webMethods CloudStreams Development Help

Version 9.12

October 2016

WEBMETHODS

This document applies to webMethods CloudStreams Version 9.12 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: WST-OH-912-20161018

Table of Contents

About this Guide

webMethods CloudStreams provides a scalable approach for the development and governance of integration flows between "Software as a Service" (SaaS) applications and "on-premise" applications.

CloudStreams provides predefined, configurable CloudStreams Connectors that enable you to connect to popular SaaS cloud applications. Using the CloudStreams plug-ins and administrative options, you configure these Connectors to govern transactions, log payloads and monitor run-time performance. You can publish and view run-time performance metrics and events using the Software AG MashZone dashboards provided by CloudStreams.

Additionally, you can use the CloudStreams framework to create custom connectors to other SaaS applications.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies storage locations for services on webMethods Integration Server, using the convention *folder.subfolder:service* .
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
Italic	Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.
`Monospace font`	Identifies text you must type or messages displayed by the system.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.

Convention	Description
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at http://documentation.softwareag.com. The site requires Empower credentials. If you do not have Empower credentials, you must use the TECHcommunity website.

Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at https://empower.softwareag.com.

To submit feature/enhancement requests, get information about product availability, and download products, go to Products.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the Knowledge Center.

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at http://techcommunity.softwareag.com. You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

1 New CloudStreams Governance Project Wizard

Use this wizard to create a CloudStreams Governance project in which you will create your virtual services, Connector Virtual Services, and their policies. You create CloudStreams Governance projects in your local file system, using the CloudStreams Development plug-in provided by Designer. Each project will contain the folders in which you will create virtual services, Connector Virtual Services, and their policies. You can create one or more projects.

To create a CloudStreams Governance project:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. The CloudStreams Governance view on the left side of the page lists all existing CloudStreams Governance projects.
3. Right-click an existing CloudStreams Governance project and click **New > CloudStreams Governance Project** (or click **File > New > Project > Software AG > CloudStreams > CloudStreams Governance Project** from the menu and click Next.

Complete the following fields in the New CloudStreams Governance Project wizard:

Project Name
A project name that is a valid resource name on your operating system. The name must not be null, cannot be an empty string, and the following invalid OS resource characters are not allowed:

- \\ (double backward slashes)
- / (forward slash)
- : (colon)
- * (asterisk)
- ? (question mark)
- " (double quote)
- < (Less Than symbol)
- > (Greater Than symbol)
- | (vertical bar)

Use Default Location
This option is selected by default. The default location is the Workspace root.

For example, if you are using C:\Workspaces\My_Workspace.. the default location would be C:\Workspaces\runtime-Eclipse Application, which is the Workspace root.

Location
Select a location in your local file system to store the new project.

Choose file system
Choose a file system, either “default” or “RSE”.

Publisher
Optional. Provide the name of the publisher of the project.

Description
Optional. Provide a description of the project.

The new CloudStreams Governance project is added to the existing projects in the CloudStreams Governance view, and it includes the default folders **Virtual Services**, **Connector Virtual Services** and **Policies**.

Note: Instead of creating a new CloudStreams Governance project, you can import an existing one. To do this, from the Designer menu click **File > Import > Software AG > CloudStreams Governance Project** and complete the dialog box that appears.

2 CloudStreams Servers Dialog Boxes

Use these dialog boxes to add and manage CloudStreams server targets. A CloudStreams server target specifies an instance of a CloudStreams server to which you will deploy your virtual services and connector virtual services.

CloudStreams Servers Dialog Box

Use this dialog box to add or remove CloudStreams servers to the target list, edit their configuration, import/export target instances, and test the server connections.

To open the CloudStreams Servers dialog box:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. Select **Window > Preferences** from the menu.
3. Expand the **Software AG** folder and click **CloudStreams Servers**.
4. In the CloudStreams Servers window, click **Add**.

Complete the following fields in the Add CloudStreams Server dialog box as follows and click **OK**:

Name
A name for the new target. Target names can contain alphanumeric characters and underscores (_) and hyphens (-).

Host
The server's host name (for example, `localhost`).

Port
The server's port number.

User
Optional. The Integration Server user who is permitted to deploy assets to this target. By default, only a member of the Integration Server's Administrator group is permitted to deploy assets to this target.

Password
Optional. The password of the Integration Server user who is permitted to deploy assets to this target. By default, the password of this user is `manage`.

Secure Connection
Indicates whether the session will be opened through HTTP or HTTPS. If you want to open an HTTPS session on the selected server using the Secure Socket Layer (SSL), select this check box. If you select this option, it is critical that you also specify the **IS Truststore Name** option for CloudStreams (in Integration Server Administrator go to **Solutions > CloudStreams > Administration > General**. Alternatively, if you want to open an HTTP session on the server, clear this check box.

Import
Use this button to import target instances from an archive file into the same Integration Server or to another instance of the server.

Export
Use this button to export target instances from the Integration Server to an archive file on the file system.

Add
Use this button to display the Add CloudStreams Servers dialog box, to add a server to the list.

Edit
Use this button to edit any parameter.

Remove
Use this button to remove the server from the list.

Test
Use this button to test the target's connection to the CloudStreams server. If the connection is not active and valid, activate the deployment endpoint and modify the user credentials as required.

Add CloudStreams Servers Dialog Box

To open the Add CloudStreams Servers dialog box: In the Designer menu, click **Window > Preferences > Software AG > CloudStreams Servers** and click the **Add** button.

Complete the following fields:

Name
A name for the new target. Target names can contain alphanumeric characters and underscores (_) and hyphens (-).

Host Name
The server's host name (for example, `localhost`).

Port
The server's port number.

User
Optional. The Integration Server user who is permitted to deploy assets to this target. By default, only a member of the Integration Server's Administrator group is permitted to deploy assets to this target.

Password
Optional. The password of the Integration Server user who is permitted to deploy assets to this target. By default, the password of this user is `manage`.

Secure Connection
Indicates whether the session will be opened through HTTP or HTTPS. If you want to open an HTTPS session on the selected server using the Secure Socket Layer (SSL), select this check box. If you select this option, it is critical that you also specify the **IS Truststore Name** option for CloudStreams (in Integration Server Administrator go to **Solutions > CloudStreams > Administration > General**. Alternatively, if you want to open an HTTP session on the server, clear this check box.

3 CloudStreams Virtual Service Editor (SOAP)

Use this editor to create and modify SOAP-based virtual services. *Virtual services* handle requests in the inbound processing scenario. When a SaaS application sends a service request, a virtual service performs security checks and other user-defined processing before sending the request to the on-premise application.

A virtual service runs on CloudStreams and acts as the consumer-facing proxy for a native service running in an on-premise application. A virtual service provides a layer of abstraction between the service consumer and the service provider, and promotes loose coupling by providing independence (of location, protocol and format) between the consuming application and the provider service. You should create a virtual service for each native service you want to expose to consumers.

When you create a virtual service, you can configure the following processing steps for the service:

- The **In Sequence step**, which you configure to manipulate the request messages. This step can include the following sub-steps:
  - The **Entry step** (provided by default), which specifies the protocol (HTTP or HTTPS) and SOAP format (1.1 or 1.2) of the requests that the virtual service will accept.
  - The **Transform step** (optional), which performs an XSLT message transformation on the request message before the virtual service submits it to the native service.
  - The **Invoke IS Service step** (optional), which pre-processes the request message before the virtual service submits it to the native service.
  - The **Routing Rule step** (provided by default), which specifies how the virtual service will route the requests to the native service endpoint. There are four ways to route HTTP or HTTPS requests:
    - "Straight Through" routing (to route requests directly to the native service endpoint).
    - "Context-Based" routing (to route specific types of messages to specific endpoints according to context-based routing rules).
    - "Content-Based" routing (to route specific types of messages to specific endpoints based on specific values that appear in the request message).
    - "Load Balancing" routing (to distribute requests among multiple endpoints).
- The service's **Out Sequence step**, which you configure to manipulate the response messages. This step can include the following sub-steps:
  - The **Transform step** (optional), which specifies how the response message from the native service provider is to be transformed before the virtual service returns it to the consuming application.
  - The **Invoke IS Service step** step (optional), which pre-processes the response message before the virtual service returns it to the consuming application.
- The service's **Error Sequence step** (provided by default). CloudStreams returns a default fault response to the consuming application, which you can customize with

context variables. This fault response is used for faults returned by the native service provider as well as faults returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors). In addition, you can:

- Choose whether or not to send the native service provider's service fault content, or just send the response message.
- Invoke IS services to pre-process or post-process the error messages.

New Virtual Service Wizard (SOAP)

To open the New Virtual Service wizard:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the CloudStreams Governance project and click **New > Virtual Service** (or expand the project, right-click the **Virtual Services** folder and click **New Virtual Service**).

Complete the following fields in the New Virtual Service wizard:

Project
The CloudStreams Governance project in which you are creating the virtual service.

Name
Assign a name for the service. Unlike native services, the names of virtual services cannot contain spaces or special characters except _ (underscore) and - (hyphen). Consequently, if you adopt a convention that involves using the name of the service as part of the virtual service name, then the names of the services themselves must not contain characters that are invalid in virtual service names.

Version
The version is always set to 1.0.

Type
Select **SOAP**.

WSDL
The WSDL that the virtual service uses. Select either **File** (and click **Browse** to select a WSDL) or select **URL** (and enter the URL of the WSDL). If you need to add a WSDL to the service later, you can leave the WSDL field blank and add the WSDL later. See "Attach WSDL Dialog Box (SOAP Virtual Service)" on page 33).

Description
Optional. A description for the virtual service. This description appears when a user displays a list of virtual services in the user interface.

General Properties (SOAP Virtual Service)

To display the general properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Click the virtual service name and then the "General" tab.

Name
(Read-only field.) The service name. You can change the service name at any time by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Service Type
(Read-only field.) **SOAP**.

Created/Last Modified
(Read-only field.) The service's creation/modification timestamps.

Target Namespace
(Read-only field.) This value is derived from the `targetNamespace` attribute of the WSDL's definition element.

Namespaces
Click the button next to this field to view the virtual service's available namespaces (see "Virtual Service Namespaces Dialog Box (SOAP Virtual Service)" on page 20).

Version
The version is always set to 1.0.

WSDL URL
Go to the "Advanced" tab and then click this URL to display the contents of the service's abstract WSDL. If a WSDL file was not added, this will be empty. You can override the WSDL by attaching a new one (see "Attach WSDL Dialog Box (SOAP Virtual Service)" on page 33).

Description
You can change the service description in the "General" tab.

Advanced Properties (SOAP Virtual Service)

To display the advanced properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.

2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Click the virtual service name and then the "Advanced" tab.

Name
(Read-only field.) The service name. You can change the name of an undeployed service by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Type
(Read-only field.) The type of the service (SOAP).

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

WSDL URL
Click this URL to display the contents of the service's abstract WSDL. You can override the WSDL by attaching a new one (see "Attach WSDL Dialog Box (SOAP Virtual Service)" on page 33).

Namespaces
Click the button next to this field to view the virtual service's available namespaces (see "Virtual Service Namespaces Dialog Box (SOAP Virtual Service)" on page 20).

Version
The version is always set to 1.0.

Description
(Read-only field.) The service description.

VSD
Click the button next to this field to view the virtual service definition (VSD). For details, see "VSD Dialog Box (SOAP Virtual Service)" on page 20.

Deployed Status
(Read-only field.) Indicates whether the service is **Deployed**, **Undeployed** or **Not Deployed** (which is the initial status before you deploy the service).

Applicable Policies
Click the button next to this field to view a list of all active policies that apply to this service. Any inactive policy that applies to the service is not listed. For details, see "Applicable Policies Dialog Box (SOAP Virtual Service)" on page 20.

Endpoint
Click the button next to this field to view the endpoint to which the virtual service is deployed, if applicable (see "Endpoint Dialog Box (SOAP Virtual Service)" on page 20).

Virtual Service Namespaces Dialog Box (SOAP Virtual Service)

This dialog box displays the virtual service's available namespaces. The namespace prefixes (such as `wsdl`, `tns`, `xsd`, `soap`, and so on) and names are displayed.

VSD Dialog Box (SOAP Virtual Service)

This dialog box displays the virtual service definition (VSD) that CloudStreams generates when you deploy a virtual service to a CloudStreams server target.

CloudStreams generates an XML document called a virtual service definition (VSD). The VSD defines the virtual service for CloudStreams, and contains all the resources required to deploy the virtual service to CloudStreams, including the policy that applies to the service.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the topic *Policy Conflict Resolution Rules* in the document *Administering webMethods CloudStreams*.

Applicable Policies Dialog Box (SOAP Virtual Service)

This dialog box lists all active policies that apply to this service. Any inactive policy that applies to the service is not listed.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the topic *Policy Conflict Resolution Rules* in the document *Administering webMethods CloudStreams*.

Endpoint Dialog Box (SOAP Virtual Service)

This dialog box displays the virtual service's CloudStreams endpoint (not the native service endpoint).

Entry Step (SOAP Virtual Service)

The Entry Step specifies the protocol (HTTP or HTTPS) and SOAP format (1.1 or 1.2) of the requests that the virtual service will accept.

This step allows you to bridge protocols between the consuming application and the native service. For example, suppose you have a native service that is exposed over HTTPS and a consuming application that submits SOAP requests over HTTP. In this situation, you can configure the virtual service's Entry Step to accept HTTP requests and configure its Routing Rule step to route the request to the Web service using HTTPS.

To configure the Entry Step:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Entry Step** and complete the following fields in the **General** page in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming restrictions.

Type
(Read-only field.) **Entry Step**.

Protocol
The protocol (HTTP or HTTPS) over which the virtual service will accept requests. To specify HTTPS, select both **HTTP** and **SSL**.

Format
The SOAP format (SOAP 1.1 or SOAP 1.2) of the requests that the virtual service will accept.

Transform Step (SOAP Virtual Service)

Add the optional Transform step if you need to transform the request message into the format required by the native service, before CloudStreams submits the message to the native service.

No message transformation is required as long as the request message structure matches the request message structure that is required by the operation associated with the `soapAction`. However, in some cases a virtual service might need to transform SOAP messages.

For example, you might need to accommodate differences between the message content that a consuming application is capable of submitting and the message content that a native service expects. For example, if the consuming application submits an order record using a slightly different structure than the structure expected by the native

service, you can use the Transform step to transform the record submitted by the consuming application to the structure required by the Web service.

In this case, you would need to create two Transform steps:

- One in the "In Sequence" step, to transform the request messages into the format required by the native service, before CloudStreams sends the requests to the native services. To do this, you pass the message to an XSLT transformation file. (Additionally in this case, the transformation is required if the virtual service has a schema validation policy that validates the requests.)
- One in the "Out Sequence" step, to transform the native service's response messages into the format required by the consumer applications, before CloudStreams returns the responses to the consumer applications.

Transform Step (Inbound, SOAP Virtual Service)

To add the Transform step (inbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Right-click **In Sequence** and click **Transform**.

   The "Transform" step is added under the Entry Step. You cannot change the order of the steps.
3. Click **Transform** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming restrictions.

XSLT Service
The XSLT file to transform the request message before it is submitted to the native service. Click **Browse** to select a file from your file system and click **Save**.

The XSL file uploaded by the user should not contain the XML declaration in it (`xml version="1.0" encoding="UTF-8"`). This is because when the virtual service is deployed to CloudStreams, CloudStreams embeds the XSL file in the virtual service definition (VSD), and since the VSD itself is in XML format, there cannot be an XML declaration line in the middle of it. This can lead to unexpected deployment issues which can be avoided by making sure the XSL file does not contain the declaration line.

> **Note:** If you make changes to the XSLT file in the future, you must re-deploy the virtual service.

Invoke IS Service Step (Inbound, SOAP Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "In Sequence" step to pre-process the request message before it is submitted to the native service. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the SOAP message.

You can use the following constructs in an IS service:

- Predefined or custom context variables. For more information, see *Using Context Variables* in the document *Administering webMethods CloudStreams*.
- The Security API provided by CloudStreams (for SOAP-based services only). For more information, see *Using the Security API in IS Services* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step:

1. Click the virtual service name in the CloudStreams Governance view.
2. Right-click **In Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the Entry Step. You cannot change the order of the steps.
3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming restrictions.

Service
The Integration Server service to pre-process the request message before it is submitted to the native service. Click **Browse** to select a file from your file system.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `MessageContext`: CloudStreams will automatically place a `MessageContext` variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these

services to extract the information they need from the `MessageContext` to build the necessary business logic.

Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Server`pub.soap.*` services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Routing Rule Step (Straight Through Routing, SOAP Virtual Service)

When you select the "Straight Through" routing protocol, the virtual service will route the requests directly to the native service endpoint you specify. You may specify how to authenticate requests (as with all routing protocols).

To configure the Routing Rule step for Straight Through routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Straight Through**.

Default To
The URL of the service to which the request is to be routed.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows:

- **Optimization Method**: Select one of the following options:
  - **None**: The default.
  - **MTOM**: Indicates that CloudStreams expects to receive a request with a Message Transmission Optimization Mechanism (MTOM) attachment, and will forward the attachment to the native service.

- **SwA**: Indicates that CloudStreams expects to receive a "SOAP with Attachment" (SwA) request, and will forward the attachment to the native service.

Bridging between SwA and MTOM is not supported. If a consumer sends an SwA request, CloudStreams can only forward SwA to the native provider. The same is true for MTOM, and applies to responses received from the native provider. That is, an SwA or MTOM response received by CloudStreams from a native provider will be forwarded to the caller using the same format it received.

When sending SOAP requests that do not contain a MTOM or SWA attachment to a virtual service for a native provider endpoint that returns an MTOM or SWA response, the request's `Accept` header must be set to `multipart/related` (or the virtual service's "In Sequence" step should include an IS service callout that sets the `BUILDER_TYPE` context variable to `multipart/related`). This is necessary so CloudStreams knows how to parse the response properly.

- **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
- **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Context-Based Routing, SOAP Virtual Service)

If you have a native service that is hosted at two or more endpoints, you can use the Context-Based routing protocol to route specific types of messages to specific endpoints according to the context-based routing rules you create.

A routing rule specifies where the requests should be routed, and the criteria by which they should be routed there. For example, requests can be routed according to certain consumers, certain dates/times, or according to requests that exceed/fall below a specified metric (Total Count, Success Count, Fault Count, etc.). You can create one or more rules. For example, you might use this capability to route requests from certain high-priority consumers to endpoints on a fast machine.

To configure the Routing Rule step for Context-Based routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Context-Based**.

Rule Name
Assign a name to the rule.

Then, click the icon next to this field and complete the Configure Routing Rule dialog box as follows:

- Choose one of the following: **Time**, **IP Address** (IPv4 or IPv6 format), **Date**, **Consumer**, **Predefined Context Variable** or **Custom Context Variable** (see the section *Using Context Variables* in the document *Administering webMethods CloudStreams*).

  Note: If you select the value **Custom Context Variable**, you must write an IS service to get/set the custom context variable, and then specify

the service in the **IS Service Name** field on the **Routing Rules** page. CloudStreams provides an API to get/set custom context variables. For more information, see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*. CloudStreams automatically declares any custom context variables you have specified; there is no need for you to declare them.

Route To

Enter the URL of the native service to route the request to, if the rule criteria are met.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows:

- **Optimization Method**: Select one of the following options:
  - **None**: The default.
  - **MTOM**: Indicates that CloudStreams expects to receive a request with a Message Transmission Optimization Mechanism (MTOM) attachment, and will forward the attachment to the native service.
  - **SwA**: Indicates that CloudStreams expects to receive a "SOAP with Attachment" (SwA) request, and will forward the attachment to the native service.

  Bridging between SwA and MTOM is not supported. If a consumer sends an SwA request, CloudStreams can only forward SwA to the native provider. The same is true for MTOM, and applies to responses received from the native provider. That is, an SwA or MTOM response received by CloudStreams from a native provider will be forwarded to the caller using the same format it received.

  When sending SOAP requests that do not contain a MTOM or SWA attachment to a virtual service for a native provider endpoint that returns an MTOM or SWA response, the request's `Accept` header must be set to `multipart/related` (or the virtual service's "In Sequence" step should include an IS service callout that sets the `BUILDER_TYPE` context variable to `multipart/related`). This is necessary so CloudStreams knows how to parse the response properly.
- **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
- **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  SSL client authentication is optional; you may leave both fields blank.
  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.

- **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

Default To
Enter a native service endpoint to route the request to in case all routing rules evaluate to False.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box, as described for the **Route To** field above.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Content-Based Routing, SOAP Virtual Service)

If you have a native service that is hosted at two or more endpoints, you can use the Context-Based routing protocol to route specific types of messages to specific endpoints based on specific values that appear in the request message.

You might use this capability, for example, to determine which operation the consuming application has requested, and route requests for complex operations to an endpoint on a fast machine.

The requests are routed according to the content-based routing rules you create. That is, they are routed based on the successful evaluation of one or more XPath expressions that are constructed utilizing the content of the request payload. For example, a routing rule might allow requests for half of the methods of a particular service to be routed to Service A, and the remaining methods to be routed to Service B.

To configure the Routing Rule step for Content-Based routing:

1. Click the virtual service name in the CloudStreams Governance view.

2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Content-Based**.

Rule Name
Assign a name to the rule.

XPath
Create an XPath expression as follows:

1. Click the icon next to this field to display the XPath Editor.
2. In the XPath Editor that appears, view the **Namespace** tab, which displays all predefined namespaces. If you want to add custom namespaces, click **Add Custom Namespace/prefix**, specify a name and value for the namespace, and click **OK**. To add additional rows, use the plus button at the end of the row to add them.
3. In the XPath Editor's **Nodes** tab, expand the namespace's node, choose the method you want for the XPath expression, and click **OK**.
4. In the XPath Editor's **Evaluator** tab, evaluate the XPath expression by specifying an argument in the **XPath Expression** field, and clicking **Evaluate**.

   The true/false result of the evaluation is displayed in the **Result** field.

To specify additional XPath expressions, use the plus button at the end of the row to add them.

> **Note:** Currently, you cannot define namespace URIs. So the XPath expressions should not include a namespace prefix.

Route To
Specify where to route the request if the rule criteria are met. Specify either the URL of the native service or a connection pool name.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows:

- **Optimization Method**: Select one of the following options:
  - **None**: The default.

- **MTOM**: Indicates that CloudStreams expects to receive a request with a Message Transmission Optimization Mechanism (MTOM) attachment, and will forward the attachment to the native service.
- **SwA**: Indicates that CloudStreams expects to receive a "SOAP with Attachment" (SwA) request, and will forward the attachment to the native service.

Bridging between SwA and MTOM is not supported. If a consumer sends an SwA request, CloudStreams can only forward SwA to the native provider. The same is true for MTOM, and applies to responses received from the native provider. That is, an SwA or MTOM response received by CloudStreams from a native provider will be forwarded to the caller using the same format it received.

When sending SOAP requests that do not contain a MTOM or SWA attachment to a virtual service for a native provider endpoint that returns an MTOM or SWA response, the request's `Accept` header must be set to `multipart/related` (or the virtual service's "In Sequence" step should include an IS service callout that sets the `BUILDER_TYPE` context variable to `multipart/related`). This is necessary so CloudStreams knows how to parse the response properly.

- **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
- **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

Default To

Enter a native service endpoint to route the request to in case all routing rules evaluate to False. Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box, as described for the **Route To** field above.

Use credentials from incoming request

Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Load Balancing Routing, SOAP Virtual Service)

If you have a Web service that is hosted at two or more endpoints, you can use the Load Balancing option to distribute requests among the endpoints.

The requests are intelligently routed based on the "round-robin" execution strategy. The load for a service is balanced by directing requests to two or more services in a pool, until the optimum level is achieved. The application routes requests to services in the pool sequentially, starting from the first to the last service without considering the individual performance of the services. After the requests have been forwarded to all the services in the pool, the first service is chosen for the next loop of forwarding.

Load-balanced endpoints also have automatic Failover capability. If a load-balanced endpoint is unavailable (for example, if a connection is refused), then that endpoint is marked as "down" for the number of seconds you specify in the **Suspend Interval** field (during which the endpoint will not be used for sending the request), and the next configured endpoint is tried. If all the configured load-balanced endpoints are down, then a SOAP fault is sent back to the client. After the suspension period expires, each endpoint marked will be available again to send the request.

To configure the Routing Rule page for Load Balancing routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Load Balancing**.

Route To
The URLs of two or more services in a pool to which the requests will be routed. The application routes the requests to services in the pool sequentially, starting from the first to the last service, without considering the individual performance of the services. After the requests have been forwarded to all the services in the pool, the first service is chosen for the next loop of forwarding.

To specify the first service, click **Endpoint** and select the URL of the Web service to route the request to.

To specify additional services, use the plus button next to the field to add rows.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows. These properties will apply to all the endpoints.

- **Optimization Method**: Select one of the following options:
  - **None**: The default.
  - **MTOM**: Indicates that CloudStreams expects to receive a request with a Message Transmission Optimization Mechanism (MTOM) attachment, and will forward the attachment to the native service.
  - **SwA**: Indicates that CloudStreams expects to receive a "SOAP with Attachment" (SwA) request, and will forward the attachment to the native service.

  Bridging between SwA and MTOM is not supported. If a consumer sends an SwA request, CloudStreams can only forward SwA to the native provider. The same is true for MTOM, and applies to responses received from the native provider. That is, an SwA or MTOM response received by CloudStreams from a native provider will be forwarded to the caller using the same format it received.

  When sending SOAP requests that do not contain a MTOM or SWA attachment to a virtual service for a native provider endpoint that returns an MTOM or SWA response, the request's `Accept` header must be set to `multipart/related` (or the virtual service's "In Sequence" step should include an IS service callout that sets the `BUILDER_TYPE` context variable to `multipart/related`). This is necessary so CloudStreams knows how to parse the response properly.
- **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
- **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.

- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

Suspend Interval
A numeric timeout value (in seconds). Default: 30. When this timeout value expires, the system routes the execution of the virtual service to the next consecutive Web service endpoint specified in the **Route To** field.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Attach WSDL Dialog Box (SOAP Virtual Service)

Use this option to attach a WSDL to an existing virtual service. The new attached WSDL will override the old WSDL. In the dialog box that appears, specify one of the following options and click **OK**:

- **URL**: Specify the URL of the WSDL to attach.
- **File**: Click **Browse** to select a WSDL from your local file system.

Note: If the new WSDL contains referenced XSDs or WSDL, they will be copied if they are resolved by CloudStreams. But if the referenced XSDs or WSDL cannot be resolved, a dialog box will prompt you whether to import the unresolved XSDs or WSDL.

Transform Step (Outbound, SOAP Virtual Service)

Add this step if you need to invoke an XSLT transformation file to transform the native service's response messages into the format required by the consumer applications, before CloudStreams returns the responses to the consumer applications. For more information about when to use the Transform step, see "Transform Step (SOAP Virtual Service)" on page 21.

To add the Transform step (outbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **Out Sequence** step in the editor.
3. Right-click **Out Sequence** and click **Transform**.

   The "Transform" step is added under the "Out Sequence" step.
4. Click **Transform** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

XSLT Service
The XSLT file to transform the response message before it is returned to the consuming application. Click **Browse** to select a file from your file system and click **Save**.

The XSL file uploaded by the user should not contain the XML declaration in it (`xml version="1.0" encoding="UTF-8"`). This is because when the virtual service is deployed to CloudStreams, CloudStreams embeds the XSL file in the virtual service definition (VSD), and since the VSD itself is in XML format, there cannot be an XML declaration line in the middle of it. This can lead to unexpected deployment issues which can be avoided by making sure the XSL file does not contain the declaration line.

> **Note:** If you make changes to the XSLT file in the future, you must re-deploy the virtual service.

Invoke IS Service Step (Outbound, SOAP Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "Out Sequence" step to pre-process the response message from the native service before it is returned to the consuming application. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the SOAP message.

You can use the following constructs in an IS service:

- Predefined or custom context variables. For more information, see *Using Context Variables* in the document *Administering webMethods CloudStreams*.
- The Security API provided by CloudStreams (for SOAP-based services only). For more information, see *Using the Security API in IS Services* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step (outbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **Out Sequence** step in the editor.
3. Right-click **Out Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the "Out Sequence" step.
4. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The Integration Server service to pre-process the request message before it is submitted to the native service. Click **Browse** to select a file from your file system.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `MessageContext`: CloudStreams will automatically place a `MessageContext` variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Error Messaging Step (SOAP Virtual Service)

CloudStreams returns a default fault response to the consuming application, which you can customize with context variables. This fault response is used for faults returned by the native service provider as well as faults returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors). In addition, you can:

- Choose whether or not to send the native service provider's service fault content, or just send the response message.
- Invoke IS services to pre-process or post-process the error messages.

You use this step to configure error messaging for a single virtual service. If you want to configure global error messaging for *all* virtual services, set the Service Fault Configuration options, which are located in the Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Service Fault Configuration**).

To configure the Error Messaging step:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **Error Sequence** step in the editor.
3. Click **Error Messaging** and complete the following fields in the Properties view.

Error Message
Select one or both of the following options:

- **Custom Failure Response Message**: Returns the following fault response to the consuming application:

  ```
  CloudStreams encountered an error:$ERROR_MESSAGE while executing
  operation:$OPERATION service:$SERVICE at time:$TIME on date:$DATE.
  The client ip was:$CLIENT_IP. The current user:$USER. The consumer
  application:$CONSUMER_APPLICATION".
  ```

  This fault response is returned in both of the following cases:

  - When a fault is returned by the native service provider.

    In this case, the `$ERROR_MESSAGE` variable in the fault response will contain the message produced by the provider's exception that caused the error. This is equivalent to the `getMessage` call on the Java Exception. This maps to the faultString element for SOAP 1.1 or the Reason element for SOAP 1.2 catch. CloudStreams discards the native service provider's fault and does not return this content to the web service caller since it could be considered a security issue, especially if the native provider is returning a stack trace with its response.

  - When a fault is returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors).

In this case, the `$ERROR_MESSAGE` variable will contain errors generated by CloudStreams.

The default fault response contains predefined fault handler variables (`$ERROR_MESSAGE`, `$OPERATION`, etc.), which are described in the document *Administering webMethods CloudStreams*.

You can customize the default fault response using the following substitution variables, where CloudStreams replaces the variable reference with the real content at run time:

- The predefined CloudStreams context variables listed in the section *The Predefined Context Variables* in the document *Administering webMethods CloudStreams*.
- Custom context variables that you declare using the CloudStreams API (see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*).

- **Native Provider Fault**: When you select this option, CloudStreams sends the native service provider's service fault content, if one is available. CloudStreams will send whatever content it received from the native service provider.

  If you select this option, the **Custom Failure Response Message** is ignored when a fault is returned by the native service provider. (Faults returned by internal CloudStreams exceptions will still be handled by the **Custom Failure Response Message** option.)

Processing Method

Optionally select either of the following:

- **Pre-Processing**: Select this option if you want to invoke an IS service to manipulate the response message before the Error Sequence step is invoked. The IS service will have access to the response message context (the axis2 `MessageContext` instance) before it is updated with the custom error message. For example, you might want to send emails or perform custom alerts based on the response payload. For more information about IS services, see "Invoke IS Service Step (Inbound, SOAP Virtual Service)" on page 23.
- **Post-Processing**: Select this option if you want to invoke an IS service to manipulate the service fault after the Error Sequence step is invoked. The IS service will have access to the entire service fault and the custom error message. You can make further changes to the fault message structure, if needed.

4 CloudStreams Virtual Service Editor (REST)

Use this editor to create and modify REST-based virtual services. *Virtual services* handle requests in the inbound processing scenario. When a SaaS application sends a service request, a virtual service performs security checks and other user-defined processing before sending the request to the on-premise application.

A virtual service runs on CloudStreams and acts as the consumer-facing proxy for a native service running in an on-premise application. A virtual service provides a layer of abstraction between the service consumer and the service provider, and promotes loose coupling by providing independence (of location, protocol and format) between the consuming application and the provider service. You should create a virtual service for each native service you want to expose to consumers.

When you create a virtual service, you can configure the following processing steps for the service:

- The **In Sequence step**, which you configure to manipulate the request messages. This step can include the following sub-steps:
  - The **Entry step** (provided by default), which specifies the protocol (HTTP or HTTPS) of the requests that the virtual service will accept. You also specify the REST resource that the service will access and the HTTP methods (GET, POST, PUT and DELETE) that the virtual service should be allowed to perform on the REST resource.
  - The **Transform step** (optional), which performs an XSLT message transformation on the request message before the virtual service submits it to the native service.
  - The **Invoke IS Service step** (optional), which pre-processes the request message before the virtual service submits it to the native service.
  - The **Routing Rule step** (provided by default), which specifies how the virtual service will route the requests to the native service endpoint. There are four ways to route HTTP or HTTPS requests:
    - "Straight Through" routing (to route requests directly to the native service endpoint).
    - "Context-Based" routing (to route specific types of messages to specific endpoints according to context-based routing rules).
    - "Content-Based" routing (to route specific types of messages to specific endpoints based on specific values that appear in the request message).
    - "Load Balancing" routing (to distribute requests among multiple endpoints).
- The service's **Out Sequence step**, which you configure to manipulate the response messages. This step can include the following sub-steps:
  - The **Transform step** (optional), which specifies how the response message from the native service provider is to be transformed before the virtual service returns it to the consuming application.
  - The **Invoke IS Service step** step (optional), which pre-processes the response message before the virtual service returns it to the consuming application.

- The service's **Error Sequence step** (provided by default). CloudStreams returns a default fault response to the consuming application, which you can customize with context variables. This fault response is used for faults returned by the native service provider as well as faults returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors). In addition, you can:
  - Choose whether or not to send the native service provider's service fault content, or just send the response message.
  - Invoke IS services to pre-process or post-process the error messages.

New Virtual Service Wizard (REST)

To open the New Virtual Service wizard:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the CloudStreams Governance project and click **New > Virtual Service** (or expand the project, right-click the **Virtual Services** folder and click **New Virtual Service**).

Complete the following fields in the New Virtual Service wizard:

CloudStreams Governance Project
The CloudStreams Governance project in which you are creating the virtual service.

Name
Assign a name for the service. Unlike native services, the names of virtual services cannot contain spaces or special characters except _ (underscore) and - (hyphen). Consequently, if you adopt a convention that involves using the name of the service as part of the virtual service name, then the names of the services themselves must not contain characters that are invalid in virtual service names.

> **Note:** If you want to change the service name after it has been created, right-click the service name in the **Virtual Services** folder and select **Rename**.

Version
The version is always set to 1.0.

Type
Select **REST**.

Description
Optional. A description for the service. This description appears when a user displays a list of services in the user interface.

REST Resources Wizard

To open the REST Resources wizard:

1. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Click the virtual service name and then click the "Advanced" tab.
2. On the **Advanced** page in the Properties view, click the **Resource** button.

Complete the following fields:

Resource
Specify the name of the REST resource that the service will access.

> **Note:** To add a REST resource to the service after the service has been created, right-click the service name and select **Attach Resource** from the context menu.

HTTP Method
The HTTP methods that the virtual service should be allowed to perform on the REST resource (GET, POST, PUT and DELETE).

It is important to specify all the HTTP methods that are supported for the virtual service. For example, if the virtual service is deployed to CloudStreams and only the GET method was selected in the virtual service definition, then CloudStreams will only permit GET invocations. A POST request will be rejected with a return of statusCode 405 even if the native service happens to support POSTs. It is also important for the native service to return the correct "Content-Type" header with its responses.

At run time, CloudStreams determines the type of a request message based on the message's HTTP method and its Content-Type. For a list of valid HTTP method/ Content-Type combinations, see the section *The Request Message's HTTP Methods and Content-Types for REST Services* in the document *Administering webMethods CloudStreams*.

Content Type
Select **Application/xml** or **Application/json**.

Query String
Specify the search string as required. Any text typed in is not case sensitive. This field is used only for documentation purposes at this time. It is not included in the service's "virtual service definition" (VSD) that is deployed to CloudStreams, so this value has no impact at runtime.

Import From
Import the schemas that the virtual service will use. Choose one of the following options. To select multiple schemas, click the plus button to add a row.

- **URL**: Specify the URL of a schema and click the **Add** button. Optionally choose the following option::
  - **URL authentication**: If you have specified a URL and the site you want to access using the URL requires user authentication, select this option. This opens an Authentication sub-dialog in which you can enter a user name and password for authentication at the URL site.
- **File**: Click **Browse** to select a schema from your local file system.

General Properties (REST Virtual Service)

To display the general properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Select the virtual service name and then select the "General" tab.

The **General** page in the Properties view displays the following properties:

Name
(Read-only field.) The service name. You can change the service name at any time by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Service Type
(Read-only field.) **REST**.

Created/Last Modified
(Read-only field.) The service's creation/modification timestamps.

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

Namespace
Specify other namespaces (such as `wsdl`, `xsd`, and so on). See "Virtual Service Namespaces Dialog Box (REST Virtual Service)" on page 45.

Version
The version is always set to 1.0.

WSDL URL
(Read-only field.) The URL of the REST resource's abstract WSDL.

Description
You can change the service description.

Advanced Properties View (REST Virtual Service)

To display the advanced properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Select the virtual service name and then select the "Advanced" tab.

Name
(Read-only field.) The service name. You can change the name of an undeployed service by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Type
(Read-only field.) The type of the service (REST).

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

WSDL URL
(Read-only field.) The URL of the REST resource's abstract WSDL.

Namespaces
Specify other namespaces (such as `wsdl`, `xsd`, and so on). See "Virtual Service Namespaces Dialog Box (REST Virtual Service)" on page 45.

Version
The version is always set to 1.0.

Description
(Read-only field.) The service description.

VSD
Click the button next to this field to view the virtual service definition (VSD). For details, see "VSD Dialog Box (REST Virtual Service)" on page 45.

Applicable Policies
Click the button next to this field to view a list of all active policies that apply to this service. Any inactive policy that applies to the service is not listed. For details, see "Applicable Policies Dialog Box (REST Virtual Service)" on page 45.

Endpoint
Click the button next to this field to view the endpoint to which the virtual service is deployed, if applicable (see "Endpoint Dialog Box (REST Virtual Service)" on page 46).

Deployed Status
(Read-only field.) Indicates whether the service is **Deployed**, **Undeployed** or **Not Deployed** (which is the initial status before you deploy the service).

Resource
Click the button next to this field to view the REST resource that the service will access. To add a REST resource to the service, right-click the service name in the CloudStreams Governance view and click **Attach Resource**.

Virtual Service Namespaces Dialog Box (REST Virtual Service)

This dialog box displays the virtual service's available namespaces. The namespace prefixes (such as `wsdl`, `tns`, `xsd`, etc.) and names are displayed.

VSD Dialog Box (REST Virtual Service)

This dialog box displays the virtual service definition (VSD) that CloudStreams generates when you deploy a virtual service to a CloudStreams server target. You cannot edit the VSD.

When you deploy a virtual service to a CloudStreams server target, CloudStreams generates an XML document called a *virtual service definition (VSD)*. The VSD defines the virtual service for CloudStreams, and contains all the resources required to deploy the virtual service to CloudStreams, including the policy that applies to the service.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the topic *Policy Conflict Resolution Rules* in the document *Administering webMethods CloudStreams* available on the Software AG Documentation website.

Applicable Policies Dialog Box (REST Virtual Service)

This dialog box lists all active policies that apply to this service. Any inactive policy that applies to the service is not listed.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined

list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the topic *Policy Conflict Resolution Rules* in the document *Administering webMethods CloudStreams*.

Endpoint Dialog Box (REST Virtual Service)

This dialog box displays the virtual service's CloudStreams endpoint (not the native service endpoint).

Entry Step (REST Virtual Service)

To configure the Entry Step:

1. Click the Virtual Service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Entry Step** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Entry Step** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Entry Step**.

Protocol
The protocol (HTTP or HTTPS) over which the virtual service will accept requests. To specify HTTPS, select both **HTTP** and **SSL**.

The Entry Step allows you to bridge protocols between the consuming application and the native service. For example, suppose you have a native service that is exposed over HTTPS and a consuming application that submits SOAP requests over HTTP. In this situation, you can configure the virtual service's Entry Step to accept HTTP requests and configure its Routing Rule step to route the request to the Web service using HTTPS.

HTTP Methods
The HTTP methods that are supported by the native service (GET, POST, PUT and DELETE).

It is important to specify all the HTTP methods that are supported for the virtual service. For example, if the virtual service is deployed to CloudStreams and only the GET method was selected in the virtual service definition, then CloudStreams will only permit GET invocations. A POST request will be rejected with a return of statusCode 405 even if the native service happens to support POSTs. It is also important for the native service to return the correct Content-Type header with its responses.

At run time, CloudStreams determines the type of a request message based on the message's HTTP method and its Content-Type. For a list of valid HTTP method/

Content-Type combinations, see the section *The Request Message's HTTP Methods and Content-Types for REST Services* in the document *Administering webMethods CloudStreams*.

Transform Step (REST Virtual Service)

Add the optional Transform step if you need to transform the request message into the format required by the native service, before CloudStreams submits the message to the native service.

As long as a consumer sends a REST request with the proper Content-Type, and as long as the HTTP method and endpoint URI are in the expected form, then CloudStreams can detect the correct service and operation; in this case, no message transformation is required. However, in some cases a virtual REST service might need to transform XML messages.

For example, you might need to accommodate differences between the message content that a consuming application is capable of submitting and the message content that a native service expects. For example, if the consuming application submits an order record using a slightly different structure than the structure expected by the native service, you can use the Transform step to transform the record submitted by the consuming application to the structure required by the Web service.

In this case, you would need to create two Transform steps:

- One in the "In Sequence" step, to transform or pre-process the request messages into the format required by the native service, before CloudStreams sends the requests to the native services. To do this, you pass the message to an XSLT transformation file. (Additionally in this case, the transformation is required if the virtual service has a schema validation policy that validates the requests.)
- One in the "Out Sequence" step, to transform or pre-process the native service's response messages into the format required by the consumer applications, before CloudStreams returns the responses to the consumer applications.

Transform Step (Inbound, REST Virtual Service)

To add the Transform step (inbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Right-click **In Sequence** and click **Transform**.

   The "Transform" step is added under the Entry Step. You cannot change the order of the steps.
3. Click **Transform** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

XSLT Service
The XSLT file to transform the request message before it is submitted to the native service. Click **Browse** to select a file from your file system and click **Save**.

The XSL file uploaded by the user should not contain the XML declaration in it (`xml version="1.0" encoding="UTF-8"`). This is because when the virtual service is deployed to CloudStreams, CloudStreams embeds the XSL file in the virtual service definition (VSD), and since the VSD itself is in XML format, there cannot be an XML declaration line in the middle of it. This can lead to unexpected deployment issues which can be avoided by making sure the XSL file does not contain the declaration line.

> **Note:** If you make changes to the XSLT file in the future, you must re-deploy the virtual service.

Invoke IS Service Step (Inbound, REST Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "In Sequence" step to pre-process the request message before it is submitted to the native service. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the SOAP message.

You can use predefined or custom context variables in an IS service. For more information, see *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step:

1. Click the virtual service name in the CloudStreams Governance view.
2. Right-click **In Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the Entry Step. You cannot change the order of the steps.
3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the request message before it is submitted to the native service.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.

- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `MessageContext`: CloudStreams will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Routing Rule Step (Straight Through Routing, REST Virtual Service)

When you select the "Straight Through" routing protocol, the virtual service will route the requests directly to the native service endpoint you specify. You may specify how to authenticate requests (as with all routing protocols).

To configure the Routing Rule step for Straight Through routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Straight Through**.

Default To
The URL of the service to which to route the request.

Configure Endpoint Properties icon
This icon displays a dialog box that enables you to configure a set of properties for each endpoint individually. In the dialog box, click the endpoint you want to configure and specify the following fields:

- **HTTP Properties**
  - **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
  - **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  Note: SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

HTTP Method
The HTTP method to pass to the native service.

Typically you want to pass each request to the native service with the same HTTP method that is contained in the request. For example, if a request contains a GET method, you allow the GET method to be passed to the native service. In this case, select the value **CUSTOM**. This variable contains the HTTP method that is contained in the request.

However, in other cases you might want to change the HTTP method of a request to a different HTTP method. In this case, you can specify the different method explicitly (by selecting the GET, POST, PUT or DELETE value), or you can specify the different method dynamically on a per-request basis. If you want to specify the method dynamically, select the **CUSTOM** option and then write an IS service to set the value of the context variable. For more information, see the section *Changing the HTTP Method of a REST Virtual Service* in the document *Administering webMethods CloudStreams*.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Context-Based Routing, REST Virtual Service)

If you have a native service that is hosted at two or more endpoints, you can use the Context-Based routing protocol to route specific types of messages to specific endpoints according to the context-based routing rules you create.

A routing rule specifies where the requests should be routed, and the criteria by which they should be routed there. For example, requests can be routed according to certain consumers, certain dates/times, or according to requests that exceed/fall below a specified metric (Total Count, Success Count, Fault Count, etc.). You can create one or more rules. For example, you might use this capability to route requests from certain high-priority consumers to endpoints on a fast machine.

To configure the Routing Rule step for Context-Based routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Context-Based**.

Rule Name
Assign a name to the rule.

Then, click the icon next to this field and complete the Configure Routing Rule dialog box as follows:

- Choose one of the following: **Time**, **IP Address** (IPv4 or IPv6 format), **Date**, **Consumer**, **Predefined Context Variable** or **Custom Context Variable** (see the section *Using Context Variables* in the document *Administering webMethods CloudStreams*).

  Note: If you select the value **Custom Context Variable**, you must write an IS service to get/set the custom context variable, and then specify the service in the **IS Service Name** field on the **Routing Rules** page. CloudStreams provides an API to get/set custom context variables. For more information, see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*. CloudStreams automatically declares any custom context variables you have specified; there is no need for you to declare them.

Route To
Enter the URL of the native service to route the request to, if the rule criteria are met.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows:

- **HTTP Properties**
  - **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
  - **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  Note: SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

HTTP Method
The HTTP method to pass to the rule.

Default To
A native service endpoint to route the request to in case all routing rules evaluate to False.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box, as described for the **Route To** field above.

HTTP Method
The HTTP method to pass to the native service.

Typically you want to pass each request to the native service with the same HTTP method that is contained in the request. For example, if a request contains a GET method, you allow the GET method to be passed to the native service. In this case, select the value **CUSTOM**. **CUSTOM** is a context variable that contains the HTTP method that is contained in the request.

However, in other cases you might want to change the HTTP method of a request to a different HTTP method. In this case, you can specify the different method explicitly (by selecting the GET, POST, PUT or DELETE value), or you can specify the different method dynamically on a per-request basis. If you want to specify the method dynamically, select the **CUSTOM** option and then write an IS service to set the value of the context variable. For more information, see the section *Changing the HTTP Method of a REST Virtual Service* in the document *Administering webMethods CloudStreams*.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Content-Based Routing, REST Virtual Service)

If you have a native service that is hosted at two or more endpoints, you can use the Context-Based routing protocol to route specific types of messages to specific endpoints based on specific values that appear in the request message.

You might use this capability, for example, to determine which operation the consuming application has requested, and route requests for complex operations to an endpoint on a fast machine.

The requests are routed according to the content-based routing rules you create.

To configure the Routing Rule step for Content-Based routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
(Read-only field.) **HTTP**.

Routing Type
Select **Content-Based**.

Rule Name
Assign a name to the rule.

XPath
The XPath field is applicable only while creating SOAP Virtual Services.

Route To
Specify where to route the request if the rule criteria are met. Specify either the URL of the native service or a connection pool name.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows:

- **HTTP Properties**
  - **Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
  - **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  Note: SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.

- **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

HTTP Method
The HTTP method to pass to the rule.

Default To
A native service endpoint to route the request to in case all routing rules evaluate to False.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box, as described for the **Route To** field above.

HTTP Method
The HTTP method to pass to the native service.

Typically you want to pass each request to the native service with the same HTTP method that is contained in the request. For example, if a request contains a GET method, you allow the GET method to be passed to the native service. In this case, select the value **CUSTOM**. **CUSTOM** is a context variable that contains the HTTP method that is contained in the request.

However, in other cases you might want to change the HTTP method of a request to a different HTTP method. In this case, you can specify the different method explicitly (by selecting the GET, POST, PUT or DELETE value), or you can specify the different method dynamically on a per-request basis. If you want to specify the method dynamically, select the **CUSTOM** option and then write an IS service to set the value of the context variable. For more information, see the section *Changing the HTTP Method of a REST Virtual Service* in the document *Administering webMethods CloudStreams*.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Routing Rule Step (Load Balancing Routing, REST Virtual Service)

If you have a native service that is hosted at two or more endpoints, you can use the Load Balancing protocol to distribute requests among the endpoints.

The requests are intelligently routed based on the "round-robin" execution strategy. The load for a service is balanced by directing requests to two or more services in a pool, until the optimum level is achieved. The application routes requests to services in the pool sequentially, starting from the first to the last service without considering the individual performance of the services. After the requests have been forwarded to all the services in the pool, the first service is chosen for the next loop of forwarding.

Load-balanced endpoints also have automatic Failover capability. If a load-balanced endpoint is unavailable (for example, if a connection is refused), then that endpoint is marked as "down" for the number of seconds you specify in the **Suspend Interval** field (during which the endpoint will not be used for sending the request), and the next configured endpoint is tried. If all the configured load-balanced endpoints are down, then a SOAP fault is sent back to the client. After the suspension period expires, each endpoint marked will be available again to send the request.

To configure the Routing Rule page for Load Balancing routing:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Routing Rule** to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Format
(Read-only field.) **HTTP**.

Routing Type
Select **Load Balancing**.

Route To
The URLs of two or more services in a pool to which the requests will be routed. The application routes the requests to services in the pool sequentially, starting from the first to the last service, without considering the individual performance of the services. After the requests have been forwarded to all the services in the pool, the first service is chosen for the next loop of forwarding.

To specify the first service, click **Endpoint** and select the URL of the Web service to route the request to.

To specify additional services, use the plus button next to the field to add rows.

Then, click the icon next to this field and complete the Configure Endpoint Properties dialog box as follows. These properties will apply to all the endpoints.

- **HTTP Properties**
  - **HTTP Connection Timeout**: The time interval (in seconds) after which a connection attempt will timeout. If a value is not specified (or if the value 0 is specified), CloudStreams will use the default value specified in Integration Server.
  - **Read Timeout**: The time interval (in seconds) after which a socket read attempt will timeout. If a value is not specified (or if the value 0 is specified), the default is 30 seconds.
- **SSL Options**: To enable SSL client authentication for the endpoint, you must specify values for both the **Client Certificate Alias** field and the **IS Keystore Alias** field. If you specify a value for only one of these fields, a deployment error will occur.

  Note: SSL client authentication is optional; you may leave both fields blank.

  - **Client Certificate Alias**: The client's private key to be used for performing SSL client authentication.
  - **IS Keystore Alias**: The keystore alias of the instance of Integration Server on which CloudStreams is running. This value (along with the value of **Client Certificate Alias**) will be used for performing SSL client authentication.

Suspend Interval
A numeric timeout value (in seconds). Default: 30. When this timeout value expires, the system routes the execution of the virtual service to the next consecutive Web service endpoint specified in the **Route To** field.

HTTP Method
The HTTP method to pass to the native service.

Typically you want to pass each request to the native service with the same HTTP method that is contained in the request. For example, if a request contains a GET method, you allow the GET method to be passed to the native service. In this case, select the value **CUSTOM**. **CUSTOM** is a context variable that contains the HTTP method that is contained in the request.

However, in other cases you might want to change the HTTP method of a request to a different HTTP method. In this case, you can specify the different method explicitly (by selecting the GET, POST, PUT or DELETE value), or you can specify the different method dynamically on a per-request basis. If you want to specify the method dynamically, select the **CUSTOM** option and then write an IS service to set the value of the context variable. For more information, see the section *Changing the HTTP Method of a REST Virtual Service* in the document *Administering webMethods CloudStreams*.

Use credentials from incoming request
Default. Authenticates requests based on the credentials specified in the HTTP header. CloudStreams passes the "Authorization" header present in the original client request to the native service.

Use specific credentials
Authenticates requests according to the values you specify in the **User**, **Password** and **Domain** fields.

Invoke service anonymously
Does not authenticate requests.

Use existing HTTP headers
Use the HTTP headers that are contained in the requests.

Customize HTTP headers
Use the HTTP headers that you specify in the **Name** and **Value** columns on the tab. If you need to specify multiple headers, use the plus button to add rows.

Transform Step (Outbound, REST Virtual Service)

Add this step if you need to invoke an XSLT transformation file to transform the native service's response messages into the format required by the consumer applications, before CloudStreams returns the responses to the consumer applications. For more information about when to use the Transform step, see "Transform Step (REST Virtual Service)" on page 47.

To add the Transform step (outbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Right-click **Out Sequence** and click **Transform**.

   The "Transform" step is added under the "Out Sequence" step. You cannot change the order of the steps.
3. Click **Transform** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

XSLT Service
The XSLT file to transform the response message before it is returned to the consuming application. Click **Browse** to select a file from your file system and click **Save**.

The XSL file uploaded by the user should not contain the XML declaration in it (`xml version="1.0" encoding="UTF-8"`). This is because when the virtual service is deployed to CloudStreams, CloudStreams embeds the XSL file in the virtual service definition (VSD), and since the VSD itself is in XML format, there cannot be an XML

declaration line in the middle of it. This can lead to unexpected deployment issues which can be avoided by making sure the XSL file does not contain the declaration line.

> **Note:** If you make changes to the XSLT file in the future, you must re-deploy the virtual service.

Invoke IS Service Step (Outbound, REST Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "Out Sequence" step to pre-process the response message from the native service before it is returned to the consuming application. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the message.

You can use predefined or custom context variables in an IS service. For more information, see the section *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step (outbound):

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **Out Sequence** step in the editor.
3. Right-click **Out Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the "Out Sequence" step. You cannot change the order of the steps.
4. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the response message before it is returned to the consuming application. Click **Browse** to select a file from your file system.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `MessageContext`: CloudStreams will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Error Messaging Step (REST Virtual Service)

CloudStreams returns a default fault response to the consuming application, which you can customize with context variables. This fault response is used for faults returned by the native service provider as well as faults returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors). In addition, you can:

- Choose whether or not to send the native service provider's service fault content, or just send the response message.
- Invoke IS services to pre-process or post-process the error messages.

You use this step to configure error messaging for a single virtual service. If you want to configure global error messaging for *all* virtual services, set the Service Fault Configuration options, which are located in the Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Service Fault Configuration**).

To configure the Error Messaging step:

1. Click the virtual service name in the CloudStreams Governance view.
2. Expand the **Error Sequence** step in the editor.
3. Click **Error Messaging** and complete the following fields in the Properties view.

Error Message
Select one or both of the following options:

- **Custom Failure Response Message**: Returns the following fault response to the consuming application:

  ```
  CloudStreams encountered an error:$ERROR_MESSAGE while executing
  operation:$OPERATION service:$SERVICE at time:$TIME on date:$DATE.
  The client ip was:$CLIENT_IP. The current user:$USER. The consumer
  application:$CONSUMER_APPLICATION".
  ```

  This fault response is returned in both of the following cases:

- When a fault is returned by the native service provider.

  In this case, the `$ERROR_MESSAGE` variable in the fault response will contain the message produced by the provider's exception that caused the error. This is equivalent to the `getMessage` call on the Java Exception. For REST service calls, the message is returned inside an `</Exception>` tag. If the response is XML, the message is returned inside `<Exception>'custom message' </Exception>`. If the response is JSON, it will be returned inside `{"Exception":"Invalid response"}`. CloudStreams discards the native service provider's fault and does not return this content to the web service caller since it could be considered a security issue, especially if the native provider is returning a stack trace with its response.

- When a fault is returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors).

  In this case, the `$ERROR_MESSAGE` variable will contain errors generated by CloudStreams.

The default fault response contains predefined fault handler variables (`$ERROR_MESSAGE`, `$OPERATION`, etc.), which are described in the document *Administering webMethods CloudStreams*.

You can customize the default fault response using the following substitution variables, where CloudStreams replaces the variable reference with the real content at run time:

- The predefined CloudStreams context variables listed in the section *The Predefined Context Variables* in the document *Administering webMethods CloudStreams*.
- Custom context variables that you declare using the CloudStreams API (see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*).

- **Native Provider Fault**: When you select this option, CloudStreams sends the native service provider's service fault content, if one is available. CloudStreams will send whatever content it received from the native service provider.

  If you select this option, the **Custom Failure Response Message** is ignored when a fault is returned by the native service provider. (Faults returned by internal CloudStreams exceptions will still be handled by the **Custom Failure Response Message** option.)

Processing Method

Optionally select either of the following:

- **Pre-Processing**: Select this option if you want to invoke an IS service to manipulate the response message before the Error Sequence step is invoked. The IS service will have access to the response message context (the axis2 `MessageContext` instance) before it is updated with the custom error message. For example, you might want to send emails or perform custom alerts based on

the response payload. For more information about IS services, see "Invoke IS Service Step (Inbound, REST Virtual Service)" on page 48.

- **Post-Processing**: Select this option if you want to invoke one or more IS services to manipulate the service fault after the Error Sequence step is invoked. The IS service will have access to the entire service fault and the custom error message. You can make further changes to the fault message structure, if needed.

5 CloudStreams Connector Virtual Service Editor (SOAP)

Use this editor to create custom SOAP-based connector virtual services. *Connector virtual services* handle requests in the outbound processing scenario. When an on-premise application sends a service request to a SaaS application, a connector virtual service handles the provider's responses and logs the requests/responses.

A connector virtual service runs on CloudStreams and acts as the consumer-facing proxy for a native service running in a SaaS application. A connector virtual service provides a layer of abstraction between the service consumer and the service provider, and promotes loose coupling by providing independence (of location, protocol and format) between the consuming application and the provider service.

CloudStreams provides a default connector virtual service for each metadata handler: the service WmCloudStreams.SoapVS (for the SOAP handler) and the service WmCloudStreams.RestVS (for the REST handler). The default services are located in the sample CloudStreams Governance project in the WmCloudStreams package. You cannot modify these default services.

Each default connector virtual service has a default policy (named Logging Policy), which logs all requests/responses to a database. You cannot modify the default policy. Alternatively, you can create additional connector virtual services with custom policies. If you create a connector virtual service with a custom policy, you can only include the actions in the "Monitoring" or "Additional" action categories; you cannot include the "WS-SecurityPolicy 1.2" actions. For example, you might want to create a custom policy that monitors run-time performance, customizes how the service invocations are logged, validates response messages against an XML schema, or optimizes server traffic.

New Connector Virtual Service Wizard (SOAP)

To open the New Connector Virtual Service wizard:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the CloudStreams Governance project and click **New > Connector Virtual Service** (or expand the project, right-click the **Connector Virtual Services** folder and click **New Connector Virtual Service**).

Project
The CloudStreams Governance project in which you are creating the connector virtual service.

Name
Assign a name for the service. Unlike native services, the names of virtual services cannot contain spaces or special characters except _ (underscore) and - (hyphen). Consequently, if you adopt a convention that involves using the name of the service as part of the virtual service name, then the names of the services themselves must not contain characters that are invalid in virtual service names.

If you want to change the service name after it has been created, right-click the service name in the **Connector Virtual Services** folder and select **Rename**. The service must be

undeployed before you can rename it (check the **Deployed Status** field in the Advanced page of the service's Properties view).

Version
The version is always set to 1.0.

Type
Select **SOAP**.

Description
Optional. A description for the service. This description appears when a user displays a list of connector virtual services in the user interface.

General Properties View (SOAP Connector Virtual Service)

To display the general properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Click the virtual service name and then select the "General" tab.

The **General** page in the Properties view displays the following properties:

Name
(Read-only field.) The service name. You can change the service name at any time by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Service Type
(Read-only field.) **SOAP**.

Created/Last Modified
(Read-only field.) The service's creation/modification timestamps.

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

Namespaces
Click the button next to this field to view other namespaces (such as `wsdl`, `xsd`, `soap`, etc.).

Version
The version is always set to 1.0.

WSDL URL
(Read-only field.) The URL of the service's WSDL.

Description
You can change the service description.

Advanced Properties View (SOAP Connector Virtual Service)

To display the advanced properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**). Click the virtual service name and then select the “Advanced” tab.

Name
(Read-only field.) The service name.

Type
(Read-only field.) The type of the service (SOAP)

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

WSDL URL
Click this URL to display the contents of the service's abstract WSDL.

Namespaces
Click the button next to this field to view other namespaces (such as `wsdl`, `xsd`, `soap`, etc.).

Version
The version is always set to 1.0.

Description
(Read-only field.) The service description.

VSD
Click the button next to this field to view the service's "virtual service definition" (VSD). This button is disabled until you deploy the connector virtual service to a CloudStreams server.

When you deploy the connector virtual service to a CloudStreams server, CloudStreams generates an XML document called a *virtual service definition (VSD)*. The VSD defines the connector virtual service for CloudStreams, and contains all the resources required to deploy the connector virtual service to a CloudStreams server, including the policy that applies to the service. You cannot edit the VSD.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective

policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the document *Administering webMethods CloudStreams*.

Deployed Status
(Read-only field.) Indicates whether the service is **Deployed**, **Undeployed** or **Not Deployed** (which is the initial status before you deploy the service).

Applicable Policies
Click the button next to this field to view a list of the active policies that apply to this service. Any inactive policy that applies to the service is not listed.

Endpoint
(Read-only field.) The endpoint is resolved when the connector service is configured and the user selects an enabled managed connection pool.

Entry Step (SOAP Connector Virtual Service)

To display the Entry Step page:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Entry Step** and view the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Entry Step**.

Protocol
(Read-only field.) The protocol of the requests that the connector virtual service will accept. The value Local means that the service can only be called from Cloud Connector Services.

Routing Rule Step (SOAP Connector Virtual Service)

To display the Routing Rule page:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and view the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
Read-only field.) **Protocol**. You cannot change the protocol over which the connector virtual service will accept requests.

Routing Type
(Read-only field.) The value **Connection Pool** means that the requests are sent to the provider using the CloudStreams connection pool. For more information about connection pools, see the documentation specific to your CloudStreams connector (for example, *webMethods CloudStreams Provider for Salesforce.com Installation and User's Guide*).

Invoke IS Service Step (Inbound, SOAP Connector Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "In Sequence" step to pre-process the request message before it is submitted to the native service. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the SOAP message.

You can use predefined or custom context variables in an IS service. For more information, see *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Right-click **In Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the Entry Step. You cannot change the order of the steps.
3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the request message before it is submitted to the native service.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `EnvelopeString`
- `MessageContext`: Integration Server will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Invoke IS Service Step (Outbound, SOAP Connector Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "Out Sequence" step to pre-process the response message from the native service before it is returned to the consuming application. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the message.

You can use predefined or custom context variables in an IS service. For more information, see the section *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step (outbound):

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Right-click **Out Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the "Out Sequence" step.
3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the response message before it is returned to the consuming application. Click **Browse** to select a file from your file system.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `EnvelopeString`
- `MessageContext`: CloudStreams will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Error Messaging Step (SOAP Connector Virtual Service)

The default connector virtual services are configured to return the native service provider's service fault, if one is available. CloudStreams will send whatever content it received from the native service provider. You can optionally invoke IS services to pre-process or post-process the error messages.

To configure the Error Messaging step:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **Error Sequence** step in the editor.
3. Click **Error Messaging** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming conventions.

Type
(Read-only field.) Error Messaging.

Error Message
Select one or both of the following options:

- **Custom Failure Response Message**: Returns the following fault response to the consuming application:

  ```
  CloudStreams encountered an error:$ERROR_MESSAGE while executing
  operation:$OPERATION service:$SERVICE at time:$TIME on date:$DATE.
  The client ip was:$CLIENT_IP. The current user:$USER. The consumer
  application:$CONSUMER_APPLICATION".
  ```

  This fault response is returned in both of the following cases:

  - When a fault is returned by the native service provider.

    In this case, the `$ERROR_MESSAGE` variable in the fault response will contain the message produced by the provider's exception that caused the error. This is equivalent to the `getMessage` call on the Java Exception. This maps to the faultString element for SOAP 1.1 or the Reason element for SOAP 1.2 catch. CloudStreams discards the native service provider's fault and does not return this content to the web service caller since it could be considered a security issue, especially if the native provider is returning a stack trace with its response.

  - When a fault is returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors).

    In this case, the `$ERROR_MESSAGE` variable will contain errors generated by CloudStreams.

  The default fault response contains predefined fault handler variables (`$ERROR_MESSAGE`, `$OPERATION`, etc.), which are described in the document *Administering webMethods CloudStreams*.

  You can customize the default fault response using the following substitution variables, where CloudStreams replaces the variable reference with the real content at run time:

  - The predefined CloudStreams context variables listed in the section *The Predefined Context Variables* in the document *Administering webMethods CloudStreams*.
  - Custom context variables that you declare using the CloudStreams API (see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*).

- **Native Provider Fault**: When you select this option, CloudStreams sends the native service provider's service fault content, if one is available. CloudStreams will send whatever content it received from the native service provider.

If you select this option, the **Custom Failure Response Message** is ignored when a fault is returned by the native service provider. (Faults returned by internal CloudStreams exceptions will still be handled by the **Custom Failure Response Message** option.)

Processing Method

Optionally select either of the following:

- **Pre-Processing**: Select this option if you want to invoke an IS service to manipulate the response message before the Error Sequence step is invoked. The IS service will have access to the response message context (the axis2 `MessageContext` instance) before it is updated with the custom error message. For example, you might want to send emails or perform custom alerts based on the response payload. For more information about IS services, see "Invoke IS Service Step (Inbound, SOAP Connector Virtual Service)" on page 68.
- **Post-Processing**: Select this option if you want to invoke one or more IS services to manipulate the service fault after the Error Sequence step is invoked. The IS service will have access to the entire service fault and the custom error message. You can make further changes to the fault message structure, if needed.

6 CloudStreams Connector Virtual Service Editor (REST)

Use this editor to create custom REST-based connector virtual services. *Connector virtual services* handle requests in the outbound processing scenario. When an on-premise application sends a service request to a SaaS application, a connector virtual service handles the provider's responses and logs the requests/responses.

A connector virtual service runs on CloudStreams and acts as the consumer-facing proxy for a native service running in a SaaS application. A connector virtual service provides a layer of abstraction between the service consumer and the service provider, and promotes loose coupling by providing independence (of location, protocol and format) between the consuming application and the provider service.

CloudStreams provides a default connector virtual service for each metadata handler: the service WmCloudStreams.RestVS (for the REST handler) and the service WmCloudStreams.SoapVS (for the SOAP handler). The default services are located in the sample CloudStreams Governance project in the WmCloudStreams package. You cannot modify these default services.

Each default connector virtual service has a default policy (named Logging Policy), which logs all requests/responses to a database. You cannot modify the default policy. Alternatively, you can create additional connector virtual services with custom policies. If you create a connector virtual service with a custom policy, you can only include the actions in the "Monitoring" or "Additional" action categories; you cannot include the "WS-SecurityPolicy 1.2" actions. For example, you might want to create a custom policy that monitors run-time performance, customizes how the service invocations are logged, validates response messages against an XML schema, or optimizes server traffic.

New Connector Virtual Service Wizard (REST)

To open the New Connector Virtual Service wizard:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the CloudStreams Governance project and click **New > Connector Virtual Service** (or expand the project, right-click the **Connector Virtual Services** folder and click **New Connector Virtual Service**).

Complete the following fields in the New Connector Virtual Service wizard:

Project
Click **Browse** and select a CloudStreams Governance project in which to create the connector virtual service.

Name
Assign a name for the service. Unlike native services, the names of virtual services cannot contain spaces or special characters except _ (underscore) and - (hyphen). Consequently, if you adopt a convention that involves using the name of the service as part of the virtual service name, then the names of the services themselves must not contain characters that are invalid in virtual service names.

If you want to change the service name after it has been created, right-click the service name in the **Connector Virtual Services** folder and select **Rename**. The service must be undeployed before you can rename it (check the **Deployed Status** field in the Advanced page of the service's Properties view).

Version
The version is always set to 1.0.

Type
Select **REST**.

Description
Optional. A description for the service. This description appears when a user displays a list of connector virtual services in the user interface.

General Properties View (REST Connector Virtual Service)

To display the general properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**.)

The **General** page in the Properties view displays the following properties:

Name
(Read-only field.) The service name. You can change the service name at any time by right-clicking the name in the **Virtual Services** folder and clicking **Rename**.

Service Type
(Read-only field.) **REST**.

Created/Last Modified
(Read-only field.) The service's creation/modification timestamps.

Target Namespace
(Read-only field.) The value is derived from the `targetNamespace` attributes of the WSDL's definition element.

Namespace
Click the button next to this field to view other namespaces (such as `wsdl`, `xsd`, etc.).

Version
The version is always set to 1.0.

WSDL URL
(Read-only field.) The URL of the service's WSDL.

Description
You can change the service description.

Advanced Properties View (REST Connector Virtual Service)

To display the advanced properties:

1. Open Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project and click the virtual service name. (If the Properties view is not already open, click **Window > Show View > Other > General > Properties**.)
3. Click the **Advanced** page in the Properties view, which displays the following properties.

Name
(Read-only field.) The service name.

Type
(Read-only field.) The type of the service (REST).

Target Namespace
(Read-only field.) The value taken from the `targetNamespace` attributes of the WSDL's definition element.

WSDL URL
Click this URL to display the contents of the service's abstract WSDL.

Namespace
Click the button next to this field to view other namespaces (such as `wsdl`, `xsd`, etc.).

Version
The version is always set to 1.0.

Description
(Read-only field.) The service description.

VSD
Click the button next to this field to view the service's "virtual service definition" (VSD). This button is disabled until you deploy the connector virtual service to a CloudStreams server.

When you deploy the connector virtual service to a CloudStreams server, CloudStreams generates an XML document called a *virtual service definition (VSD)*. The VSD defines the connector virtual service for CloudStreams, and contains all the resources required to deploy the connector virtual service to a CloudStreams server, including the policy that applies to the service. You cannot edit the VSD.

Note: If multiple policies apply to the service, CloudStreams combines all those policies into a single policy known as the *effective policy*. The effective

policy is a simple UNION of the run-time actions specified in all policies that apply to a service. To create the effective policy, CloudStreams evaluates the combined list of actions from all policies, using a set of internal rules known as Policy Conflict Resolution rules. For details, see the document *Administering webMethods CloudStreams*.

Applicable Policies
Click the button next to this field to view a list of the active policies that apply to this service. Any inactive policy that applies to the service is not listed.

Endpoint
Click the button next to this field to view the endpoint to which the virtual service is deployed (if applicable).

Deployed Status
(Read-only field.) Indicates whether the service is **Deployed**, **Undeployed** or **Not Deployed** (which is the initial status before you deploy the service).

Entry Step (REST Connector Virtual Service)

To display the Entry Step page:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Entry Step** and view the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming convention restrictions.

Type
(Read-only field.) **Entry Step**.

Protocol
(Read-only field.) The protocol of the requests that the connector virtual service will accept. The value "Local" means that the service can be called only from Cloud Connector Services.

HTTP Methods
The HTTP methods that the virtual services should be allowed to perform on the native services.

It is important to specify all the HTTP methods that are supported for the virtual services. For example, if a virtual service is deployed to CloudStreams and only the GET method was selected here, then CloudStreams will only permit GET invocations. A POST request will be rejected with a return of statusCode 405 even if the native service happens to support POSTs. It is also important for the native service to return the correct Content-Type header with its responses.

At run time, CloudStreams determines the type of a request message based on the message's HTTP method and its Content-Type. For a list of valid HTTP method/ Content-Type combinations, see the section *The Request Message's HTTP Methods and Content-Types for REST Services* in the document *Administering webMethods CloudStreams*.

Routing Rule Step (REST Connector Virtual Service)

To display the Routing Rule page:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **In Sequence** step in the editor.
3. Click **Routing Rule** and view the following fields in the Properties view.

Name
The step name, **Routing Rule**, which you may modify. There are no naming convention restrictions.

Type
(Read-only field.) **Routing Rule**.

Protocol
Read-only field.) **Protocol**. You cannot change the protocol over which the connector virtual service will accept requests.

Routing Type
(Read-only field.) The value **Connection Pool** means that the requests are sent to the provider via the CloudStreams connection pool. For more information about connection pools, see the documentation specific to your CloudStreams connector (for example, *webMethods CloudStreams Provider for Salesforce.com Installation and User's Guide*).

Invoke IS Service Step (Inbound, REST Connector Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "In Sequence" step to pre-process the request message before it is submitted to the native service. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services.

You can use predefined or custom context variables in an IS service. For more information, see *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step:

1. Click the connector virtual service name in the CloudStreams Governance view.

2. Right-click **In Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the Entry Step. You cannot change the order of the steps.

3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the request message before it is submitted to the native service.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `EnvelopeString`
- `MessageContext`: CloudStreams will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Invoke IS Service Step (Outbound, REST Connector Virtual Service)

An IS (Integration Server) service is a user-defined Integration Server flow service that you can invoke in the "Out Sequence" step to pre-process the response message from the native service before it is returned to the consuming application. You can create multiple "Invoke IS Service" steps.

An IS service must be running on the same Integration Server as CloudStreams. It can call out a C++ or Java or .NET function. It can also call other IS services to manipulate the message.

You can use predefined or custom context variables in an IS service. For more information, see the section *Using Context Variables* in the document *Administering webMethods CloudStreams*.

To add the Invoke IS Service step (outbound):

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Right-click **Out Sequence** and click **Invoke IS Service**.

   The "Invoke IS Service" step is added under the "Out Sequence" step.
3. Click **Invoke IS Service** and complete the following fields in the Properties view.

Name
You can optionally change the step name from **Invoke IS Service** to any other name. There are no naming convention restrictions.

Service
The IS Service to pre-process the response message before it is returned to the consuming application. Click **Browse** to select a file from your file system.

When you define the IS service, the **Pipeline In** section of the service should have the following input variables:

- `proxy.name`: This is the name of the virtual service.
- `SOAPEnvelope`: This is of the Java type org.apache.axiom.soap.SOAPEnvelope
- `EnvelopeString`
- `MessageContext`: CloudStreams will automatically place a MessageContext variable into the pipeline before executing the IS service call. `MessageContext` is of the Java type `org.apache.axis2.context.MessageContext`.

  Integration Server users can use the Axis2 `MessageContext` object to manipulate the incoming SOAP request. The Integration Server provides built-in services (the pub.soap.* services) to work with the `MessageContext` object to get/set/modify the SOAP body, header, properties, etc. Integration Server users should use these services to extract the information they need from the `MessageContext` to build the necessary business logic.

  Users do not need to understand Axis2 or Axiom (the XML object model based on StAX) to work with the SOAP request, because if they are familiar with the Integration Serverpub.soap.* services, they can accomplish most of the tasks. For more information about these related Integration Server services, see the *webMethods Integration Server Built-In Services Reference*.

Error Messaging Step (REST Connector Virtual Service)

The default connector virtual services are configured to return the native service provider's service fault, if one is available. CloudStreams will send whatever content it received from the native service provider. You can optionally invoke IS services to pre-process or post-process the error messages.

To configure the Error Messaging step:

1. Click the connector virtual service name in the CloudStreams Governance view.
2. Expand the **Error Sequence** step in the editor.
3. Click **Error Messaging** and complete the following fields in the Properties view.

Name
You can optionally change the step name to any other name. There are no naming conventions.

Type
(Read-only field.) Error Messaging.

Error Message
Select one or both of the following options:

- **Custom Failure Response Message**: Returns the following fault response to the consuming application:

  ```
  CloudStreams encountered an error:$ERROR_MESSAGE while executing
  operation:$OPERATION service:$SERVICE at time:$TIME on date:$DATE.
  The client ip was:$CLIENT_IP. The current user:$USER. The consumer
  application:$CONSUMER_APPLICATION".
  ```

  This fault response is returned in both of the following cases:

  - When a fault is returned by the native service provider.

    In this case, the `$ERROR_MESSAGE` variable in the fault response will contain the message produced by the provider's exception that caused the error. This is equivalent to the `getMessage` call on the Java Exception. CloudStreams discards the native service provider's fault and does not return this content to the web service caller since it could be considered a security issue, especially if the native provider is returning a stack trace with its response.

  - When a fault is returned by internal CloudStreams exceptions (policy violation errors, cloud connection errors and cloud connector service errors).

    In this case, the `$ERROR_MESSAGE` variable will contain errors generated by CloudStreams.

The default fault response contains predefined fault handler variables (`$ERROR_MESSAGE`, `$OPERATION`, etc.), which are described in the document *Administering webMethods CloudStreams*.

You can customize the default fault response using the following substitution variables, where CloudStreams replaces the variable reference with the real content at run time:

- The predefined CloudStreams context variables listed in the section *The Predefined Context Variables* in the document *Administering webMethods CloudStreams*.
- Custom context variables that you declare using the CloudStreams API (see the section *The API for Context Variables* in the document *Administering webMethods CloudStreams*).

- **Native Provider Fault**: When you select this option, CloudStreams sends the native service provider's service fault content, if one is available. CloudStreams will send whatever content it received from the native service provider.

  If you select this option, the **Custom Failure Response Message** is ignored when a fault is returned by the native service provider. (Faults returned by internal CloudStreams exceptions will still be handled by the **Custom Failure Response Message** option.)

Processing Method

Optionally select either of the following:

- **Pre-Processing**: Select this option if you want to invoke an IS service to manipulate the response message before the Error Sequence step is invoked. The IS service will have access to the response message context (the axis2 `MessageContext` instance) before it is updated with the custom error message. For example, you might want to send emails or perform custom alerts based on the response payload. For more information about IS services, see "Invoke IS Service Step (Outbound, REST Connector Virtual Service)" on page 79.
- **Post-Processing**: Select this option if you want to invoke one or more IS services to manipulate the service fault after the Error Sequence step is invoked. The IS service will have access to the entire service fault and the custom error message. You can make further changes to the fault message structure, if needed.

7 CloudStreams Policy Editor

Use this editor to create policies for virtual services and connector virtual services.

A *policy* provides run-time governance capabilities to a virtual service or a connector virtual service. A policy is a sequence of actions that are carried out by CloudStreams when a consumer requests a particular service through CloudStreams. The actions in a policy perform activities such as identifying/authenticating consumers, validating digital signatures and capturing performance measurements.

You should create a policy for each virtual service. You can apply a single policy to one or more virtual services. A policy for virtual services can include the following kinds of actions:

- **WS-SecurityPolicy 1.2 actions:**

  CloudStreams provides two kinds of actions that support WS-SecurityPolicy 1.2: authentication actions and XML security actions.

  The authentication actions verify that the requests for virtual services contain a specified WS-SecurityPolicy element:

  - **Require SAML Token**: Requires that a WSS Security Assertion Markup Language (SAML) assertion token be present in the SOAP message header to validate service consumers.
  - **Require WSS Username Token**: Requires that a WSS username token and password be present in the SOAP message header to validate service consumers.
  - **Require X.509 Token**: Requires that a WSS X.509 token be present in the SOAP message header to validate service consumers.

  The XML security actions provide confidentiality (through encryption) and integrity (through signatures) for request and response messages. CloudStreams includes the following XML security actions:

  - **Require Signing**: Requires that a request's XML element (which is represented by an XPath expression) be signed.
  - **Require Encryption**: Requires that a request's XML element (which is represented by an XPath expression) be encrypted.
  - **Require SSL**: Requires that requests be sent via SSL client certificates and can be used with both SOAP and REST services.
  - **Include Timestamps**: Requires that timestamps be included in the request header. CloudStreams checks the timestamp value against the current time to ensure that the request is not an old message. This serves to protect your system against attempts at message tampering, such as replay attacks.

- **Monitoring actions:**

  CloudStreams includes the following run-time monitoring actions:

  - **Monitor Service Performance**: This action monitors a user-specified set of run-time performance conditions for a virtual service, and sends alerts to a specified destination when these performance conditions are violated.

- **Monitor Service Level Agreement**: This action provides the same functionality as "Monitor Service Performance", but this action is different because it enables you to monitor a virtual service's run-time performance especially for particular consumer(s). You can configure this action to define a *Service Level Agreement* (SLA), which is set of conditions that defines the level of performance that a specified consumer should expect from a service.
- **Throttling Traffic Optimization**: Limits the number of service invocations during a specified time interval, and sends alerts to a specified destination when the performance conditions are violated. You can use this action to avoid overloading the back-end services and their infrastructure, to limit specific consumers in terms of resource usage, etc.

- **Additional actions:**

  CloudStreams provides the following actions, which you can use in conjunction with the actions above.

  - **Identify Consumer**: You use this action in conjunction with an authentication action ("Require WSS Username Token", "Require X.509 Token", or "Require HTTP Basic Authentication"). Alternatively, this action can be used alone to identify consumers only by host name or IP address.
  - **Require HTTP Basic Authentication**, which uses HTTP basic authentication to verify the user name and passwords of consumers against the Integration Server's user account.
  - **Authorize User**, which authorizes consumers against a list of users and/or a list of groups registered in the Integration Server. You use this action in conjunction with an authentication action ("Require WSS Username Token", "Require SAML Token", or "Require HTTP Basic Authentication").
  - **Log Invocation**, which logs request/response payloads.
  - **Validate Schema**, which validates all XML request and/or response messages against an XML schema referenced in the WSDL.

Each default connector virtual service has a default policy, which you cannot modify. However, you can create additional connector virtual services with custom policies. If you create a connector virtual service with a custom policy, you can include only the monitoring, logging, and schema validation actions. (The virtual services, which receive the inbound requests, handle the security.) For example, you might want to create a custom policy that monitors run-time performance, customizes how the service invocations are logged, or optimizes server traffic.

When you create or modify a policy, you:

1. Specify the services to which the policy should apply. A policy can apply to one or more virtual services or to one or more connector virtual services, but not to both types of services.
2. Add the desired actions to the policy and configure their parameters.

3. Activate the policy when you are ready to put it into effect. When you deploy the virtual services or connector virtual services to which the policy is applied, the policy will also be deployed.

Create a New Policy Wizard

To open the New Policy wizard:

1. Open Designer and display the CloudStreams Development perspective.
2. In the CloudStreams Governance view, expand your CloudStreams Governance project folder, right-click the **Policies** folder and click **New Policy**.

Project
The CloudStreams Governance project in which you are creating the policy.

Name
Assign a name for the policy. A policy name can contain any character (including spaces).

> **Note:** If you want to change the policy name after it has been created, right-click the policy name in the **Policies** folder and select **Rename**.

Service Type
Specify whether the policy will be applied to a virtual service or to a connector virtual service.

Description
Optional. A description for the policy. This description appears when a user displays a list of policies in the user interface.

Criteria
Click "Next" to apply the policy to services that meet certain criteria.

In the next dialog box, specify the criteria as follows:

1. In the **Criteria** field, specify a value (**SOAP** or **REST**) for the **Service Type** attribute. That is, specify whether the policy should apply to all SOAP services or all REST services.
2. Click the plus button next to the **Criteria** field to add a new row, and choose another criteria attribute (**Name** or **Description**) and choose an operator and value for it. For example, specify whether the policy should apply to all SOAP services that equals, starts with or contains the prefix `Abc_`.
3. Repeat step 2 if desired to specify additional criteria.
4. If you specify multiple criteria, use the **Condition** field to connect the criteria by the AND or OR operator. The default operator is AND.

Note: If you do not specify any criteria, the policy will apply to all virtual services.

Caution: CloudStreams checks for policy conflicts when you deploy a virtual service. If the service has only one policy applied to it (e.g., the policy you are applying here), that policy is deployed to CloudStreams, and CloudStreams executes the policy's run-time actions in the order in which they are specified in the policy. However, if the service already has another policy applied to it, a policy conflict might occur. A policy conflict might have unintended consequences. CloudStreams will warn you of policy conflicts. For more information, see the section *What Happens When You Deploy a Service?* in the document *Administering webMethods CloudStreams*.

General Properties View (Policy)

To edit General properties, click the policy name in the CloudStreams Governance **view.**

Name
(Read-only field.) The policy name. You can change the name by right-clicking it in the **Policies** folder and clicking **Rename**.

Status
(Read-only field). Indicates whether the policy is **Active** or **Inactive**. To activate/deactivate the policy, right-click the policy name in the CloudStreams Governance view and click **Active** or **Inactive**. You will not be allowed to activate the policy unless all of its action parameters have been set.

Virtual Service Type
(Read-only field). Virtual Service or Connector Virtual Service.

Description
You can change the description.

Criteria
Click the button next to this field to change the criteria for the services to which the policy applies. (Alternatively, right-click the policy name in the **Policies** folder and click **Criteria**.)

In the Criteria dialog box that appears, specify the criteria as follows:

1. In the **Criteria** field, specify a value (**SOAP** or **REST**) for the **Service Type** attribute. That is, specify whether the policy should apply to all SOAP services or all REST services.
2. Click the plus button next to the **Criteria** field to add a new row, and choose another criteria attribute (**Name** or **Description**) and choose an operator and value for it. For example, specify whether the policy should apply to all SOAP services that equals, starts with or contains the prefix `Abc_`.
3. Repeat step 2 if desired to specify additional criteria.

4. If you specify multiple criteria, use the **Condition** field to connect the criteria by the AND or OR operator. The default operator is AND.

Action: Authorize User

Note: Dependency requirement: A policy that includes this action must also include one of the following actions: Require HTTP Basic Authentication, Require WSS Username Token or Require SAML Token.

This action authorizes consumers against a list of users and/or a list of groups registered in the Integration Server on which CloudStreams is running.

To set the Authorize User action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, click **Authorize User** in the **Applied Actions** list, and set the following action parameters.

User
Authorizes consumers against a list of users who are registered in the Integration Server instance on which CloudStreams is running.

Group
Authorizes consumers against a list of groups who are registered in the Integration Server instance on which CloudStreams is running.

Note: By default, both of these input parameters are selected. If you de-select one of these parameters, the fields showing the list of users (or groups) is not displayed.

Action: Identify Consumer

This action specifies the kind of consumer identifier (IP address, HTTP authorization token, etc.) that CloudStreams will use to identify consumer applications. You can select only one identifier. Alternatively, this action provides an option to allow anonymous users to send requests, without restriction.

To set the Identify Consumer action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Identify Consumer** in the **Applied Actions** list, and set the following action parameters.

Anonymous Usage Allowed
Specifies whether to allow anonymous users to send requests, without restriction.

IP Address

Right-click the action name and click **Add IP Address** to identify consumer applications based on their originating IP addresses.

Host Name

Right-click the action name and click **Add Host Name** to identify consumer applications based on a host name.

HTTP Token

Right-click the action name and click **Add HTTP Token** if you want to use HTTP Basic authentication to verify the consumer's authentication credentials contained in the request's Authorization header. CloudStreams authorizes the credentials against the list of users registered in the Integration Server on which CloudStreams is running. This type of consumer authentication is referred to as "preemptive authentication". If you want to use "preemptive authentication", you should also include the action "Require HTTP Basic Authentication" in the policy.

If you choose to omit "Require HTTP Basic Authentication", the client will be presented with a security challenge. If the client successfully responds to the challenge, the user is authenticated. This type of consumer authentication is referred to as "non-preemptive authentication".

> **Note:** If you select the value **HTTP Token**, do not include the "Authorize Against Registered Consumers" action in the policy. This is an invalid combination.

WSS Header Token

Right-click the action name and click **Add WSS Header Token** to validate user names and passwords that are transmitted in the SOAP message header in the WSS Username Token. If you select this option, you should also include the action **Require WSS Username Token** in the policy.

XPATH Token

Right-click the action name and click **Add XPATH Token** to validate consumer applications based on an XML element (represented by an XPATH expression you specify in the **XPATH to Identify Token** field).

Consumer Certificate

Right-click the action name and click **Add Consumer Certificate** to identify consumer applications based on information in a WSS X.509 certificate. If you select this option, you should also include the **Require X.509 Token** or the **Require Signing** action in the policy.

User ID

Right-click the action name and click **Add User ID** if you are applying the Identify Consumer action to a connector virtual service. You must select the **User ID** identifier; no other identifier is valid. **User ID** identifies consumer applications based on a list of users who are registered in the Integration Server on which CloudStreams is running. (You need to apply the Identify Consumer action to a connector virtual service if you apply the following actions to the connector virtual service: "Monitor Service Level Agreement" or "Throttling Traffic Optimization" (if you select its **Limit Traffic for Applications** option)).

Action: Include Timestamps

Note: Dependency requirement: A policy that includes this action must also include all of the following actions: Require SSL, Require Signing and Require Encryption.

This action requires that timestamps be included in the request header. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

CloudStreams checks the timestamp value against the current time to ensure that the request is not an old message, which serves to protect your system against attempts at message tampering, such as replay attacks.

CloudStreams rejects the request if either of the following things happen:

- CloudStreams receives a timestamp that exceeds the time defined by the timestamp element.
- A timestamp element is not included in the request.

There are no input parameters.

Action: Log Invocation

This action logs request/response payloads. You can log the payloads in the database and/or send the payloads in the form of email alerts. This action also logs other information about the request/response, including the service name, operation name, the Integration Server user, a timestamp, the response time, and more.

To edit the Log Invocation action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Log Invocation** in the **Applied Actions** list, and set the following action parameters.

Log Generation Frequency
Specifies how frequently to log the payload.

- **Always**: Log all requests and/or responses.
- **On Success**: Log only the successful responses and/or requests.
- **On Failure**: Log only the failed requests and/or responses.

Log the Following Payloads
Specifies whether to log all request payloads, all response payloads, or both.

- **Request**: Log all request payloads.

- **Response**: Log all response payloads.

Send Data To

By default, this action logs the payloads to the CloudStreams Analytics database.

> **Note:** Ensure that you select the **Database Publishing** option in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Database**), as described in the section *Setting the Database Options for Publishing Run-Time Metrics and Events* in the document *Administering webMethods CloudStreams*.

Alert Email

Right-click the action name and click **Add Alert Email** to send the payloads in an email alert to the email address you specify in the **Email ID** field. You can select **Add Alert Email** multiple times to add multiple email addresses.

> **Note:** Ensure that you select the email options in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Email**), as described in the section *Setting the Email Options for Logging Payloads and Sending Performance Monitoring Alerts* in the document *Administering webMethods CloudStreams*.

Action: Monitor Service Performance

This action monitors a user-specified set of run-time performance conditions for a virtual service, and sends alerts to a specified destination when the performance conditions are violated.

For the counter-based metrics (Total Request Count, Success Count, Fault Count), CloudStreams sends an alert as soon as the performance condition is violated, without having to wait until the end of the metrics tracking interval. CloudStreams sends only one alert the first time the condition is violated during the interval. (It will send another alert the next time a condition is violated during a subsequent interval.) For information about intervals, see the section *The Intervals for Metric Publishing* in the document *Administering webMethods CloudStreams*.

For the aggregated metrics (Average Response Time, Minimum Response Time, Maximum Response Time), CloudStreams aggregates the response times at the end of the interval, and then sends an alert if the performance condition is violated.

By default, this action does not include metrics for failed invocations. To include metrics for failed invocations, set the `pg.PgMetricsFormatter.includeFaults` parameter to true in *IntegrationServer_directory* \packages\WmCloudStreams\config\resources\wst-config.properties.

To set the Monitor Service Performance action parameters

1. In the CloudStreams Governance view, click the policy name.

2. In the policy editor on the right side of the page, double-click **Monitor Service Performance** in the **Applied Actions** list, and set the following action parameters.

Alert Interval
Number. The time period (in minutes) in which to monitor performance before sending an alert if a condition is violated.

Alert Frequency
String. Specifies how frequently to issue alerts for the counter-based metrics (Total Request Count, Success Count, Fault Count).

- **Every Time**: Issues an alert every time one of the specified conditions is violated.
- **Only Once**: Issues an alert only the first time one of the specified conditions is violated.

Alert Message
Optional. Specify a text message to include in the alert.

Send Data To
By default, this action logs the alerts to the CloudStreams Analytics database.

> **Note:** Ensure that you select the **Database Publishing** option in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Database**), as described in the section *Setting the Database Options for Publishing Run-Time Metrics and Events* in the document *Administering webMethods CloudStreams*.

Metrics Collection Level
The run-time performance metrics for a virtual service (which is invoked only in the inbound run-time scenario), are collected at the service level. That is, the metrics for all invocations of a single virtual services are aggregated together during your specified metrics publishing interval and then published.

In contrast, the metrics for a connector virtual service (which is invoked only in the outbound run-time scenario) can be collected at two different levels of metric collection:

- **Cloud Connector Service**: Remember that a single connector virtual service can be used by multiple cloud connector services. Select this option if you want to collect the metrics for the connector virtual service broken down by each separate cloud connector service that uses it. For example, if a connector virtual services is used by three cloud connector services, then this option will collect the metrics of that service separately, broken down by each of the three cloud connector services that use it.
- **Connector Virtual Service** (default): Select this option if you want to aggregate all the metrics for a single connector virtual service, even if it is used by multiple cloud connector services. For example, if a connector virtual service is used by three cloud connector services, then this option will collect the combined metrics for the connector virtual service by all three of the cloud connector services that use it.

Action Configuration

Right-click the action name and click **Add Action Configuration** to specify a condition to monitor. To do this, select a condition **Name** (the metric to monitor), an **Operator**, and a **Value** for the condition. You can select **Add Action Configuration** multiple times to add multiple conditions. Multiple conditions are connected by the AND operator.

Name: The metric to monitor, which can be:

- **Availability**: Indicates whether the service was available to the specified consumers in the current interval. A value of 100 indicates that the service was always available. If invocations fail due to policy violations, this parameter could still be as high as 100. That is, SOAP faults returned by the native provider or faults due to CloudStreams policy enforcements do not impact Availability. Only errors that CloudStreams interprets as a provider service being down will impact Availability.
- **Average Response**: The average amount of time it took the service to complete all invocations in the current interval. Response time is measured from the moment CloudStreams receives the request until the moment it returns the response to the caller.
- **Fault Count**: The number of faults returned in the current interval.
- **Maximum Response** : The maximum amount of time to respond to a request in the current interval.
- **Minimum Response**: The minimum amount of time to respond to a request in the current interval.
- **Successful Request Count**: The number of successful requests in the current interval.
- **Total Request Count**: The total number of requests (successful and unsuccessful) in the current interval.

Alert Email

Right-click the action name and click **Add Alert Email** if you want to send the monitoring alerts to an email address you specify in the **Email ID** field. You can select **Add Alert Email** multiple times to add multiple email addresses.

Note: Ensure that you select the email options in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Email**), as described in the section *Setting the Email Options for Logging Payloads and Sending Performance Monitoring Alerts* in the document *Administering webMethods CloudStreams*.

Action: Monitor Service Level Agreement (SLA)

Note: Dependency requirement: A policy that includes this action must also include the Identify Consumer action.

This action is similar to the Monitor Service Performance action. Both actions can monitor the same set of run-time performance conditions for a virtual service, and then send alerts when the performance conditions are violated. This action is different because it enables you to monitor run-time performance for *one or more specified consumers*.

You can configure this action to define a *Service Level Agreement* (SLA), which is set of conditions that defines the level of performance that a consumer should expect from a service. You can use this action to identify whether a service's threshold rules are met or exceeded. For example, you might define an agreement with a particular consumer that sends an alert to the consumer if responses are not sent within a certain maximum response time. You can configure SLAs for each virtual service/consumer application combination.

For the counter-based metrics (Total Request Count, Success Count, Fault Count), CloudStreams sends an alert as soon as the performance condition is violated, without having to wait until the end of the metrics tracking interval. You can choose whether to send an alert only once during the interval, or every time the violation occurs during the interval. (CloudStreams will send another alert the next time a condition is violated during a subsequent interval.) For information about intervals, see the section *The Intervals for Metric Publishing* in the document *Administering webMethods CloudStreams*.

For the aggregated metrics (Average Response Time, Minimum Response Time, Maximum Response Time), CloudStreams aggregates the response times at the end of the interval, and then sends an alert if the performance condition is violated.

By default, this action does not include metrics for failed invocations. To include metrics for failed invocations, set the `pg.PgMetricsFormatter.includeFaults` parameter to true in *IntegrationServer_directory* \packages\WmCloudStreams\config\resources\wst-config.properties.

To set the Monitor Service Level Agreement (SLA) action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Monitor Service Level Agreement (SLA)** in the **Applied Actions** list, and set the following action parameters.

Alert Interval
Number. The time period (in minutes) in which to monitor performance before sending an alert if a condition is violated.

Alert Frequency
String. Specifies how frequently to issue alerts for the counter-based metrics (Total Request Count, Success Count, Fault Count).

- **Every Time**: Issues an alert every time one of the specified conditions is violated.
- **Only Once**: Issues an alert only the first time one of the specified conditions is violated.

Alert Message
Optional. Specify a text message to include in the alert.

Send Data To

By default, this action logs the alerts to the CloudStreams Analytics database.

> **Note:** Ensure that you select the **Database Publishing** option in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Database**), as described in the section *Setting the Database Options for Publishing Run-Time Metrics and Events* in the document *Administering webMethods CloudStreams*.

Metrics Collection Level

The run-time performance metrics for a virtual service (which is invoked only in the inbound run-time scenario), are collected at the service level. That is, the metrics for all invocations of a single virtual services are aggregated together during your specified metrics publishing interval and then published.

In contrast, the metrics for a connector virtual service (which is invoked only in the outbound run-time scenario) can be collected at two different levels of metric collection:

- **Cloud Connector Service**: Remember that a single connector virtual service can be used by multiple cloud connector services. Select this option if you want to collect the metrics for the connector virtual service broken down by each separate cloud connector service that uses it. For example, if a connector virtual services is used by three cloud connector services, then this option will collect the metrics of that service separately, broken down by each of the three cloud connector services that use it.
- **Connector Virtual Service** (default): Select this option if you want to aggregate all the metrics for a single connector virtual service, even if it is used by multiple cloud connector services. For example, if a connector virtual service is used by three cloud connector services, then this option will collect the combined metrics for the connector virtual service by all three of the cloud connector services that use it.

Action Configuration

Right-click the action name and click **Add Action Configuration** to specify a condition to monitor. To do this, select a condition **Name** (the metric to monitor), an **Operator**, and a **Value** for the condition. You can select **Add Action Configuration** multiple times to add multiple conditions. Multiple conditions are connected by the AND operator.

Name: The metric to monitor, which can be:

- **Availability**: Indicates whether the service was available to the specified consumers in the current interval. A value of 100 indicates that the service was always available. If invocations fail due to policy violations, this parameter could still be as high as 100. That is, SOAP faults returned by the native provider or faults due to CloudStreams policy enforcements do not impact Availability. Only errors that CloudStreams interprets as a provider service being down will impact Availability.
- **Average Response**: The average amount of time it took the service to complete all invocations in the current interval. Response time is measured from the moment

CloudStreams receives the request until the moment it returns the response to the caller.

- **Fault Count**: The number of faults returned in the current interval.
- **Maximum Response** : The maximum amount of time to respond to a request in the current interval.
- **Minimum Response**: The minimum amount of time to respond to a request in the current interval.
- **Successful Request Count**: The number of successful requests in the current interval.
- **Total Request Count**: The total number of requests (successful and unsuccessful) in the current interval.

Alert for Applications

Right-click the action name and click **Add Alert for Applications** to specify the consumer application to which this Service Level Agreement will apply. You can select **Add Alert for Applications** multiple times to add multiple consumer applications.

Alert Email

Right-click the action name and click **Add Alert Email** if you want to send the monitoring alerts to an email address you specify in the **Email ID** field. You can select **Add Alert Email** multiple times to add multiple email addresses.

> **Note:** Ensure that you select the email options in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Email**), as described in the section *Setting the Email Options for Logging Payloads and Sending Performance Monitoring Alerts* in the document *Administering webMethods CloudStreams*.

Action: Require Encryption

This action requires that an XML element (which is represented by an XPath expression) be encrypted. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

Prerequisites:

1. Configure Integration Server: Set up keystores and truststores in Integration Server (see the section *Securing Communications with the Server* in the document *webMethods Integration Server Administrator's Guide*).
2. Configure CloudStreams: In the Integration Server Administrator, navigate to **Solutions > CloudStreams > Administration > General** and complete the **IS Keystore Name**, **IS Truststore Name** and **Alias (signing)** fields, as described in the section *Setting the General Options* in the document *Administering webMethods CloudStreams*).

When this policy action is set for the virtual service, CloudStreams provides decryption of incoming requests and encryption of outgoing responses. CloudStreams can encrypt

and decrypt only individual elements in the SOAP message body that are defined by the XPath expressions configured for the policy action. CloudStreams requires that requests contain the encrypted elements that match those in the XPath expression. You must encrypt the entire element, not just the data between the element tags. CloudStreams rejects requests if the element name is not encrypted.

Note: Do not encrypt the entire SOAP body because a SOAP request without an element will appear to CloudStreams to be malformed.

CloudStreams attempts to encrypt the response elements that match the XPath expressions with those defined for the policy. If the response does not have any elements that match the XPath expression, CloudStreams will not encrypt the response before sending. If the XPath expression resolves a portion of the response message, but CloudStreams cannot locate a certificate to encrypt the response, then CloudStreams sends a SOAP fault exception to the consumer and a Policy Violation event notification to CloudStreams.

How CloudStreams Encrypts Responses

The Require Encryption action encrypts the response back to the client by dynamically setting a public key alias at run time. CloudStreams determines the public key alias as follows:

1. If CloudStreams can access the X.509 certificate of the client (based on the incoming request signature), it will use "useReqSigCert" as the public key alias.

   OR

2. If the Identify Consumer action is present in the policy (and it successfully identifies a consumer application), then CloudStreams will look for a public key alias with that consumer name in the "IS Keystore Name" property. The "IS Keystore Name" property is specified in the Integration Server Administrator, under **Solutions > CloudStreams > Administration > General**. This property should be set to an Integration Server keystore that CloudStreams will use.

   For an Identify Consumer action that allows for anonymous usage, CloudStreams does not require a consumer name in order to send encrypted responses. In this case, CloudStreams can use one of the following to encrypt the response in the following order, depending on what is present in the security element:

   a. A signing certificate.

   b. Consumer name.

   c. WSS username, SAML token or X.509 certificate.

   d. HTTP authorized user.

   OR

3. If CloudStreams can determine the current IS user from the request (that is, if an Integration Server WS-Stack determined that Subject is present), then the first principal in that subject is used.

OR

4. If the above steps all fail, then CloudStreams will use either the WS-Security username token or the HTTP Basic-Auth user name value. There should be a public key entry with the same name as the identified username.

To set the Require Encryption action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Require Encryption** in the **Applied Actions** list, and set the following action parameters.

Element Required To Be Encrypted
An XPath expression that represents the XML element that is required to be encrypted.

Namespace Prefix
Optional. Right-click the action name and click **Add Namespace Prefix** if you want to specify the namespace prefix of the element required to be encrypted. Enter the namespace prefix in the following format:

`xmlns:<prefix-name>`

For example: `xmlns:soapenv`. For more information, see the XML Namespaces specifications at http://www.w3.org/TR/REC-xml-names/#ns-decl.

The generated XPath element in the policy should look similar to this:

```
<sp:SignedElements xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
              <sp:XPath
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">//soapenv:Body</sp
:XPath>
           </sp:SignedElements>
```

Action: Require HTTP Basic Authentication

This action uses HTTP Basic authentication to verify the consumer's authentication credentials contained in the request's Authorization header. CloudStreams authorizes the credentials against the list of users registered in the Integration Server on which CloudStreams is running. This type of consumer authentication is referred to as "preemptive authentication". If you want to perform "preemptive authentication", a policy that includes this action must also include the Identify Consumer action. This action supports WS-SecurityPolicy 1.2.

If the user/password value in the Authorization header cannot be authenticated as a valid Integration Server user (or if the Authorization header is not present in the request), a 500 SOAP fault is returned, and the client is presented with a security challenge. If the client successfully responds to the challenge, the user is authenticated. This type of consumer authentication is referred to as "non-preemptive authentication". If the client does not successfully respond to the challenge, a 401 "WWW-Authenticate: Basic" response is returned and the invocation is not routed to the policy engine. As a

result, no events are recorded for that invocation, and its key performance indicator (KPI) data are not included in the performance metrics

If you choose to omit the "Require HTTP Basic Authentication" action (regardless of whether an Authorization header is present in the request or not), then:

- CloudStreams forwards the request to the native service, without attempting to authenticate the request.
- The native service returns a 401 "WWW-Authenticate: Basic" response, which CloudStreams will forward to the client; the client is presented with a security challenge. If the client successfully responds to the challenge, the user is authenticated.

In the case where a consumer is sending a request with both transport credentials (HTTP basic authentication) and message credentials (WSS username or X.509 token), the message credentials take precedence over the transport credentials when Integration Server is determining which credentials it should use for the session. For more information, see "Action: Require WSS Username" on page 102, and "Action: Require X.509 Token" on page 102. In addition, you must ensure that the service consumer that connects to the virtual service has an Integration Server user account.

To set the Require HTTP Basic Authentication action parameter

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Require HTTP Basic Authentication** in the **Applied Actions** list, and set the following action parameter.

Authenticate Credentials
Authorizes consumers against the list of users registered in the Integration Server on which CloudStreams is running. If you select this option, you must also include the Identify Consumer action in the policy.

Action: Require SAML Token

Requires that a WSS Security Assertion Markup Language (SAML) assertion token be present in the SOAP message header to validate service consumers. CloudStreams supports SAML 1.1 and 2.0 tokens. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

Note: When a Require SAML Token action is generated, CloudStreams also implicitly selects the "timestamp" and "signing" assertions. You should not add the Require Timestamps and Require Signing actions to a virtual service if the Require SAML Token action is already applied.

To set the Require SAML Token action parameter

1. In the CloudStreams Governance view, click the policy name.

2. In the policy editor on the right side of the page, double-click **Require SAML Token** in the **Applied Actions** list, and set the following action parameter.

SAML Version
Specifies the version of the WSS SAML Token to use.

- **SAML 1.1**: Default.
- **SAML 2.0**

Note: For important usage information, see the section *Require SAML Token* in the document *Administering webMethods CloudStreams*

Action: Require Signing

Note: Dependency requirement: A policy that includes this action must also include the Identify Consumer action.

This action requires that an XML element (represented by an XPath expression) be signed. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

Prerequisites:

1. Configure Integration Server: Set up keystores and truststores in Integration Server (see the section *Securing Communications with the Server* in the document *webMethods Integration Server Administrator's Guide*).
2. Configure CloudStreams: In the Integration Server Administrator, navigate to **Solutions > CloudStreams > Administration > General** and complete the **IS Keystore Name**, **IS Truststore Name** and **Alias (signing)** fields, as described in the section *Setting the General Options* in the document *Administering webMethods CloudStreams*). CloudStreams uses the signing alias specified in the **Alias (signing)** field to sign the response.

When this policy action is set for the virtual service, CloudStreams validates that the requests are properly signed, and provides signing for responses. CloudStreams provides support both for signing an entire SOAP message body or individual elements of the SOAP message body.

CloudStreams uses a digital signature element in the security header to verify that all elements matching the XPath expression were signed. If the request contains elements that were not signed or no signature is present, then CloudStreams rejects the request.

Note: You must map the public certificate of the key used to the sign the request to an Integration Server user. If the certificate is not mapped, CloudStreams returns a SOAP fault to the caller.

To set the Require Signing action parameters

1. In the CloudStreams Governance view, click the policy name.

2. In the policy editor on the right side of the page, double-click **Require Signing** in the **Applied Actions** list, and set the following action parameters.

Element Required To Be Signed
An XPath expression that represents the XML element that is required to be signed.

Namespace Prefix
Optional. Right-click the action name and click **Add Namespace Prefix** if you want to specify the namespace prefix of the element required to be encrypted. Enter the namespace prefix in the following format:

`xmlns:<prefix-name>`

For example: `xmlns:soapenv`. For more information, see the XML Namespaces specifications at http://www.w3.org/TR/REC-xml-names/#ns-decl.

The generated XPath element in the policy should look similar to this:

```
<sp:SignedElements xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <sp:XPath
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">//soapenv:Body</sp
:XPath>
          </sp:SignedElements>
```

Action: Require SSL

This action ensures that requests are sent to the server using the HTTPS protocol (SSL). This action supports WS-SecurityPolicy 1.2 and can be used by both SOAP and REST services.

In addition, setting the **Client Certificate Required** parameter to True allows CloudStreams to verify the client sending the request.

Ensure that you specify an HTTPS port in the Integration Server Administrator (go to **CloudStreams > Administration > General**).

To set the Require SSL action parameter

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Require SSL** in the **Applied Actions** list, and set the following action parameter.

Client Certificate Required
Specifies whether client certificates are required for the purposes of:

- Verifying the signature of signed SOAP requests or decrypting encrypted SOAP requests.
- Signing SOAP responses or encrypting SOAP responses.

Values:

- **True**: Requires client certificates. If a valid client certificate is not presented, CloudStreams rejects the message. Ensure that the Integration Server HTTPS port is configured to request or require a client certificate.
- **False**: Default. Does not require client certificates.

Action: Require WSS Username

Note: Dependency requirement: A policy that includes this action must also include the Identify Consumer action.

Requires that a WSS username token and password be present in the SOAP message header to validate service consumers. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

CloudStreams rejects requests that do not include the username token and password of an Integration Server user. CloudStreams only supports clear text passwords with this kind of authentication.

In the case where a consumer is sending a request with both transport credentials (HTTP basic authentication) and message credentials (WSS username or X.509 token), the message credentials take precedence over the transport credentials when Integration Server is determining which credentials it should use for the session.

There are no input parameters.

Action: Require X.509 Token

Note: Dependency requirement: A policy that includes this action must also include the Identify Consumer action.

Requires that a WSS X.509 token be present in the SOAP message header to validate service consumers. This action supports WS-SecurityPolicy 1.2 and cannot be used with REST virtual services or connector virtual services.

In the case where a consumer is sending a request with both transport credentials (HTTP basic authentication) and message credentials (X.509 token or WSS username), the message credentials take precedence over the transport credentials when Integration Server is determining which credentials it should use for the session. In addition, you must ensure that the service consumer that connects to the virtual service has an Integration Server user account.

There are no input parameters.

Action: Throttling Traffic Optimization

> **Note:** Dependency requirement: A policy that includes this action must also include the Identify Consumer action if the **Limit Traffic for Applications** option is selected.

This action limits the number of service invocations allowed during a specified time interval, and sends alerts to a specified destination when the performance conditions are violated.

Reasons for limiting the service invocation traffic include:

- To avoid overloading the back-end services and their infrastructure.
- To limit specific consumers in terms of resource usage (that is, you can use the "Monitor Service Level Agreement" (SLA) action in addition to "Throttling Traffic Optimization").
- To shield vulnerable servers, services, and even specific operations.
- For service consumption metering (billable pay-per-use services).

To set the Throttling Traffic Optimization action parameters

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Throttling Traffic Optimization** in the **Applied Actions** list, and set the following action parameters.

Soft Limit
Optional. Specifies the maximum number of invocations allowed per **Interval** before issuing an alert. Reaching the soft limit will not affect further processing of requests (until the **Hard Limit** is reached).

> **Note:** The limit is reached when the total number of invocations coming from all the consumer applications (specified in the **Limit Traffic for Applications** field) reaches the limit.

Hard Limit
Required. Specifies the maximum number of invocations allowed per **Interval** before stopping the processing of further requests and issuing an alert. Typically, this limit should be higher than the soft limit.

> **Note:** The limit is reached when the total number of invocations coming from all the consumer applications (specified in the **Limit Traffic for Applications** field) reaches the limit.

Alert Interval
Specifies the amount of time for the soft limit and hard limit to be reached.

Alert Frequency
Specifies how frequently to issue alerts.

- **Every Time**: Issue an alert every time one of the specified conditions is violated.
- **Only Once**: Issue an alert only the first time one of the specified conditions is violated.

Alert Message For Soft Limit
Optional. Specify a text message to include in the soft limit alert.

Alert Message For Hard Limit
Optional. Specify a text message to include in the hard limit alert.

Send Data To
By default, this action logs the alerts to the CloudStreams Analytics database.

> **Note:** Ensure that you select the **Database Publishing** option in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Database**), as described the section *Setting the Database Options for Publishing Performance Metrics and Events* in the document *Administering webMethods CloudStreams*.

Metrics Collection Level
The run-time performance metrics for a virtual service (which is invoked only in the inbound run-time scenario), are collected at the service level. That is, the metrics for all invocations of a single virtual services are aggregated together during your specified metrics publishing interval and then published.

In contrast, the metrics for a connector virtual service (which is invoked only in the outbound run-time scenario) can be collected at two different levels of metric collection:

- **Cloud Connector Service**: Remember that a single connector virtual service can be used by multiple cloud connector services. Select this option if you want to collect the metrics for the connector virtual service broken down by each separate cloud connector service that uses it. For example, if a connector virtual services is used by three cloud connector services, then this option will collect the metrics of that service separately, broken down by each of the three cloud connector services that use it.
- **Connector Virtual Service** (default): Select this option if you want to aggregate all the metrics for a single connector virtual service, even if it is used by multiple cloud connector services. For example, if a connector virtual service is used by three cloud connector services, then this option will collect the combined metrics for the connector virtual service by all three of the cloud connector services that use it.

Limit Traffic For Applications
Specifies the consumer application(s) that this action applies to. To specify multiple consumer applications, use the plus button to add rows.

Alert Email
Right-click the action name and click **Add Alert Email** if you want to send the monitoring alerts to an email address you specify in the **Email ID** field. You can select **Add Alert Email** multiple times to add multiple email addresses.

> **Note:** Ensure that you set the email options in Integration Server Administrator (go to **Solutions > CloudStreams > Administration > Email**), as described in *Setting the Email Options for Logging Payloads and Sending Performance Monitoring Alerts* in the document *Administering webMethods CloudStreams*.

Action: Validate Schema

This action validates all XML request and/or response messages against an XML schema referenced in the WSDL. This action cannot be used with connector virtual services.

CloudStreams can enforce this policy action for messages sent between services. When this policy is set for the virtual service, CloudStreams validates XML request messages, response messages, or both, against the XML schema referenced in the WSDL. Ensure that you provide a schema.

To set the Validate Schema action parameter

1. In the CloudStreams Governance view, click the policy name.
2. In the policy editor on the right side of the page, double-click **Validate Schema** in the **Applied Actions** list, and set the following action parameter.

Validate SOAP Message(s)
Validates the request and/or response messages.

> **Note:** CloudStreams does not remove `wsu:Id` attributes that may have been added to a request by a consumer as a result of security operations against request elements (signatures and encryptions). In this case, to avoid schema validation failures you would have to add a Transform sub-step to the virtual service's In Sequence step so that the requests are passed to an XSLT transformation file that removes the `wsu:Id`s.

8 CloudStreams Deploy Dialog Box

You can deploy Virtual Services and Connector Virtual Services to CloudStreams server targets in two ways:

- Deploy all Virtual Services, and any custom Connector Virtual Services, that are contained in a particular CloudStreams Governance project.

  OR

- Deploy a single Virtual Service or custom Connector Virtual Service. Generally, this is useful for testing purposes.

Note: CloudStreams does not support sharing of Connector Virtual Services, Virtual Services, and Policies across nodes in a clustered setup. These artifacts should be manually deployed to a clustered node as needed.

Note: CloudStreams automatically deploys the default Connector Virtual Services WmCloudStreams.SoapVS and WmCloudStreams.RestVS; there is no need for you to deploy them.

When you execute the deployment operation, CloudStreams will immediately deploy the service(s) and the following items to the CloudStreams server target(s) that you specify:

- The policies of each service, as well as any other artifacts that you associated with the services when you created them.
- The VSD (virtual service definition) of each virtual service or connector virtual service.

  When you deploy a Virtual Service or a Connector Virtual Service, CloudStreams generates an XML document called a "virtual service definition (VSD)". The VSD defines the virtual service or connector virtual service for CloudStreams, and contains all the resources required to deploy the service to a CloudStreams server, including the policy that applies to the service. You cannot edit the VSD, but you can view it in the Advanced page in the Properties view of each service.

Before you deploy a virtual service, you should:

- Ensure that all policies of the services are Active; the value of the **Status** field in the Properties view of each policy should be **Active**. If it is not, right-click the policy name in the CloudStreams Governance view and click **Active**. You will not be allowed to activate a policy unless all of its action parameters have been set.
- Ensure that at least one CloudStreams server target has already been defined, as described in "Add CloudStreams Servers Dialog Box" on page 13.

- Ensure that the server's specified deployment URL is active and the user credentials of Integration Server are valid.
- Test the server connection from the Designer menu by clicking **Window > Preferences > Software AG > CloudStreams Servers** and using the **Test** button. If the connection is not active and valid, activate the deployment endpoint and modify the user credentials as required.

If CloudStreams encounters a problem deploying or redeploying a service, it displays a failure message, which is logged to the deployment log at the bottom of the page. In this case, it is up to the CloudStreams administrator to take corrective action and redeploy the service. If the reason for the failure is that the CloudStreams server is unavailable, and then you restart the CloudStreams server, it loads all information about any previously deployed services. For more information, see the topic *What Happens When You Deploy a Service?* in the document *Administering webMethods CloudStreams*.

To deploy all services in a CloudStreams Governance project:

When you deploy a CloudStreams Governance project, all virtual services in the project are deployed at once. If any custom connector virtual services are defined in the project, they are deployed too.

When you deploy a project, Integration Server automatically creates a package to support the project. The package name is the same as your project name. This package includes startup/shutdown services to manage the registration of the virtual service definitions (VSDs) when Integration Server restarts.

1. Open Software AG Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the project you want to deploy and click **Deploy**.
3. In the Deploy dialog box, choose one or more CloudStreams server targets to which to deploy the services and click **OK**. The services are immediately deployed.

   If only one CloudStreams server target is available to select, this dialog box will not appear.

   The services are immediately deployed to the following location:

   IntegrationServer_directory \packages*<PackageName><ProjectName* \config\proxies *VirtualService*

To deploy a single virtual service or connector virtual service:

1. Open Software AG Designer and display the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Governance view, right-click the service name you want to deploy and click **Deploy**.
3. In the Deploy dialog box, choose one or more CloudStreams server targets to which to deploy the service and click **OK**. The service is immediately deployed.

If only one CloudStreams server target is available to select, this dialog box will not appear.

The service is immediately deployed to the following location:

IntegrationServer_directory \packages*<PackageName><ProjectName* \config\proxies *VirtualService*

9 Custom Cloud Connector Screens

Use these screens to create a custom cloud connector, which you can deploy to CloudStreams. You use the CloudStreams Development plug-in to create and configure custom cloud connectors. You can create custom cloud connectors for both SOAP-based and REST-based SaaS providers.

The New CloudStreams Provider Project Wizard

To open the CloudStreams Provider Project wizard:

1. In Software AG Designer, open the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. Click **File > New > CloudStreams Provider Project** from the main menu.
3. In the "New CloudStreams Provider Project" wizard, assign a name to the new project using any combination of letters, numbers, and the underscore character. The project name must be a valid resource name on your operating system, must not be null, and cannot be an empty string.

   CloudStreams Provider project names are validated according to the same rules that apply to Integration Server package names. Keep the following guidelines in mind when naming new packages:

   - Start all package names with an uppercase letter and capitalize the first letter of subsequent words (for example, PurchaseOrder).
   - Keep package names short. Use abbreviations instead of full names. For example, instead of ProcessPurchaseOrder, use ProcessPO.
   - Ensure that the package name describes the functionality and purpose of the services it contains.
   - Control characters and special characters like periods (.), including:
   - Avoid creating package names with random capitalization (for example, cOOLPkgTest).
   - Avoid using articles (for example, "a," "an," and "the") in the package name. For example, instead of TestTheService, use TestService.
   - Avoid using the prefix "Wm". Integration Server and Designer use the "Wm" prefix for predefined packages that contain services, IS document types, and other files.
   - Avoid using control characters and special characters like periods (.) in a package name. The watt.server.illegalNSChars setting in the server.cnf file (which is located in the *IntegrationServer_directory* \instances*instance_name* \config directory) defines all the characters that you cannot use when naming packages. Additionally, the operating system on which you run the Integration Server might have specific requirements that limit package names.

4. The “Use Default Location” option is selected by default. The default location is the Workspace root. For example, if you are using C:\Workspaces\My_Workspace.. the default location would be C:\Workspaces\runtime-Eclipse Application, which is the Workspace root.
5. Select a location in your local file system to store the new project in the “Location” field.
6. Choose a file system, either “default” or “RSE”.
7. Enter the name of the publisher of the Package/Provider in the “Publisher” field. This field is optional.
8. Provide a description of the project in the “Description” field. This field is optional.
9. Click **Finish**.

To manage a Provider project, right-click the project and select a menu item such as:

- **Export**: Exports the Provider project to your local file system. Complete the wizard to indicate the export destination. A project with deployed artifacts should be undeployed before being exported.
- **Import**: Imports the Provider project from your local file system. Complete the wizard to indicate the import destination and click Finish.
- **Delete**: Deletes the Provider project from the CloudStreams Development perspective.

The New Cloud Connector Wizard

To create a new cloud connector, right-click the **Connectors** folder and click **New Cloud Connector** (or right-click the CloudStreams Provider project you just created and click **New Cloud Connector**). Complete the following fields in the New Cloud Connector wizard:

Project
Click **Browse** and select the CloudStreams Provider project you just created.

Name
Assign a name for the cloud connector. The name must start with an alpha character and may contain numerals and the following special characters:

- - (hyphen)
- _ (underscore)
- ' (apostrophe)
- , (comma)
- " (double quotes)
- . (period)

- & (ampersand)
- () (parentheses)
- ! (exclamation)

Version
Assign a version identifier for the cloud connector. The version identifier is a required attribute that you should increment when a connector is modified to indicate that the cloud connector has been updated. This is a "public" version identifier that CloudStreams shows to developers when it displays the list of connectors. The name may contain numerals and the following special characters:

- - (hyphen)
- _ (underscore)
- . (period)

ID
Assign a unique identifier for the connector. This value must start with an alpha character and may contain numerals and the following special characters:

- - (hyphen)
- _ (underscore)
- . (period)

Provider Group
Optional. You can specify that the connector should belong to a particular group. A group is a logical grouping of a collection of connectors.

For example, if you have multiple connectors for the same provider, you might want to group them together for convenience. Suppose you have two connectors for the Amazon provider: one connector that is provided by Software AG, for example, the webMethods CloudStreams Amazon EC2 Connector and another connector for the Amazon provider that was custom-built. You might want to group them together into a group called AmazonProvider.

To specify a group for the connector, type a group name in this field or select an existing group name from the drop-down list. The name must start with an alpha character and may contain numerals and the following special characters:

- - (hyphen)
- _ (underscore)
- ' (apostrophe)
- , (comma)
- " (double quotes)
- . (period)
- & (ampersand)

- () (parentheses)
- ! (exclamation)

If you specify a group, the connector will be added to the <*group_name*> folder (under CloudStreams > Providers).

If you do not specify a group, the connector will be added to your CloudStreams Provider project.

> **Note:** The group will also be visible in the Integration Server Administrator's Connector List (under **Solutions > CloudStreams > Providers**) if at least one connector is in the deployed state.

Metadata Handler
CloudStreams provides two kinds of metadata handlers, which provide the appropriate SOAP data model for the SaaS provider. Click **Browse** and select a metadata handler.

- For a SOAP-based SaaS provider, select the SOAP metadata handler **WsdlConnectorMetadataHandler**.
- For a REST-based SaaS provider, select the REST metadata handler **RestConnectorMetadataHandler**.

Description
Optional. Type a description of the cloud connector.

Click **Next** and on the next page, create a cloud connector service based on the provider's WSDL or XSD that you specify. (If you click **Finish**, you can create the cloud connector service later, using the Services Configuration page, as described later.) Complete the fields on page 2 of the wizard as follows.

Service Name
Assign a name for the cloud connector service. The name must start with an alpha character and should not contain special characters other than _ (underscore).

WSDL (SOAP only)
Specify the SaaS provider's WSDL that CloudStreams will use to generate the document types by selecting either:

- **File**. Specify the WSDL file name, or click **Browse** to select the WSDL from your local file system.
- **URL**. Specify the URL of the WSDL.

XSD (REST only)
Specify the SaaS provider's XSD that CloudStreams will use to generate the document types by selecting either:

- **Namespace**. Specify the XSD's namespace (for example `myConnector_v1.doctypes`). Alternatively, click **Browse** and select a `doctype` that has already been generated in Integration Server.

- **XSD**. Specify the URL of the XSD in the text field, or click **Browse** and select an XSD.

Package
Assign a name for the DocTypes package, which will be deployed to the CloudStreams target server.

The name must be a valid resource name on your operating system. The name must not be null and cannot be an empty string. The name cannot contain:

- Reserved words and characters that are used in Java or C/C++ (such as *for*, *while*, and *if*).
- Digits as their first character.
- Spaces.
- Control characters and special characters like periods (.), including:

```
?    '    -    #    =    )    (    .    /    \    ;

&    @    ^    !    |    }    {    `    >    <

%    *    :    $    ]    [    "    +    ,    ~
```

- Characters outside of the basic ASCII character set, such as multi-byte characters.

CloudStreams will generate the document types from the provider's WSDL or XSD. However, if the Namespace option is chosen in the XSD field, then doctypes will not be generated.

CloudStreams automatically generates a name for the namespace that will contain the provider's document types. The name's form is: *packageName* .*connector_ID* .doctypes. When additional services are added, CloudStreams adds the document types to this namespace.

Description
Optional. Type a description of the cloud connector service.

Click **Finish**. The new cloud connector is added to your CloudStreams Provider project, in the **Connectors** folder. In addition, if you completed page 2 of the wizard, CloudStreams creates a service for the cloud connector, based on the WSDL or XSD you specified in the wizard.

The Services Configuration Page (SOAP)

In this task, you will configure the cloud connector service you just created in the New Cloud Connector wizard. You will:

- Configure the operations for the cloud connector service and map their signatures.

- Select any abstract objects that will be needed by the service's Complex type operations (if any).

To configure cloud connector services using the Services Configuration page:

1. In Software AG Designer, open the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Connectors view, expand your CloudStreams Provider project and click the cloud connector you just created in the New Cloud Connector wizard. The **Overview** page is displayed, showing the general information you defined in the wizard.
3. Click the **Services** link in the Plug-In Contents section of the page (or click the **Services** tab at the bottom of the page). The Services Configuration page is displayed. If you already defined a cloud connector service on page 2 of the New Cloud Connector wizard, this page will show your new service and the default folders **Abstract Objects** and **Operations**.
4. If you did *not* define a cloud connector service on page 2 of the New Cloud Connector wizard, right-click the **Services** node and click **Add Service**.
5. Add any abstract objects that will be needed by the service's Complex type operations.

   CloudStreams supports the abstract object types businessObject and schemaObject.

   For a businessObject, perform the following steps:

   a. Click the **Abstract Objects** node.

   b. In the Configuration section of the page, in the **Type** field, select **businessObject**.

   c. In the **Document Name** field, select the document name of the abstract object from the drop-down list.

   d. Next to the **Business Object > List** field, click the Add icon.

      The Lookup Selection window appears, displaying the list of lookup services that implement the `boList` lookup type.

   e. Next to the **Business Object > Describe** field, click the Add icon.

      The **Lookup Selection** window appears, displaying the list of lookup services that implement the `boDescribe` lookup type.

   f. In the Lookup Selection dialog boxes, select the lookup services that you implemented for the abstract object and click **OK**.

      The selected services will be shown in the **Service** table.

   For a schemaObject, perform the following steps:

   a. Click the **Abstract Objects** node.

   b. In the Configuration section of the page, in the **Type** field, select **schemaObject**.

c. In the **Document Name** field, select the document name of the abstract object from the drop-down list.

d. Next to the **Schema Object > List** field, click the Add icon.

The **Lookup Selection** window appears, displaying the list of lookup services that implement the `soList` lookup type.

e. In the Lookup Selection dialog boxes, select the lookup service that you implemented for the abstract object and click **OK**.

The selected service will be shown in the **Service** table.

6. Click the **Operations** folder and select the operation type for each operation in the Configuration section of the page as follows:

Field	Description
Name	(Read-only field.) The operation name.
Display Name	The operation display name.
Type	Select the type of the operation: ■ **SIMPLE**: This is any operation that has all the information needed to build the messages for a connector's operation based solely on the WSDL. A simple operation neither requires dynamic signature updating nor uses an abstract type definition. ■ **COMPLEX**: This is any operation that requires additional efforts to capture the metadata needed to build messages and to invoke a provider's service because the WSDL by itself does not suffice. Not every provider will have Complex operations. ■ **METADATA**: Metadata operations are special operations provided by the provider which are used by the connector to capture the additional information that is needed for a complex operation. Not every provider will have Metadata operations. ■ **LOGIN** or **LOGOUT**: The Login and Logout operations are those that are invoked when a managed connection pool is enabled (login) or disabled (logout). Some providers require login/ logout methods to be invoked in order to setup a session for the user to use when invoking any of the business operations. Other providers will not require them.

Field	Description
	Alternatively, you can select the types for the operations individually, by clicking an operation and then selecting its type.
Hide	If you select this option for any operation, the operation will not be visible while configuring a Cloud connector service.
Description	Optional description for the operation.

7. Add the operation's input parameters as follows.

   You can add predefined parameters (if the operation has any), and you can add additional ones as well.

   a. Right-click the operation and select **Add Parameters**.

      The Configuration section of the page will display the operation's predefined parameters (if any).

   b. If the operation has any predefined parameters, select the check box next to each one you want to add. Mandatory parameters are selected by default and you cannot un-select them.

   c. Complete the following fields in the Configuration section.

Field	Description
Name	The parameter's name. (Read-only field for predefined parameters.)
Style	The parameter style, for example URI_CONTEXT. (Read-only field for predefined parameters.)
Default Value	You can provide a default value for any parameter by typing a value in the **Default Value** field. If the variable is null in the input pipeline, this default value will be used at run time. The value given at run time always takes precedence over the default value. However, if the existing default value is of type "fixed default", the overwrite will fail. **Note:** Parameters have various data validation constraints that apply to them. These constraints are indicated by an icon next to each parameter. For information about these constraints, see

Field	Description
	Viewing the Constraints that Apply to Variables in the document *Administering webMethods CloudStreams*.
Description	Optional description of the parameter.
Required	Specifies whether the parameter is required.

d. If you want to add additional parameters, click the **Add** button and complete the fields in the Configuration section (described above).

e. Click **OK**.

8. Specify the input/output mapping for an operation as follows:

a. Right-click an operation and click **Add Mapping**.

b. In the Configuration section of the page, right-click a parameter you want to map and click **Set Configuration**.

c. In the dialog box that appears, complete the following fields:

Field	Description
Name	Assign a name to the mapping.
Data Type	Select the data source type: ■ **Cookie**: HTTP cookies. For example, the Salesforce.com connector inserts the session token from a valid login in the SOAP header of the business operations to be executed. Other providers do the same thing; however, the token is managed via cookies instead of the SOAP header. ■ **Header**: Request or response HTTP transport headers for the support connection factory implementation. ■ **IData**: IData is a variable name that is associated with the connection instance when the service is invoked. It is a subset of those configuration fields from the selected groups. Not all fields are eligible for use as a mapping step since their values may not be changed or have any useful meaning in this context. ■ **Literal**: A constant value. ■ **Parameter**: Primarily used for REST handlers. ■ **Service**: The Service type applies to the source, not to the target. Select Service if you want the source to call a given

Field	Description
	service to perform certain tasks and to map the output of the service to a target. The service must adhere to wm.cloudstreams.service.common.lookup.specs:mapServiceSpec. If an error occurs related to service validation or execution, CloudStreams throws a Mapping Exception. ■ **XPath**: Enables you to define an XPath expression.
Value	Select the appropriate connection group field from the drop-down list. The list of fields displayed in the drop-down list depends on the type of the connection group you configure in the Connection Configuration page (see *The Connections Configuration Page*).

9. Define global mappings, if required by your provider.

   Global mappings are mapping statements that must be executed for all Simple and Complex type operations (if required by your provider). These global mapping steps are used by the provider to inject the session token into the SOAP header before invoking the service. Some providers might have configuration values that could be included for every operation too. Other providers have configuration content in their SOAP header too.

   To specify global mapping, right-click the service name, click **Global Mapping** and complete the fields in the Configuration section of the page as follows:

Field	Description
Mapping Name	Assign a name for the global mapping.
Type	Select **IN** or **OUT**.
Mapping Key Type	Select the source mapping type, which can be: ■ **Cookie** ■ **Header** ■ **IData** ■ **Literal** ■ **Parameter** ■ **Service** ■ **XPath**

Field	Description
	For descriptions, see the previous step.
Mapping Key Key	Enter the source mapping key. For example, if your source mapping type is IData, you might enter the key `cr.username`.
Mapping Value Type	Select the target mapping type, which can be: ■ **Cookie** ■ **Header** ■ **IData** ■ **Literal** ■ **Parameter** ■ **Service** ■ **XPath**
Mapping Value Key	Enter the target mapping key. For example, if your target mapping type is XPath, you might enter the key `tns:login/tns:us`.
Description	Optional. Enter a description of the mapping.

10. You can add/delete additional services in the Services page, as long as the connector is not deployed.
11. View the **Manifest** node, which shows read-only fields containing attributes whose values were captured from your cloud connector definition. The version of the CloudStreams Development Plug-in (Created-By) is also displayed. For imported plug-ins created in a Designer release prior to 9.7, this information is not shown.

The Services Configuration Page (REST)

In this task, you will configure the cloud connector service you just created in the New Cloud Connector wizard. You need to create at least one cloud connector service for each REST resource on which the connector can operate.

To configure cloud connector services using the Services Configuration page:

1. In Software AG Designer, open the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Connectors view, expand your CloudStreams Provider project and click the cloud connector you just created in the New Cloud Connector wizard.

The **Overview** page is displayed, showing the general information you defined in the wizard.

3. Click the **Services** link in the Plug-In Contents section of the page (or click the **Services** tab at the bottom of the page). The Services Configuration page is displayed. If you already defined a cloud connector service on page 2 of the New Cloud Connector wizard, this page will show your new service and the default folder **Resources**.
4. If you did *not* define a cloud connector service on page 2 of the New Cloud Connector wizard, right-click the **Services** node and click **Add Service**.
5. Define any necessary global mappings to be used by all the REST resources in the service. To do this, right-click the service, select **Add Global Mapping** and complete the fields as follows.

Field	Description
Mapping Name	Assign a name for the global mapping.
Type	Select **IN** or **OUT**.
Description	Optional description for the mapping.
Required	Specify whether this is a required mapping.
Mapping Key Type	Select the source mapping type, which can be: ■ **Cookie**: HTTP cookies. For example, the Salesforce.com connector inserts the session token from a valid login in the SOAP header of the business operations to be executed. Other providers do the same thing; however, the token is managed via cookies instead of the SOAP header. ■ **Header**: Request or response HTTP transport headers for the support connection factory implementation. ■ **IData**: IData is a variable name that is associated with the connection instance when the service is invoked. It is a subset of those configuration fields from the selected groups. Not all fields are eligible for use as a mapping step since their values may not be changed or have any useful meaning in this context. ■ **Literal**: A constant value. ■ **Parameter**: Primarily used for REST handlers. ■ **Service**: The Service type applies to the source, not to the target. Select Service if you want the source to call a given service to perform certain tasks and to map the

Field	Description
	output of the service to a target. The service must adhere to wm.cloudstreams.service.common.lookup.specs:mapServiceSpec. If an error occurs related to service validation or execution, CloudStreams throws a Mapping Exception. ■ **XPath**: Enables you to define an XPath expression.
Mapping Key	Select the target mapping type, which can be: ■ **Cookie** ■ **Header** ■ **IData** ■ **Literal** ■ **Parameter** ■ **Service** ■ **XPath**
Mapping Value Key	Enter the target mapping key. For example, if your target mapping type is Header, you might enter the target mapping key `X-SFDC-Session`.
Document Name	The document type, based on the XSD.

6. Add a REST resource by right-clicking the **Resources** node, selecting **Add REST Resource** and completing the following fields in the wizard.

Field	Description
Name	Assign a name for the resource.
Method	Select an available HTTP method (GET, PUT, POST, DELETE).
Path	Specify the path to the resource.
Description	Optional description for the resource.

7. Click **Next**.
8. Add a Request to a REST resource by completing the fields as follows.

Field	Description
Request Name	Specify the request name, for example `tns:jobInfo`.
Incoming Parsing Type	The Content-Type of the request, for example, **application/octet+idataoref**.
Outgoing Serialization Type	The Content-Type for the response, for example, **application/xml**.
Document Reference Type	Click **Browse** and select a document reference. For example, `myConnector_v1.doctypes:docTypeRef_tns_JobInfo`.
Exclude document root	Select this option to exclude the root element of the JavaScript Object Notation (JSON) document type, for REST resource's request and response. See the *Administering webMethods CloudStreams* Guide for information on how to handle JSON representations of REST resources.

9. Click **Next**.

10. Add one or more Responses to a REST resource by completing the fields as follows.

Field	Description
Response Name	Specify the request name, for example `tns:jobInfo`.
Response Codes	Specify one or more codes for the response, such as 201 or 400. Response codes should be comma separated.
Incoming Parsing Type	For example, **application/xml**.
Outgoing Serialization Type	For example, **application/octet+idataoref**.
Document Reference Type	Click **Browse** and select a document reference. For example, `myConnector_v1.doctypes:docTypeRef_tns_JobInfo` or `myConnector_v1.doctypes:docTypeRef_tns_Error`.
Exclude document root	Select this option to exclude the root element of the JavaScript Object Notation (JSON) document type, for REST resource's request and response. See the

Field	Description
	Administering webMethods CloudStreams Guide for information on how to handle JSON representations of REST resources.

11. Click **Next**.
12. Select the predefined input parameters for the REST resource as desired. Note that:
    - Mandatory parameters are selected by default and you cannot deselect them.
    - You can provide a default value for any parameter by typing a value in the **Default Value** field. If the variable is null in the input pipeline, this default value will be used at run time. The value given at run time always takes precedence over the default value. However, if the existing default value is of type "fixed default", the overwrite will fail.
    - Parameters have various data validation constraints that apply to them. These constraints are indicated by an icon next to each parameter. For information about these constraints, see *Viewing the Constraints that Apply to Variables* in the document *Administering webMethods CloudStreams*.
13. Optionally create additional input parameters for the REST resource by clicking the **Add** button and completing the following fields.

Field	Description
Name	Specify a parameter name.
Document Reference	For QUERYSTRING_PARAM type parameters only. If the parameter is a complex parameter involving indices where an IS document type is required, specify the fully qualified name of the IS document type.
Formatter Service	For QUERYSTRING_PARAM type parameters only. If you have used a parameter formatter to format input data into a custom format, specify your custom formatter service here, and then provide the input in the form of "key:value" pairs for the arguments specified in the service. For details about parameter formatters, see *Parameter Formatters for REST Connector Services* in the document *Administering webMethods CloudStreams*.
Style	Select the parameter's style, which determines how the parameter should be used, (e.g., URI_CONTEXT, QUERYSTRING_PARAM or CFG_PARAM).

Field	Description
Default Value	Specify a default value for the parameter. If the variable is null in the input pipeline, this default value will be used at run time. The value given at run time always takes precedence over the default value. However, if the existing default value is of type "fixed default", the overwrite will fail. **Note:** Parameters have various data validation constraints that apply to them. These constraints are indicated by an icon next to each parameter. For information, see *Viewing the Constraints Applied to Variables* in the document *Administering webMethods CloudStreams*.
Description	Optional description of the parameter.
Required	Specifies whether the parameter is required.

14. Click **Finish**.
15. Define the local mappings for the REST resource by right-clicking the resource name, selecting **Add Mapping** and completing the fields as follows.

Field	Description
Name	Assign a name for the local mapping. This mapping will be used only by this particular resource.
Type	Select **IN** or **OUT**.
Description	Optional description for the mapping.
Required	Specify whether this is a required mapping.
Mapping Key Type	Select the source mapping type, which can be: ■ **Cookie**: HTTP cookies. For example, the Salesforce.com connector inserts the session token from a valid login in the SOAP header of the business operations to be executed. Other providers do the same thing; however, the token is managed via cookies instead of the SOAP header. ■ **Header**: Request or response HTTP transport headers for the support connection factory implementation.

Field	Description
	■ **IData**: IData is a variable name that is associated with the connection instance when the service is invoked. It is a subset of those configuration fields from the selected groups. Not all fields are eligible for use as a mapping step since their values may not be changed or have any useful meaning in this context. ■ **Literal**: A constant value. ■ **Parameter**: Primarily used for REST handlers. ■ **Service**: The Service type applies to the source, not to the target. Select Service if you want the source to call a given service to perform certain tasks and to map the output of the service to a target. The service must adhere to wm.cloudstreams.service.common.lookup.specs:mapServiceSpec. If an error occurs related to service validation or execution, CloudStreams throws a Mapping Exception. ■ **XPath**: Enables you to define an XPath expression.
Mapping Key	Enter the source mapping key. For example, if your source mapping type is Literal, you might enter the key `application/xml`.
Mapping Value Type	Select the target mapping type, which can be: ■ **Cookie** ■ **Header** ■ **IData** ■ **Literal** ■ **Parameter** ■ **Service** ■ **XPath**
Mapping Value Key	Enter the target mapping key. For example, if your target mapping type is Header, you might enter the key `Content-Type`.
Document Name	The document type, based on the XSD.

16. View the **Manifest** node, which shows read-only fields containing attributes whose values were captured from your cloud connector definition. The version of the

CloudStreams Development Plug-in (Created-By) is also displayed. For imported plug-ins created in a Designer release prior to 9.7, this information is not shown.

Understanding REST Parameters

CloudStreams REST connector services allow you to set parameters which become part of the outgoing request.

REST services rely on HTTP methods like GET, POST to make request to a SaaS provider, so the parameters are closely tied to these HTTP methods, where they are sent as part of these HTTP method requests.

The parameters are typically part of the HTTP URI which may be of the following format:

[scheme:][//authority][path][?query]

CloudStreams supports the following parameter styles:

Field	Description
Name	Specify a parameter name.
Data Type	For QUERYSTRING_PARAM type parameters only. For a complex parameter involving indices where an IS document type is required, select Record. For normal string entries, select String.
Document Reference	For QUERYSTRING_PARAM type parameters only. If the parameter is a complex parameter involving indices where an IS document type is required, specify the fully qualified name of the IS document type.
Formatter Service	For QUERYSTRING_PARAM type parameters only. If you have used a parameter formatter to format input data into a custom format, specify your custom formatter service here, and then provide the input in the form of "key:value" pairs for the arguments specified in the service. For details about parameter formatters, see *Parameter Formatters for REST Connector Services* in the document *Administering webMethods CloudStreams*.
Style	Select the parameter's style, which determines how the parameter should be used, (e.g., URI_CONTEXT, QUERYSTRING_PARAM or CFG_PARAM). For more information, see *Understanding REST Parameters* below.

Field	Description
Default Value	Specify a default value for the parameter. If the variable is null in the input pipeline, this default value will be used at run time. The value given at run time always takes precedence over the default value. However, if the existing default value is of type "fixed default", the overwrite will fail. **Note:** Parameters have various data validation constraints that apply to them. These constraints are indicated by an icon next to each parameter. For information, see *Viewing the Constraints Applied to Variables* in the document *Administering webMethods CloudStreams*.
Description	Optional description of the parameter.
Required	Specifies whether the parameter is required.

Type	URI Scope
URI_CONTEXT	path
QUERYSTRING_PARAM	query
CFG_PARAM	authority, path

URI_CONTEXT parameters are passed as the path component of a REST resource URI, and the parameter names correspond to the URI path variable names specified in the {} annotation. For example, a sample request might look like this:

```
services/async/25.0/job/{jobId}
```

In the above sample request, the URI path variable name `jobId` is specified as a parameter to the job resource. The annotation {} is set to the variable name `jobId`. At service run-time, the variable is substituted with its runtime value to form the dynamic path.

A sample resource definition with URI_CONTEXT parameter:

```
<resource name="Job" method="POST" path="services/async/25.0/job/{jobId}">
  <parameters>
     <parameter name="jobId" isRequired="true" style="URI_CONTEXT"/>
  </parameters>
</resource>
```

QUERYSTRING_PARAM parameters are passed as the query component of a REST resource invocation request.

The following example demonstrates a typical HTTP GET request with parameters that form a query string of the resource URI.

```
GET  /status?key1=value1&key2=value2 HTTP/1.1
Host: www.softwareag.com
Content-Length: 0
```

Notice that the parameters are added to the path after a "?", and specified as ampersand (&) separated list of key-value pairs, with the corresponding Content-Length set accordingly. The key & values passed as parameters are URL encoded by CloudStreams.

A sample resource definition with QUERYSTRING_PARAM parameter:

```
<resource name="GetStatus" method="GET" path="/status">
  <parameters>
     <parameter name="key1" isRequired="true" style="QUERYSTRING_PARAM"/>
     <parameter name="key2" isRequired="false" style="QUERYSTRING_PARAM"/>
  </parameters>
</resource>
```

CFG_PARAM parameters signify an internal contract between the connector tier and the connecter-specific authentication scheme along with the virtual runtime layer.

The allowed set of parameter names, which can be specified as CFG_PARAM, depends on the authentication scheme used for the connector definition.

Example:

`aws.bucketName` is a parameter which is used by the Amazon Authentication Scheme version 3 for specifying the dynamic host based on the parameter value.

While executing a resource with such parameter, the service endpoint is prefixed with the appropriate bucket name.

```
<resource name="GetBucket" method="GET" path="/">
  <parameters>
      <parameter name="aws.bucketName" isRequired="true" style="CFG_PARAM"/>
   </parameters>
</resource>
```

Parameter Data Types

CloudStreams supports the data types String and Record.

The String data type represents a simple parameter which is an individual string key-value parameter. This is the most commonly used data type and the default type, if not specified explicitly.

The Record data type handles complex parameters involving a collection of related key-value pairs. These parameters can have indices for one or more parameter entry. Such parameters can ideally be represented with an IS document type, and configured as a "Record" data type.

For example, consider a complex parameter structure as follows:

```
+ Filter[]
  - Name
  + Value[]
```

This needs to be represented as a query string like:

```
Filter.1.Name=instance-
type&Filter.1.Value.1=m1.small&Filter.1.Value.2=t1.micro
```

Such a parameter can be defined by creating an IS document type, and referring to the same as a "Record" data type parameter within the resource definition.

CloudStreams provides a capability to represent and transform such complex parameters into the desired format using its predefined formatter implementation. The resource's parameter definition can be enhanced to refer a formatter as follows:

```
<parameter name="Filter" dataType="Record"
documentRef="documents.paramType:FilterList" style="QUERYSTRING_PARAM">
  <formatter service="wm.cloudstreams.service.util.formatters:paramFormatter"
type="paramFormatter"/>
</parameter>
```

At run time, the resource PATH would look like:

```
GET /?Filter.1.Name=instance-
type&Filter.1.Value.1=m1.small&Filter.1.Value.2=t1.micro
```

For more details on formatters and customizing the formatter behavior, see the *Understanding REST Parameters* section in the document *Administering webMethods CloudStreams*.

The Connections Configuration Page (SOAP)

You need to create one or more run-time connections to the SaaS provider.

To configure connections using the Connections Configuration page:

1. In Software AG Designer, open the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Connectors view, expand your CloudStreams Provider project and click the cloud connector you just created. The **Overview** page is displayed, showing the general information you defined in the New Cloud Connector wizard.
3. Click the **Connections** link in the Plug-In Contents section of the page (or click the **Connections** tab at the bottom of the page). The Connections Configuration page is displayed.
4. Create a run-time connection by right-clicking the **Connections** node, clicking **Add Connection** and assigning a name and optional description to the connection. The name cannot contain special characters. CloudStreams creates the connection in the **Connections** node, and by default it will contain a **Groups** node.
5. Right-click on the **Groups** node and click **Add Group**. The **New Group** window appears. Select one or more groups in the **New Group** window that should be allowed to access the connection. The **Groups** node contains a default group called **connection**. You cannot select any other types for the connection group in the Configuration page. The Type, Name, and Description of the groups are also displayed. Select the groups,

click **Finish**, and then complete the fields in the Configuration section of the page as follows:

Field	Description
Name	The group name. You may rename this group. The name cannot have spaces or use special characters reserved by Integration Server or Designer. For more information about the use of special characters, see the *Designer Service Development* online help.
Group Type	Only one instance of each group type shown below may be selected for a provider connector's connection configuration. ■ **oauth**: Indicates that the group is defined with the authentication type of OAuth. ■ **oauth_v10a**: Indicates that the group is defined with the details of OAuth V1.0a authentication scheme. ■ **oauth_v20**: Indicates that the group is defined with the details of OAuth V2.0 authentication scheme. ■ **protocol**: Indicates that the group is defined with the HTTP transport protocol that the connection will use. ■ **connection**: Indicates that the group is defined with the login endpoint to initiate communication with the SaaS provider. ■ **RequestHeaders**: Indicates that the group is defined with the names of the HTTP request headers to include when sending the login request. ■ **credentials**: Indicates that the group is defined with a user account on the SaaS provider that the connection will use to connect to the SaaS provider. ■ **custom**: A user-defined group. ■ **aws_v2**: Indicates that the user will use Signature Version 2 to sign Amazon Web Services Query API requests. ■ **aws_s3**: Indicates that the group is defined for the Amazon S3 authentication scheme and it uses the Access Key and the Secret Key of the client to authenticate the requests. ■ **aws_v4**: Indicates that the user will use Signature Version 4 to sign Amazon Web Services Query API requests.
Description	Optional. Type a description for the connection group.

Field	Description
Fields	Based on the group type you selected above, CloudStreams displays the applicable fields for which you should specify values. Required fields are marked with an asterisk. Refer to the table below.

If the group type is...	The available fields are...
oauth	**OAuth Config Alias**: The alias of a configured OAuth token.
oauth_v10a	■ Consumer ID: The 'Consumer Key' issued by the Service Provider and used by the consumer to identify itself to the Service Provider. ■ Consumer Secret: A secret used by the Consumer to establish ownership of the 'Consumer Key'. ■ Access Token: A value used by the Consumer to gain access to the Protected Resources on behalf of the User, instead of using the User's Service Provider credentials. ■ Access Token Secret: A secret used by the Consumer to establish ownership of a given 'Access Token'.
oauth_v20	■ Consumer ID: A 'client identifier' issued to the client to identify itself to the authorization server. ■ Consumer Secret: A secret matching to the 'client identifier'. ■ Access Token: A token used by the client to make authenticated requests on behalf of the resource owner. ■ Instance URL: Optional field, used to specify a runtime host, if applicable. This may be required in some backends like Salesforce. ■ Refresh Access Token: Option to refresh the 'Access Token'. OAuth 2.0 access tokens typically have a very short lifetime. When an access token expires, the OAuth profile does not automatically refresh the expired access token. Select this option if you want an expired access token to be refreshed automatically. If you select this option, you must also specify the relevant refresh parameters. The access token is refreshed whenever the session expires. Session expiration is handled according to the setting of the Session Management property in your connection. Note that if Session Management is set to "none", then you

If the group type is...	The available fields are...

must manually modify the access token in the OAuth alias. (The Refresh Access Token option will not be applicable in this case). Default is 'false'.

- Refresh Token: A token used by the client to obtain a new access token without having to involve the resource owner.
- Refresh URL: The provider specific URL to refresh an 'Access Token'. This is required when 'Refresh Access Token' is enabled (configured to 'true') and Refresh URL Request is configured to 'URL Query String' or 'Body Query String'.
- Refresh URL Request: Options for sending the parameters in the 'Access Token' refresh request. The options are 'URL Query String', 'Body Query String', and 'Custom ESB Service'. Default is 'Body Query String'.

- URL Query String: The refresh request parameters, for example, refresh_token, grant_type, and so on, and their values are sent as query strings in the URL of the POST request.

Example:

```
www.examplebackend.com/o/
oauth2/token?grant_type=refresh_token&client_id=
842428530070-pubfebfgfqkgj6t54m4ns6&client_secret=
4adQT95cAtUxWINbDxGP9SJ4&refresh_token=
1%2Fn072P4BXpuNObjCLUtiZTc4fMH6YersmxBIv8QN3bhw
```

- Body Query String: The refresh request parameters, for example, refresh_token, grant_type, and so on, and their values are sent as query strings in the body of the POST request.

Example:

```
POST /o/oauth2/token HTTP/1.1
Host: accounts.backend.com
Content-length: 163
content-type: application/x-www-form-urlencoded
client_secret4adQT95cAtUxWINbDxGP9SJ4&
grant_type=refresh_token&refresh_token=
1%2Fn072P4BXpuNObjCLUtiZTc4fMH6Yersmx
BIv8QN3bhw&client_id=407408718192
```

- Custom ESB Service: If the backend requires the refresh request in a custom format, for example, requests which need more parameters than the ones specified by OAuth v2.0, or the backend uses some custom way of organizing

If the group type is...	The available fields are...
	parameters, or expects some other HTTP method request (other than POST), use the "Custom ESB Service" option. Refresh Custom ESB Service: User implemented service for refreshing the 'Access Token'. This is required when the 'Custom ESB Service' option is selected as the 'Refresh URL Request'. This service must strictly conform to the specification: `- wm.cloudstreams.service.common.lookup .specs:oauthTokenRefreshServiceSpec` Authorization Header Prefix: The prefix to be used with the 'Access Token' in the Authorization header. Options are 'Bearer' and 'OAuth'. Default is 'Bearer'.
protocol	■ **Element Character Set**: The encoding to use for the HTTP request line, headers, etc. ■ **HTTP Content Character Set**: The encoding to use for the request message. ■ **HTTP Protocol Version**: The HTTP version (HTTP/0.9, HTTP/1.0 or HTTP/1.1. The default value for the connection factory is HTTP/1.1. ■ **User Agent**: The value to the connection configuration will send for the User-Agent request header. ■ **Use Expect Continue**: If true, use the Expect/Continue HTTP/1.1 handshake and send the Expect request header. ■ **Wait For Continue Time**: The number of milliseconds that the connection factory's client connection should wait for a "100 Continue" response from the server. ■ **Strict Transfer Encoding**: If true, the connection factory connection raise an exception if the "Transfer-Encoding" header is invalid. ■ **Use Chunking**: If true, use HTTP/1.1 chunking, using a chunk size that matches the socket buffer size. ■ **Follow Server Redirects**: If true, follow server redirects. ■ **Server Redirect Maximum Tries**: Maximum number of times to follow a server redirect.
connection	■ **Server URL**: The native provider endpoint target for the connection configuration. The default configuration field provided with the connection factory is `cn.providerURL`.

If the group type is...	The available fields are...
	■ **Min Pool Connections**: The minimum number of socket connections to reserve for a connection configuration alias. ■ **Max Pool Connections**: The maximum number of socket connections to reserve for a connection configuration alias. ■ **Connection TimeOut**: The number of milliseconds a connection attempt will wait before giving up. (0 will wait indefinitely). ■ **Socket Read Timeout**: The number of milliseconds in which the the client must read a response message from the server. (0 will wait indefinitely). ■ **Use Stale Checking**: If true, the connection factory performs additional processing to test the socket to see if it is still functional each time it is used. ■ **Connection Retry Count**: How many times should the connection factory attempt to execute a failed invocation. ■ **Retry on Response Failure**: If true, the retry mechanism will be used for failed responses even if the request was sent successfully. ■ **Use TCP NoDelay**: If true, do not use Nagles algorithm as a socket optimization technique. ■ **Socket Linger**: Determines how quickly a socket should close. ■ **Socket Buffer Size**: The size of the read and write socket buffers, in bytes. ■ **Socket Reuse Address**: If true, the socket will be reused even if it is in TIME_WAIT due to a previous socket closure. ■ **Hostname Verifier**: Fully qualified class name that implements the Apache HC org.apache.http.conn.ssl.X509HostnameVerifier interface. Guards against "man-in-the-middle" attacks. ■ **Proxy Server Alias**: The alias to a web proxy server configuration in Integration Server. ■ **Trust Store Alias**: Alias for the Integration Server trust store configuration. ■ **Session Token**: Session token for a stateful session.
requestHeaders	■ **Request Header Names**: An array of request header names to include for this connection configuration. The value

If the group type is...	The available fields are...
	should be a comma-delimited list of header names; for example `Content-Type,SOAPAction`. ■ **Request Header Values**: An array of request header values to include for this connection configuration. The value should be comma-delimited list of values in the same order as the header names; for example, `text/xml,login`.
credentials	■ **Username**: The username credentials for the current connection configuration. ■ **Password**: The password credentials for the current connection configuration ■ **Preemptive Auth**: If true, basic auth credentials will be included when a request is sent. (It will not wait for a 401 response challenge.) ■ **Authorization Type**: The string identifying the authentication protocol scheme to use for the connection configuration. ■ **Domain Name**: The domain/security realm for the current connection configuration. ■ **Keystore Alias**: Alias for the Integration Server key store configuration. ■ **Client Key Alias**: Alias to reference a key inside a key store file.
custom	User-defined fields of a custom group.

6. Add additional connection group types, if desired, by right-clicking the **Groups** node and clicking **Add Group**.
7. If your provider requires a Login Sequence, configure it as follows:
   a. Right-click the **Login Sequence** node and select **Add Operation**.

      The Login Sequence/Logout Sequence will be enabled for SOAP based connections only if you have configured any Login/Logout Operation under Services. The Login Sequence/Logout Sequence will be enabled by default for REST based connections.

   b. Right-click the login operation under the Login Sequence node and select **Add Mapping**.
   c. In the Configuration section of the page assign a name to the step (for example `XYZSoapService:login`), select the **Login** operation and optionally enter a description.

A **Mapping** node is added under the login operation.

d. Now the Configuration section of the page shows the document types that were generated for the login service WSDL for the request and response messages. Define the mappings by inserting values into the request message or extracting values from the response message as needed. For the Salesforce.com connector, for example, the username and password values are inserted into the request message by selecting the configured values that are defined in the managed connection page. Then, the session token and a server URL are extracted from the response message to be inserted into special connection factory fields. These fields are used when invoking any of the Simple or Complex operations.

e. Right-click the request message's username (for example, **HDR1:username**) and select **Set configuration**.

f. In the Set Configuration dialog that appears, assign a name to the mapping, select the connection user name key field (for example **cr.username**), and select one of the following types:

- **Cookie**: HTTP cookies. For example, the Salesforce.com connector inserts the session token from a valid login in the SOAP header of the business operations to be executed. Other providers do the same thing; however, the token is managed via cookies instead of the SOAP header.
- **Header**: Request or response HTTP transport headers for the support connection factory implementation.
- **IData**: IData is a variable name that is associated with the connection instance when the service is invoked. It is a subset of those configuration fields from the selected groups. Not all fields are eligible for use as a mapping step since their values may not be changed or have any useful meaning in this context.
- **Literal**: A constant value.
- **Parameter**: Primarily used for REST handlers.
- **Service**: The Service type applies to the source, not to the target. Select Service if you want the source to call a given service to perform certain tasks and to map the output of the service to a target. The service must adhere to wm.cloudstreams.service.common.lookup.specs:mapServiceSpec. If an error occurs related to service validation or execution, CloudStreams throws a Mapping Exception.
- **XPath**: Enables you to define an XPath expression.

g. Click **OK**.

A green check mark is shown next to the request message field you just mapped.

The Connections Configuration Page (REST)

You need to create one or more run-time connections to the SaaS provider.

To configure a connection using the Connections Configuration page:

1. In Software AG Designer, open the CloudStreams Development perspective by clicking **Window > Open Perspective > Other > CloudStreams Development**.
2. In the CloudStreams Connectors view, expand your CloudStreams Provider project and click the cloud connector you just created. The **Overview** page is displayed, showing the general information you defined in the New Cloud Connector wizard.
3. Click the **Connections** link in the Plug-In Contents section of the page (or click the **Connections** tab at the bottom of the page). The Connections Configuration page is displayed.
4. Create a run-time connection by right-clicking the **Connections** node, clicking **Add Connection** and assigning a name and optional description to the connection. The name cannot contain special characters. CloudStreams creates the connection in the **Connections** node, and by default it will contain a **Groups** node.
5. Right-click on the **Groups** node and click **Add Group** to select one or more groups in the **New Group** window that should be allowed to access the connection. The **Groups** node contains a default group called **connection**. You cannot select any other types for the connection group in the Configuration page. The Type, Name, and Description of the groups are also displayed. Select the groups, click **OK**, and then complete the fields in the Configuration section of the page as follows:

Field	Description
Name	The group name. You may rename this group. The name cannot have spaces or use special characters reserved by Integration Server or Designer. For more information about the use of special characters, see the *Designer Service Development* online help.
Group Type	Only one instance of each group type shown below may be selected for a provider connector's connection configuration. ■ **oauth**: Indicates that the group is defined with the authentication type of OAuth. ■ **oauth_v10a**: Indicates that the group is defined with the details of the OAuth V1.0a authentication scheme. ■ **oauth_v20**: Indicates that the group is defined with the details of the OAuth V2.0 authentication scheme. ■ **protocol**: Indicates that the group is defined with the HTTP transport protocol that the connection will use. ■ **connection**: Indicates that the group is defined with the login endpoint to initiate communication with the SaaS provider.

Field	Description
	■ **requestHeaders**: Indicates that the group is defined with the names of the HTTP request headers to include when sending the login request. ■ **credentials**: Indicates that the group is defined with a user account on the SaaS provider that the connection will use to connect to the SaaS provider. ■ **aws_v4**: Indicates that the user will use Signature Version 4 to sign Amazon Web Services Query API requests. ■ **aws_v2**: Indicates that the user will use Signature Version 2 to sign Amazon Web Services Query API requests. ■ **aws_s3**: Indicates that the group is defined for the Amazon S3 authentication scheme and it uses the Access Key and the Secret Access of the client to authenticate the requests. ■ **custom**: A user-defined group.
Description	Optional. Type a description for the connection group.
Fields	Based on the group type you selected above, CloudStreams displays the applicable fields for which you should specify values. Required fields are marked with an asterisk. Refer to the table below.

If the group type is...	The available fields are...
oauth	**OAuth Config Alias**: The alias of an OAuth token that was configured in Integration Server Administrator.
oauth_v10a	■ Consumer ID: The 'Consumer Key' issued by the Service Provider and used by the consumer to identify itself to the Service Provider. ■ Consumer Secret: A secret used by the Consumer to establish ownership of the 'Consumer Key'. ■ Access Token: A value used by the Consumer to gain access to the Protected Resources on behalf of the User, instead of using the User's Service Provider credentials. ■ Access Token Secret: A secret used by the Consumer to establish ownership of a given 'Access Token'.

If the group type is...	The available fields are...
oauth_v20	■ Consumer ID: A 'client identifier' issued to the client to identify itself to the authorization server. ■ Consumer Secret: A secret matching to the 'client identifier'. ■ Access Token: A token used by the client to make authenticated requests on behalf of the resource owner. ■ Instance URL: Optional field, used to specify a runtime host, if applicable. This may be required in some backends like Salesforce. ■ Refresh Access Token: Option to refresh the 'Access Token'. OAuth 2.0 access tokens typically have a very short lifetime. When an access token expires, the OAuth profile does not automatically refresh the expired access token. Select this option if you want an expired access token to be refreshed automatically. If you select this option, you must also specify the relevant refresh parameters. The access token is refreshed whenever the session expires. Session expiration is handled according to the setting of the Session Management property in your connection. Note that if Session Management is set to "none", then you must manually modify the access token in the OAuth alias. (The Refresh Access Token option will not be applicable in this case). Default is 'false'. ■ Refresh Token: A token used by the client to obtain a new access token without having to involve the resource owner. ■ Refresh URL: The provider specific URL to refresh an 'Access Token'. This is required when 'Refresh Access Token' is enabled (configured to 'true') and ‘Refresh URL Request’ is configured to 'URL Query String' or 'Body Query String'. ■ Refresh URL Request: Options for sending the parameters in the 'Access Token' refresh request. The options are 'URL Query String', 'Body Query String', and 'Custom ESB Service'. Default is 'Body Query String'. ■ URL Query String: The refresh request parameters, for example, refresh_token, grant_type, and so on, and their values are sent as query strings in the URL of the POST request. Example:

If the group type is...	The available fields are...

	`www.examplebackend.com/o/oauth2/token?grant_type=refresh_token&client_id=842428530070-pubfebfgfqkgj6t54m4ns6&client_secret=4adQT95cAtUxWINbDxGP9SJ4&refresh_token=1%2Fn072P4BXpuNObjCLUtiZTc4fMH6YersmxBIv8QN3bhw`
	■ Body Query String: The refresh request parameters, for example, refresh_token, grant_type, and so on, and their values are sent as query strings in the body of the POST request.
	Example:
	`POST /o/oauth2/token HTTP/1.1`
	`Host: accounts.backend.com`
	`Content-length: 163`
	`content-type: application/x-www-form-urlencoded`
	`client_secret4adQT95cAtUxWINbDxGP9SJ4&grant_type=refresh_token&refresh_token=1%2Fn072P4BXpuNObjCLUtiZTc4fMH6YersmxBIv8QN3bhw&client_id=407408718192`
	■ Custom ESB Service: If the backend requires the refresh request in a custom format, for example, requests which need more parameters than the ones specified by OAuth v2.0, or the backend uses some custom way of organizing parameters, or expects some other HTTP method request (other than POST), use the 'Custom ESB Service' option.
	Refresh Custom ESB Service: User implemented service for refreshing the 'Access Token'. This is required when the 'Custom ESB Service' option is selected as the 'Refresh URL Request'. This service must strictly conform to the specification:
	`- wm.cloudstreams.service.common.lookup.specs:oauthTokenRefreshServiceSpec`
	Authorization Header Prefix: The prefix to be used with the 'Access Token' in the Authorization header. Options are 'Bearer' and 'OAuth'. Default is 'Bearer'.

protocol	■ **Element Character Set**: The encoding to use for the HTTP request line, headers, etc. ■ **HTTP Content Character Set**: The encoding to use for the request message. ■ **HTTP Protocol Version**: The HTTP version (HTTP/0.9, HTTP/1.0 or HTTP/1.1. The default value for the connection factory is HTTP/1.1. ■ **User Agent**: The value to the connection configuration will send for the User-Agent request header.

If the group type is...	The available fields are...
	■ **Use Expect Continue**: If true, use the Expect/Continue HTTP/1.1 handshake and send the Expect request header. ■ **Wait For Continue Time**: The number of milliseconds that the connection factory's client connection should wait for a "100 Continue" response from the server. ■ **Strict Transfer Encoding**: If true, the connection factory connection raise an exception if the "Transfer-Encoding" header is invalid. ■ **Use Chunking**: If true, use HTTP/1.1 chunking, using a chunk size that matches the socket buffer size. ■ **Follow Server Redirects**: If true, follow server redirects. ■ **Server Redirect Maximum Tries**: Maximum number of times to follow a server redirect.
connection	■ **Server URL**: The native provider endpoint target for the connection configuration. The default configuration field provided with the connection factory is `cn.providerURL`. ■ **Min Pool Connections**: The minimum number of socket connections to reserve for a connection configuration alias. ■ **Max Pool Connections**: The maximum number of socket connections to reserve for a connection configuration alias. ■ **Connection TimeOut**: The number of milliseconds a connection attempt will wait before giving up. (0 will wait indefinitely). ■ **Socket Read Timeout**: The number of milliseconds in which the the client must read a response message from the server. (0 will wait indefinitely). ■ **Use Stale Checking**: If true, the connection factory performs additional processing to test the socket to see if it is still functional each time it is used. ■ **Connection Retry Count**: How many times should the connection factory attempt to execute a failed invocation. ■ **Retry On Response Failure**: If true, the retry mechanism will be used for failed responses even if the request was sent successfully. ■ **Use TCP NoDelay**: If true, do not use Nagles algorithm as a socket optimization technique.

If the group type is...	The available fields are...
	■ **Socket Linger**: Determines how quickly a socket should close. ■ **Socket Buffer Size**: The size of the read and write socket buffers, in bytes. ■ **Socket Reuse Address**: If true, the socket will be reused even if it is in TIME_WAIT due to a previous socket closure. ■ **Hostname Verifier**: Fully qualified class name that implements the Apache HC org.apache.http.conn.ssl.X509HostnameVerifier interface. Guards against "man-in-the-middle" attacks. ■ **Proxy Server Alias**: The alias to a web proxy server configuration in Integration Server. ■ **Trust Store Alias**: Alias for the Integration Server trust store configuration. ■ **Session Token**: Session token for a stateful session.
requestHeaders	■ **Request Header Names**: An array of request header names to include for this connection configuration. The value should be a comma-delimited list of header names; for example `Content-Type,SOAPAction`. ■ **Request Header Values**: An array of request header values to include for this connection configuration. The value should be comma-delimited list of values in the same order as the header names; for example, `text/xml,login`.
credentials	■ **Username**: The username credentials for the current connection configuration. ■ **Password**: The password credentials for the current connection configuration ■ **Preemptive Auth**: If true, basic auth credentials will be included when a request is sent. (It will not wait for a 401 response challenge.) ■ **Authorization Type**: The string identifying the authentication protocol scheme to use for the connection configuration. ■ **Domain Name**: The domain/security realm for the current connection configuration. ■ **Keystore Alias**: Alias for the Integration Server key store configuration.

If the group type is...	The available fields are...
	■ **Client Key Alias**: Alias to reference a key inside a key store file.
aws_v4	■ **Access Key**: This is a username. It is an alphanumeric text string that uniquely identifies the user who owns the account. No two accounts can have the same AWS Access Key. ■ **Secret Key**: This key plays the role of a password. It is called secret because it is assumed to be known only by the owner. When you type the secret key, it is displayed as asterisk or dots. ■ **Region**: An area-specific value.
aws_v2	■ **Signing Algorithm**: Explicitly specify the signing algorithm (e.g. HMAC-SHA1 Signatures) used to sign the message. ■ **Access Key**: This is a username. It is an alphanumeric text string that uniquely identifies the user who owns the account. No two accounts can have the same AWS Access Key. ■ **Secret Key**: This key plays the role of a password. It is called secret because it is assumed to be known only by the owner. When you type the secret key, it is displayed as asterisk or dots. ■ **Region**: An area-specific value.
aws_s3	■ **Access Key**: This is a username. It is an alphanumeric text string that uniquely identifies the user who owns the account. No two accounts can have the same AWS Access Key. ■ **Secret Key**: This key plays the role of a password. It is called secret because it is assumed to be known only by the owner. When you type the secret key, it is displayed as asterisk or dots. ■ **Region**: An area-specific value.
custom	User-defined fields of a custom group.

6. Add additional connection group types, if desired, by right-clicking the **Connections** node and clicking **Add Group**.
7. If your provider requires a Login Sequence, configure one as follows:

a. Right-click the **Login Sequence** node, select **Add Resource**, select the Type **Login**, and click **Next**.

The Login Sequence/Logout Sequence will be enabled for SOAP based connections only if you have configured any Login/Logout Operation under Services. The Login Sequence/Logout Sequence will be enabled by default for REST based connections.

b. Configure a Login resource by completing the fields as follows.

Field	Description
Name	Specify a name for the Login resource.
Document Reference	Click **Browse** and select a Document Reference.
Content Type	Specify the Content-Type of the Document Reference.

c. Click **Next**.

d. Create a Request for the Login resource by completing the fields as follows.

Field	Description
Name	Specify a name for the Request.
Document Reference	Click **Browse** and select a Document Reference, for example **myConnector_v1.customDoctypes:docTypeRef_LoginInput**.
Content Type	Specify the Content-Type of the Document Reference, for example, **application/xml**.

e. Click **Next**.

f. Create one or more Responses for the Login resource by completing the fields as follows.

Field	Description
Name	Specify a name for the Response.
Document Reference	Click **Browse** and select a Document Reference, for example **myConnector_v1.customDoctypes:docTypeRef_LoginOutput**.

Field	Description
Code	Specify a code for the Response, such as 201 or 400. Response codes should be comma separated.
Content Type	Specify the Content-Type of the Document Reference for example, **application/xml**.

g. Click **Next**.

h. Create a parameter for the Login resource by completing the fields as follows.

Field	Description
Name	Specify a name for the parameter.
Active	Specifies whether the parameter is active.
Type	Select the parameter's type, for example **URI_CONTEXT**. For more information, see Understanding REST Parameters at the end of this procedure.
Description	Optional description of the parameter.

i. Click **Finish**.

j. Define the input/output mappings for the Login Sequence by right-clicking the Login Sequence name, selecting **Add Mapping**, and completing the fields as follows.

Field	Description
Type	Select **IN** or **OUT**.
Mapping fields	For example, for input fields, you might enter the display names `Username` and `Password`, and the values `cr.username` (the connection user name key field) and `cr.password`, respectively. And for output fields, you might enter the following display names and values: ■ `Server URL` (with value `cx.serverUrl`). ■ `Provider URL` (with value `cn.providerUrl`). ■ `Session Token` (with value `cn.sessionToken`).

Field	Description
	■ `Fault String` (with value `cx.faultString`).

8. Configure a **Logout Sequence** in a similar manner.

   The Login Sequence/Logout Sequence will be enabled for SOAP based connections only if you have configured any Login/Logout Operation under Services. The Login Sequence/Logout Sequence will be enabled by default for REST based connections.

9. View the **Manifest** node, which shows read-only fields containing attributes whose values were captured from your cloud connector definition. The version of the CloudStreams Development Plug-in (Created-By) is also displayed. For imported plug-ins created in a Designer release prior to 9.7, this information is not shown.

Understanding REST Parameters for Global Mappings

CloudStreams REST connector services allow you to set parameters which become part of the outgoing request.

REST services rely on HTTP methods like GET, POST to make request to a SaaS provider, so the parameters are closely tied to these HTTP methods, where they are sent as part of these HTTP method requests.

The parameters are typically part of the HTTP URI which may be of the following format:

[scheme:][//authority][path][?query]

CloudStreams supports the following parameter styles:

Type	URI Scope
URI_CONTEXT	path
QUERYSTRING_PARAM	query
CFG_PARAM	authority, path

URI_CONTEXT parameters are passed as the path component of a REST resource URI, and the parameter names correspond to the URI path variable names specified in the {} annotation. For example, a sample request might look like this:

```
services/async/25.0/job/{jobId}
```

In the above sample request, the URI path variable name `jobId` is specified as a parameter to the job resource. The annotation {} is set to the variable name `jobId`. At service run time, the variable is substituted with its runtime value to form the dynamic path.

A sample resource definition with URI_CONTEXT parameter:

```
<resource name="Job" method="POST" path="services/async/25.0/job/{jobId}">
  <parameters>
     <parameter name="jobId" isRequired="true" style="URI_CONTEXT"/>
  </parameters>
</resource>
```

QUERYSTRING_PARAM parameters are passed as the query component of a REST resource invocation request.

The following example demonstrates a typical HTTP GET request with parameters that form a query string of the resource URI.

```
GET  /status?key1=value1&key2=value2 HTTP/1.1
Host: www.softwareag.com
Content-Length: 0
```

Notice that the parameters are added to the path after a "?", and specified as ampersand (&) separated list of key-value pairs, with the corresponding Content-Length set accordingly. The key and values passed as parameters are URL-encoded by CloudStreams.

A sample resource definition with QUERYSTRING_PARAM parameter:

```
<resource name="GetStatus" method="GET" path="/status">
  <parameters>
     <parameter name="key1" isRequired="true" style="QUERYSTRING_PARAM"/>
     <parameter name="key2" isRequired="false" style="QUERYSTRING_PARAM"/>
  </parameters>
</resource>
```

CFG_PARAM parameters signify an internal contract between the connector tier and the connecter-specific authentication scheme along with the virtual runtime layer.

The allowed set of parameter name, which can be specified as CFG_PARAM depends on the authentication scheme used for the connector definition.

Example

`aws.bucketName` is a parameter which is used by the Amazon Authentication Scheme version 3 for specifying the dynamic host based on the parameter value.

While executing a resource with such parameter, the service endpoint is prefixed with the appropriate bucket name.

```
<resource name="GetBucket" method="GET" path="/">
  <parameters>
      <parameter name="aws.bucketName" isRequired="true" style="CFG_PARAM"/>
   </parameters>
</resource>
```