RSA NETWITNESS® PLATFORM

Cloud Behavioral Analytics Gateway 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.

August 2018

Contents

RSA Cloud Behavioral Analytics **5**

Provision a Cloud Gateway **6**

Mapping Cloud Gateway Analytic Streams **10**

Considerations 10

Analytic Stream Deployment Example - Two Gateways 10

Analytic Stream Deployment Example - One Gateway 11

Prerequisites 12

Create Cloud Gateway Analytic Stream Mappings 13

Deploy Cloud Gateway Analytic Stream Mappings 17

Update a Mapping 18

Undeploy a Mapping 18

Delete a Mapping 18

Change the Lag Time 19

Monitor the Cloud Gateway 21

Cloud Gateway References **23**

Cloud Gateway Config View Certificate Tab 24

What do you want to do? 24

Related Topics 24

Certificate Tab 24

Certificate Information 26

Toolbar Actions 26

Cloud Gateway Analytic Stream Mappings 28

Workflow 28

What do you want to do? 29

Related Topics 29

Quick Look 30

Toolbar 31

Cloud Gateway Analytic Stream Mappings 31

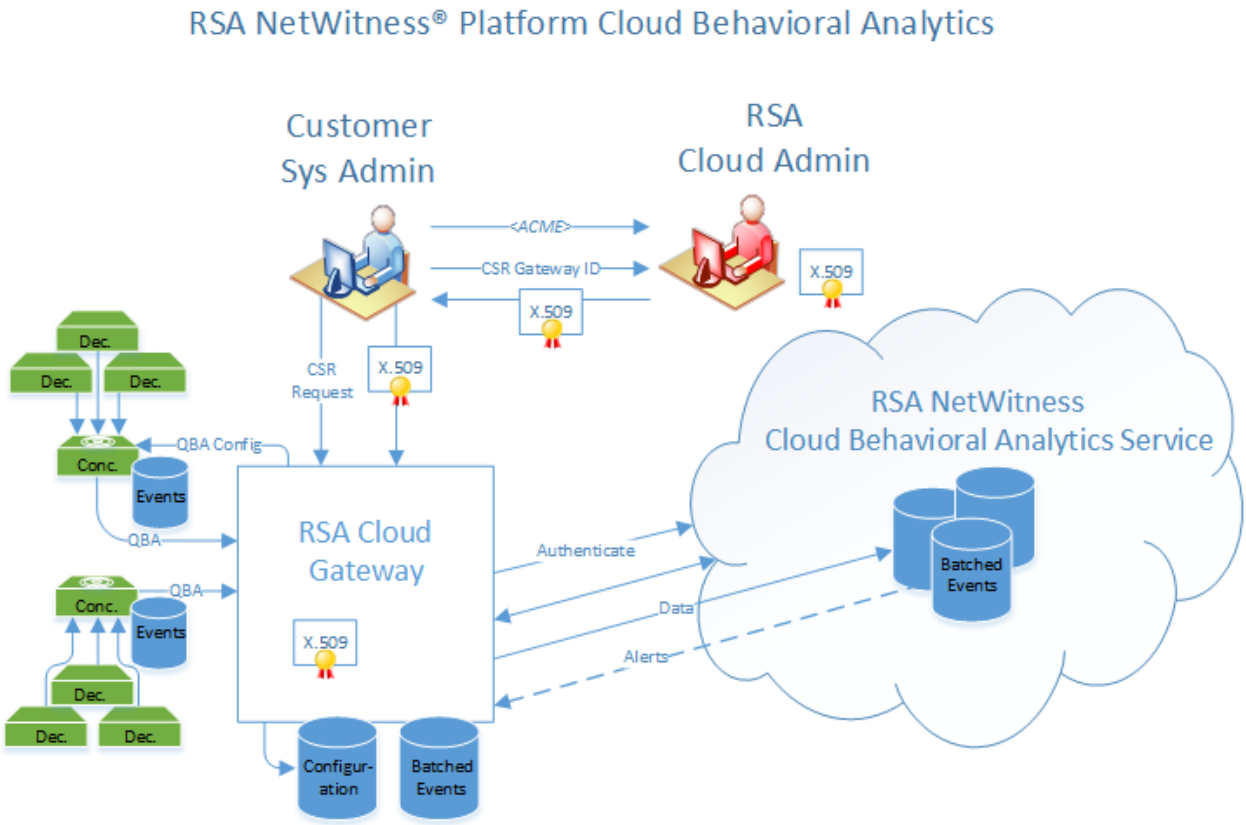
Analytic Stream Settings 34

What do you want to do? 34

Related Topics 34
Analytic Stream Settings 34
Configuration 35

RSA Cloud Behavioral Analytics

RSA NetWitness® Platform Cloud Behavioral Analytics (CBA) provides the ability to analyze your data in the cloud, instead of on your premises, and send alerts of potential threats. With data analysis in the cloud, RSA Data Scientists can study the effectiveness of the data models used to perform the analysis and update them more frequently to better respond to current threats.



To prepare a secure data connection to the RSA NetWitness Cloud Behavioral Analytics service, you must provision the RSA Cloud Gateway service. To do this, you create a Certificate Signing Request (CSR) for the Cloud Gateway. You then provide the CSR and the Gateway ID to the RSA Cloud Administrator. The RSA Cloud Administrator will provide you with a signed certificate for you to install on the NetWitness Platform host where your gateway service is installed. See the following step-by-step instructions to provision the Cloud Gateway.

Note: RSA NetWitness® Platform Cloud Behavioral Analytics is a pre-General Availability release. If you are interested in participating as a design partner to help shape and improve CBA for General Availability, please contact your Sales Representative.

The procedures in this guide should be completed by a NetWitness Platform Administrator.

Provision a Cloud Gateway

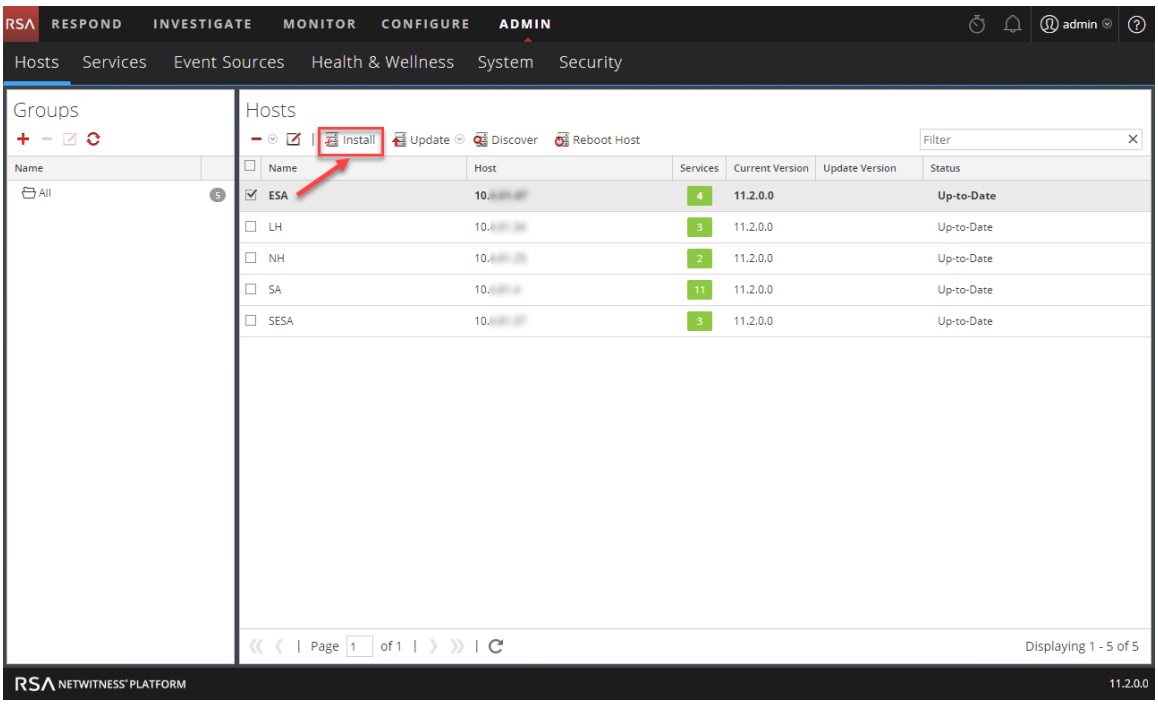
RSA Cloud Gateway Server services must be provisioned before using them for Cloud Behavioral Analytics. This is a one-time procedure per gateway service.

You can install the Cloud Gateway service on any NetWitness Platform host. RSA recommends using a dedicated host that you provision for your Cloud Gateway, but it is not required. The following list shows the preferred locations for the Cloud Gateway in order of preference:

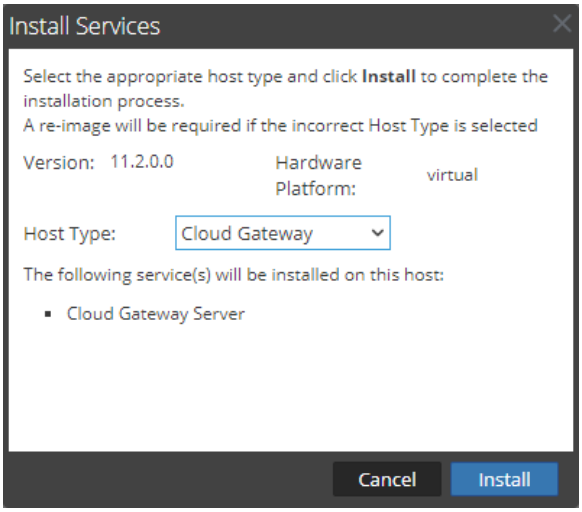
- Provision your own dedicated host
- ESA Host
- NetWitness Server Host

Follow these instructions to install a Cloud Gateway and create a Certificate Signing Request (CSR) for the Cloud Gateway. You must provide the CSR and the Gateway ID to the RSA Cloud Administrator. The RSA Cloud Administrator will provide you with a signed certificate to install in your Cloud Gateway service.

1. To install the Cloud Gateway, log in to NetWitness Platform and go to **ADMIN > Hosts**.
2. In the Hosts view, select the NetWitness host where you want to install the Cloud Gateway Server service and click **Install**.

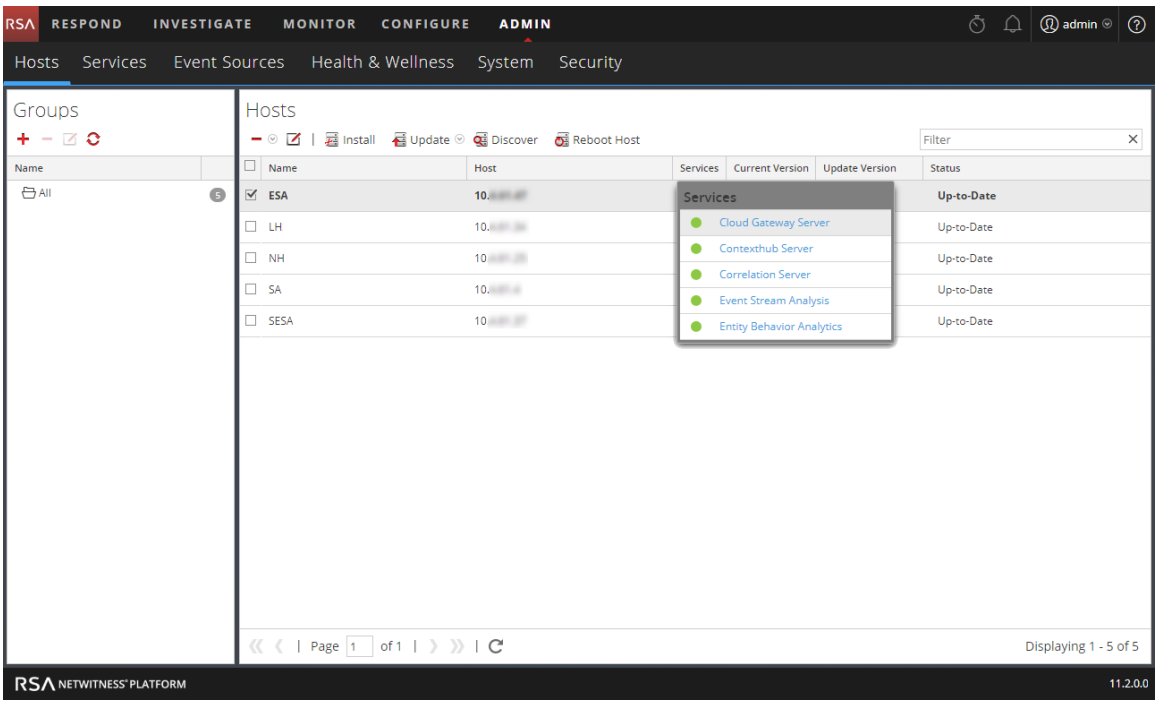


3. In the Install Services dialog, in the **Host Type** field, select **Cloud Gateway**.



4. Click **Install** to install the Cloud Gateway Server on the selected host.

5. To verify the installation, in the Hosts view, click the box in the **Services** column of the selected host.



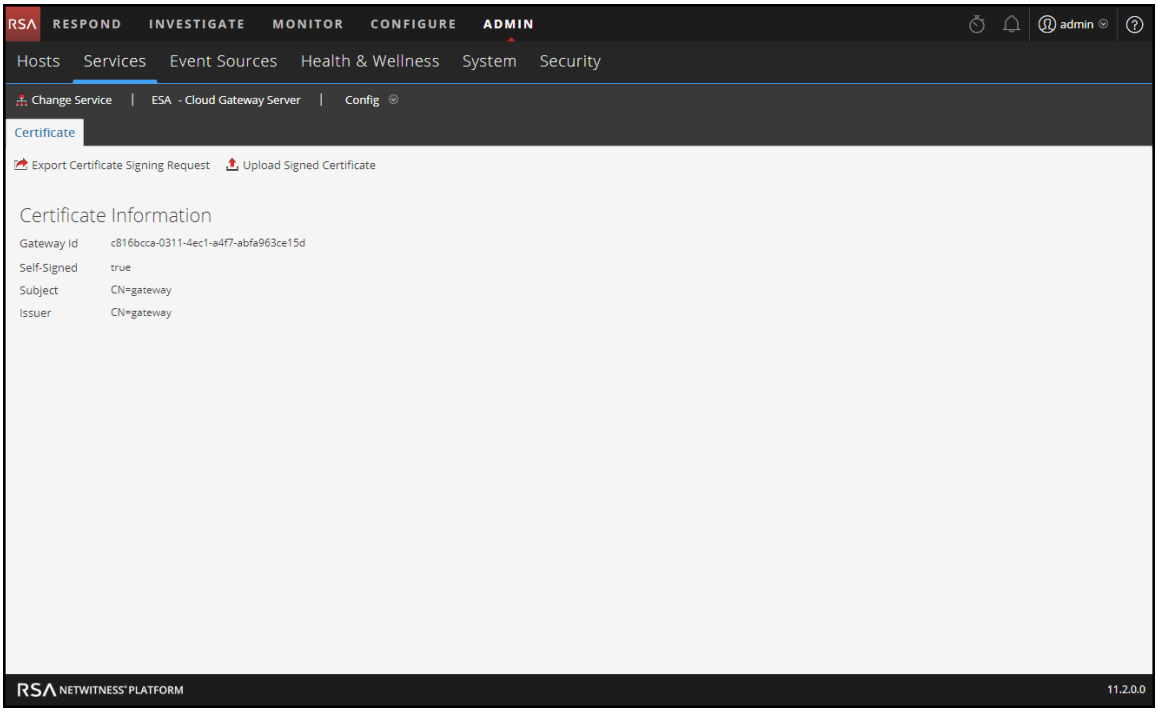
You should see the Cloud Gateway Server service in the services list for that host.

6. Click the **Cloud Gateway Server** service in the list to go to the Services view (**ADMIN > Services**).

7. To get the CSR for the gateway:

   a. In the Services view, select the Cloud Gateway Server service and then select > **View** > **Config**.

   In the Services Config view, the **Gateway ID** is listed.



   b. Click **Export Certificate Signing Request**.

   The service creates and downloads the CSR file for you.

> **Caution:** Do not generate multiple Certificate Signing Requests. The signed certificate file received in step 8 must match the CSR generated in this step. If there is a mismatch, the uploading of the signed certificate file fails.

8. Send the CSR file and Gateway ID to the RSA Cloud Administrator, who will provide you with a signed certificate file.

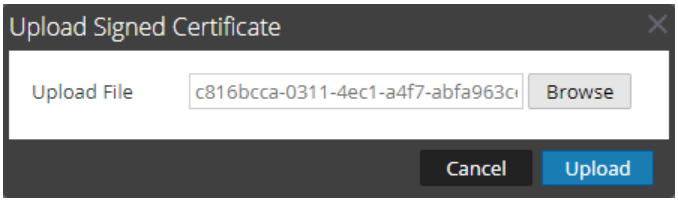
> **Caution:** Do not rename the Gateway CSR file. The name of the file must be the Gateway ID.

9. Copy the signed certificate file to the NetWitness Platform host where the Cloud Gateway Server service is installed.

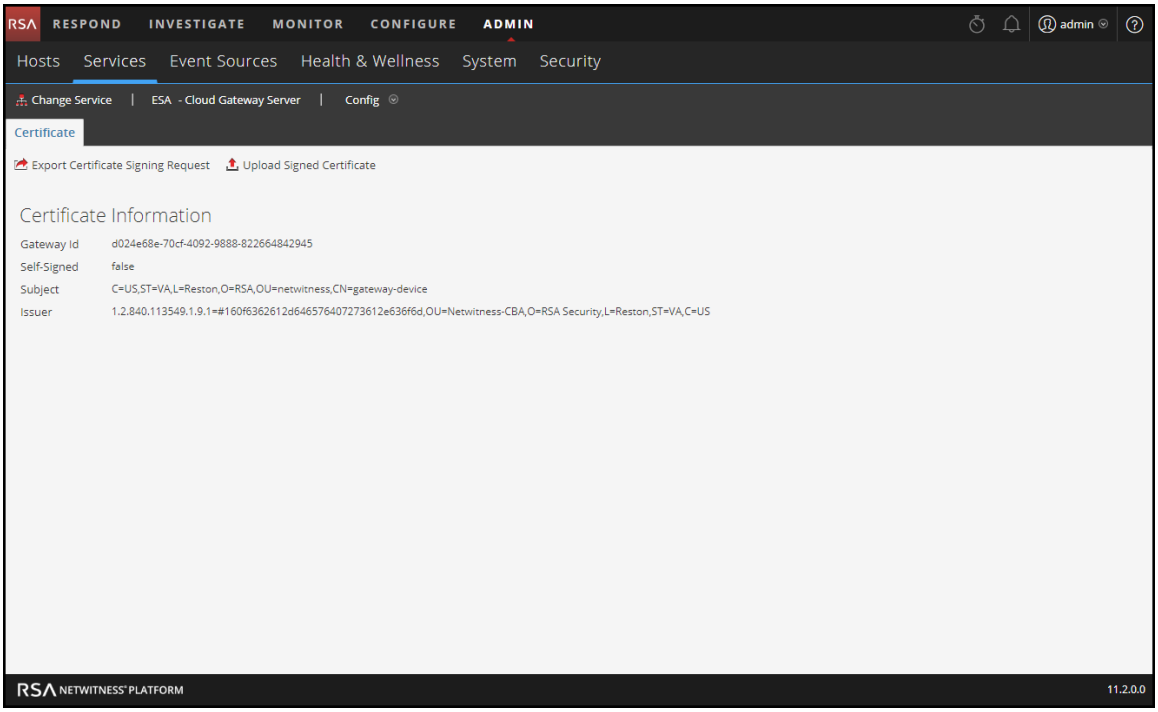
10. To install the signed certificate in your Cloud Gateway Server service:

    a. In the Services Config view, click **Upload Signed Certificate**.

    b. In the Upload Signed Certificate dialog, select your signed certificate and click **Upload**.



The following figure shows the results of setting the signed certificate on the Cloud Gateway.



After a signed certificate file is properly uploaded to the Cloud Gateway, the **Self-Signed** field shows as **false**, which indicates that the installed certificate is now properly signed by **Netwitness-CBA**.

Mapping Cloud Gateway Analytic Streams

You can configure the RSA Cloud Gateway to automatically upload Analytic Streams from one or more Concentrators to Cloud Behavioral Analytics (CBA). An *Analytic Stream* is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.

When you deploy your mapping, the selected Cloud Gateway service uses query-based aggregation to collect the appropriate filtered events for the selected Analytic Stream from the Concentrators. Query-based aggregation is a predefined query that only transfers data for the selected Analytic Stream. Only the data required by the Analytic Stream is transferred from the Concentrator to Cloud Behavioral Analytics.

Considerations

When creating and deploying your Analytic Stream mappings, keep the following important considerations in mind:

1. Each Analytic Stream that you deploy places an additional load on the Internet egress points on the network.
2. Every Analytic Stream that you add impacts the Concentrators.
3. Ensure that you map Analytic Streams to Concentrators that actively collect that type of information. For example, HTTP Analytic Streams should only be activated on Concentrators that collect HTTP activity.

Analytic Stream Deployment Example - Two Gateways

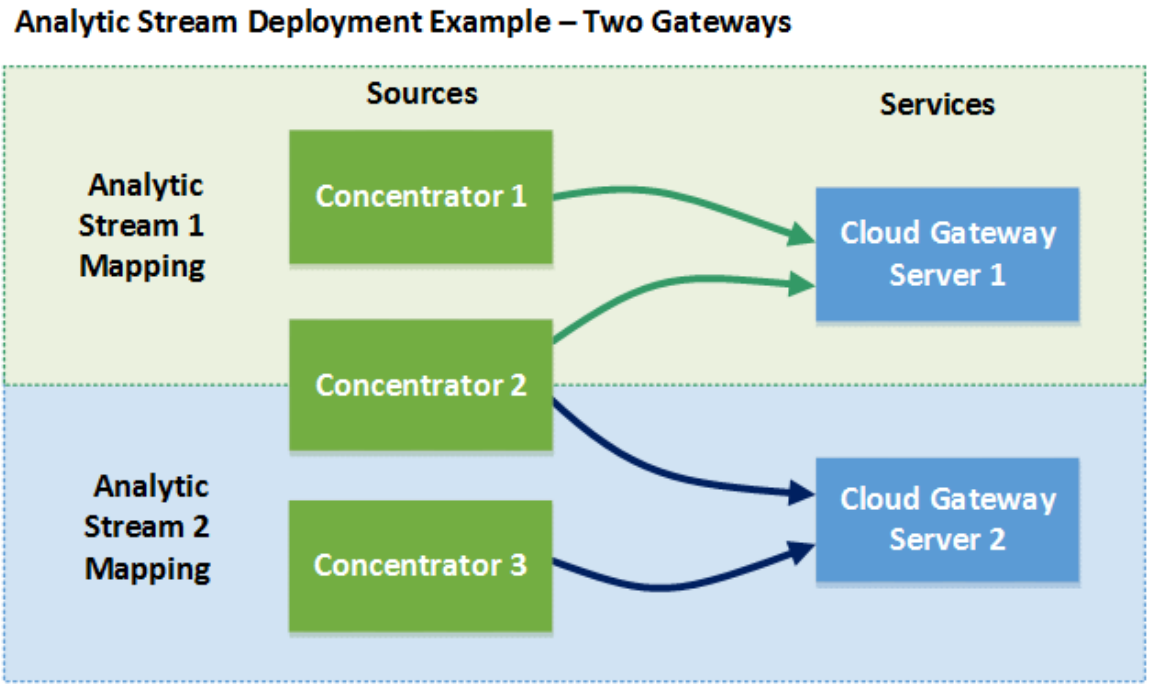
To take advantage of your additional Concentrator capacity, you can map an Analytic Stream to a Cloud Gateway service and deploy it to analyze data from multiple data sources at the same time.

For example, if you have three Concentrators and two Cloud Gateway services, you can create and deploy the following mappings:

- Map Analytic Stream 1 to the Concentrator 1 and 2 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 sends Analytic Stream 1 filtered traffic from Concentrators 1 and 2 to CBA in the Cloud.

- Map Analytic Stream 2 traffic to the Concentrator 2 and 3 sources and the Cloud Gateway Server 2 service. Cloud Gateway Server 2 sends Analytic Stream 2 filtered traffic from Concentrators 2 and 3 to CBA in the Cloud.

In this example, Analytic Stream 1 represents an Analytic Stream, such as HTTP, and Analytic Stream 2 represents another Analytic Stream, such as FTP in another location. Concentrator 1 collects HTTP activity, Concentrator 2 collects HTTP and FTP activity, and Concentrator 3 collects FTP activity.



This example shows how both services can process data from the same Concentrator. Notice that Cloud Gateway services 1 and 2 can both process data from Concentrator 2. Cloud Gateway Server 1 queries data for Analytic Stream 1 HTTP traffic and Cloud Gateway Server 2 queries different data for Analytic Stream 2 FTP traffic.

Analytic Stream Deployment Example - One Gateway

In addition to creating Analytic Stream mappings that are processed by different Cloud Gateway services, you can map more than one Analytic Stream to the same Cloud Gateway service.

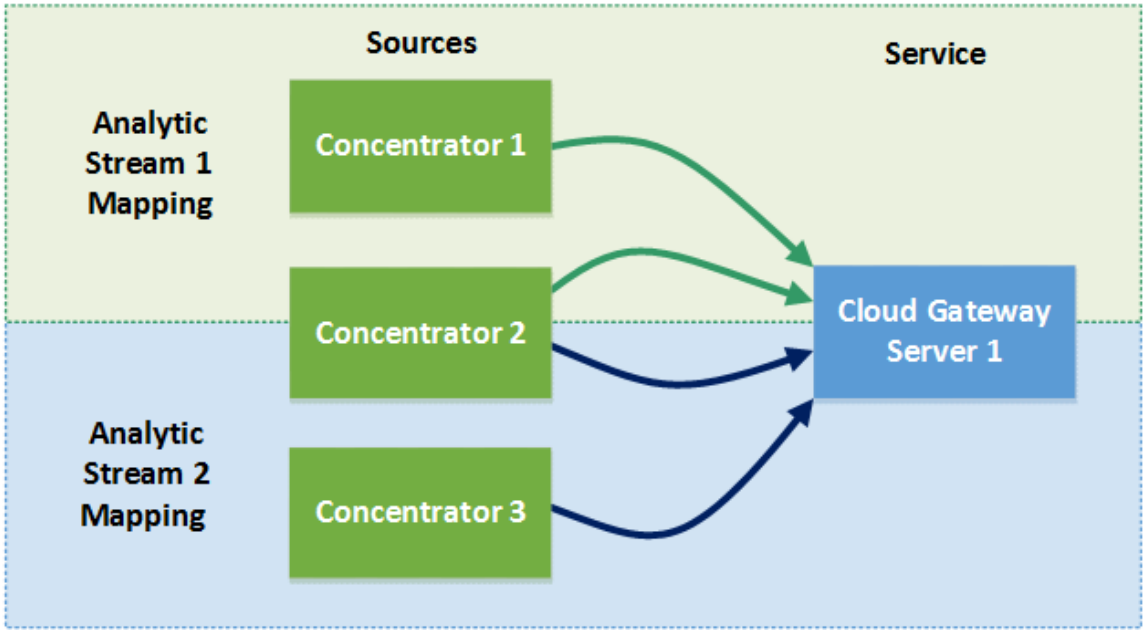
For example, if you have three Concentrators and one Cloud Gateway service, you can create and deploy the following mappings:

- Map Analytic Stream 1 to the Concentrator 1 and 2 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 sends Analytic Stream 1 filtered traffic from Concentrators 1 and 2 to CBA in the Cloud.

- Map Analytic Stream 2 to the Concentrator 2 and 3 sources and the Cloud Gateway Server 1 service. Cloud Gateway Server 1 also sends Analytic Stream 2 filtered traffic from Concentrators 2 and 3 to CBA in the Cloud.

In this example, Analytic Stream 1 represents an Analytic Stream, such as HTTP, and Analytic Stream 2 represents another Analytic Stream, such as FTP in another location. Concentrator 1 collects HTTP activity, Concentrator 2 collects HTTP and FTP activity, and Concentrator 3 collects FTP activity.

Analytic Stream Deployment Example – One Gateway



This example shows how one service can process data from more than one Analytic Stream. Notice that Cloud Gateway Server 1 can process data from Concentrators 1 and 2 for Analytic Stream 1. It also processes data from Concentrators 2 and 3 for Analytic Stream 2. Cloud Gateway Server 1 queries data for Analytic Stream 1 HTTP traffic and queries different data for Analytic Stream 2 FTP traffic and then sends that data to CBA in the Cloud for analytics processing.

Caution: Ensure that all NetWitness Platform host services are in sync with a consistent time source.

Prerequisites

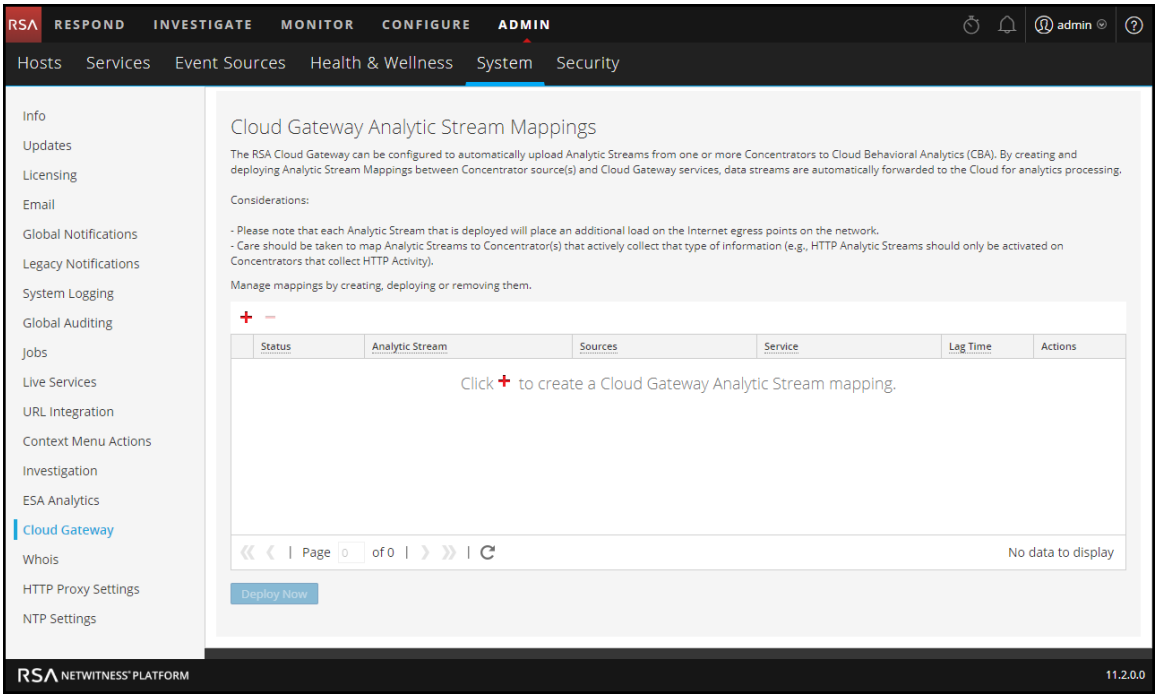
- All NetWitness Platform host services must be in sync with a consistent time source.
- The Concentrator hosts and services must be discovered and available in the NetWitness Platform user interface.
- The Cloud Gateway Server service must be provisioned. See Provision a Cloud Gateway.

Create Cloud Gateway Analytic Stream Mappings

The following procedure tells you how to map Analytic Streams to sources and services. After creating and reviewing the mappings, you deploy them so that they can start aggregating data.

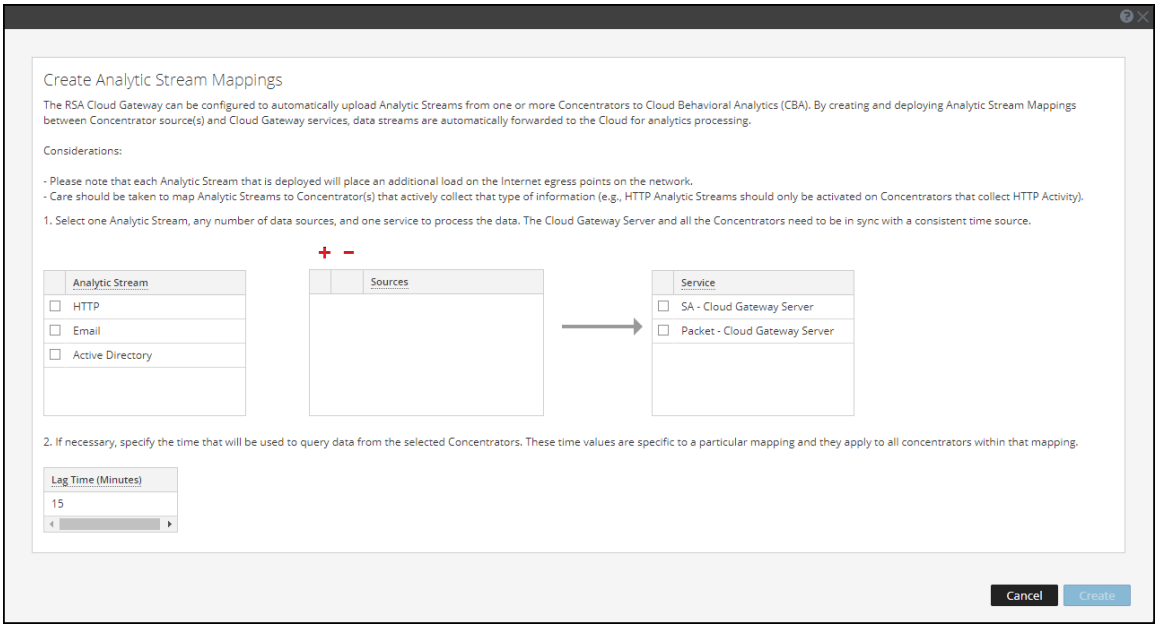
1. Go to **ADMIN > System**, and in the options panel, select **Cloud Gateway**.

   The Cloud Gateway Analytic Stream Mappings panel is displayed.



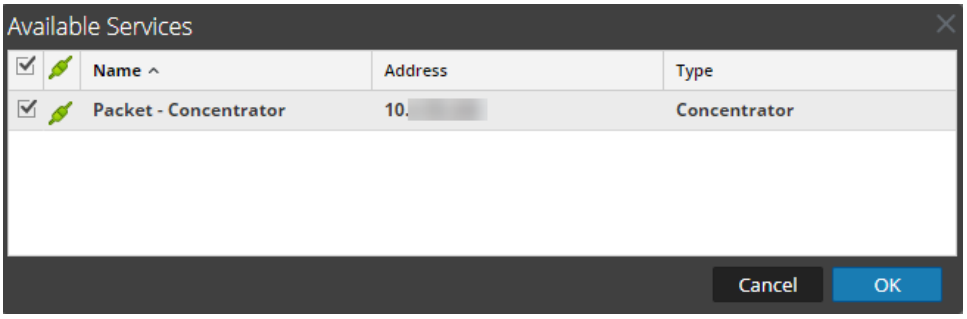
2. Click + to create an Analytic Stream mapping. Create a separate mapping for each Analytic Stream.

The **Create Analytic Stream Mappings** dialog is displayed.



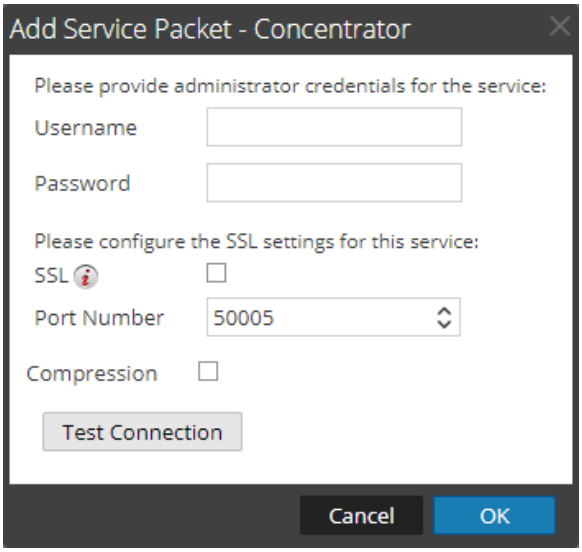
3. In the **Analytic Stream** list, select an Analytic Stream.
4. Configure one or more data sources (Concentrators) for your mappings. Do the following for each Concentrator:
   a. Click + .

      The Available Services dialog shows the data sources that are available from the ADMIN > Services view.



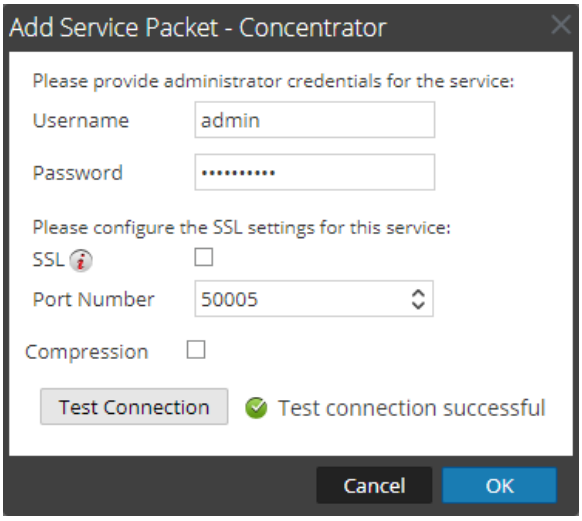
b. In the **Available Services** dialog, select a Concentrator and click **OK**.

The Add Service dialog is displayed.



c. In the **Add Service** dialog, type the Administrator username and password for the Concentrator.

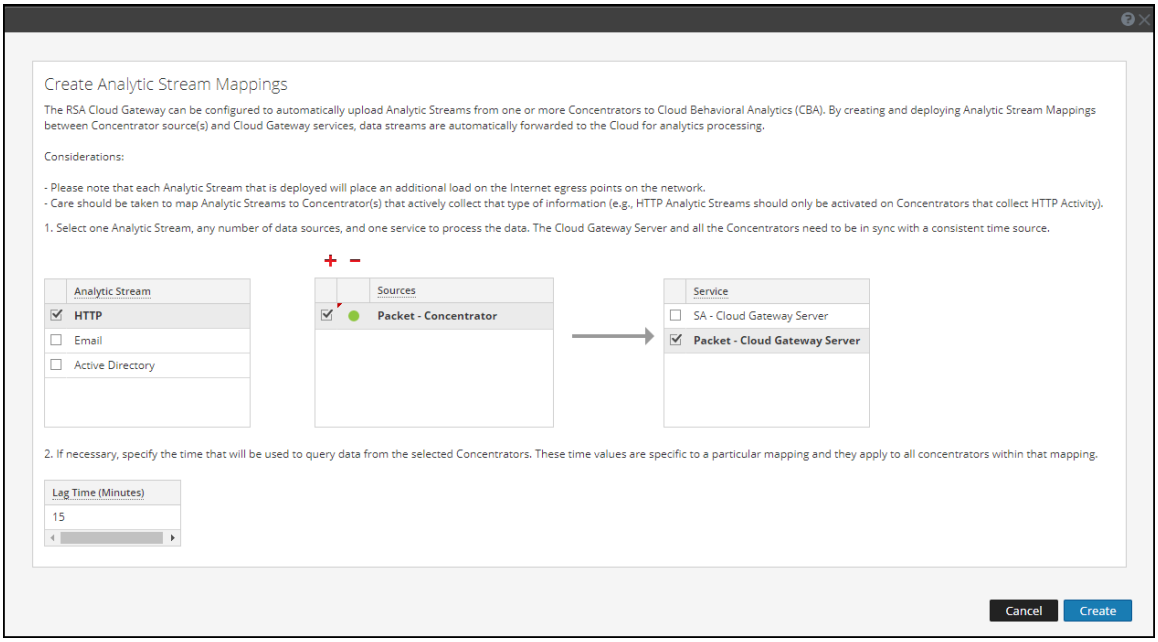
d. Click **Test Connection** to make sure that it can communicate with the Cloud Gateway service.



e. Click **OK**.

After you configure your data sources and they appear in the Sources list, you can reuse them for additional mappings.

5. In the **Sources** list, select one or more data sources to aggregate the data for the Analytic Stream.



A solid colored green circle indicates a running service and a white circle indicates a stopped service.

6. In the **Service** list, select a Cloud Gateway service to process the data for the Analytic Stream.

7. If necessary, specify the Lag Time that will be used to query data from the selected Concentrators. **Lag Time (Minutes)** specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay.

   The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data. Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window. This provides an adequate delay to ensure that all events generated in the enterprise can be processed by CBA.

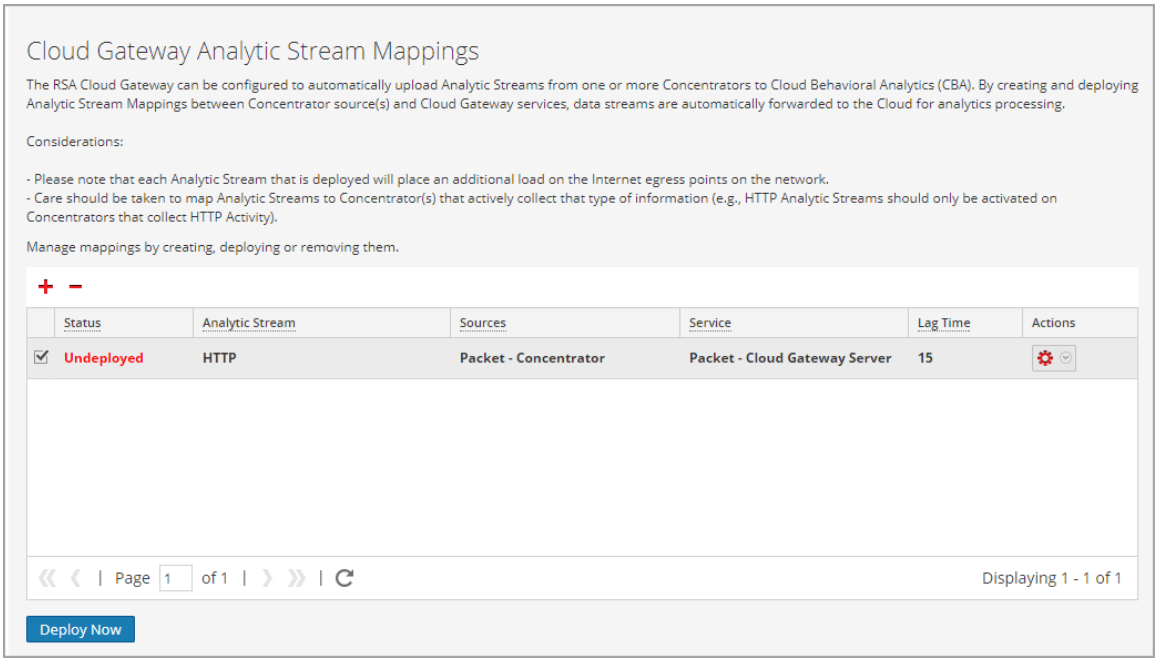
   For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on.

   Important: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data.

> **Caution:** RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation.

8. Click **Create**.

   The mappings that you create appear in the list of existing mappings with a status of **Undeployed**.



   Important: To start an Analytic Stream so that it starts aggregating data, you must deploy it.

Deploy Cloud Gateway Analytic Stream Mappings

After you create your mappings, you must deploy them in order to start aggregating data for the Analytic Streams.

1. In the list of mappings, verify that the status of the mappings that you want to deploy show as **Undeployed**.

2. Select one or more mappings with a status of Undeployed and select **Deploy Now**.

   All selected mappings in the Undeployed state start to aggregate data as configured in the mapping.

   The mapping status changes to **Deployed**.

   You cannot deploy a mapping that has already been deployed.

Update a Mapping

You can only have one mapping per Analytic Stream. If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that Analytic Stream.

You can make the following updates to a deployed mapping without deleting it:

- Undeploy the mapping
- Change the Lag Time

You can also change the Lag Time for an undeployed Analytic Stream mapping.

Undeploy a Mapping

If you want to stop aggregating data for an Analytic Stream mapping, but you do not want to delete the mapping, you can undeploy it. This gives you the option of deploying it at a later time. When you undeploy a mapping, the specified Cloud Gateway service stops pulling data from the data source for that Analytic Stream.

Caution: Undeploying a mapping with a status of Deployed affects data aggregation for that Analytic Stream.

Note: (This note applies to version 11.1.0.1 and later.) If you undeploy and then redeploy a mapping, data aggregation for that Analytic stream will start again from the last point in the aggregation when the mapping was undeployed.

To undeploy a mapping:

1. In the Cloud Gateway Analytic Stream Mappings panel, select the deployed mapping that you want to undeploy.
2. In the **Actions** column, select > **Undeploy**.

   The status changes from Deployed to Undeployed and data aggregation stops.

Delete a Mapping

You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not running, it does not affect data aggregation.

You should undeploy a mapping with a status of Deployed before deleting it. Undeploying and deleting a mapping clears the configuration on the Cloud Gateway Server, reverts the deployment for that mapping, and stops pulling data from the data source for that Analytic Stream.

Caution: Undeploying and deleting a mapping affects data aggregation for that Analytic Stream.

Note: (This note applies to version 11.1.0.1 and later.) If you undeploy and delete a mapping, then subsequently recreate the mapping, data aggregation from that Analytic Stream will start from the last point in the aggregation when the original mapping was deleted, rather than at the beginning of the original mapping.

To delete a mapping:

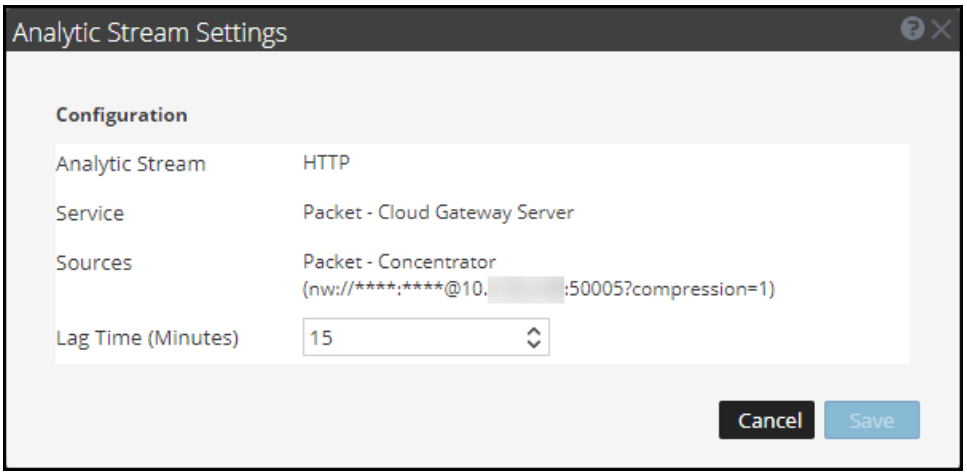
1. In the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to delete. You can only delete one mapping at a time.
2. Click .

Change the Lag Time

If necessary, you can change the Lag Time for the Analytic Stream. The Lag Time defines the buffer between the current (system) time and the time when the Analytic Stream ingests the data.

1. In the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to change and in the **Actions** column, select > **Edit stream**.

   The Analytic Stream Settings dialog shows the selected Analytic Stream, Cloud Gateway service, and data sources for the mapping. The data sources show the URLs used to communicate with the Cloud Gateway service.



2. If necessary, you can adjust the **Lag Time (Minutes)** to give the Concentrators in the mapping additional time to finish aggregating all of the data.
3. Click **Save**.

   Changes DO NOT take effect immediately. For the settings to take effect, you must undeploy and redeploy the mapping.

4. To undeploy the mapping, in the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to undeploy and then select > **Undeploy**.

   Data aggregation stops for the selected mapping.

5. To redeploy the mapping, select the mapping that you want to deploy and then select > **Deploy**.

   The selected mapping deploys and starts to aggregate data as configured in the mapping.

Monitor the Cloud Gateway

You can monitor the RSA Cloud Gateway service statistics in NetWitness Platform.

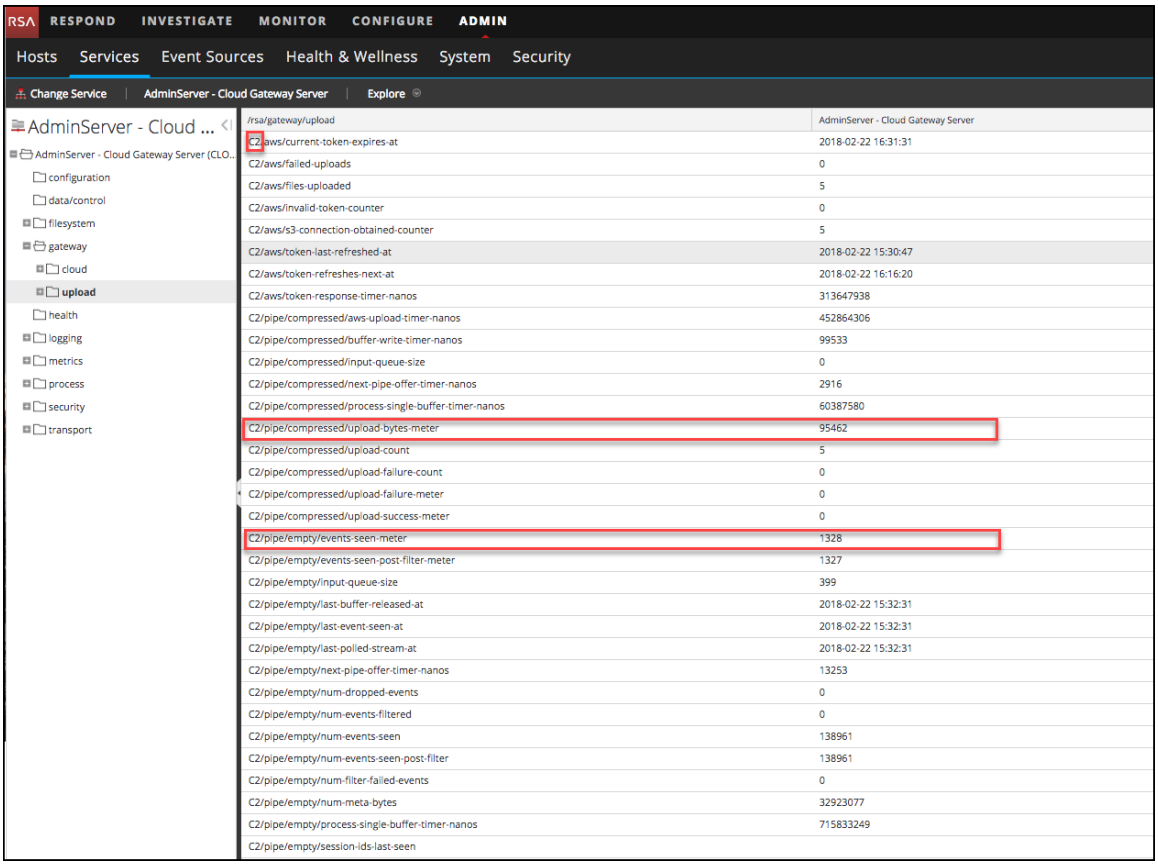
In the Services view, select the Cloud Gateway Server service and then select > **View** > **Explore**. In the Explore view, you can see important statistics that you should monitor for the Cloud Gateway. You can adjust your Analytic Stream Mappings as required.

The following figure shows two important statistics that you should look at for each stream:

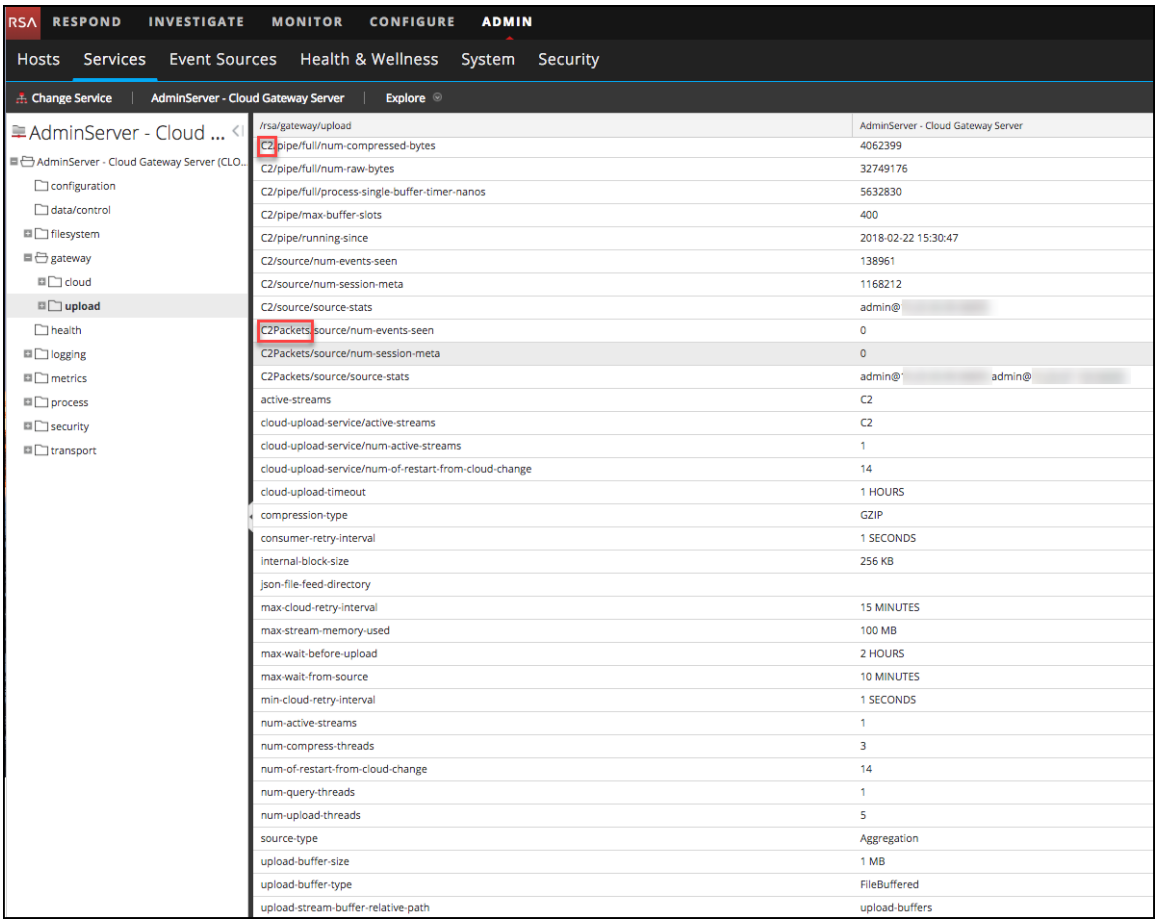
- **upload-bytes-meter**: This statistic shows the average bytes uploaded per second. It is the upload rate (bytes).
- **events-seen-meter**: This statistic shows the number of events pulled from the Concentrator per second. It is the reading rate (number).

The first part of the statistic name shows the Analytic Stream name, in this example the Analytic Stream Name is **C2**:

C2/pipe/compressed/upload-bytes-meter



If you scroll down, you can see the rest of the statistics. If you have more than one Analytic Stream, you can see statistics for that stream, too. In this example, you can see statistics for the **C2** and **C2Packets** Analytic Streams.



Note:
- Each Analytic Stream that you deploy places an additional load on the Internet egress points on the network. Look at the upload statistics, such as **upload-bytes-meter**.
- Every Analytic Stream that you add impacts the Concentrators. Look at the **events-seen-meter** statistic and see the "Monitor Service Details" topic in the *System Maintenance Guide*.
- Ensure that you map Analytic Streams to Concentrators that actively collect that type of information. For example, HTTP Analytic Streams should only be activated on Concentrators that collect HTTP activity.

Cloud Gateway References

This section contains reference information for Cloud Gateway.

See the following topics for details:

- Cloud Gateway Config View Certificate Tab
- Cloud Gateway Analytic Stream Mappings
- Analytic Stream Settings

Cloud Gateway Config View Certificate Tab

An RSA Cloud Gateway must be provisioned before it can be used for Cloud Behavioral Analytics (CBA). The Services Config view Certificate tab for the Cloud Gateway Server service enables you to provision the Cloud Gateway and view the status of the provisioning. After you provision the gateway, you can map data sources to Analytic Streams, such as HTTP or FTP traffic.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Provision the Cloud Gateway.	Provision a Cloud Gateway
Administrator	Configure data aggregation for the Cloud Gateway.	Mapping Cloud Gateway Analytic Streams
Administrator, Analyst	View detected threats.	See *NetWitness Respond User Guide* and *NetWitness Investigate User Guide*.

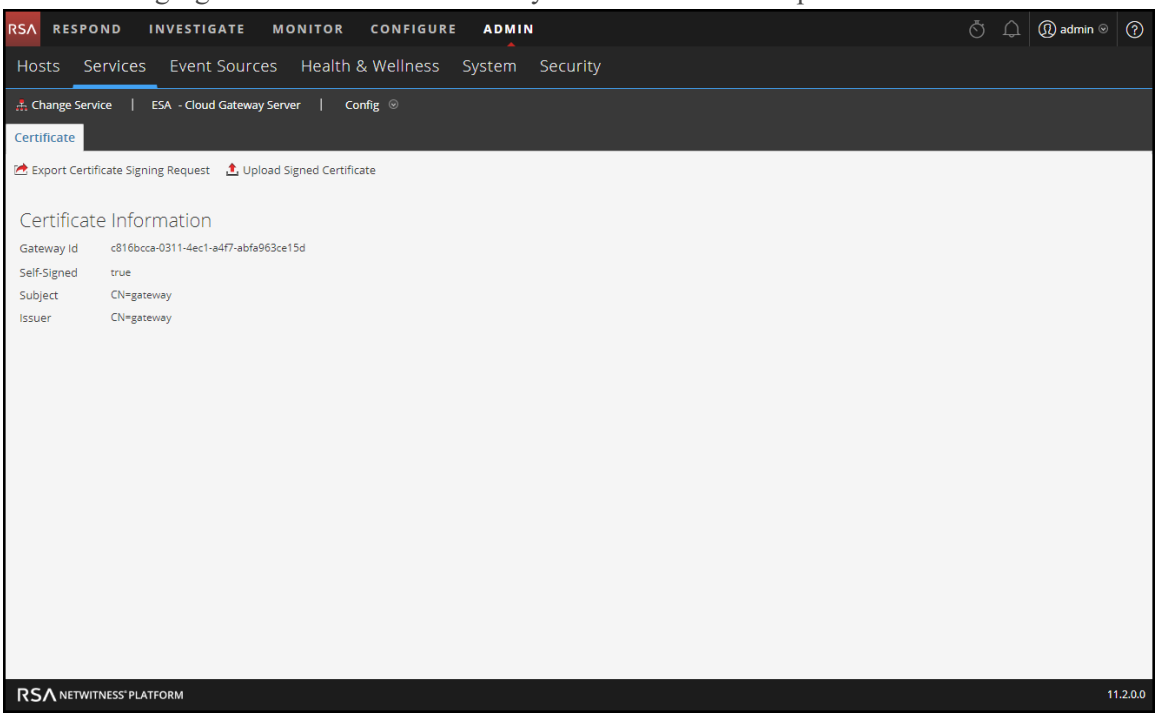
Related Topics

- RSA Cloud Behavioral Analytics
- Cloud Gateway Analytic Stream Mappings

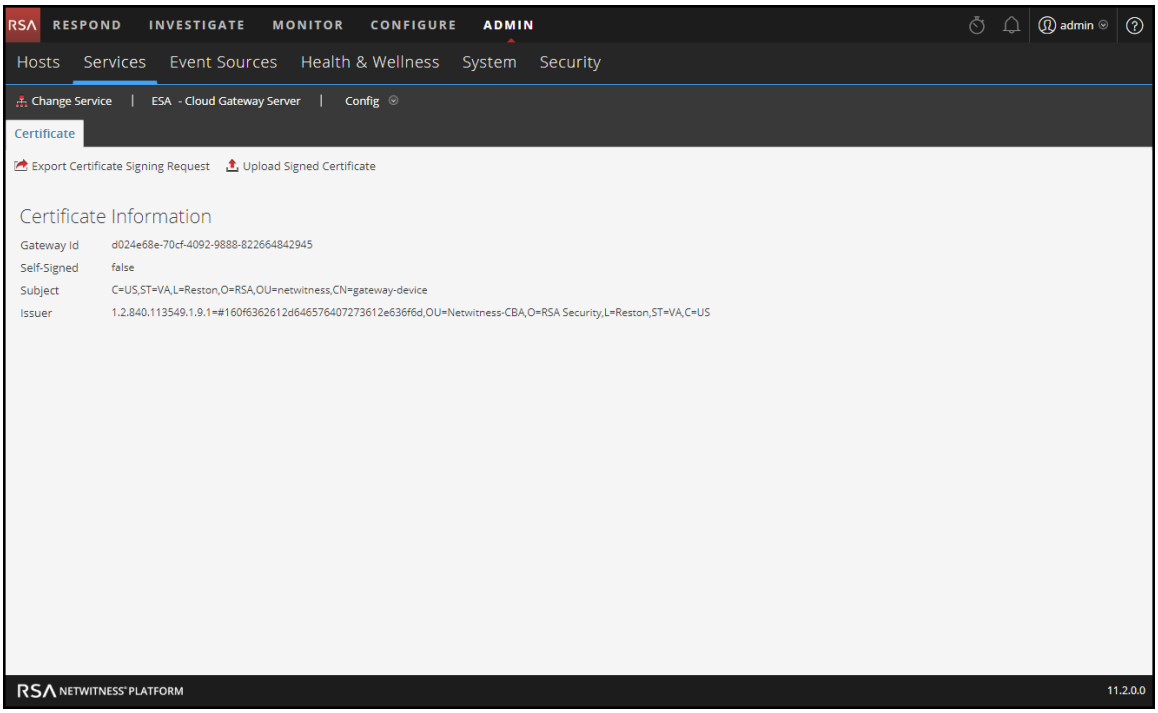
Certificate Tab

To access the Services Config view Certificate tab, in the Services view (**ADMIN > Services**), select the Cloud Gateway Server service and then select **> View > Config**.

The following figure shows a Cloud Gateway service that is NOT provisioned.



The following figure shows a provisioned Cloud Gateway service.



Certificate Information

The Certificate Information section enables you to view the provisioning status of the Cloud Gateway service.

The following table describes the Cloud Gateway Certificate Information fields.

Field	Description
Gateway ID	The Gateway ID, also known as the Service ID, identifies the gateway for RSA. You send the Gateway ID along with the CSR file to the RSA Cloud Administrator, who will provide you with a signed certificate file.
Self-Signed	If **true**, it indicates a default generated certificate. If **false**, it indicates a signed-certificate provided by RSA.
Subject	The Subject shows "CN=gateway" when the Cloud Gateway is not provisioned. It shows more detailed information when it is provisioned: • **C** = Country (for example, US) • **ST** = State or Province Name (for example, VA) • **L** = Locality Name (for example, Reston) • **O** = Organization Name (for example, RSA) • **CN** = Common Name (for example, gateway-device)
Issuer	The Issuer shows the provider of the certificate. The Issuer shows "CN=gateway" when the Cloud Gateway is not provisioned.

Toolbar Actions

This table lists the toolbar actions available in the Cloud Gateway Config view Certificate tab.

Option	Description
Export Certificate Signing Request	Click this link to create and download the Certificate Signing Request (CSR) file for your Cloud Gateway. Provide the CSR file and the Gateway ID to the RSA Cloud Administrator, who will provide you with a signed certificate.

Option	Description
Upload Signed Certificate	Click this link to install the signed certificate that you received from the RSA Cloud Administrator in your Cloud Gateway Server service.

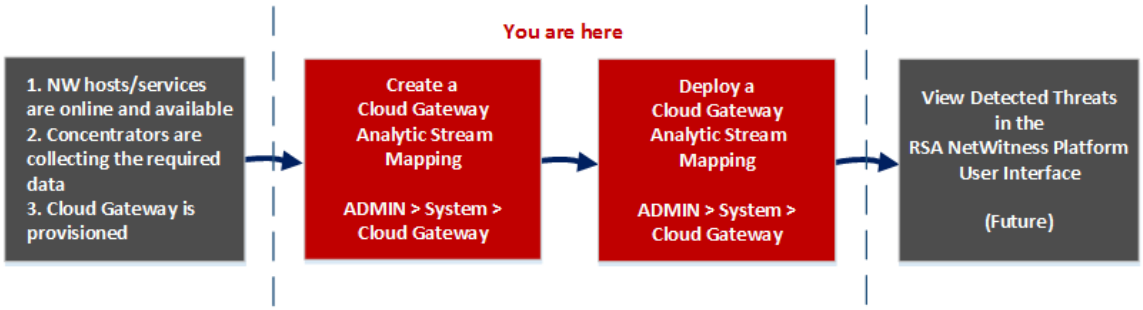
Cloud Gateway Analytic Stream Mappings

In the Cloud Gateway Analytic Stream Mappings panel (ADMIN > System > Cloud Gateway), you define the resources that RSA NetWitness Platform Cloud Behavioral Analytics (CBA) uses to automatically detect advanced threats.

You can configure the RSA Cloud Gateway to automatically upload Analytic Streams from one or more Concentrators to Cloud Behavioral Analytics (CBA). An *Analytic Stream* is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.

Workflow

This workflow shows the process for creating and enabling a Cloud Gateway Analytic Stream mapping to start automatically detecting advanced threats.



Before you create a Cloud Gateway Analytic Stream Mappings mapping, ensure that the NetWitness Platform hosts and services that you want to use for your mappings are online and available. All of the services must be in sync with a consistent time source. Ensure that the Concentrators are collecting the required data. Cloud Gateway services must be provisioned to enable Cloud Behavioral Analytics.

When you create a mapping, you select an Analytic Stream to map, such as HTTP. Then you select the data sources, such as Concentrators, to use for that Analytic Stream along with a Cloud Gateway service to process the data. When you are ready to start aggregating data, you deploy the mapping. (Future) Analysts can view detected threats for that Analytic Stream in the NetWitness Platform user interface (UI).

What do you want to do?

Role	I want to ...	Show me how
Administrator	Verify that the NetWitness Platform hosts and services are online and available.	ADMIN > Hosts and ADMIN > Services See *Hosts and Services Getting Started Guide*.
Administrator	Ensure that the Concentrators are collecting the required data.	See *Broker and Concentrator Configuration Guide*
Administrator	Provision the Cloud Gateway.	Provision a Cloud Gateway
Administrator	Create Cloud Gateway Analytic Stream mappings*	Mapping Cloud Gateway Analytic Streams
Administrator	Deploy Cloud Gateway Analytic Stream mappings*	Mapping Cloud Gateway Analytic Streams
Administrator, Analyst	View detected threats.	See *NetWitness Respond User Guide* and *NetWitness Investigate User Guide*.

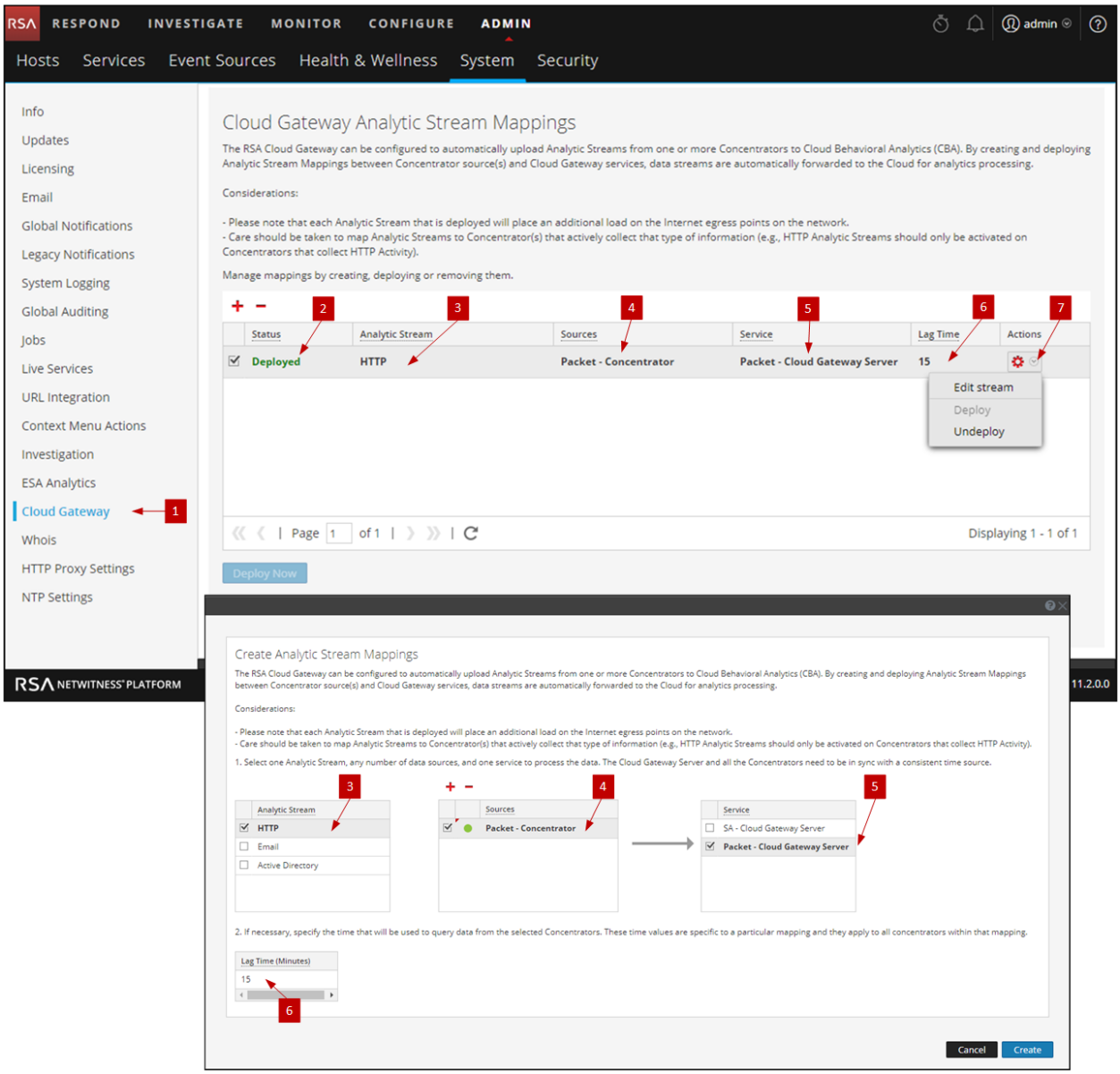
*You can complete these tasks here (that is in the Cloud Gateway Analytic Stream Mappings panel).

Related Topics

- RSA Cloud Behavioral Analytics
- Cloud Gateway Config View Certificate Tab
- Update a Mapping
- Undeploy a Mapping
- Delete a Mapping
- Change the Lag Time
- Analytic Stream Settings

Quick Look

The following example illustrates a Cloud Gateway Analytic Stream mapping. The configuration defines the data sources for the selected Analytic Stream and the Cloud Gateway service that will process the events from those data sources.



1	Displays the Cloud Gateway Analytic Stream Mappings panel.
2	Shows the status of the mapping.
3	The name of the Analytic Stream that is mapped.
4	Data sources, such as Concentrators, assigned to the mapping.

5	Cloud Gateway service that processes the data for the mapping.
6	Lag Time configuration (in minutes) on the data sources for the mapping.
7	Actions for changing Analytic Stream settings, deploying mappings, and undeploying mappings.

Toolbar

The following table describes the toolbar actions.

Icon / Button	Descripton
+	Opens the Create Mappings dialog where you can create a mapping. Create a separate mapping for each Analytic Stream. After creating and reviewing the mappings, you deploy them.
−	Deletes a Mapping. • You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not deployed and is not running, it does not affect data aggregation. • Deleting a deployed mapping clears the configuration on the host server, reverts the deployment for that mapping, and stops pulling data from the data source for that Analytic Stream. You should undeploy a mapping with a status of Deployed before deleting it.
Deploy Now	After you create your mappings, you must deploy them in order to start aggregating data for the Analytic Streams. You can select one or more mappings with a status of Undeployed to deploy.

Note: If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that Analytic Stream.

Cloud Gateway Analytic Stream Mappings

The following table describes the listed Cloud Gateway Analytic Stream mappings.

Icon / Field	Description
☑	To select an individual mapping, select the checkbox next to the mapping.

Icon / Field	Description
Status	Shows the status of the mapping. There are two statuses: **Undeployed** - An undeployed mapping maps an Analytic Stream to sources and a Cloud Gateway service. It does not start aggregating data for the Analytic Stream until you deploy the mapping. **Deployed** - A deployed mapping is deployed and running. In a deployed mapping, the selected Cloud Gateway service uses query-based aggregation to collect the appropriate filtered traffic for the selected Analytic Stream from the Concentrators.
Analytic Stream	Indicates the selected Analytic Stream. An Analytic Stream is a pipeline of selected traffic activity used for analytics processing. For example, Analytic Streams can include HTTP, FTP, SMB, or DNS traffic. By creating and deploying Analytic Stream mappings between Concentrator sources and Cloud Gateway services, data streams are automatically forwarded to the Cloud for analytics processing.
Sources	Sources are the data sources, such as Concentrators, from which the Cloud Gateway will aggregate the data for the specified Analytic Stream.
Service	Indicates the Cloud Gateway service that will process the data for the specified Analytic Stream. The selected service must be in sync with a consistent time source.

Icon / Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data. Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window. This provides an adequate delay to ensure that all events generated in the enterprise can be processed by CBA. For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation.
	Provides additional actions for the selected Analytic Stream mapping: • **Edit stream** - Enables you to configure the Lag Time for the selected mapping. • **Deploy** - Deploys the selected mapping. The specified Cloud Gateway service starts pulling data from the data sources for that Analytic Stream. • **Undeploy** - Undeploys the selected mapping. The specified Cloud Gateway service stops pulling data from the data sources for that Analytic Stream. **Caution:** Undeploying a mapping with a status of Deployed affects data aggregation for that Analytic Stream.

Analytic Stream Settings

After you create or deploy an Analytic Stream mapping in the Cloud Gateway Analytic Stream Mappings panel (ADMIN > System > Cloud Gateway), you have the option to change Analytic Stream configurations for that mapping.

What do you want to do?

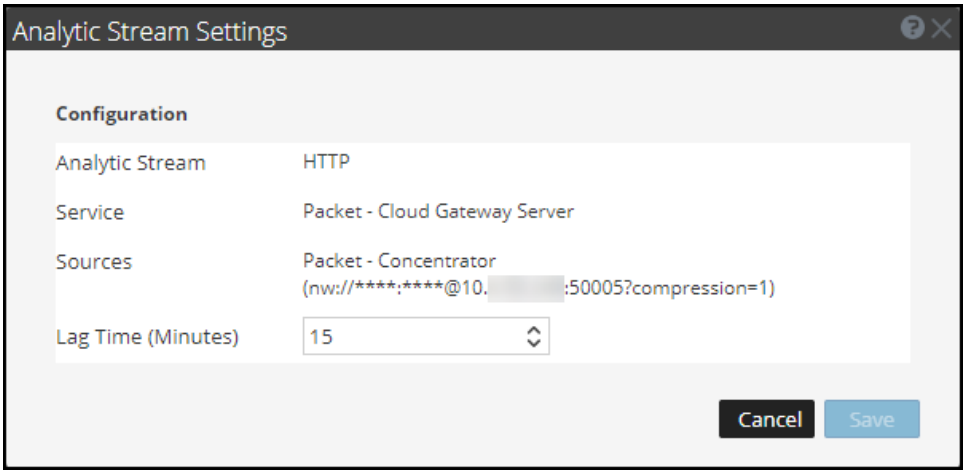
Role	I want to ...	Show me how
Administrator	Change the Lag Time for a Cloud Gateway Analytic Stream mapping.	Change the Lag Time
Administrator	Undeploy and redeploy an Analytic Stream mapping.	Change the Lag Time

Related Topics

- Mapping Cloud Gateway Analytic Streams
- Cloud Gateway Analytic Stream Mappings

Analytic Stream Settings

To access the Analytic Stream settings, in the Cloud Gateway Analytic Stream Mappings panel, select the mapping that you want to change and in the **Actions** column, select > **Edit stream**.



Configuration

The Configuration section enables you to view the Analytic Stream configuration and change the Lag Time setting.

The following table describes the settings available for a Cloud Gateway Analytic Stream mapping.

Field	Description
Analytic Stream	Shows the name of the mapped Analytic Stream.
Service	Shows the Cloud Gateway service that processes the data for the mapping.
Sources	Shows the mapped data sources and the URLs used to communicate with the Cloud gateway.

Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag Time parameter gives the Concentrator a chance to finish aggregating all of the data. Data aggregates at **Current (System) Time - Lag Time**. Setting Lag Time is useful when a Concentrator is slow in aggregating data. The Lag Time guarantees that Cloud Behavioral Analytics (CBA) does not process data that arrives to the Concentrator within the Lag Time window. This provides an adequate delay to ensure that all events generated in the enterprise can be processed by CBA. For example, if Lag Time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag Time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag Time defines the buffer between the current time and the time when the Analytic Stream ingests the data. The Lag Time value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two Analytic Streams with different Lag Times, the Concentrator uses separate Lag Time values for each Analytic Stream mapping. **Caution:** RSA recommends that Administrators adjust the Lag Time parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. To determine the correct Lag Time, add together the following to get an environmental Lag Time: 1. **Log or Packet Latency** - This is the time it takes for the Log Decoder to receive the logs or the (Packet) Decoder to receive packets. For example, the Log Decoder may get logs every 20 minutes. In this case, you would want to set Lag Time to at least 20 minutes, preferably 25 minutes, so that you do not miss events. 2. **Aggregation Latency** - This is the time it takes to get the data from the Log Decoder to the Concentrator. 3. **Other Buffer** - Add in any additional time delay specific to your environment.