure group aggregation as described in Step 4. (Optional) Configuring Group Aggregation
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, 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 select  > **View** > **Config**.

The Services Config view for the selected service is displayed.

Aggregate Services

Address	Port	Rate	Max	Behind	Collection	Status

System Configuration

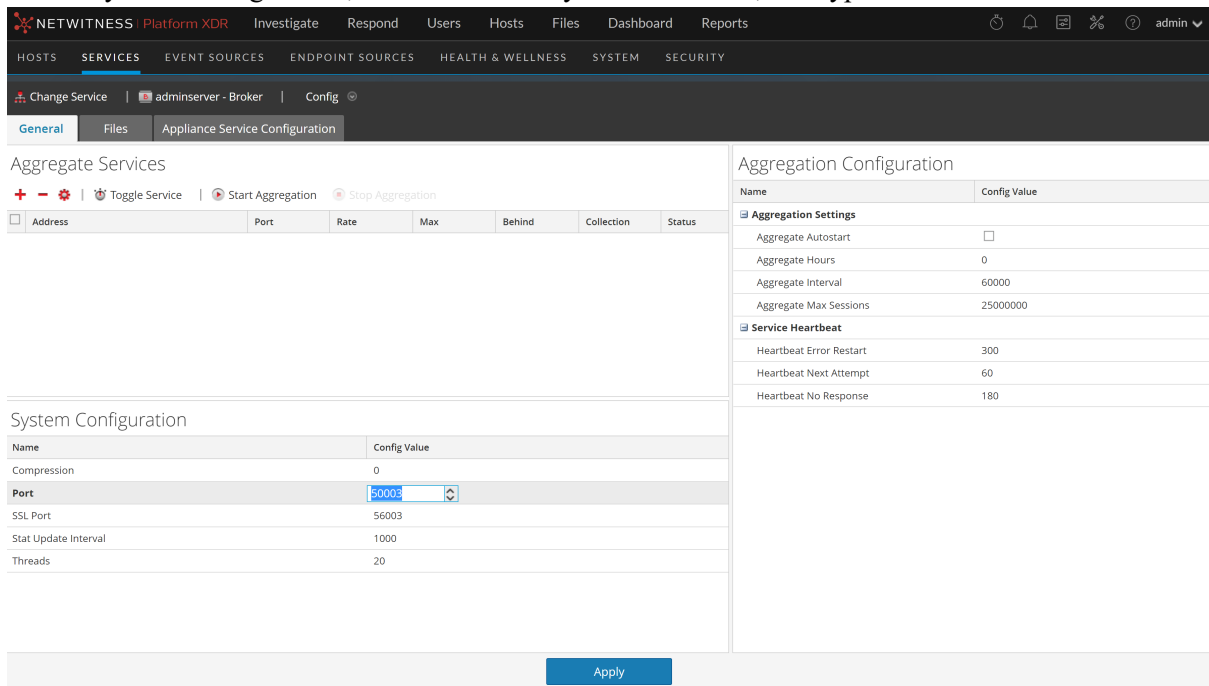
Name	Config Value
Compression	0
Port	50003
SSL Port	56003
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

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



The screenshot shows the NetWitness Platform XDR configuration interface. The top navigation bar includes links for Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The 'Services' tab is active, and the 'Appliance Service Configuration' sub-tab is selected. The interface is divided into two main sections: 'Aggregate Services' on the left and 'Aggregation Configuration' on the right.

Aggregate Services

Buttons: +, -, ⚙️, 🔄 Toggle Service, 🟢 Start Aggregation, 🛑 Stop Aggregation

Address	Port	Rate	Max	Behind	Collection	Status

System Configuration

Name	Config Value
Compression	0
Port	50003
SSL Port	56003
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

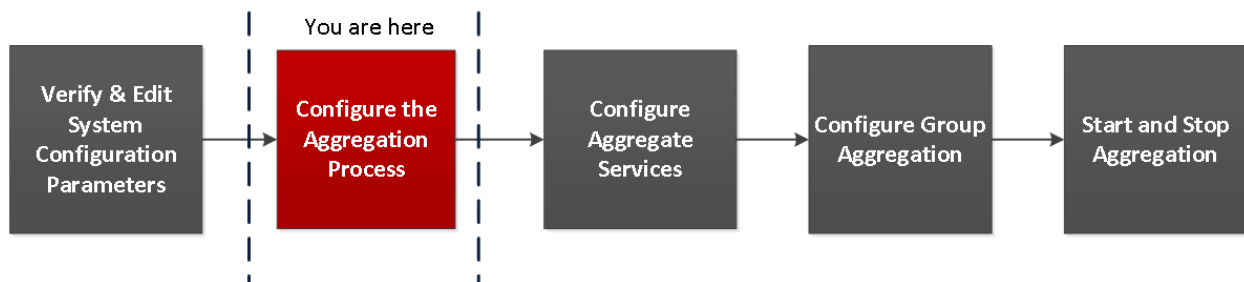
Apply

- 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.

Aggregate Services

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
192.168.1.100	50002	0	15	0			no		consuming

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL Port	56005
Stat Update Interval	1000
Threads	20

Apply

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	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

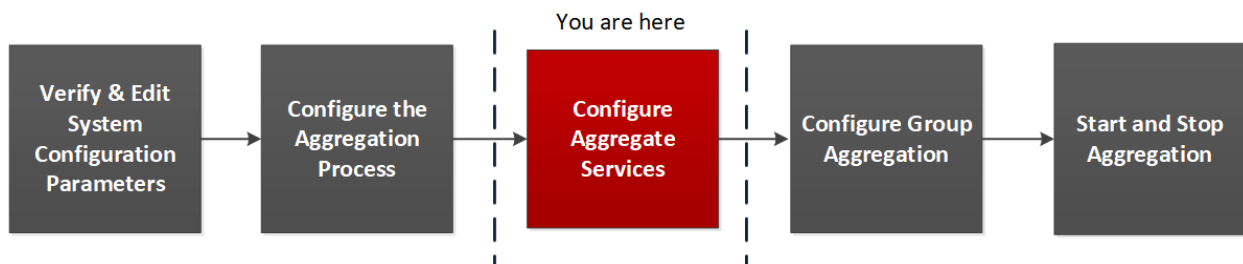
4. (Optional) Edit any of the aggregation settings: the hours back to begin aggregation, the milliseconds between rounds of aggregation, and maximum number of sessions per aggregation round.
5. (Optional) Edit any of the Service Heartbeat settings, which specify the timing of the first attempt to reconnect 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 [Step 4. \(Optional\) Configuring Group 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**.
2. In the **Services** view, select a Broker or Concentrator, and select  > **View** > **Config**.
The Services Config view for the selected service is displayed.

The screenshot shows the configuration page for 'endpointloghybrid1 - Concentrator'. The interface includes a top navigation bar with tabs like HOSTS, SERVICES, EVENT SOURCES, etc. The 'SERVICES' tab is active, and the 'Config' sub-tab is selected. The main content area is divided into two sections: 'Aggregate Services' and 'System Configuration'.

Aggregate Services

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
10.10.10.10	50002	0	15	0			no		consuming

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL Port	56005
Stat Update Interval	1000
Threads	20

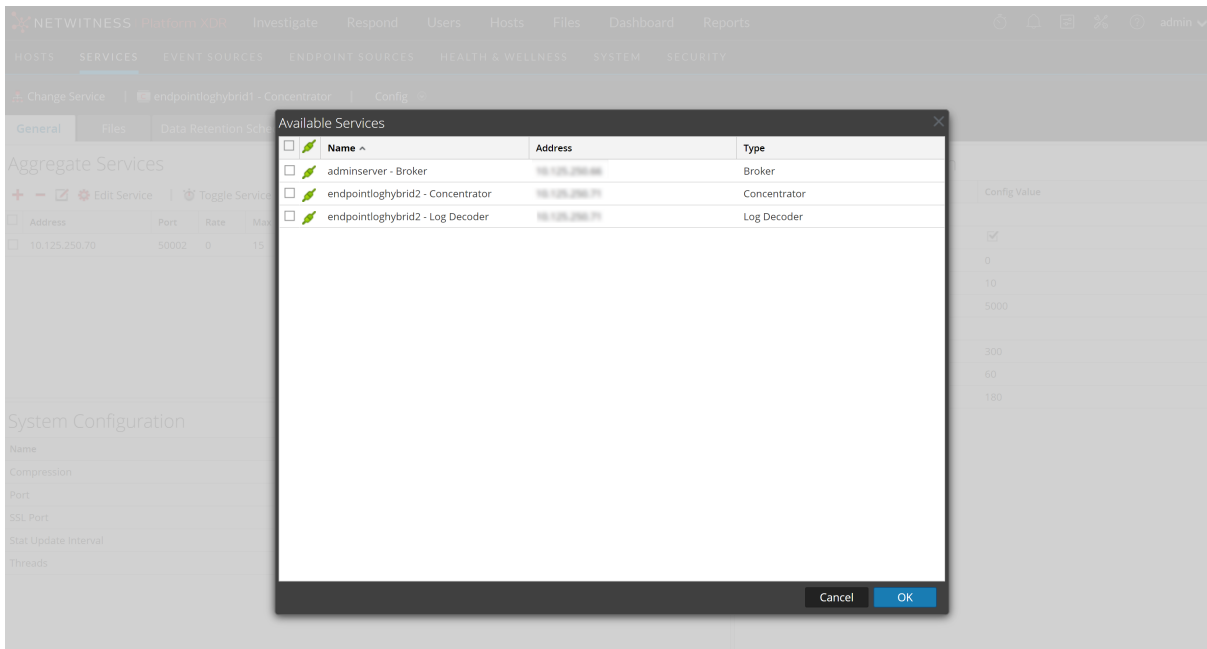
Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

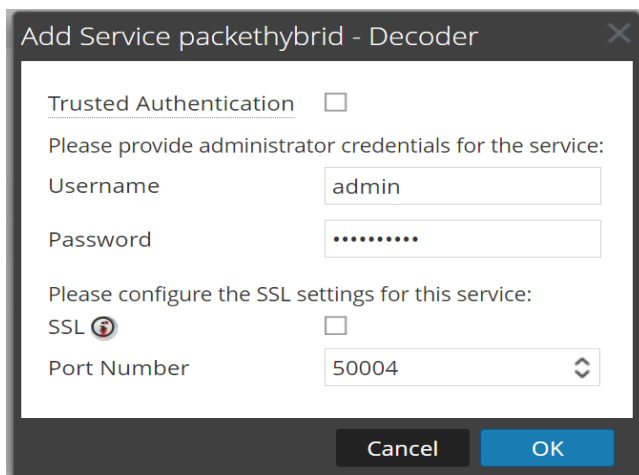
An 'Apply' button is located at the bottom right of the configuration area.

3. Click  in the **Aggregate Services** toolbar.

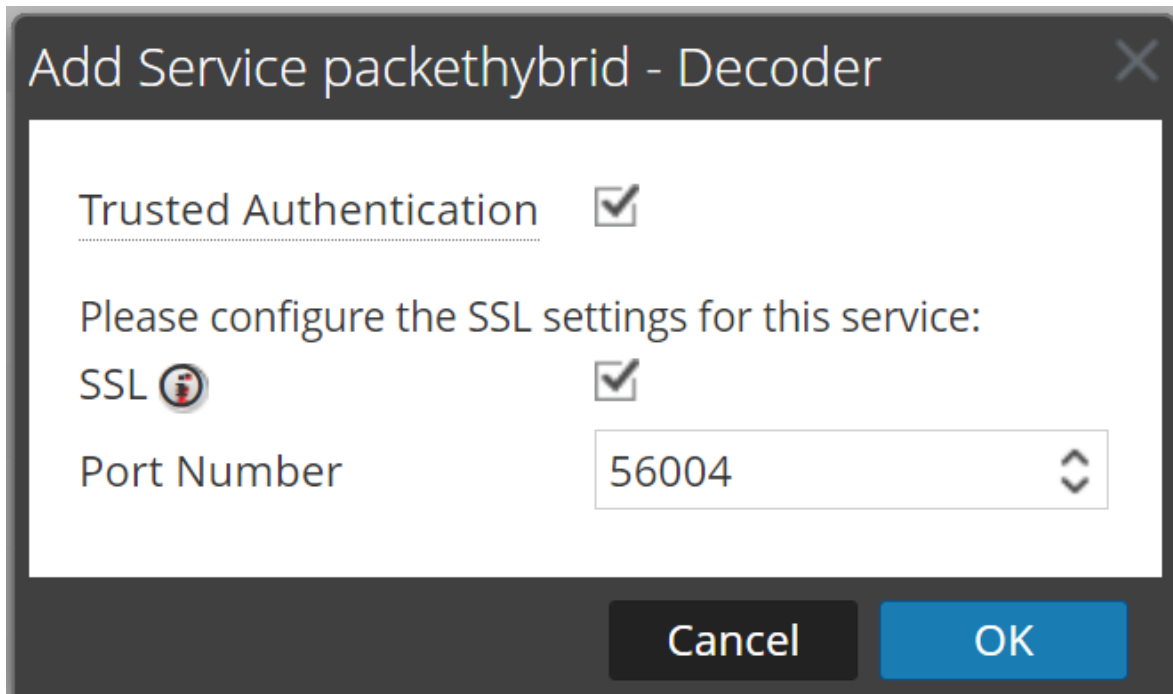
The Available Services dialog is displayed.



4. Select one or more services to be added and click **OK**.
5. Use one of the following ways to add a service for aggregation:
- Use Password-Based Authentication. Enter the Administrator username and password. Click **OK**.



- Select **Trusted Authentication**. Click **OK**.



A dialog box titled "Add Service packethybrid - Decoder" with a close button (X) in the top right corner. The dialog contains the following elements:

- Trusted Authentication**: A checkbox that is checked.
- Please configure the SSL settings for this service:**: A text prompt.
- SSL**: A checkbox with an information icon (i) to its left, which is checked.
- Port Number**: A text input field containing the value "56004" and a dropdown arrow on the right.
- Buttons**: "Cancel" and "OK" buttons at the bottom right.

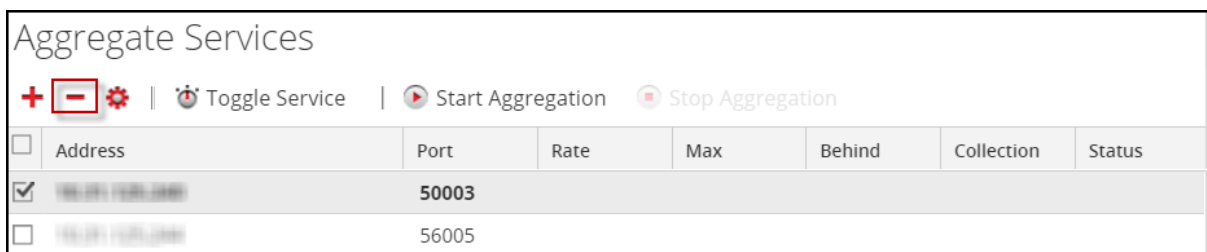
The added services are listed in the Aggregate Services list.

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.



A screenshot of the "Aggregate Services" window. It features a toolbar with icons for adding (+), removing (-), and configuring (gear) services, along with "Toggle Service", "Start Aggregation", and "Stop Aggregation" buttons. Below the toolbar is a table with the following columns: Address, Port, Rate, Max, Behind, Collection, and Status.

	Address	Port	Rate	Max	Behind	Collection	Status
<input checked="" type="checkbox"/>	192.168.1.100:50003	50003					
<input type="checkbox"/>	192.168.1.100:56005	56005					


The service is removed from Aggregate Services list.

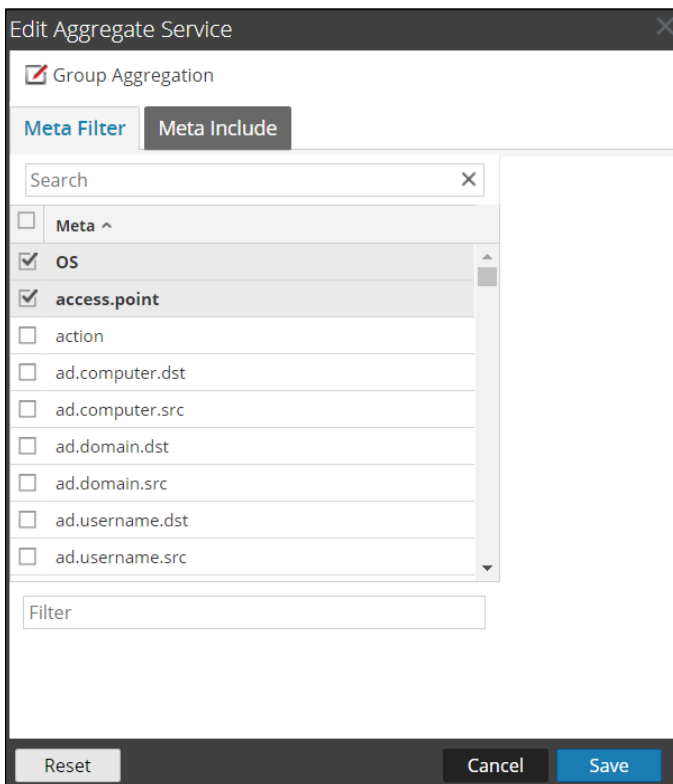
3. To save the change, click **Apply**.

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  in the toolbar. Enter the authentication information in the pop up dialog box.
 - If the service was added on a different instance of NetWitness, you must add it to this instance of NetWitness 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 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**.



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

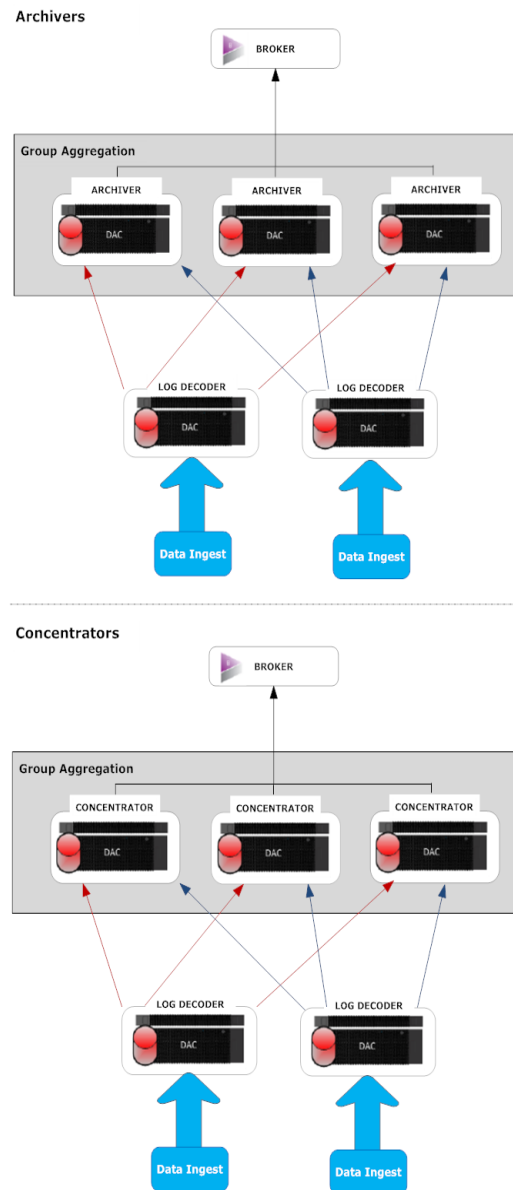
RSA recommends the following deployment for Group Aggregation:

- 1 - 2 Log Decoders
- 3 - 5 Archivers or Concentrators

Advantages of Using Group Aggregation

- Increases the speed of NetWitness 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 sessions 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 10,000, the services would divide the session between themselves as illustrated in the following table.

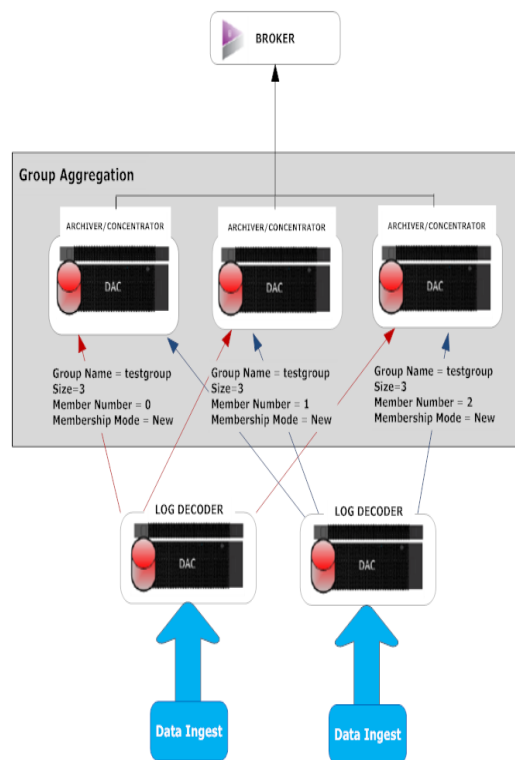
Archiver 0 or Concentrator 0	Archiver 1 or Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

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.



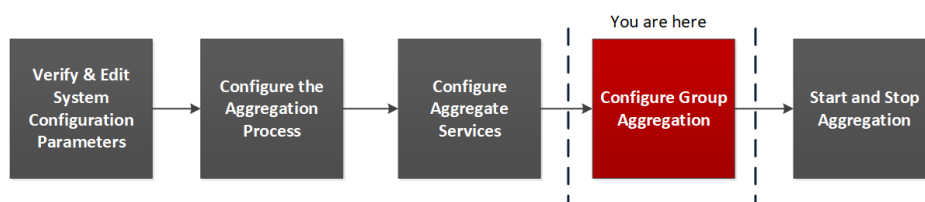
Ensure that you understand the Group aggregation parameters in the following table, and create a group aggregation plan.

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.
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: <ul style="list-style-type: none"> • 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.

Note: The 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.



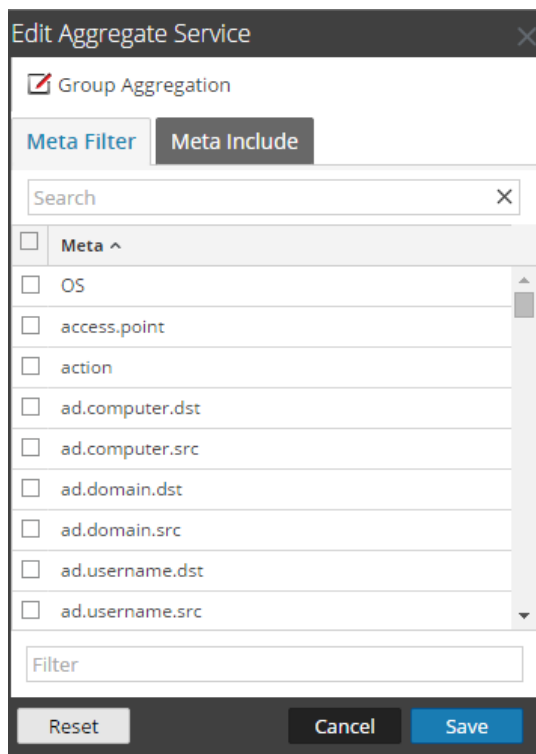
Complete the following steps to set up group aggregation.

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 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 .

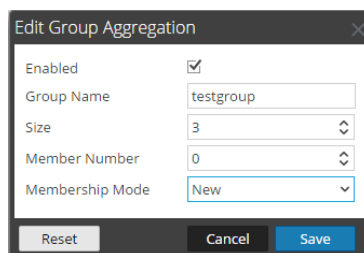
The **Edit Aggregate Service** dialog is displayed.



The **Edit Aggregate Service** dialog is shown. It has a title bar with a close button. Inside, there's a checkbox for **Group Aggregation** which is checked. Below it are two tabs: **Meta Filter** (selected) and **Meta Include**. Under the **Meta Filter** tab, there's a search box labeled "Search" with a clear button. Below the search box is a list of meta filters, each with a checkbox: **Meta** (expanded), **OS**, **access.point**, **action**, **ad.computer.dst**, **ad.computer.src**, **ad.domain.dst**, **ad.domain.src**, **ad.username.dst**, and **ad.username.src**. At the bottom of the list is a **Filter** input field. At the very bottom are three buttons: **Reset**, **Cancel**, and **Save**.

- f. Click .

The **Edit Group Aggregation** dialog is displayed.



The **Edit Group Aggregation** dialog is shown. It has a title bar with a close button. Inside, there's an **Enabled** checkbox which is checked. Below it are four fields: **Group Name** (text box with "testgroup"), **Size** (spin box with "3"), **Member Number** (spin box with "0"), and **Membership Mode** (dropdown menu with "New" selected). At the bottom are three buttons: **Reset**, **Cancel**, and **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, 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**.

The screenshot displays the NetWitness Platform XDR configuration interface. The top navigation bar includes links for Investigate, Respond, Users, Hosts, Files, Dashboard, and Reports. The main menu on the left shows various sections like HOSTS, SERVICES, EVENT SOURCES, and SECURITY. The current view is the 'Config' page for the 'endpointloghybrid1 - Concentrator' service, specifically the 'Appliance Service Configuration' tab.

The interface is divided into two main panels. The left panel, titled 'Aggregate Services', contains a table with columns for Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. A single service is listed with Port 50002, Rate 0, Max 15, and Status 'no consuming'.

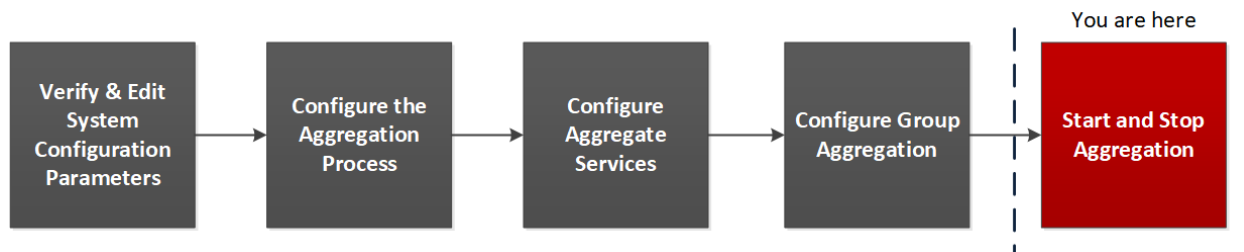
The right panel, titled 'Aggregation Configuration', contains two sub-sections: 'Aggregation Settings' and 'Service Heartbeat'. The 'Aggregation Settings' section includes parameters like 'Aggregate Autostart' (checked), 'Aggregate Hours' (0), 'Aggregate Interval' (10), and 'Aggregate Max Sessions' (10000, highlighted with a red box). The 'Service Heartbeat' section includes parameters like 'Heartbeat Error Restart' (300), 'Heartbeat Next Attempt' (60), and 'Heartbeat No Response' (180).

Below the 'Aggregate Services' table is a 'System Configuration' section with a table listing parameters like Compression, Port, SSL Port, Stat Update Interval, and Threads, along with their respective configuration values.

An 'Apply' button is located at the bottom right of the configuration area.

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.



Note: The Aggregate Configuration Settings (in the [Services Config View - Broker or Concentrator General Tab](#)) determine whether Aggregate autostart is enabled, as well as the size of a round of aggregation and time between rounds.

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

1. Go to  (Admin) > Services.
2. In the Services view, select a Broker or Concentrator, and select  > View > System.

The screenshot shows the NetWitness Platform XDR interface. The top navigation bar includes tabs for Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The 'Services' tab is active, and the 'System' view is selected for the 'endpointloghybrid1 - Concentrator' service.

Concentrator Service Information

Name	endpointloghybrid1 (Concentrator)
Version	12.1.0.0 (Rev null)
Memory Usage	158 MB (0.99% of 16046 MB)
CPU	4%
Running Since	2022-Sep-26 14:08:56
Uptime	1 day 21 hours 9 minutes 16 seconds
Current Time	2022-Sep-28 11:18:12

Concentrator User Information

Name	admin
Groups	Administrators
Roles	aggregate, concentrator.manage, connections.manage, database.manage, index.manage, logs.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Appliance Service Information

Name	endpointloghybrid1 (Host)
Version	12.1.0.0 (Rev null)
Memory Usage	31688 KB (0.19% of 16046 MB)
CPU	4%
Running Since	2022-Sep-26 14:08:56
Uptime	1 day 21 hours 9 minutes 16 seconds
Current Time	2022-Sep-28 11:18:12

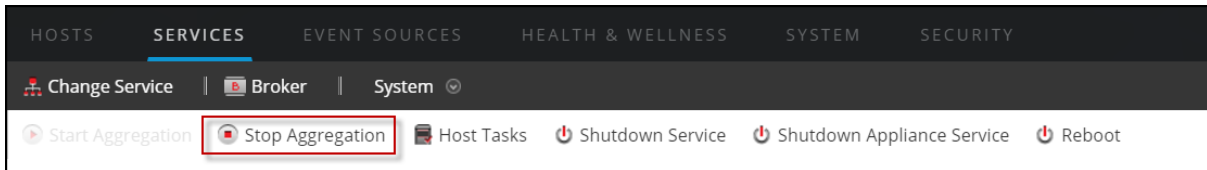
Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

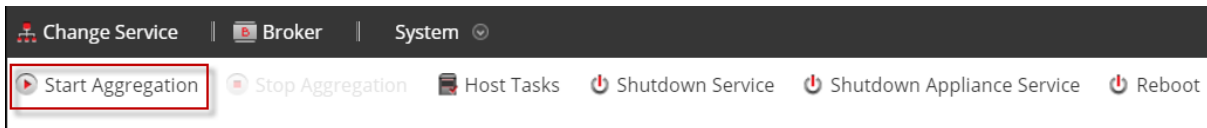
Session	User	IP Address	Login Time	Active Queries
502	admin	10.125.255.255	2022-Sep-26 14:09:17	0
532	admin	10.125.255.255	2022-Sep-26 14:09:20	0
628	escalateduser	10.125.255.255	2022-Sep-26 14:24:15	0
3493	admin	10.125.255.255	2022-Sep-27 09:46:15	0

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.





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

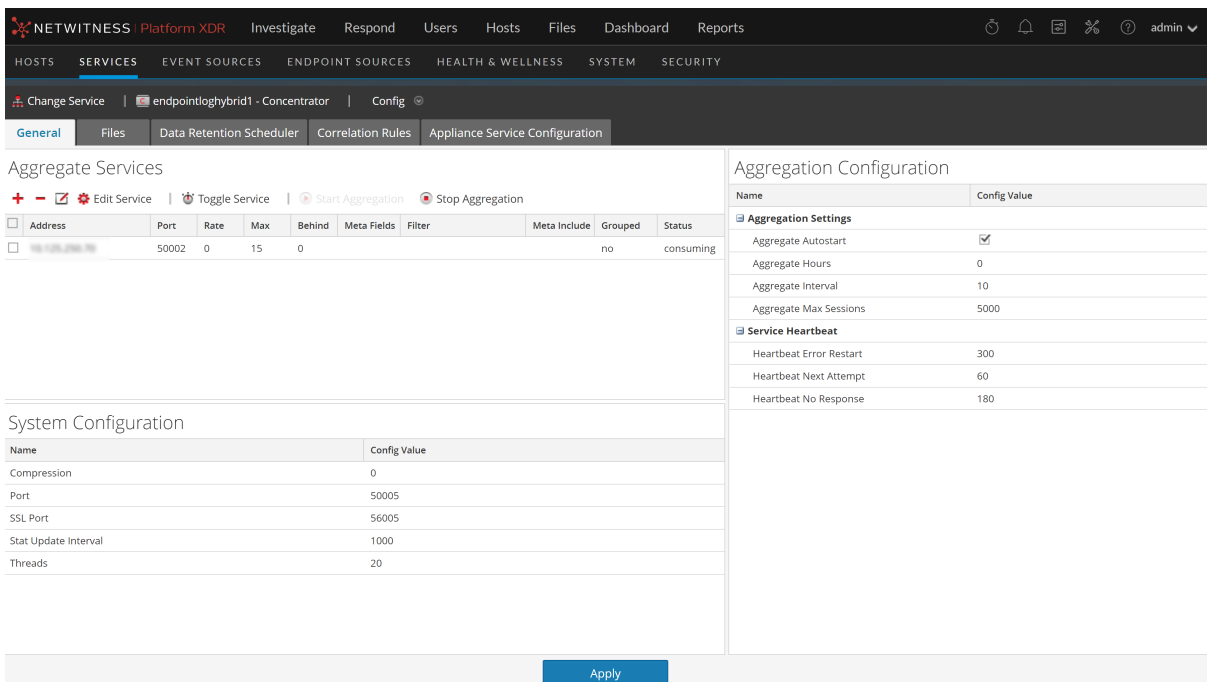
You can now investigate the captured data in the Investigation module.




To start and stop aggregation in the services config view:

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 Aggregate Services section, is displayed.



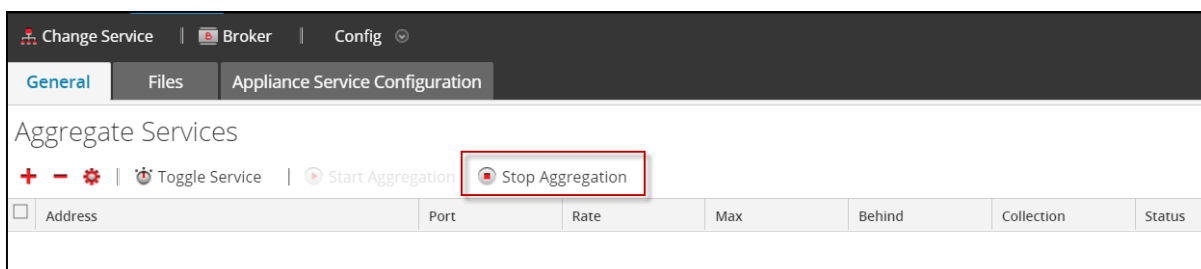
3. To start aggregation on the selected Broker or Concentrator, click  in the **Aggregate Services** toolbar.

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.



4. To stop aggregation, click  **Stop Aggregation** in the **Aggregate Services** toolbar.

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.



Broker and Concentrator Configuration References

You can configure Brokers and Concentrators using the NetWitness 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.

NETWITNESS Platform XDR Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service endpointloghybrid1 - Concentrator Config

General Files Data Retention Scheduler Correlation Rules Appliance Service Configuration

Aggregate Services

+ - Edit Service Toggle Service Start Aggregation Stop Aggregation

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
10.10.10.10	50002	0	15	0				no	consuming

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL Port	56005
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregate Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

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

NETWITNESS Platform XDR Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service endpointloghybrid1 - Concentrator Config

General Files Data Retention Scheduler Correlation Rules Appliance Service Configuration

Aggregate Services

+ - Edit Service Toggle Service Start Aggregation Stop Aggregation

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
10.10.10.10	50002	0	15	0				no	consuming

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL Port	56005
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregate Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

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 Retention Scheduler

Correlation Rules

Appliance Service Configuration

Aggregate Services

Edit Service

Toggle Service

Start Aggregation

Stop Aggregation

<input type="checkbox"/>	Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
<input type="checkbox"/>	10.31.125.245	50004	0	0	0				no	consuming
<input type="checkbox"/>	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.
	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: <ul style="list-style-type: none"> • 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 <code>ip.src !=127.0.0.1 && word exists</code>
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: <ul style="list-style-type: none"> • 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	<input type="checkbox"/>
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: <ul style="list-style-type: none"> • 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	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
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	<p>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.</p> <ul style="list-style-type: none"> 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. <p>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:</p> <ul style="list-style-type: none"> 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.

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	Services System View - Broker or Concentrator
Administrator	Manage System Configuration	Services System View - Broker or Concentrator

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**.
2. Select a Concentrator or Broker, and select   > **View** > **System**.
The System view for the selected Concentrator or Broker is displayed.

NETWITNESS Platform XDR Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service | endpointloghybrid1 - Concentrator | System

Start Aggregation Stop Aggregation Host Tasks Shutdown Service Shutdown Appliance Service Reboot

Concentrator Service Information

Name: endpointloghybrid1 (Concentrator)

Version: 12.1.0.0 (Rev null)

Memory Usage: 158 MB (0.99% of 16046 MB)

CPU: 3%

Running Since: 2022-Sep-26 14:08:56

Uptime: 1 day 21 hours 26 minutes 46 seconds

Current Time: 2022-Sep-28 11:35:42

Appliance Service Information

Name: endpointloghybrid1 (Host)

Version: 12.1.0.0 (Rev null)

Memory Usage: 31952 KB (0.19% of 16046 MB)

CPU: 3%

Running Since: 2022-Sep-26 14:08:56

Uptime: 1 day 21 hours 26 minutes 46 seconds

Current Time: 2022-Sep-28 11:35:42

Concentrator User Information

Name: admin

Groups: Administrators

Roles: aggregate, concentrator.manage, connections.manage, database.manage, index.manage, logs.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name: admin

Groups: Administrators

Roles: appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

Session	User	IP Address	Login Time	Active Queries
502	admin	10.128.255.46	2022-Sep-26 14:09:17	0
532	admin	10.128.255.46	2022-Sep-26 14:09:20	0
628	escalateduser	10.128.255.46	2022-Sep-26 14:24:15	0
3493	admin	10.128.255.46	2022-Sep-27 09:46:15	0

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

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service | Broker | System

Start Aggregation Stop Aggregation Host Tasks Shutdown Service Shutdown Appliance Service 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.