Informatica® Cloud Application Integration
October 2022

Connectors for Cloud Application Integration

Informatica Cloud Application Integration Connectors for Cloud Application Integration
October 2022

Publication Date: 2023-10-05

Table of Contents

Preface 4

Chapter 1: Connectors for Cloud Application Integration 5

Connectors for Application Integration 5

Types of Connectors 5

Informatica Cloud Connectors 6

Listener-Based Connectors 7

High availability, load balancing, and clustering for listener-based connectors 7

Starting and stopping listener-based connections 8

Preface

Refer to the *Connectors for Cloud Application Integration Guide* for information about the different types of connectors available in Informatica Intelligent Cloud Services℠ Application Integration.

CHAPTER 1

Connectors for Cloud Application Integration

This chapter includes the following topics:

- Connectors for Application Integration, 5
- Informatica Cloud Connectors, 6
- Listener-Based Connectors, 7

Connectors for Application Integration

Application Integration offers multiple connectors designed to work with the connections and processes you configure for integration with web services and applications. All the supported connectors allow you to interact with services or data sources outside Informatica Intelligent Cloud Services℠. You can also run specific operations against an API, web service, or database.

Types of Connectors

You can use the following types of connectors:

Application Integration Connectors

Application Integration connectors are designed to access data to and from the cloud for each of your applications. Connectors for JDBC, Workday, SAP, OData, and Salesforce are in this category.

Message-Based Connectors

Message-based connectors are designed so you can configure queue-based message brokers like ActiveMQ and JMS. The AMQP and Amazon SQS connectors are in this category.

Listener-Based Connectors

Listener-based connectors are designed to perform the following tasks:

- Monitor file-based systems for files or objects on a file system or other type of storage. You can retrieve files and process the contents of the files or perform file operations like moving or reading file metadata. For example, you can parse comma-delimited file, make the file contents available in a process object as XML, and archive the processed file in another directory. The file or object metadata, such as the number of rows or time stamp, is also available in a process object. The File, FTP, and Amazon S3 connectors are in this category.

- Access event services to perform tasks like reading XML from a process object and creating comma-delimited files or reading binary files from a process stream and writing that binary content to the target file system.

Service Connectors

Service connectors are designed with Process Designer to specify the parameters and actions that associate with a specific service that you want to make available in a process.

Event Sources and Event Targets

With the listener-based connectors, you also define:

- Event Sources, which act as consumers or start events to trigger processes.
- Event Targets, which act as event services that you can use to invoke external systems.

Informatica Cloud Connectors

Informatica certifies that the following connectors work with Application Integration. If you want to certify a connector that is not in this list, contact your sales representative.

JDBC

JDBC (Java Database Connectivity) is a Java API that enables Java programs to execute SQL statements and interact with any SQL-compliant database. JDBC makes it possible to write a single database application that can run on different platforms and interact with different DBMS systems. Ensure that you use the latest database driver version that your database supports.

Note: Informatica provides two JDBC connectors: JDBC and JDBC_IC. Only the JDBC_IC connector is used by Application Integration.

OData

OData Connector helps you to integrate systems like SharePoint and Team Foundation Server that are OData compliant with other on-premise or cloud applications. It is a standardized protocol for creating and consuming data APIs. OData builds on core protocols like HTTP and commonly accepted methodologies like REST.

Salesforce

Salesforce Connector lets you create guides and processes that read information from and write information to Salesforce. Outbound messages from Salesforce can trigger processes that perform background processing of information and write information back to Salesforce.

SAP

You can use SAP BAPI Connector to integrate with SAP BAPIs and read, create, change, or delete data in SAP. SAP BAPI Connector is available as a service call in Informatica Cloud Application Integration. For example, to update the sales order data in SAP, you can configure an SAP BAPI connection to access the BAPI_SALESORDER_CHANGE function.

Workday

Workday Connector allows you to integrate data with Workday applications. For example, you can retrieve information about an employee and th employee's dependents or onboard a new hire.

Cloud Application Integration Connectors

Application Integration provides several connectors. For more information, see the documentation for the specific connector (such as Amazon S3 Connector or File Connector).

Listener-Based Connectors

Application Integration supports several types of listener-based connectors that can be used for event-based processing of messages and files. Process Designer exposes a wide range of attributes in the connectors so you can use many file listener properties when you configure a listener-based connection.

These connectors, like the AMQP Connector (message-based) and File Connector (file/storage-based), act as message brokers or file monitors that can be reused to make data objects, service calls, and events available to the Process Designer.

High availability, load balancing, and clustering for listener-based connectors

If the Process Server uses a Secure Agent group, the following listener-based connectors support high availability, load balancing, and clustering:

- Amazon S3
- Amazon SQS
- AMQP
- File
- FTP
- Kafka
- RabbitMQ
- Salesforce

You can use Secure Agent groups to deploy Process Server services using the following Secure Agent configurations:

Secure Agent load balanced configuration

Use this configuration to evenly distribute the workload across Process Server instances within a group. When you deploy an asset to a Secure Agent group, Informatica Intelligent Cloud Services performs load balancing. You can use the Secure Agent load balanced configuration to distribute requests if you process stateless requests or use the Secure Agent only to serve OData requests.

You can add multiple Secure Agents to a group to balance the distribution of tasks across Process Servers. At run time, Informatica Intelligent Cloud Services dispatches incoming requests to available Secure Agents in a round-robin manner.

Note: When the Process Server uses the Secure Agent group with the load balanced configuration, data duplication might occur. To avoid data duplication, Informatica recommends using the Secure Agent Cluster configuration on the Secure Agent group.

Secure Agent Cluster configuration

Use this configuration to provide high availability with Process Server instance clustering. You can cluster two or more agent groups into a single logical Process Server instance.

When the Process Server uses a Secure Agent cluster configuration, only one listener is active at any point of time. All Process Servers in the cluster share the PostgreSQL database of the master agent. When you deploy an asset to a Secure Agent Cluster, all Process Servers receive information about the process execution activity. The master Secure Agent receives information and informs the other Secure Agents. If a Secure Agent fails during process execution, the process fails over and continues to execute on another Secure Agent within the cluster.

In some fail-over situations, data duplication can occur. For example, there might be a short time lag between the time an agent shuts down and the time when another agent takes over. In this time period, if there is any in-flight data, the data might be duplicated in the agent that takes over the process execution.

If you use multiple listener-based connections, the Process Server distributes the routes across different Secure Agent machines in a Secure Agent group to ensure load balancing.

For more information about configuring the Process Server for high availability, load balancing, and clustering, see the Administrator help.

Starting and stopping listener-based connections

For listener-based connections that run on a Secure Agent or a Secure Agent group, you can start and stop event sources from the **Connections** page in Application Integration Console. You can also start and stop event sources in Kafka connections that have been published on the Cloud Server.

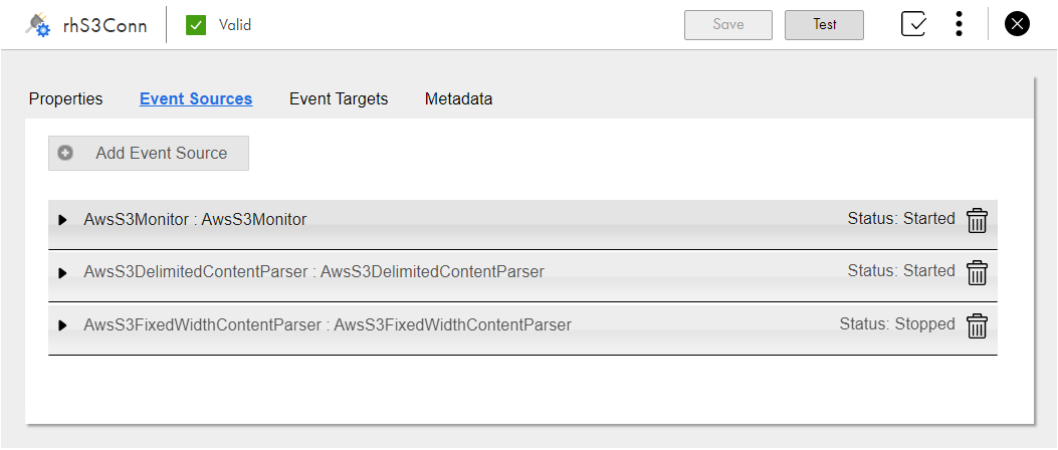
Application Integration updates the event source status on the **Event Sources** tab of the listener-based connections. You can view the status of each event source in the published connection. For a connection that runs a Secure Agent or a Secure Agent group, if the status of the event source is stopped, you can republish the connection and restart the event source. However, when you republish the connection, all the event sources in the connection start by default provided the Secure Agent is up and running. The status is updated on the **Event Sources** tab and on the **Connections** page in Application Integration Console. If you unpublish the connection, all the active event sources in the connection are stopped and the connection is removed from the **Connections** page in Application Integration Console. This behavior also applies to the event sources in Kafka connections that have been published on the Cloud Server.

Note: You can publish Kafka connections only on the AWS PODs on the Cloud Server.

When a connection runs on a Secure Agent group, if the event source is started for even one Secure Agent, the event source status is displayed as started. To stop an event source on a Secure Agent group, the event source must be stopped on all the Secure Agents in a group from Application Integration Console, only then the status of the event source is updated to stopped on the **Event Sources** tab. If you choose to stop an event source only on a selected Secure Agent for some reason, such as stability or connectivity issues with the endpoint, the event source is stopped on that specific Secure Agent. However, the status on the **Event Sources** tab is not updated because the event source is still running on the other Secure Agents in the group.

Note: The status is not displayed for invalid, unpublished, and outdated connections.

The following image shows the event source status for a listener-based connection:



Note: You might need to refresh the connection to view the updated status.

For more information about starting and stopping event sources in listener-based connections, see *Monitor*.