Informatica® Intelligent Cloud Services
Spring 2020 April

What's New
# Table of Contents

**Preface** ................................................................. 7

Informatica Resources .................................................. 7
Informatica Documentation ............................................. 7
Informatica Intelligent Cloud Services web site .................. 7
Informatica Intelligent Cloud Services Communities ............ 7
Informatica Intelligent Cloud Services Marketplace ............. 7
Data Integration connector documentation ...................... 8
Informatica Knowledge Base .......................................... 8
Informatica Intelligent Cloud Services Trust Center .......... 8
Informatica Global Customer Support .............................. 8

**Chapter 1: What’s New in Informatica Intelligent Cloud Services** .......... 9

**Chapter 2: API Manager** ............................................. 10

New features and enhancements ...................................... 10
OAuth 2.0 authentication for managed APIs ....................... 10
Prevent potential privacy policy breaches ......................... 10
Identify the version of an invoked managed API ................. 11
New features and enhancements in Fall 2019 December ........ 11
Changed behavior ....................................................... 11
Changed behavior in Fall 2019 December ........................ 12

**Chapter 3: Application Integration** ................................ 13

New features and enhancements in the Spring April 2020 release. 13
New features and enhancements in the January 2020 release .... 14
Changed behavior in the January 2020 release .................... 15

**Chapter 4: B2B Gateway** ............................................ 19

New features and enhancements ...................................... 19
Trigger file transfer tasks in inbound and outbound flows .... 19
Exchange files with trading partners through B2B Partners Portal. 19
B2B Partners Portal ..................................................... 19
SFTP file transfer ....................................................... 20
Home page ............................................................. 20
B2B Gateway connector ............................................. 20
Support additional X12 and EDIFACT messages Fall 2019 Jan and Feb. 20
Support additional X12 versions .................................. 21
Support additional EDIFACT ........................................ 21
Changed behavior ...................................................... 21
Privileges to access B2B Gateway ................................. 21
<table>
<thead>
<tr>
<th>Chapter 5: B2B Partners Portal</th>
<th>22</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features and enhancements</td>
<td>22</td>
</tr>
<tr>
<td>Exchange files with the portal provider</td>
<td>22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6: Cloud Integration Hub</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features and enhancements</td>
<td>23</td>
</tr>
<tr>
<td>Consume partial data with an API</td>
<td>23</td>
</tr>
<tr>
<td>Define retention period for unconsumed data</td>
<td>23</td>
</tr>
<tr>
<td>Asset management</td>
<td>23</td>
</tr>
<tr>
<td>Private publication repository</td>
<td>24</td>
</tr>
<tr>
<td>Changed behavior</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7: Data Integration</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features and enhancements</td>
<td>26</td>
</tr>
<tr>
<td>Asset management</td>
<td>26</td>
</tr>
<tr>
<td>Mappings</td>
<td>27</td>
</tr>
<tr>
<td>Transformations</td>
<td>28</td>
</tr>
<tr>
<td>Tasks</td>
<td>30</td>
</tr>
<tr>
<td>Taskflows</td>
<td>30</td>
</tr>
<tr>
<td>Data Integration Elastic</td>
<td>31</td>
</tr>
<tr>
<td>Parameter files</td>
<td>32</td>
</tr>
<tr>
<td>Expression editor</td>
<td>33</td>
</tr>
<tr>
<td>File listener</td>
<td>33</td>
</tr>
<tr>
<td>REST API</td>
<td>33</td>
</tr>
<tr>
<td>Changed behavior</td>
<td>34</td>
</tr>
<tr>
<td>Data Integration Elastic</td>
<td>34</td>
</tr>
<tr>
<td>Intelligent Structure Discovery</td>
<td>34</td>
</tr>
<tr>
<td>Transformations</td>
<td>34</td>
</tr>
<tr>
<td>Connectors</td>
<td>35</td>
</tr>
<tr>
<td>New connectors</td>
<td>36</td>
</tr>
<tr>
<td>Enhanced connectors</td>
<td>36</td>
</tr>
<tr>
<td>Changed behavior</td>
<td>44</td>
</tr>
<tr>
<td>Upgrading to Spring 2020</td>
<td>45</td>
</tr>
<tr>
<td>Preparing for the upgrade</td>
<td>45</td>
</tr>
<tr>
<td>Netezza Connector pre-upgrade tasks</td>
<td>46</td>
</tr>
<tr>
<td>Snowflake Cloud Data Warehouse V2 Connector pre-upgrade tasks</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8: Data Profiling</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features and enhancements</td>
<td>47</td>
</tr>
</tbody>
</table>
Chapter 9: Data Quality ......................................................... 49
New features and enhancements. ........................................... 49
Assets. ........................................................................ 49

Chapter 10: Mass Ingestion. .................................................. 51
New features and enhancements. ......................................... 51
Mass Ingestion Databases. .................................................. 51
Mass Ingestion Streaming. ................................................. 52
Common ingestion enhancements. ....................................... 54

Chapter 11: MDM - Reference 360. ....................................... 55
New features and enhancements. ......................................... 55
REST API. .................................................................... 55
Workflow email notification enhancements. ......................... 55
Improved loading of larger data sets. .................................... 56

Chapter 12: Operational Insights. ......................................... 57
New features and enhancements. ......................................... 57
Operational Insights for Application Integration. ................. 57
Operational Insights for Data Profiling. ............................... 57
Data Integration monitoring enhancements. ......................... 57
Secure Agent alerts. ..................................................... 58
Alert notifications. ....................................................... 59
Changed behavior. .......................................................... 59
Data Integration Overview page. ....................................... 59
PowerCenter workflow alerts. ............................................ 59
Upgrading to Spring 2020. ............................................... 60
Preparing for the Upgrade. ............................................... 60

Chapter 13: Administrator. .................................................. 61
New features and enhancements. ........................................ 61
Serverless runtime environments. ....................................... 61
Data Integration Elastic. .................................................. 61
Schedule export and import. ............................................. 62
Scheduled jobs reassignment. .......................................... 63
Source control. ................................................................ 63
File servers. ................................................................... 63
Changed behavior. .......................................................... 64
Data Integration Elastic. .................................................. 64
Upgrading to Spring 2020. ............................................... 64
Preparing for the upgrade. ............................................... 64
Netezza Connector pre-upgrade tasks ................................. 65
Snowflake Cloud Data Warehouse V2 Connector pre-upgrade tasks. .......................... 65
After You Upgrade. ............................................................................................ 65

Chapter 14: Monitor. ................................................................................. 67
New features and enhancements. ................................................................. 67
Session logs. ................................................................................................. 67
File transfer logs. .......................................................................................... 67
Monitor failed file events. ............................................................................. 67
Changed behavior. ......................................................................................... 68
Job details. ...................................................................................................... 68
Session log file names. .................................................................................. 68

Index. .......................................................................................................... 69
Preface

Read What’s New to learn about new features, enhancements, and behavior changes in Informatica Intelligent Cloud Services for the Spring 2020 release. You can also learn about upgrade steps that you might need to perform.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

Developers can learn more and share tips at the Cloud Developer community:

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:
Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB.Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, go to https://status.informatica.com/ and click SUBSCRIBE TO UPDATES. You can then choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or online.

For online support, click Submit Support Request in Informatica Intelligent Cloud Services. You can also use Online Support to log a case. Online Support requires a login. You can request a login at https://network.informatica.com/welcome.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.
What's New in Informatica Intelligent Cloud Services

The Spring 2020 April of Informatica Intelligent Cloud Services™ includes new features, enhancements, and changed behaviors.

The following services include updates in this release:

- Application Integration
- Data Integration
- Data Profiling
- Data Quality
- Mass Ingestion
- MDM - Reference 360
- Operational Insights
- Administrator
- Monitor
CHAPTER 2

API Manager

The Spring 2020 April release of Informatica Intelligent Cloud Services™ API Manager includes the following updates.

New features and enhancements

The Spring 2020 April release of API Manager includes the following new features and enhancements.

OAuth 2.0 authentication for managed APIs

You can enable OAuth 2.0 authentication for managed APIs that invoke a Cloud Application Integration process that uses basic authentication.

You cannot enable authentication for managed APIs that invoke a Cloud Application Integration process that uses anonymous authentication.

API Manager supports the client credentials grant type for OAuth 2.0 authentication. To enable OAuth 2.0 authentication, you create an OAuth 2.0 client in API Manager, and assign the client to APIs and API groups. You send the client ID and client secret to API consumers. API consumers use the client ID and secret to generate the OAuth 2.0 token that they have to provide to invoke the API. The token is valid for 20 minutes.

For more information, see the API Manager help.

Prevent potential privacy policy breaches

You can configure the API-specific privacy policies to issue warnings or block requests and responses that contain sensitive information.

For every type of information, you can apply one of the following actions to take when a request or a response contains that type of information:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>Issue a warning message in the security log that there was a privacy policy leakage in the request or the response. Don’t block the request or response.</td>
</tr>
<tr>
<td>Block</td>
<td>Block the request or response and issue a warning message in the security log that the message was blocked because of a potential privacy policy breach in the request or the response.</td>
</tr>
</tbody>
</table>

You can apply different actions to requests and responses for each type of information.
Identify the version of an invoked managed API

The activity log shows the API version for all API access instances.

New features and enhancements in Fall 2019 December

The Fall 2019 December release included the following new features and enhancements:

Reduce redundant backend load by creating response caching policies

You can create a response caching policy for a managed API. The policy determines the amount of time that API Manager stores API responses in the cache. API Manager removes the responses from the cache after the defined timeout. The maximum cache timeout is 3,600 seconds.

For more information, see “API-specific response caching policy” in the API Manager help.

API and API group management

You can more easily manage managed APIs and API groups with the following user experience improvements:

- Activate and deactivate a managed API on the API Details page.
- Create a managed APIs group and rename a group in the API Groups page.
- Add and remove managed APIs to and from a managed API group in the Group Details page.
- Add a managed API to a managed API group in the API Details page.

For more information, see “Managed API groups” in the API Manager help.

Context identification of managed API groups

You can add context to a managed API group. When you add context to a group, API Manager adds the context to all API URLs of the APIs that belong to the group. You can then sort the API URLs by group. For example, if you send API consumers a list of APIs that is based on the API URLs, APIs that belong to the same group are listed together.

For more information, see “Managed API groups” in the API Manager help.

API versioning

You can create multiple versions of a managed API that link to different Application Integration services. You can choose a default version.

For more information, see “Version management” in the API Manager help.

Changed behavior

The Spring 2020 April release includes the following changed behavior:

Organization policies

On the Policies page, rate limit and IP filtering organization policies are grouped under an Access tab.

Previously, the Policies page didn't contain tabs.
Analytics properties

The following properties are renamed in the activity and event logs:

<table>
<thead>
<tr>
<th>Name in previous releases</th>
<th>Renamed to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Consumer</td>
<td>Name of the user who initiated the managed API call. For managed APIs that use OAuth 2.0 authentication, consumer details also include the ID of the OAuth 2.0 client that invoked the API.</td>
</tr>
<tr>
<td>Consumer IP</td>
<td>IP Address</td>
<td>IP address that accessed the managed API.</td>
</tr>
</tbody>
</table>

Changed behavior in Fall 2019 December

The Fall 2019 December release included the following changed behavior:

**Organization IP filtering policy**

When you create or edit the organization IP filtering policy, you can define rules that apply to any range of IP addresses.

Previously, the IP range applied to a Class C network and only the last octets in the range could differ from each other.

**API Registry properties**

API-specific rate limits do not appear on the API Registry page. For each managed API, the API-specific rate limit appears on the API details page.

Previously, API-specific rate limits appeared on both the API Registry page and the API details page.
Chapter 3

Application Integration

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Application Integration includes the following updates:

New features and enhancements in the Spring April 2020 release

The Spring 2020 April release of Application Integration includes the following new features and enhancements:

Operational Insights for Application Integration

You can view analytics for Application Integration assets using Operational Insights. Operational Insights offers several charts that help you quickly and visually assess the status and usage of your Application Integration assets and take appropriate corrective actions if needed. You can view analytics related to API calls, processes, connections, and licensing.

For more information, see the Operational Insights online help.

Note: Informatica is introducing Operational Insights support for Application Integration in phases. Operational Insights will be enabled first on a regional basis and then to specific customers upon request before enabling it broadly for all Application Integration customers. If you would like to use Operational Insights with Application Integration before it is broadly released, contact your Customer Success Manager.

OAuth2 authentication for processes

You can enable OAuth2 authentication for a process by configuring the process to accept only HTTP authorization requests from the API Gateway. If you enable OAuth2 authentication, you can invoke the process only if you provide an OAuth token. You cannot invoke the process by using the service URL alone.

You must first create an OAuth2 client in API Manager, and get the client ID and client secret. Pass the client ID and client secret to the Informatica Intelligent Cloud Services Authz microservice to authenticate the user and get an OAuth token as the response. You can then use the OAuth token to invoke the process.

For more information about OAuth2 authentication, see the API Manager online help.
Asset dependencies

You can view asset dependencies for a process, service connector, app connection, guide, and process object from the corresponding asset designer page. You can view a list of objects that the asset depends on and a list of objects that the asset is dependent on.

You might want to view dependencies before performing certain operations on an asset. For example, you cannot delete an asset if another object depends on the asset. You must first delete the dependent objects and then delete the asset. You can find out the dependent objects by viewing the asset dependencies.

For more information, see Asset Management.

New features and enhancements in the January 2020 release

The January 2020 release of Application Integration included the following new features and enhancements:

Ability to create process objects by importing WSDL, XSD, or Swagger files

You can easily and simultaneously create multiple large and hierarchical process objects by importing one or more WSDL, XSD, or Swagger files. With this feature, you can save time and effort because you do not have to manually create process objects.

For more information, see Design.

Ability to create process inputs and run a process with process inputs

After you publish a process, you can create a process input, and run the process with the process input for testing purposes. You can also create multiple process inputs and run the process with all the inputs. You can create process inputs in the JSON or XML format.

After you run the process, you can view details of the successful and unsuccessful executions of the process instances.

For more information, see Invoke.

Process restart

Users who have the Admin or Operator role can restart a process from the Application Integration Console.

You can restart a process that meets the following criteria:

- The process was run at least once on the Cloud Server or on an agent.
- The process is in one of the following states:
  - Completed
  - Faulted
  - Suspended
- The tracing level for the process is set to Normal or Verbose.
- If the process contains attachments, the persistence type is set to Full or Persist.

For more information, see Monitor.
Swagger endpoint URL generation for OData-enabled JDBC connections

When you publish an OData-enabled JDBC connection, Application Integration generates an OData Swagger URL in addition to the OData Service URL. You can use the OData Swagger URL to view details of the endpoint and metadata of the OData API.

For more information, see JDBC Connector Guide.

Ability to disable Cloud access to OData endpoint URLs

In JDBC and Salesforce connections that are OData-enabled and configured to run on a Secure Agent machine or a Secure Agent group, you can choose to disable Cloud access to the OData endpoint URLs for security purposes.

Use the OData Cloud Access Enabled option in the connection to enable or disable Cloud access to the OData endpoint URLs. If you disable access, you cannot invoke the OData endpoint URLs from Cloud. You can invoke the OData endpoint URLs only from an agent. If you enable access, you can invoke the OData endpoint URLs from both Cloud and an agent.

For more information, see JDBC Connector Guide and Salesforce Connector Guide.

Unique API name override for processes

When you publish a process, Application Integration generates a unique API name for the process that is used in the service URLs.

You can use the Override API Name option while creating a process to override the auto-generated API name, and specify a meaningful name.

For more information, see Design.

Improved runtime information logging for the Assignment step

You can view runtime information for the Assignment step by using one of the following options:

- Set X-Debug=true as the HTTP header in the request.
- Use the Run Using option to create process inputs and run a process with one or more process inputs.

For more information, see Monitor.

JDBC advanced query support

In a process that uses a JDBC connection, when you assign a value to a field, you can select the Use Database-specific WHERE Clause Syntax option to use nested queries and other database-specific querying options.

For more information, see JDBC Connector Guide.

Changed behavior in the January 2020 release

The January 2020 release of Application Integration included the following changed behavior:

Improved XML and JSON recognition code in Service Connectors

Effective in the January 2020 release, if the response Content-Type header contains the term application in the first part and the term json in a subsequent part, Application Integration infers the response payload type as JSON. Similarly, if the response Content-Type header has the term text in the first part and the term xml in a subsequent part, Application Integration infers the payload type as XML.
Previously, if the response Content-Type header was `application/json`, Application Integration inferred the response payload type as JSON. If the response Content-Type header was `text/xml`, Application Integration inferred the response payload type as XML. If the response Content-Type header did not match the `application/json` or `text/xml` values, for example, `application/vnd.api+json; charset=UTF-8`, Cloud Application Integration treated the response payload as an attachment.

Informatica supports backward compatibility for this changed behavior. Therefore, if you had created a service connector in a previous release in which the response payload was treated as an attachment, after you upgrade to the January 2020 release, the service connector will continue to work as is. However, Informatica recommends that you redesign the service connector to take advantage of the improved content recognition feature. With this feature, you can simplify your service connector to get a normal JSON/XML response instead of working with an attachment.

For more information, see Design.

Support for multiple attachments in Service Connectors

Effective in the January 2020 release, a service connector can handle a multipart response appropriately and create multiple attachments for different response parts. The part related metadata information is available in the attachment properties.

A service connector can also recognize the payload part. The first JSON/XML/Text part is used as the payload. You can extract data from the payload in the output field expressions of the action as you would normally do when you work with non-multipart responses. Note that the selected payload will not be available as an attachment.

In the Output tab, you can use the Get from Attachments option to work with multiple attachments and pass the entire list of attachments to the selected variable except the part used as the payload. The following image shows the Get from Attachments option:

You can also use an expression to work with attachments in service connectors. Several new functions have been introduced to work with attachments. When you open the Expression Editor, you can find the new functions in the Functions tab, under the Output Attachments section as shown in the following image:
When you test a service connector, all the attachments are displayed. You can also download and review them.

For more information, see Design.

Get from Attachment option renaming

Effective in the January 2020 release, in the Get From list in the Output tab, the Attachment option is renamed to Entire Response As Attachment. The following image shows the Entire Response As Attachment option:

Note that only the label name has been changed. The Entire Response As Attachment option preserves backward compatibility. If you had created a service connector with a single attachment in a previous release, it will continue to work as is, and no manual changes are needed.

However, Informatica recommends that you use the new feature of handling multipart responses as multiple attachments to simplify the design. With the new feature, you do not have to manually split
attachments. You can also use the processing logic for attachments within the service connector itself instead of doing it within a process. Therefore, you can use a service connector within multiple processes without having to design the processing logic in multiple processes. You can also use the new functions available to work with output attachments.

For more information, see Design.
Chapter 4

B2B Gateway

The Spring 2020 April release of Informatica Intelligent Cloud Services™ B2B Gateway includes the following updates.

New features and enhancements

The Spring 2020 April release of B2B Gateway includes the following new features and enhancements.

Trigger file transfer tasks in inbound and outbound flows

You can select file transfer tasks to perform actions on inbound and outbound files.

File transfer tasks are available for selection when you use a file sever connection type and can include the following actions:

- Actions on inbound files: decompress, decrypt.
- Actions outbound files: compress, encrypt.

For more information, see the B2B Gateway help.

Exchange files with trading partners through B2B Partners Portal

You can enable your trading partners to send and receive files over HTTPS.

Partners can upload and download files through B2B Partners Portal.

For more information, see the B2B Partners Portal help.

B2B Partners Portal

Starting with the Fall 2019 January release, you can enable your partners to track and monitor events with B2B Partners Portal. Use B2B Partners Portal to share information with your trading partners and enable them to track and monitor file events for messages that they exchange with your organization.

Configure an Informatica Intelligent Cloud Services user with the appropriate user role for each user in your partners’ organizations. Then add your partners and users to B2B Partners Portal.

For more information about B2B Partners Portal, see the B2B Partners Portal help.

For more information about creating a B2B Partners Portal user, see the Administrator help.
SFTP file transfer

Starting with the Fall 2019 January release, you can use a cloud-based SFTP file server to exchange files with your partners. Configure an SFTP file server to send and receive files. Then select the File Servers connection type when you configure the partner.

For more information about configuring file servers, see the Administrator help.

Home page

Starting with the Fall 2019 January release, you can view the events in a specific graph on the Home page. To view the events in a specific graph, click the graph.

You can view events for the following graphs:

- Events status
- Number of events per partner
- Number of events per day

When you select to view events, the Events page opens with the appropriate filters applied.

B2B Gateway connector

Starting with the Fall 2019 January release, information about source files in inbound flows is added to B2B Gateway connector.

The field ORIGINAL_FILE_NAME contains the name of the source file that the inbound mapping processes.

Support additional X12 and EDIFACT messages Fall 2019 Jan and Feb

The following additional X12 messages were made available for exchange with partners in the Fall 2019 January and February releases:

- 211 - Motor Carrier Bill of Lading
- 215 - Motor Carrier Pickup Manifest
- 225 - Response to a Cartage Work Assignment
- 240 - Motor Carrier Package Status
- 309 - Customs Manifest
- 310 - Freight Receipt and Invoice
- 350 - Customs Status Information Document
- 353 - Customs Events Advisory Details
- 355 - U.S. Customs Acceptance/Rejection
- 357 - U.S. Customs In-Bond Information
- 358 - Customs Consist Information
- 838 - Trading Partner Profile

The following additional EDIFACT messages were made available for exchange with partners in the Fall 2019 January release:

- CUSRES - Customs Response Message
• CUSREP - Customs Conveyance Report Message
• IFTSTA - International Multimodal Status Report Message
• INVRPT - Inventory Report Message

Support additional X12 versions

Starting with the Fall 2019 January release, B2B Gateway supports the following additional X12 version:

• 6050
• 7010

Support additional EDIFACT

Starting with the Fall 2019 February release, B2B Gateway supports EDIFACT version 05B.

Changed behavior

The Spring 2020 April release of B2B Gateway includes the following changed behaviors.

Privileges to access B2B Gateway

To perform actions B2B Gateway you must have read privileges for Secure Agent group in Administrator.

In previous releases, Informatica Intelligent Cloud Services didn't verify that users have privileges for Secure Agent group when they accessed B2B Gateway.

File servers connection type

Starting with the Fall 2019 January release, if you want to use an AS2 server connection for an inbound partner flow, select the File Servers connection type and then select the appropriate file server user.

Previously, to use an AS2 server connection, you selected AS2 Server.
The Spring 2020 April release of Informatica Intelligent Cloud Services™ B2B Partners Portal includes the following updates.

New features and enhancements

The Spring 2020 April release of B2B Partners Portal includes the following new features and enhancements.

Exchange files with the portal provider

You can use B2B Partners Portal to exchange files with the portal provider over an HTTPS server.

To send files to the portal provider, upload the files to the portal. To receive files from the portal provider, download files that the portal provider uploads to the portal.

For more information, see the B2B Partners Portal help.
Chapter 6

Cloud Integration Hub

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Cloud Integration Hub includes the following updates.

New features and enhancements

The Spring 2020 April release of Cloud Integration Hub includes the following new features and enhancements.

Consume partial data with an API

An aggregate subscription that consumes data with the Consume Data REST API can consume partial topic data.

Consuming partial data lowers the amount of data that the subscription consumes in a single API subscription call.

For more information, see "Consume Data REST API" in the Cloud Integration Hub help.

Define retention period for unconsumed data

You can define how long Cloud Integration Hub retains unconsumed topic data in the publication repository before it deletes the data.

The retention period for unconsumed topic data must be between the retention period for consumed data and 90.

For more information, see the Cloud Integration Hub help.

Asset management

The Fall 2019 January release included the following asset management new features:

Create topic tables from a connection

You can create topic tables from objects in relational, flat file, and Salesforce connections.

View and manage publications and subscriptions on the topic page

The topic page lists publications that publish to the topic and subscriptions that subscribe to the topic, including information about the publication or subscription. You can perform actions on existing publications and subscriptions and create new publications and subscriptions on the topic page.
The following image shows a sample topic page with the **Publications** and **Subscriptions** areas:

For more information, see the Cloud Integration Hub help.

**Private publication repository**

Starting with the Fall 2019 January release, if you use a private publication repository, you can configure Cloud Integration Hub to bypass the Publication Repository Service (PRS) in publication and subscription flows to improve system performance.

For more information, see the Cloud Integration Hub help.

**Changed behavior**

The Spring 2020 April release includes the following changed behavior:

**Creating synchronization tasks for subscriptions in Cloud Integration Hub**

When you create a subscription that triggers a Data Integration synchronization task, you can create the task in the subscription page in Cloud Integration Hub.

Previously, you had to create the task in Data Integration before you created the subscription.

**Explore page**

You can view Data Integration assets in your organization on the **Explore** page in Cloud Integration Hub.

Previously, you could view only Cloud Integration Hub assets on the **Explore** page in Cloud Integration Hub.

**Consuming data into a private publication repository**

The amount of data that a private publication repository can consume is not limited.

Previously, a private publication repository could consume up to 5 MB of data.
Topic data retention period for consumed data

You define the data retention period for consumed data in the field Retention period for consumed data.

Previously, you defined the data retention period for both consumed and unconsumed data in the field Publication data retention period.
Chapter 7

Data Integration

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Data Integration includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Data Integration includes the following new features and enhancements.

Asset management

This release includes the following enhancements to asset management.

Source control

This release includes the following source control enhancements.

View source control information on the Dependencies page

You can view source control information and perform source control actions on the Dependencies page. To view source control information, you can add the following columns to the page:

- Git Hash
- Checked Out By
- Last Check In
- Last Pull Time

You can also perform source control actions on the Dependencies page such as check in, check out, unlink, or pull, using the Actions menu.

Deploy mapping updates

When you update a mapping that has a dependent mapping task, the changes to the mapping automatically deploy to the mapping task without the need to check out the mapping task.

Undo check out for renamed or moved objects

If a checked-out object is renamed or moved after it was checked out, an Undo Checkout action will restore the object’s name and location to its name and location before checkout.

Pull multiple projects

You can pull multiple projects from Git in one action instead of pulling projects one at a time.
Force undo checkout

An administrator can undo the checkout of objects that are checked out by another user. For example, if a user who has checked out assets leaves the company, the administrator can undo the checkout of those assets.

Unlink multiple objects

You can unlink multiple objects in one action.

Schedule export and import

You can migrate schedules from one organization to another organization.

Migrate schedules by exporting them from one organization and importing them into another organization. Export the schedules in Administrator and then import the schedules in the service that uses the schedules.

For example, you want to use a schedule that is defined in Organization A for Data Integration mapping tasks that reside in Organization B. In Organization A, you open Administrator and export the schedule. In Organization B, you open Data Integration and import the schedule.

Mappings

This release includes the following enhancements to mappings.

Mapping data preview

When you build a mapping, you can preview data for individual transformations to test the mapping logic. Data Integration displays the mapping results for the selected transformation and for the upstream transformations.

You can view the results on the Preview panel, as shown in the following image:

![Preview panel image]

For more information about previewing data in mappings, see Mappings.
Data flow run order
You can specify the data flow run order in a mapping that has multiple data flows. Specify the data flow run order when you want Data Integration to load the targets in the mapping a particular order. For example, you might want to specify the flow run order when inserting, deleting, or updating tables with primary or foreign key constraints.

For more information about setting the data flow run order, see Mappings.

Transformations
This release includes the following enhancements to transformations.

Lookup transformation
The Lookup transformation has the following enhancements:

Ignoring fields in comparison for dynamic caches
When you use a dynamic lookup cache, you can configure some lookup fields to be ignored when Data Integration compares the values in the lookup fields with the values in the associated incoming fields.

For example, the source data includes a column that indicates whether the row contains data you need to update. To improve performance, you can ignore all lookup fields in the comparison except for the field that indicates whether to update the row in the cache and target table.

File name prefix for persistent cache files
You can specify a file name prefix to use with persistent lookup cache files.

Rebuilding a persistent lookup cache
You can configure the Lookup transformation to rebuild a persistent lookup cache. You might want to rebuild the cache if the persistent cache is not synchronized with the lookup source.

For more information about the Lookup transformation, see Transformations.

Structure Parser transformation
The Structure Parser transformation has the following enhancements:

Non-relational output types
The Structure Parser transformation can generate the following non-relational output types:

- JSON
- JSON lines
- XML
- Avro
- Parquet
- ORC

Real-time sources
You can connect a real-time source to the Structure Parser transformation. For example, connect a Kafka connector to the transformation.

For more information about the Structure Parser transformation, see Transformations.

Target transformation
The Target transformation has the following enhancements:
Dynamic file names for flat file targets

If you create a flat file target at run time, you can specify a dynamic file name. A dynamic file name uses an expression to generate the file name.

You can use a dynamic file name to create a new target file every time the mapping task runs. You can also use a dynamic file name in a mapping that contains a Transaction Control transformation to write data to a different target file each time a transaction boundary changes.

The following image shows the Target Object dialog box with the Use a Dynamic File Name option enabled:

Target Object

Select an existing target object or create a new one. Any new target objects will be created when the mapping task is executed.

Target Object: Existing  Create New at Runtime
Formatting Options...

Use a Dynamic File Name

Name the file using an expression

Built-in functions

Expression

Validate

Target update override for relational targets

You can override the default UPDATE statement for each relational target in a mapping.

By default, Data Integration updates target tables based on key values. If you want to update the target based on non-key columns, you can enter an update override in the target advanced properties.

For more information about the Target transformation, see Transformations.

Transaction Control transformation

You can use the Transaction Control transformation to commit or roll back sets of rows during a mapping run. Use the Transaction Control transformation to commit or roll back transactions from transactional targets such as relational, XML, Amazon Redshift, and REST V2 targets. You can also use the transformation in a mapping to write data to a different flat file each time that Data Integration starts a new transaction.

You might want to use a Transaction Control transformation in a mapping that processes large amounts of data. You can use the Transaction Control transformation to commit the data at certain intervals to prevent data loss.
To use the Transaction Control transformation, you need the appropriate license.

For more information about the Transaction Control transformation, see *Transformations*.

**Union transformation**

You can configure the Union transformation to merge data from two or more data sources.

By default, the transformation contains two input groups. If you want to merge data from more than two sources, add an input group for each additional source. You can rename input groups. You can also delete input groups as long as there are at least two remaining input groups.

For more information about the Union transformation, see *Transformations*.

**Tasks**

This release includes the following enhancements to tasks.

**Mass ingestion sources and targets**

You can use the Databricks Delta connector as a source and target for mass ingestion tasks.

If the source is Databricks Delta, the target must be Microsoft Azure Data Lake Store Gen2. The output file is in the parquet format. If the target is Databricks Delta, only the parquet file format is supported, and the source must be Microsoft Azure Data Lake Store Gen2.

For more information about connectors that you can use in mass ingestion tasks, see *Tasks*.

**Search for connections in tasks**

You can search for connections when you configure a connection in a mapping task or synchronization task. You can search by connection name or connection type. Enter a full or partial string.

For more information about configuring tasks, see *Tasks*.

**Taskflows**

Taskflows include the following new features:

**File Watch Task step**

You can add a File Watch Task step to a taskflow to listen to files in a defined location and monitor file events. In the File Watch Task step, you can select a file listener.

You can use file events to orchestrate taskflow execution. For example, you can wait for a file to arrive at a particular location and then consume the file in a subsequent step.

For more information, see *Taskflows*.

**Ingestion Task step**

You can add an Ingestion Task step to leverage a mass ingestion task for taskflow orchestration. In the Ingestion Task step, you can select an existing mass ingestion task.

You might want to perform data integration operations after accessing files or moving them into a repository. In this scenario, you can use the Ingestion Task step in conjunction with the Data Task step.

For example, you can use the Ingestion Task step to read a large number of files from a source location and write them to an intermediate location. You can then use the Data Task step to perform data
integration operations on the files and use another Ingestion Task step to write the updated files to the final target location.

For more information, see Taskflows.

Taskflow dependencies

You can view object dependencies for a taskflow from the taskflow designer page. You can view a list of objects that the taskflow depends on and a list of objects that the taskflow is dependent on.

You might want to view dependencies before performing certain operations on a taskflow. For example, you cannot delete a taskflow if another object depends on the taskflow. You must first delete the dependent objects and then delete the taskflow. You can find the dependent objects by viewing the taskflow dependencies.

For more information, see Asset Management.

Data Integration Elastic

Data Integration Elastic includes the following new features:

CLAIRE Tuning

You can use CLAIRE Tuning to tune a mapping task that is based on an elastic mapping. CLAIRE, Informatica’s AI engine, runs the mapping task several times and uses machine learning to assess the performance of each run. It uses the information to create a tuning recommendation for the set of Spark properties that optimizes task performance.

You can configure the number of times that CLAIRE runs the mapping task and you can set resource limits on your cloud environment. For example, if you know that you can allocate only 4 GB to the Spark driver, you can configure `spark.driver.memory=4G` in the mapping task. CLAIRE will honor the pre-defined Spark property to create a tuning recommendation for other Spark properties.

Sequence Generator transformation

You can use the Sequence Generator transformation in an elastic mapping.

When you run the mapping task, the task shows the current value and initial value of the sequence. The current value changes after each run.
The following image shows where you can view the sequence values:

![Image of sequence values](image)

Java transformation enhancements

The Java transformation in an elastic mapping has the following enhancements:

**Sorting and grouping data**

You can sort data, group rows into partitions, and sort data in each partition before the Java code runs. If you group rows into partitions, the Java code runs for each partition in the transformation.

**invokeJExpression**

You can use the invokeJExpression API method to invoke an expression.

For more information, see *Transformations*.

**Unconnected lookups**

You can use an unconnected Lookup transformation in an elastic mapping.

For more information, see *Transformations*.

Parameter files

This release includes the following enhancements to parameter files.

**Parameter file templates**

When you use parameters in a mapping, you can download a parameter file template that contains the mapping parameters and their default values. Download a parameter file template to specify parameter values when you run the mapping task or to copy mapping parameters to another parameter file. You download a mapping parameter file template on the *Schedule* tab when you configure the mapping task.

The parameter file template contains the input and in-out parameters that can be overridden at run time with their default values.

Save file to a location that is accessible by the Secure Agent and use it to apply parameter values when you run the mapping task.

For more information about parameter file templates, see *Mappings*. 
Cloud-hosted parameter files

When you specify parameter values in a mapping task, you can provide values in a parameter file that is saved on a cloud platform. You can save a parameter file on a cloud platform with the following connection types:

- Amazon S3
- Google Storage V2
- Azure Data Lake Store Gen2

To use a parameter file that is saved on a cloud platform, select Cloud Hosted on the Schedule tab. Then select the connection and object to use.

For more information about parameter files, see Mappings.

Expression editor

You can use the following system variables in field expressions used in mappings and mapping tasks:

- $CurrentTaskName
- $CurrentMappingName
- $CurrentTime
- $CurrentDate
- $CurrentRunId

File listener

The file listener includes the following new features:

Support for HTTPS server

You can configure a file listener to listen to events on the HTTPS server. You can use REST APIs to create and run HTTPS server file listeners.

For more information, see Components.

Resiliency

A file listener runs at regular intervals based on a predefined schedule. After certain events, such as temporary network disruptions or secure agent upgrade, the existing file listener gets automatically submitted to the agent.

For more information, see Components.

REST API

This release includes the following enhancements to the Informatica Intelligent Cloud Services REST API.

Secure Agent configuration migration

You can use import and export resources to migrate a Secure Agent’s configuration. You might want to migrate Secure Agent configuration when you want to apply the configuration settings of one Secure Agent to another Secure Agent or to a Secure Agent group.

Schedule export and import

You can use export and import resources to migrate schedules from one organization to another.
You might want to migrate a schedule when you migrate an asset that uses the schedule or when you want to use a schedule in multiple organizations.

**Changed behavior**

The Spring 2020 April release of Informatica Intelligent Cloud Services Data Integration includes the following changed behaviors.

**Data Integration Elastic**

Integration At Scale is now called Data Integration Elastic.

The following table lists the terms that have changed accordingly:

<table>
<thead>
<tr>
<th>Previous Term</th>
<th>Current Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-scale mapping</td>
<td>elastic mapping</td>
</tr>
<tr>
<td>at-scale cluster</td>
<td>elastic cluster</td>
</tr>
<tr>
<td>at-scale configuration</td>
<td>elastic configuration</td>
</tr>
<tr>
<td>At-Scale Server</td>
<td>Elastic Server</td>
</tr>
</tbody>
</table>

**Intelligent Structure Discovery**

Intelligent Structure Discovery enhanced the handling of data types in input data.

Discovery of data types in the input is more accurate than in previous versions.

**Transformations**

This release includes the following behavior changes for transformations.

**Sequence Generator transformation**

You can use the Sequence Generator transformation as a midstream transformation that can have incoming fields from an upstream transformation. You can pass the incoming fields to downstream transformations.
The following image shows a mapping that uses the Sequence Generator transformation as a midstream transformation:

Previously, the Sequence Generator transformation could not have incoming fields. To toggle the behavior, use **Disable incoming fields** in the transformation advanced properties.

The default behavior differs based on the release when the mapping was created:

- In new mappings that you create in the Spring 2020 April release, **Disable incoming fields** is deselected and the Sequence Generator transformation is a midstream transformation by default.
- In existing mappings, **Disable incoming fields** is selected by default.

For more information, see **Transformations**.

**Source transformation**

When you create a Source transformation that joins related objects using a custom relationship, you can configure the join type. You can configure an inner, left outer, or right outer join. You can also specify the join operator.

Previously, the join type was always an inner join, and the join operator was always "equals."

For more information about joining related objects in a Source transformation, see **Transformations**.

**Target and Output transformations**

You can search for fields that contain or that start with a specified string when you map fields in a Target or Output transformation.

Previously, you could search for fields that started with a specified string.

**Connectors**

The Spring 2020 April release includes the following new connectors and enhanced connectors.
New connectors

This release includes the following new connectors.

Databricks Delta Connector

You can use Databricks Delta Connector to connect to Databricks Delta Lake from Data Integration. Use Databricks Delta connections in mass ingestion tasks to transfer a large number of tables from a Databricks Delta Lake source to a Microsoft Azure Data Store Gen2 target or transfer a large number of Parquet files from a Microsoft Azure Data Store Gen2 source to a Databricks Delta Lake target.

VSAM CDC Connector

You can use VSAM CDC Connector to connect to a PowerExchange CDC for CICS/VSAM environment from Data Integration. Use VSAM CDC Connector connections to retrieve metadata for VSAM source data sets on z/OS and to extract change records that PowerExchange captured from these data sets. Add VSAM sources in mappings, and then run the associated mapping tasks to transmit change records to a Microsoft SQL Server or an Oracle target.

Enhanced connectors

This release includes enhancements to the following connectors.

Amazon Redshift V2 Connector

This release includes the following enhancements for Amazon Redshift V2 Connector:

- You can provide the Amazon S3 bucket region, which is different from the Amazon Redshift cluster region.
- When you create mappings, you can parameterize the connection, source objects and target objects. You can also override parameters at runtime.
- You can enable the usage of KMS for the external accounts by specifying the Amazon Resource Name (ARN) and create encrypted resources.
- You can enable full pushdown optimization for reading data from Amazon S3 V2 sources and writing data to Amazon Redshift V2 targets.
- Amazon Redshift V2 Connector supports AWS SDK 1.11.665.

Amazon S3 V2 Connector

This release includes the following enhancements for Amazon S3 V2 Connector:

- The write operation supports the hierarchical data types for Avro, JSON and Parquet files in elastic mappings, when you select the CreateTarget option.
- When you create mappings, you can parameterize the connection, source objects and target objects. You can also override parameters at runtime.
- You can use the following data types when you perform a read or write operation on a flat file:
  - String
  - BigInt
  - Number
  - Nstring
- You can use the following data types when you perform a read or write operation on a Parquet file:
  - Date
  - Time
• Amazon S3 V2 Connector supports AWS SDK 1.11.665.

CDM Folders Connector
CDM Folders Connector uses schema version 0.9 for read and write operations.

Db2 for i CDC Connector
This release includes the following enhancements for Db2 for i CDC Connector:
• The Db2 for i CDC Connector now supports connectivity to PowerExchange 10.4.x Listeners.
• You can use the PWX Token option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
• You can configure an override SQL update statement in a mapping to update the data in a Microsoft SQL Server or Oracle target table. Configure the override statement in the Update Override field in the target object advanced properties. The SQL update statement overrides the default update statements that the Secure Agent uses to update targets based on key columns. You define an override update statement to update target tables based on non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

For more information, see the Db2 for i CDC Connector help information.

Db2 for LUW CDC Connector
This release includes the following enhancements for Db2 for LUW CDC Connector:
• The Db2 for LUW CDC Connector now supports connectivity to PowerExchange 10.4.x Listeners.
• You can use the PWX Token option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
• You can configure an override SQL update statement in a mapping to update the data in a Microsoft SQL Server or Oracle target table. Configure the override statement in the Update Override field in the target object advanced properties. The SQL update statement overrides the default update statements that the Secure Agent uses to update targets based on key columns. You define an override update statement to update target tables based on non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

For more information, see the Db2 for LUW CDC Connector help information.

Db2 for z/OS CDC Connector
This release includes the following enhancements for Db2 for z/OS CDC Connector:
• The Db2 for z/OS CDC Connector now supports connectivity to PowerExchange 10.4.x Listeners.
• You can use the PWX Token option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
• You can configure an override SQL update statement in a mapping to update the data in a Microsoft SQL Server or Oracle target table. Configure the override statement in the Update Override field in the target object advanced properties. The SQL update statement overrides the default update statements that the Secure Agent uses to update targets based on key columns. You define an override update statement to update target tables based on non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

For more information, see the Db2 for z/OS CDC Connector help information.
Google BigQuery Connector

You can read or write data of the NUMERIC data type when you use a Google BigQuery source or target. The NUMERIC data type stores numeric values with 38 digits of precision and 9 decimal digits of scale. When you read or write data using the NUMERIC data type, the Secure Agent maps the NUMERIC data type to the Decimal transformation data type and the allowed precision is up to 28.

Google BigQuery V2 Connector

This release includes the following enhancements for Google BigQuery V2 Connector:

- You can configure a Lookup transformation in Google BigQuery V2 mappings. You can retrieve data from a Google BigQuery V2 lookup object based on the lookup condition that you specify.
- You can specify an SQL override statement to override the default SQL query that reads data from a Google BigQuery source. In the mapping, specify the SQL statement to override in the advanced properties of the Source transformation.
- You can create a mapping to read the real-time or changed data from a Change Data Capture (CDC) source and load data into Google BigQuery. You must select Data Driven as the target operation to capture changed data. You can resume the extraction of changed data from the point of interruption when a mapping fails or is stopped.
- When you create mappings, you can parameterize the connection, source objects, target objects and also overwrite it at the runtime.
- When you configure a Google BigQuery V2 connection to use simple or hybrid connection mode, you can perform upsert, update, and delete operations on columns of Record data type.
- When you configure a mass ingestion task to transfer files from a Google Cloud Storage source to a Google BigQuery target, you can select Avro, Parquet, or ORC as the data format of the source file.

Google Cloud Storage V2 Connector

This release includes the following enhancements for Google Cloud Storage V2 Connector:

- You can configure the following advanced properties when you read data from a Google Cloud Storage source:
  
  **Google Cloud Storage Path**
  
  Overrides the Google Cloud Storage path to the file that you specified in the Google Cloud Storage Source transformation.
  
  Specify the Google Cloud Storage path in the following format:
  
  gs://<bucket name> or gs://<bucket name>/<folder name>
  
  **Source File Name**
  
  Overrides the Google Cloud Storage source file name specified in the Google Cloud Storage transformation.
  
  **Is Directory**
  
  Reads all the files in the folder specified in the Google Cloud Storage Path advanced source property.

- You can use the following data types when you perform a read operation or write operation on a flat file object:
  
  - String
  - BigInt
  - Number
  - NString
• You can use the following data types when you perform a read or write operation on an Avro file:
  - Datetime
  - Decimal

• When you create mappings, you can parameterize the connection, source objects, target objects and also overwrite it at the runtime.

**Greenplum Connector**

You can use the Secure Agent runtime environment hosted on Windows to connect and run Greenplum tasks.

**Hadoop Files V2 Connector**

This release includes the following enhancements for Hadoop Files V2 Connector:

You can use the following distributions on a Kerberos or non-Kerberos cluster:

• HDP 3.1
• HDI 4.0

You can use the following data types when you read or write data from a complex file object in Parquet format:

• Date
• Time
• Decimal

**Hive Connector**

You can use the following distributions on a Kerberos or non-Kerberos cluster:

• HDP 3.1
• HDI 4.0

**JDBC V2 Connector**

This release includes the following enhancements for JDBC V2 Connector:

• Effective in this release, JDBC V2 Connector is no longer a preview functionality and it is available for use in your production environment.

• When you configure a JDBC V2 mapping to read from or write data to a database that supports the Type 4 JDBC driver, you can specify the number of partitions to optimize the mapping performance at run time. Specify the number of partitions on the Partitions tab in the JDBC V2 Source and Target transformations. The Spark engine determines the way the partitions are created based on the number of partitions and the partition key you specified. The default number of partitions is 1. You can specify a maximum of 64 partitions.

For more information, see the *Cloud Data Integration JDBC V2 Connector Guide*.

**Kafka Connector**

This release includes the following enhancements for Kafka Connector:

• You can configure additional configuration properties to connect to a Kafka broker over SSL. You can configure these properties in the Additional Security Properties of the Kafka connection.

• You can specify configuration properties for the Kafka consumer in the Source transformation to override the Additional Connection Properties or Additional Security Properties specified for the Kafka connection. Specify comma-separated list of configuration properties in Consumer Configuration Properties.
• You can specify configuration properties for the Kafka producer in the Target transformation to override the Additional Connection Properties or Additional Security Properties specified for the Kafka connection. Specify comma-separated list of configuration properties in Producer Configuration Properties.

• When you specify configuration properties in Additional Security Properties, the value that you specify is masked.

• You can configure PLAIN security for a Kafka broker in Additional Connection Properties or Additional Security Properties.

Microsoft Azure Data Lake Storage Gen2 Connector

This release includes the following enhancements for Microsoft Azure Data Lake Storage Gen2 Connector:

• When you import source or target objects, you can read or write the data in the FileName field. The FileName field stores the absolute path of the source file from which the Secure Agent reads the data at run time. The FileName field applies to the following file formats:
  - Flat file
  - Avro
  - ORC
  - Parquet

• You can configure the Azure Government end-points in mappings.

• You can configure the authenticated proxy server settings for the Secure Agent to connect to Microsoft Azure Data Lake Storage Gen2.

• You can use the following data types when you read or write data from a flat file object:
  - String
  - BigInt
  - Number
  - Nstring

• You can use the following data types when you read or write data from a complex file object in Parquet format:
  - Date
  - Time
  - Decimal

• You can use a parameter file to define parameter values for source and target connections and source and target objects in mapping tasks.

For more information, see the Cloud Data Integration Microsoft Azure Data Lake Storage Gen2 Connector Guide.

Microsoft Azure SQL Data Warehouse V3 Connector

This release includes the following enhancements for Microsoft Azure SQL Data Warehouse V3 Connector:

• You can use Microsoft Azure Data Lake Storage Gen2 as temporary storage to stage the files.

• You can parameterize the database name, table name, and schema name in pre SQL, post SQL, and SQL override for Source, Lookup, and Target transformations.

• You can use a parameter file to define parameter values for source and target connections and source and target objects in mapping tasks.

For more information, see the Cloud Data Integration Microsoft Azure SQL Data Warehouse V3 Connector Guide.
Microsoft SQL Server CDC Connector

This release includes the following enhancements for Microsoft SQL Server CDC Connector:

- The Microsoft SQL Server CDC Connector now supports connectivity to PowerExchange 10.4.x Listeners.
- You can use the PWX Token option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
- You can configure an override SQL update statement in a mapping to update the data in a Microsoft SQL Server or Oracle target table. Configure the override statement in the Update Override field in the target object advanced properties. The SQL update statement overrides the default update statements that the Secure Agent uses to update targets based on key columns. You define an override update statement to update target tables based on non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

For more information, see the Microsoft SQL Server CDC Connector help information.

Microsoft SQL Server Connector

This release includes the following enhancements for Microsoft SQL Server Connector:

- You can use Microsoft SQL Server Connector to write to Azure SQL Database and Azure SQL Managed Instance from CDC sources.
- You can specify the additional properties for the JDBC driver to fetch the metadata. Specify the parameters in the Metadata Advanced Connection Properties field of the Microsoft SQL Server connection. If you specify more than one property, separate each key-value pair with a semicolon.
- You can also specify the additional properties for the ODBC driver to run mappings. Specify the parameters in the Runtime Advanced Connection Properties field of the Microsoft SQL Server connection. If you specify more than one property, separate each key-value pair with a semicolon.
- You can configure an override update SQL statement in a mapping to update the data in a Microsoft SQL Server target table. Configure the update statement in the Update Override field in the Microsoft SQL Server target object advanced properties. The update SQL statement overrides the default update statement generated by the Secure Agent.

For more information, see the Cloud Data Integration Microsoft SQL Server Connector Guide.

MongoDB Connector

This release includes the following enhancements for MongoDB Connector:

- You can configure a Lookup transformation in MongoDB mappings. You can retrieve data from a MongoDB lookup object based on a specific lookup condition.
- You can read data from multiple source objects and write data to multiple target objects.
- You can use the Hierarchical Parser transformation to read data from a MongoDB source, process the JSON input and provide relational output to the target.
- You can use the Hierarchical Builder transformation to read data from any relational source, convert it to JSON format and write data to a MongoDB target.
- You can use the upsert operation to update rows in a table in a MongoDB collection.
- You can write data to empty collections in MongoDB in JSON format.

For more information, see the Cloud Data Integration MongoDB Connector Guide.
MySQL CDC Connector

This release includes the following enhancements for MySQL CDC Connector:

- The MySQL CDC Connector now supports connectivity to PowerExchange 10.4.x Listeners.
- You can use the PWX Token option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
- You can configure an override SQL update statement in a mapping to update the data in a Microsoft SQL Server or Oracle target table. Configure the override statement in the Update Override field in the target object advanced properties. The SQL update statement overrides the default update statements that the Secure Agent uses to update targets based on key columns. You define an override update statement to update target tables based on non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

For more information, see the MySQL CDC Connector help information.

MySQL Connector

This release includes the following enhancements for MySQL Connector:

- You can specify the additional properties for the JDBC driver to fetch the metadata. Specify the parameters in the Metadata Advanced Connection Properties field of the MySQL connection. If you specify more than one property, separate each key-value pair with a semicolon.
- You can also specify the additional properties for the ODBC driver to run mappings. Specify the parameters in the Runtime Advanced Connection Properties field of the MySQL connection. If you specify more than one property, separate each key-value pair with a semicolon.
- You can configure an override update SQL statement in a mapping to update the data in a MySQL target table. Configure the update statement in the Update Override field in the MySQL target object advanced properties. The update SQL statement overrides the default update statement generated by the Secure Agent.

For more information, see the Cloud Data Integration MySQL Connector Guide.

NetSuite Connector

This release includes the following enhancements for NetSuite Connector:

- NetSuite connections use version 2019_2_0 of the NetSuite WSDL URL by default.
- You can use NetSuite Connector with version 2019_2_0 of the NetSuite WSDL URL to read data from NetSuite advanced search.

ODBC Connector

This release includes the following enhancements for ODBC Connector:

- You can configure an override update SQL statement in a mapping to update the data in an ODBC target table. The update override property is applicable for all ODBC subtypes in the ODBC connection except for Snowflake. Configure the update statement in the Update Override field in the ODBC target object advanced properties. The update SQL statement overrides the default update statement generated by the Secure Agent.

For more information, see the Cloud Data Integration ODBC Connector Guide.
• When you configure a mapping with pushdown optimization to a Snowflake database using the Snowflake ODBC connection, you can configure the following properties:
  - You can create a new target at run time. To create a target object at run time, configure a Snowflake target transformation and then select **Create New at Runtime** in the Snowflake target object properties.
  - You can configure an unconnected Lookup transformation in a Snowflake mapping.
  - You can configure a Sequence Generator transformation in a Snowflake mapping.
  - You can configure the Message-Digest algorithm 5 (MD5) function to calculate the checksum of an input value. MD5 is a one-way cryptographic hash function that calculates a unique value for each input. For more information, see the **Cloud Data Integration ODBC Connector Guide** or the **Cloud Data Integration Snowflake Cloud Data Warehouse V2 Connector Guide**.

**Oracle CDC V2 Connector**

This release includes the following enhancements for Oracle CDC V2 Connector:

• The Oracle CDC V2 Connector now supports connectivity to PowerExchange 10.4.x Listeners.
• You can use the **PWX Token** option in the CDC runtime properties to specify a PowerExchange restart token value as a restart point for the mapping task. Specifying a restart token value allows for greater granularity when extracting data from the PowerExchange Logger.
• You can configure an override update SQL statement in a mapping to update the data in an Oracle target table. Configure the update statement in the **Update Override** field in the Oracle target object advanced properties. The update SQL statement overrides the default update statement generated by the Secure Agent. You can configure this property to update targets that are based on key or non-key columns.

For more information, see the **Oracle CDC V2 Connector** help information.

**Oracle Connector**

This release includes the following enhancements for Oracle Connector:

• You can use an Oracle connection in a mapping to read or write data that contains the CLOB and BLOB data types.
• You can configure an override SQL update statement in a mapping to update the data in an Oracle target table. Configure the override statement in the **Update Override** field in the Oracle target object advanced properties.

For more information, see the **Cloud Data Integration Oracle Connector Guide**.

**Oracle Financials Cloud V1 Connector**

You can parameterize the following attributes when you create mappings:

• Source connection
• Target connection
• Request message in the Source transformation.
• Field mapping in the Source transformation.

**Salesforce Analytics Connector**

You can use version 48.0 of the Salesforce Analytics API to create a Salesforce Analytics connection and access Salesforce Analytics objects.

For more information, see the **Cloud Data Integration Salesforce Analytics Connector Guide**.

**Salesforce Connector**

You can use version 48.0 of the Salesforce API to create a Salesforce connection and access Salesforce objects.
For more information, see the Cloud Data Integration Salesforce Connector Guide.

REST V2 Connector
This release includes the following enhancements for REST V2 Connector:
- You can configure the JSON Web Token (JWT) authentication method to create a REST V2 connection.
- You can read data from a real-time source and write to a REST V2 real-time target.
- You can use qualified namespace objects in request and response messages.
- You can configure the number of connection retry attempts as an advanced field in the connection properties.

For more information, see the Cloud Data Integration REST V2 Connector Guide.

Snowflake Cloud Data Warehouse V2 Connector
This release includes the following enhancements for the Snowflake Cloud Data Warehouse V2 connection:
- You can use Authorization Code as the authentication type to implement token-based authentication while accessing Snowflake. Select the authentication type as AuthorizationCode in the Snowflake Cloud Data Warehouse V2 connection and then specify the authentication properties for the user to access Snowflake resources.
- You can use Snowflake Cloud Data Warehouse V2 connection to read data from and write data to Snowflake that is hosted on Google Cloud Platform.

For more information, see the Cloud Data Integration Snowflake Cloud Data Warehouse V2 Connector Guide.

Web Service Consumer Connector
You can use Windows NTLM V2 authentication to authenticate the web services in Web Service Consumer Connector.

For more information, see the Cloud Data Integration Web Service Consumer Connector Guide.

Workday V2 Connector
You can parameterize the following attributes in Workday V2 Connector:
- Source connection
- Target connection
- Request message in the Source transformation

For more information, see the Cloud Data Integration Workday V2 Connector Guide.

Changed behavior
This section describes the changes in connectors to the following connectors.

Google BigQuery V2 Connector
Effective in this release, Google BigQuery V2 Connector has the following changes:
- When you configure a Google BigQuery V2 connection to use the simple connection mode, you can configure upsert operations for columns of the Record data type. Previously, when you configured a Google BigQuery V2 connection to use the simple connection mode, you could not configure upsert operations for columns of the Record data type.
When you configure a Google BigQuery V2 connection to use the hybrid connection mode, you can configure update, upsert, and delete operations for columns of the Record data type. Previously, when you configured a Google BigQuery V2 connection to use the hybrid connection mode, you could not configure update, upsert, and delete operations for columns of the Record data type.

Kafka Connector
Effective in this release, when you use a Kafka target object in binary format, the timestamp field in the Fields tab no longer exists in the target.

Previously, when you configured a Kafka target object in binary format, the timestamp field was available as a read-only field. Therefore, if existing mappings have the timestamp field mapped, the timestamp field will not appear in the field mapping.

ODBC Connector
Effective in this release, when you use the Snowflake ODBC connection with the Snowflake ODBC subtype in a mapping configured for pushdown optimization to Snowflake, and you add the DATE_DIFF() function, the date arguments are passed in the order supported by Snowflake.

Previously, the syntax of the arguments passed for the DATE_DIFF() function were not in the order supported by Snowflake.

Upgrading to Spring 2020
The following topics provide information about tasks that you might need to perform before or after an upgrade to Spring 2020.

Preparing for the upgrade
The Secure Agent upgrades the first time that you access the Informatica Intelligent Cloud Services Spring 2020 release.

Files that you added to the following directory are preserved after the upgrade:

\<Secure Agent installation directory\>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra

Perform the following steps to ensure that the Secure Agent is ready for the upgrade:

1. Ensure that each Secure Agent machine has sufficient disk space available for upgrade.
   The machine must have 5 GB free space or the amount of disk space calculated using the following formula, whichever is greatest:
   
   Minimum required free space = 3 * (size of current Secure Agent installation directory - space used for logs directory)

2. Close all applications and open files to avoid file lock issues, for example:
   - Windows Explorer
   - Notepad
   - Windows Command Processor (cmd.exe)
Netezza Connector pre-upgrade tasks

Before you use Netezza Connector or existing Netezza mappings from an earlier release, you must download the Netezza JDBC driver.

Perform the following tasks before you run Netezza mappings:

1. Download the Netezza JDBC driver version from the IBM website.
   To download the Netezza JDBC driver on Windows, follow the download instructions from the following Knowledge Base article: https://kb.informatica.com/howto/6/Pages/23/619186.aspx

   If you want to use the Netezza JDBC driver on Linux, you can use the Netezza JDBC driver downloaded for Windows on the Linux machine.

2. After you download the Netezza JDBC driver, navigate to the following location on the Secure Agent location:
   <Secure Agent installation directory>/apps/Data_Integration_Server/ext/, and then manually create the following directory structure:
   deploy_to_main/bin/rdtm-extra/Netezza

3. Copy the Netezza JDBC driver jar file, nzjdbc.jar, to the following directory you created on the Secure Agent machine:
   <Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra/Netezza

4. Restart the Secure Agent.

Snowflake Cloud Data Warehouse V2 Connector pre-upgrade tasks

Before you use Snowflake Cloud Data Warehouse V2 Connector in the Spring 2020 release or you use existing Snowflake Cloud Data Warehouse V2 mappings from an earlier release, you must specify the Java heap space memory in the Secure Agent properties to avoid failures of tasks that read data from Snowflake.

This update applies to Snowflake Cloud Data Warehouse V2 mappings and mapping tasks that read data from Snowflake, but does not apply to mass ingestion tasks and mappings configured for pushdown optimization using the Snowflake ODBC connection.

If you already configured a heap size value that is higher than 256 MB in the JVM options, do not change it.

Perform the following steps to configure the JVM memory:

1. In Administrator, select the Secure Agent listed on the Runtime Environments tab.
2. Click Edit.
3. In the System Configuration Details section, select Data Integration Service as the service and DTM as the type.
4. Edit the JVMOption1 property, and enter \-Xms256m\.
5. Click Save.
Chapter 8

Data Profiling

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Data Profiling includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Data Profiling includes the following new features and enhancements.

Supported data sources

Data Profiling supports the following new data sources:

- Microsoft Common Data Model
- Salesforce cloud solutions such as Salesforce Sales Cloud, Salesforce Service Cloud, Salesforce Financial Cloud, and Salesforce Health Cloud.
- Applications you create on Force.com such as Veeva.

Create queries and view query results

You can create a query to retrieve the rows from a profiled source object that has a data quality problem. You can query based on field values, inferred patterns, data types, and rule outputs. You can view the query results in the Data Preview area or in the query results file.

For example, you can create and run a query that can retrieve source rows that are 'Invalid,' where 'Invalid' is a business rule that you define in a rule specification or if the postal code pattern is not 9(5).

Add Data Quality assets to a profile

You can add cleanse and verifier assets as rules to a profile.

Auto-assign rules to a profile

Informatica offers predefined Data Quality rules that Data Profiling can automatically assign based on the source type. For example, when a user creates a data profiling task for Salesforce, Data Profiling compares the parameters in the predefined Data Quality rules for Salesforce to the source object attributes. If the parameters for a rule and the attributes match, it adds the rule to the profile.

View Data Profiling task jobs in Operational Insights

You can monitor and view the data profiling jobs and job progress for the last 24 hours in Operational Insights. The Data Profiling page shows jobs, job properties, subtasks, subtask properties, and job progress.
Change connection and source objects

You can edit an existing profile to change the connection and source object for the next profile run.

View outliers

In the detailed view, the outliers are highlighted in the bar graph and value distribution statistics table.
The Spring 2020 April release of Informatica Intelligent Cloud Services℠ Data Quality includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services℠ Data Quality includes the following new features and enhancements.

Assets

This release includes the following new assets:

**Deduplicate**

Use a deduplicate asset to analyze the levels of duplication across the records in a data set and optionally to consolidate clusters of duplicate records into a single, preferred record.

Deduplicate assets analyze the identity information in the records. In a data quality context, an identity is a group of data values in a record that identify a person or an organization.

You add a deduplicate asset to a Deduplicate transformation when you configure a mapping in Data Integration.

**Parse**

Use a parse asset to parse the words or strings in an input field into discrete output fields based on the types of information that the words or strings contain.

You can use a dictionary to identify the values to parse from the input field, or you can define a regular expression to identify the values.

You add a parse asset to a Parse transformation when you configure a mapping in Data Integration.

This release includes new features in the following asset:

**Rule specification**

You can add the following function expressions to a rule statement in a rule specification:

**Convert to Date**

Converts a value in a string data type to a date/time data type.
**Convert to Float**

Converts a value in a string data type to a float data type.

**Convert to Integer**

Converts a value in a string data type to an integer data type.

**Is Spaces**

Returns a value that indicates whether the input string contains character spaces only.

**Substring**

Returns a substring from an input value of a length that you specify, beginning at a position that you specify. Select a string or numeric data type as the input.

**To Char**

Converts a numeric value or a date value to a string value.
Mass Ingestion

The Spring 2020 April release of the Informatica Intelligent Cloud Services™ Mass Ingestion service includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services Mass Ingestion service includes the following new features and enhancements.

Mass Ingestion Databases

The Spring 2020 April release of Mass Ingestion Databases includes the following new features and enhancements:

GitHub source control

You can configure source control for your organization to enable version management for Mass Ingestion Databases projects, folders, and assets from the Explore page. After you configure source control, you can version and store objects in a GitHub repository.

The source control actions that you can perform depend on how your organization administrator configures repository access for your organization:

**Read/write access to the source control repository**

When read/write access is configured, users in your organization can check out and check in objects, undo a check out, delete an object, pull an object version from the repository to add it to your organization, and restore objects to a previous version. You might want to configure read/write access for an organization in which you develop projects and assets.

**Read-only access to the source control repository**

When read-only access is configured, users in your organization can pull versions of source-controlled objects from the repository but cannot check out or check in objects. You might want to configure read-only access so that users can test or run the latest versions of assets but not change them.

Show asset dependencies

You can drill down on a database ingestion task to view object dependencies.
On the Explore page, select the row for a database ingestion task and then select Show Dependencies from the Actions menu. The Uses tab lists the objects that the selected task uses. A database ingestion task uses the following object types: source and target connections and a runtime environment. The Used By tab lists the objects that use the selected task. You can continue to drill down on listed objects to the smallest dependency.

**Note:** Before you view object dependencies for a database ingestion task the first time, you must save the task again. If the Save button is not available, make a minor edit to the task, such as a change in the Description field. The Save button then appears.

**Schema drift support**

Mass Ingestion Databases adds support for automatic schema drift detection and handling. Schema drift occurs when you change the schema of a source table. For example, you add, modify, drop, or rename columns.

Previously, Mass Ingestion Databases ignored all changes to source table schema, leaving the target structure unchanged. In the current release, Mass Ingestion Databases can be configured to automatically detect source schema changes and alter the target to be consistent with the source changes. By default, this feature is not enabled.

This feature is available for database ingestion incremental tasks and combined initial and incremental tasks that propagate change data from Oracle sources to Kafka, Microsoft Azure SQL Data Warehouse, or Snowflake targets. When you define a task, you can configure the types of source schema changes to propagate and how to handle them on the target. For example, you can configure schema drift options to ignore the changes, replicate them, or stop the job or subtask when a schema change occurs. If you choose to stop the job, you can use the Resume With Options command to resume the job with an override schema drift option.

**Asset export and import**

You can use asset export and import functionality to migrate Mass Ingestion Databases assets from one organization to another organization.

To migrate assets, you can export one or more selected assets to an export file and then import the file into another organization. During the import operation, you can refine the list of selected assets to import, select the target project, select different connections or runtime environment to use on the target, and indicate whether to overwrite assets on the target that have the same names as imported assets.

You can also migrate projects or folders. When you export a project or folder, you can export all assets in the project or folder, with or without object dependencies, or filter objects based on the object type. When you import the export file, you can select the assets to import and whether to overwrite existing assets that have same names as imported assets.

**Alerts**

When you view details for a database ingestion job from the Mass Ingestion page in Monitor or from the My Jobs page in Mass Ingestion, the Alerts tab displays alert messages when a source schema change is detected. The Alerts tab displays messages for all detected schema changes even if you set the schema drift options for the associated task to Ignore.

**Mass Ingestion Streaming**

The Spring 2020 April release of Mass Ingestion Streaming includes the following new features and enhancements:
**Splitter transformation**

You can use a Splitter transformation to process incoming data from a streaming source.

For more information about the Splitter transformation, see *Transformations in Mass Ingestion Streaming*.

**Technical Preview Notice:** Effective in the Spring 2020 April release of Informatica Intelligent Cloud Services™ Mass Ingestion Streaming, Splitter transformation is available for technical preview. Preview functionality is supported for evaluation purposes but is unwarranted and is not production-ready. Informatica recommends that you use in non-production environments only. Informatica intends to include the preview functionality in an upcoming release for production use, but might choose not to in accordance with changing market or technical circumstances. For more information, contact Informatica Global Customer Support. To use the functionality, your organization must have the appropriate licenses.

**Sub-organizations support**

If your organization has the Organization Hierarchy license, you can create one or more sub-organizations within your organization. You can use Mass Ingestion Streaming on any sub-organizations within an organization that is licenced for Mass Ingestion Streaming.

**Start and stop streaming ingestion jobs**

You can start a streaming ingestion job that is in the Stopped state. After the job starts, the status changes to Up and Running, Running with Warning, or Running with Error based on the previous state of the job.

You can stop a streaming ingestion job that is in the Up and Running, Running with Warning, or Running with Error state.

**New features and enhancements in Fall 2019 January**

The Fall 2019 January release of Informatica Intelligent Cloud Services Mass Ingestion Streaming included the following new features and enhancements:

**Python transformation**

You can use a Python transformation to process incoming data from a streaming source.

**Microsoft Azure Data Lake Storage Gen2**

You can write data to Microsoft Azure Data Lake Storage Gen2 by using a streaming ingestion task.

Use Microsoft Azure Data Lake Storage Gen2 connector to connect to Microsoft Azure Data Lake Storage. Microsoft Azure Data Lake Storage is a highly scalable data streaming platform and event ingestion service that receives and processes events.

**Amazon Kinesis Streams**

You can read data from to Amazon Kinesis Streams by using a streaming ingestion task.

Use Amazon Kinesis connector to connect to Amazon Kinesis Streams. Kinesis Streams is a real-time data stream processing service that Amazon Kinesis offers within the AWS ecosystem.

**Source control**

You can configure source control for your organization to enable version management for projects, folders, and assets. When you configure source control, you can store versions of objects in a Git repository.
You can configure source control for your organization in the following ways:

• Configure read/write access to the source control repository. When you configure read/write access, users in your organization can check in and check out objects, pull versions of objects, and revert objects to a previous version. You might want to configure read/write access for an organization in which you develop projects and assets.

• Configure read-only access to the source control repository. When you configure read-only access, users in your organization can pull versions of source-controlled objects from the repository. However, users cannot check out or check in objects. You might want to configure read-only access for a test or production organization so that users can test or run the latest versions of assets.

Common ingestion enhancements

This section describes enhancements that apply to both Mass Ingestion Databases and Mass Ingestion Streaming.

Enhanced sorting of ingestion jobs

On the My Jobs page in Mass Ingestion or on the All Jobs tab of the Mass Ingestion page in Monitor, you can sort jobs by clicking the Sort icon in the upper right corner and selecting a field from the sort menu.

Customization of the columns that are displayed does not affect the fields that you can use for sorting.

Ability to adjust the row height in ingestion job lists

On the My Jobs page in Mass Ingestion service or on the All Jobs tab on the Mass ingestion page in Monitor, you can adjust the height of rows in the jobs list for as long as the page is displayed.

Click the Settings icon in the upper right corner and select one of following options:

• Comfortable - greatest
• Cozy
• Compact - least

Resizeable columns in ingestion job lists

You can resize columns in the list of ingestion jobs on the My Jobs page in Mass Ingestion.
The Spring 2020 April release of MDM - Reference 360 includes the following updates.

New features and enhancements

The Spring 2020 April release of Reference 360 includes the following new features and enhancements.

REST API

The Reference 360 REST API includes enhancements to the following resources:

codelist
- You can retrieve the code values in a code list that were modified between a specified time range by using the List modified code values by time range API.
- You can retrieve the modified code value relationships in a hierarchy between a specified time range by using the List modified code value relationships in hierarchy by time range API.

export
- You can export code values and value mappings in JSON format.

For more information, see the Reference 360 REST API.

Workflow email notification enhancements

This release includes the following enhancements to workflow email notifications:

Notifications triggered by approvers
- When an approver performs an action on an approval request, the approver receives an email notification confirming their action. Other approvers for the approval request also receive an email notification about the action. Actions that trigger notifications include approving, rejecting, or sending back approval requests.

Notifications triggered by requesters
- When you send an approval request or cancel an approval request, you receive an email notification confirming your action. Also, when you cancel an approval request, approvers receive an email notification about the canceled approval request.

For more information, see the MDM - Reference 360 help.
Improved loading of larger data sets

You can reduce the loading time for data sets and hierarchies by loading a subset of code values at a time.
Chapter 12

Operational Insights

The Spring 2020 April release of Operational Insights includes the following updates.

New features and enhancements

The Spring 2020 release of Operational Insights includes the following new features and enhancements.

Operational Insights for Application Integration

You can use the Operational Insights service to view analytics for Application Integration assets.

Operational Insights offers several charts that help you quickly and visually assess the status and usage of your Application Integration assets and take appropriate corrective actions if needed. You can view analytics related to API calls, processes, connections, and licensing.

Note: Informatica is introducing Operational Insights support for Application Integration in phases. Operational Insights will be enabled first on a regional basis and then to specific customers upon request before enabling it broadly for all Application Integration customers. If you would like to use Operational Insights with Application Integration before it is broadly released, contact your Customer Success Manager.

Operational Insights for Data Profiling

You can monitor and view the data profiling jobs and job progress for the last 24 hours in Operational Insights. The Data Profiling page shows jobs, job properties, subtasks, subtask properties, and job progress.

For more information, see the Operational Insights User Guide.

Data Integration monitoring enhancements

You can view your Data Integration asset analytics on the following pages:

Top Projects and Top Folders panels

On the Data Integration Overview page, you can view a summary of jobs run for the top five projects and top five folders in your organization.

To display job details, drill down on the Top Projects or Top Folders panel.

To view analytics on the total number of rows read and jobs run during the selected period of time, click Detailed Charts in the Top Projects or the Top Folders panel.
Data Volume panel

On the Data Integration Overview page, the Data Volume panel displays a weekly summary of rows processed every hour. You can view the actual or the average number of jobs run.

If you view actual data for one week, you can view details about the jobs that completed in the time period. Click the rectangle to view details about the jobs.

The following image shows the Data Volume panel:

Export jobs data

You can export jobs data form the Jobs page to CSV file. When you export jobs data, Operational Insights exports the data with the current page filters applied.

To export jobs data, click Export on the Jobs page.

To view details about the export job, click the file name in the Exports panel.

Asset job history

You can view the job history for a specific mapping or task. The Job History page displays details about each instance of the mapping or task. Use the Job History page to view job run analytics such as runtime and completion status.

To view the job history for an asset, click the asset name on the Jobs page.

Secure Agent alerts

Alerts for Secure Agents include the following enhancements.

Disk usage alerts

You can configure Operational Insights to send an alert when the disk usage by a Secure Agent crosses a configurable threshold.

Secure Agent service alerts

You can configure Operational Insights to send alerts for individual services on a Secure Agent.

You can configure alerts for the following events for a Secure Agent service:

- The service is unavailable
- CPU usage by the service crosses a configurable threshold
- Memory usage by the service crosses a configurable threshold

You can create alert scripts that Operational Insights executes to perform additional actions when an alert is triggered.
Alert notifications

When Operational Insights sends an email alert, the same alert appears in the notifications in Operational Insights.

Changed behavior

The Spring 2020 release of Operational Insights includes the following changed behaviors.

Data Integration Overview page

The Data Integration Overview page includes the following changes.

Top Sources and Top Targets panels

You can view the number of jobs run for the top sources or the top targets in your organization. Use the menu to switch between the top sources and top targets.

The following image shows the Top Targets panel:

Previously, you viewed top sources and top targets in different panels.

Top Secure Agents

You can view job run information for the three most used Secure Agents in your organization in the Top Secure Agents panel.

Previously, you viewed job run information for the top runtime environments.

PowerCenter workflow alerts

On the Alert Settings tab for PowerCenter, Custom Alerts is renamed to Alert Rules. To configure an alert rule that notifies a user when an issue occurs in a PowerCenter workflow, click PowerCenter on the navigation bar, select Alert Settings, and then select Alert Rules.
Previously, on the Alert Settings tab in PowerCenter, you selected Custom Alerts to configure an alert condition for issues that occur in a PowerCenter workflow.

Upgrading to Spring 2020

The following topics provide information about tasks that you might need to perform before or after an upgrade to Spring 2020.

Preparing for the Upgrade

Effective in the Informatica Intelligent Cloud Services Spring 2020 release, Informatica Operation Insights includes the following updates:

30-day data retention policy

If you are using the base edition of Informatica Operational Insights for the PowerCenter, Data Engineering Integration, and Data Engineering Quality domains, the 30-day data retention period is applicable in the Spring 2020 release.

If you have been viewing historical data from the PowerCenter workflow or Data Engineering Integration and Data Engineering Quality jobs in earlier releases, you will no longer be able to view this data. You are now limited to viewing data only from the last 30 days.

For any queries about the 30-day data retention policy, log a support ticket with Informatica Global Customer Support.

IP address ranges to include in the firewall

If your organization uses Informatica Operational Insights, and you use a protective firewall, you must update the Informatica Operational Insights IP address ranges for your region in your list of approved IP addresses in the firewall settings.

The IP address must also include the Informatica Intelligent Cloud Services IP address ranges so that the Secure Agent and related services can connect to Informatica Intelligent Cloud Services servers to perform all the required tasks.

For more information about the list of IP address ranges that you must add to your list of approved IP addresses, see the following Knowledge Base article: KB article 532624
CHAPTER 13

Administrator

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Administrator includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Administrator includes the following new features and enhancements.

Serverless runtime environments

If you use Data Integration, you can create a serverless runtime environment that is hosted in Informatica’s virtual private cloud on the AWS cloud platform. When you use a serverless runtime environment, you do not need to install and configure a Secure Agent or Secure Agent group.

The serverless runtime environment connects to your private cloud through a cross-account elastic network interface (ENI). When you configure a connection or a mapping task, you can specify the serverless runtime environment.

If you create a serverless runtime environment to run elastic mappings and associated mapping tasks, the serverless runtime environment is configured with all of the prerequisites to create an elastic cluster and to run elastic jobs on the cluster.

Technical Preview Notice: Effective in the Spring 2020 April release, serverless runtime environments are available for technical preview. Preview functionality is supported for evaluation purposes but is unwarranted and is not production-ready. Informatica recommends that you use in non-production environments only. Informatica intends to include the preview functionality in an upcoming release for production use, but might choose not to in accordance with changing market or technical circumstances. For more information, contact Informatica Global Customer Support. To use the functionality, your organization must have the appropriate licenses.

Data Integration Elastic

Data Integration Elastic includes the following new features:

Initialization scripts

Cluster nodes can run an initialization script based on an init script path that you specify in an elastic configuration. Each node runs the script when the node is created, and the script can reference other init scripts.
You might want to run an init script to install additional software on the cluster. For example, your enterprise policy might require each cluster node to contain monitoring and anti-virus software to protect your data.

The init script path must be in cloud storage. You can place the scripts in a unique path on Amazon S3 or Blob Storage, or you can place the scripts in the staging location. All scripts must be in the same folder.

**Note:** To run an init script in an AWS environment, you must run the `generate-policies-for-userdefined-roles.sh` command to regenerate policies for user-defined master and worker roles. If you use default master and worker roles, no action is necessary.

For more information, see *Administrator*.

### High availability

An elastic cluster can become highly available to eliminate a single point of failure.

A cluster can become highly available based on your environment:

- In an AWS environment, you can enable high availability in the elastic configuration.
- In a Microsoft Azure environment, high availability is automatically enabled if the region supports multiple availability zones.

For more information, see *Administrator*.

### Storage scaling

The size of the EBS volume or Azure disk that is attached to a worker node in an elastic cluster can scale up based on job requirements. You can specify the minimum and maximum storage size in an elastic configuration.

Auto-scaling includes the following benefits:

- Allows jobs to consume fewer resources during smaller workloads.
- Accommodates for bursts in the processing load.
- Reduces the number of storage-related failures during processing.

**Note:** To scale EBS volumes in an AWS environment, you must run the `generate-policies-for-userdefined-roles.sh` command to regenerate policies for user-defined master and worker roles. If you use default master and worker roles, no action is necessary.

For more information, see *Administrator*.

### Mapping task timeout

You can specify a timeout in an elastic configuration to limit the amount of time that mapping tasks can run. For example, if a task hangs at run time, the timeout ensures that the task is terminated and that cluster resources are not unproductive.

The value in the elastic configuration applies to all mapping tasks that run on the elastic cluster, but you can override the value for a specific mapping task in the advanced session properties for the task.

For more information about elastic configuration properties, see *Administrator*. For more information about mapping tasks, see *Tasks* in the Data Integration help.

### Schedule export and import

You can export schedules from one organization and import them into a different organization.

Export schedules from the **Schedules** page in Administrator. Import schedules on the **Explore** page in another service such as Data Integration. After you import a schedule, you can associate the schedule with assets in the target organization.
Scheduled jobs reassignment

You can assign a user’s scheduled jobs to a different user. You must reassign a user’s scheduled jobs before you can delete the user.

For more information about reassigning a user’s scheduled jobs, see Administrator.

Source control

Source control has the following enhancements:

**Undo a check out for other users**
Administrators can undo a check out on objects that were checked out by another user. You might want to undo a check out for another user when the user goes on vacation or leaves the organization and has checked out objects that other users need to access.

For more information about undoing a check out for other users, see Administrator. For more information about checking in and checking out objects, see Asset Management in the Data Integration help.

**Disabling source control**
Administrators can disable source control for an organization. Before you disable source control, you must unlink all assets.

For more information about enabling and disabling source control, see Administrator.

File servers

File servers include the following new features and enhancements:

**Support for HTTPS server**
You can set up and manage HTTPS servers to exchange files through HTTPS servers. You must have the HTTPS license to exchange files through HTTPS servers.

**File transfer tasks**
Use the pre-defined file transfer tasks to run actions when you receive files from or send files to file servers. The pre-defined tasks are read-only and cannot be updated. You can use the REST APIs to run the following processes or trigger them from B2B Gateway:

- In inbound flow tasks: decompress, decrypt
- In outbound flow tasks: compress, encrypt

**PGP command line interface**
Use the PGP Command Line Interface (PGP-CLI) to manage the PGP keys and key rings. In case of multiple secure agents with File Integration Service (FIS), you can place the key rings in a shared directory and specify the path in the file servers global settings. You must restart the File Integration Service application if any changes are made in the file servers global settings.

**File server user authentication**
You can define user authentication for AS2 and SFTP servers to be either a password or a certificate.
Upload restrictions for AS2 server

The following upload restrictions are available while configuring an AS2 server:

- You can add a timestamp suffix to the name of the file.
- You can select the resolution type if you receive a file which already exists in the folder.

For more information on the new features and enhancements on file servers, see Administrator.

Changed behavior

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Administrator includes the following changed behaviors.

Data Integration Elastic

If you use credential-based security for direct access to Amazon data sources and you want to set up cross-account access, you can provide credentials for multiple Amazon accounts at the connection level instead of configuring bucket policies that permit cross-account access.

Upgrading to Spring 2020

The following topics provide information about tasks that you might need to perform before or after an upgrade to Spring 2020.

Preparing for the upgrade

The Secure Agent upgrades the first time that you access the Informatica Intelligent Cloud Services Spring 2020 release.

Files that you added to the following directory are preserved after the upgrade:

<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra

Perform the following steps to ensure that the Secure Agent is ready for the upgrade:

1. Ensure that each Secure Agent machine has sufficient disk space available for upgrade.
   - The machine must have 5 GB free space or the amount of disk space calculated using the following formula, whichever is greatest:
     
     Minimum required free space = 3 * (size of current Secure Agent installation directory - space used for logs directory)

2. Close all applications and open files to avoid file lock issues, for example:
   - Windows Explorer
   - Notepad
Netezza Connector pre-upgrade tasks

Before you use Netezza Connector or existing Netezza mappings from an earlier release, you must download the Netezza JDBC driver.

Perform the following tasks before you run Netezza mappings:

1. Download the Netezza JDBC driver version from the IBM website. To download the Netezza JDBC driver on Windows, follow the download instructions from the following Knowledge Base article: https://kb.informatica.com/howto/6/Pages/23/619186.aspx
   If you want to use the Netezza JDBC driver on Linux, you can use the Netezza JDBC driver downloaded for Windows on the Linux machine.

2. After you download the Netezza JDBC driver, navigate to the following location on the Secure Agent location: <Secure Agent installation directory>/apps/Data_Integration_Server/ext/, and then manually create the following directory structure:
   deploy_to_main/bin/rdtm-extra/Netezza

3. Copy the Netezza JDBC driver jar file, nzjdbc.jar, to the following directory you created on the Secure Agent machine:
   <Secure Agent installation directory>/apps/Data_Integration_Server/ext/
   deploy_to_main/bin/rdtm-extra/Netezza

4. Restart the Secure Agent.

Snowflake Cloud Data Warehouse V2 Connector pre-upgrade tasks

Before you use Snowflake Cloud Data Warehouse V2 Connector in the Spring 2020 release or you use existing Snowflake Cloud Data Warehouse V2 mappings from an earlier release, you must specify the Java heap space memory in the Secure Agent properties to avoid failures of tasks that read data from Snowflake.

This update applies to Snowflake Cloud Data Warehouse V2 mappings and mapping tasks that read data from Snowflake, but does not apply to mass ingestion tasks and mappings configured for pushdown optimization using the Snowflake ODBC connection.

If you already configured a heap size value that is higher than 256 MB in the JVM options, do not change it.

Perform the following steps to configure the JVM memory:

1. In Administrator, select the Secure Agent listed on the Runtime Environments tab.
2. Click Edit.
3. In the System Configuration Details section, select Data Integration Service as the service and DTM as the type.
4. Edit the JVMOption1 property, and enter -Xms256m.
5. Click Save.

After You Upgrade

Perform the following tasks after you upgrade to the Spring 2020 release.
Data Integration Elastic post-upgrade tasks

If you use Data Integration Elastic in an AWS environment, regenerate policies for user-defined master and worker roles after you upgrade. No action is necessary for default master and worker roles.

To regenerate the policies, run the generate-policies-for-userdefined-roles.sh command. In the Spring 2020 April release, the command generates policies that are more refined. The command also generates additional policies that are required to auto-scale EBS volumes, to access the initialization script path for the elastic cluster, and to access the S3 location that stores the init script and cloud-init logs.

For more information about the command and the policies, see Administrator.
Chapter 14

Monitor

The Spring 2020 April release of Informatica Intelligent Cloud Services™ Monitor includes the following updates.

New features and enhancements

The Spring 2020 April release of Informatica Intelligent Cloud Services Monitor includes the following new features and enhancements.

Session logs

Session logs include a header that contains the following information:
- Task Name
- Agent Group ID
- Agent Group Name
- Agent ID
- Agent Name

File transfer logs

You can monitor the HTTPS and integration file transfer logs.
- The HTTPS file transfer logs lists the status of upload, download, and APIs specific to the HTTPS server.
- The integration file transfer logs lists the status of the Collect and Release commands of APIs, and file transfer tasks.

For more information, see Monitor.

Monitor failed file events

You can monitor and troubleshoot failed file events using information on when the failure occurred on the file transfer type.

For more information, see Monitor.
Changed behavior

The Spring 2020 April release of Informatica Intelligent Cloud Services Monitor includes the following changed behaviors.

Job details

The Individual Source/Target Results area on the Job Details page displays Target transformation names. Target transformation names are also displayed in the session log.

Previously, the Job Details page and the session log displayed target object names.

Session log file names

When you download a session log, the log file name is <task/object name>_<instance ID>.log. For example, if you download a log for the fourth run of the task MyMappingTask, the log file name is MyMappingTask_4.log.

Previously, session log file names were log.txt.
# Index

**A**
- Administrator
  - changed behavior 64
  - new features 61
  - post-upgrade tasks 65
  - asset migration 52

**B**
- behavior changes
  - Administrator 64

**C**
- CLAIRE Tuning
  - new feature 31
- Cloud Application Integration community
  - URL 7
- Cloud Developer community
  - URL 7

**D**
- Data Integration community
  - URL 7
- Data Integration Elastic 34
  - data preview
    - mappings 27

**E**
- elastic clusters
  - new features 61
  - export and import 52

**I**
- import and export 52
- Informatica Intelligent Cloud Services
  - web site 7
- Integration At Scale 34
- IP address
  - upgrade preparation 60

**J**
- Java transformation
  - enhancements 31

**L**
- Lookup transformation
  - enhancements 28, 31

**M**
- maintenance outages 8
- mappings
  - previewing data 27
- Mass Ingestion Databases
  - asset migration 52
  - migrating assets 52

**N**
- new features and enhancements
  - Administrator 61

**O**
- organizations
  - source control configuration 51
- Output transformation
  - search for fields 34

**P**
- post-upgrade tasks
  - Administrator 65

**R**
- REST API
  - enhancements 33
- retention policy
  - IP address 60
  - upgrade preparation 60

**S**
- scheduled jobs
  - reassigning 63
- schedules
  - exporting 62
  - importing 62
  - reassigning scheduled jobs 63
- Secure Agents
  - upgrade preparation 45, 64
Sequence Generator transformation enhancements 31
joining source objects 34
serverless runtime environment new feature 61
source control configuration 51
disabling 63
undo check out for other users 63
Source transformation joining source objects 34
status Informatica Intelligent Cloud Services 8
Structure Parser transformation enhancements 28
system status 8
Target transformation enhancements 28
search for fields 34
Transaction Control transformation new feature 28
transformations enhancements 28
trust site description 8
Union transformation enhancements 28
upgrade notifications 8
upgrade preparation IP address 60
Secure Agent preparation 45, 64
Web site 7