Informatica® Cloud Data Integration
Summer 2019 September

What's New
# Table of Contents

**Preface** ................................................................. 5
Informatica Resources ...................................................... 5
  Informatica Documentation. .......................................... 5
  Informatica Intelligent Cloud Services web site. .................. 5
  Informatica Intelligent Cloud Services Communities. .......... 5
  Informatica Intelligent Cloud Services Marketplace. .......... 5
Data Integration connector documentation. ........................... 6
Informatica Knowledge Base. ........................................... 6
Informatica Intelligent Cloud Services Trust Center. ............ 6
Informatica Global Customer Support. ................................ 6

**Chapter 1: Summer 2019 September** ................................. 7
New features and enhancements. ......................................... 7
  Intelligent Structure Discovery and Structure Parser transformation. ... 7
Changed behavior. .......................................................... 8
  Integration At Scale. .................................................. 8
  Intelligent Structure Discovery and Structure Parser Transformation. ... 9
Connectors. .................................................................. 9
  New Connectors. ....................................................... 9
  Enhanced Connectors. ................................................ 9
  Changed behavior. ...................................................... 10

**Chapter 2: Summer 2019 July** ........................................... 11
New features and enhancements. ......................................... 11
  Integration At Scale. .................................................. 11
  Intelligent Structure Discovery. ....................................... 11
  Mapping Designer. ...................................................... 12
  Transformations. ........................................................ 12
  Mapping parameters. ................................................... 13
  Parameter files. .......................................................... 14
  Masking tasks. ........................................................... 14
  Mass ingestion tasks. ................................................... 14
  Taskflows. ................................................................. 15
  View asset dependencies. ............................................. 16
Administrator. ............................................................... 16
RESAPI. .................................................................... 17
RunAJob utility. .............................................................. 18
Changed behavior. .......................................................... 18
  Intelligent Structure Discovery. ....................................... 18
  Transformations. ........................................................ 18
Table of Contents

Chapter 3: Upgrading to Summer 2019

Preparing for the upgrade

After you upgrade

Secure Agent post-upgrade tasks

Amazon Redshift V2 Connector post-upgrade tasks

Cvent Connector post-upgrade tasks

Integration At Scale post-upgrade tasks

Microsoft Azure Data Lake Store V3 Connector post-upgrade tasks

Microsoft Azure SQL Data Warehouse V3 Connector post-upgrade tasks

Tableau V2 Connector post-upgrade tasks

Tableau V3 Connector post-upgrade tasks

Taskflows post-upgrade tasks

AS2 file servers

Index
Preface

What's New contains a brief overview of new features, enhancements, and changed behaviors for the Summer 2019 release. It also includes 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 Data Integration editions and applications as well as information about other 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:

To find resources on using Application Integration (the Informatica Cloud Real Time service), access the community at:
https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-application-integration/content

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 the Informatica Intelligent Cloud Services Status page 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.
New features and enhancements

The Summer 2019 September release of Informatica Intelligent Cloud Services℠ Data Integration includes the following new features and enhancements.

Intelligent Structure Discovery and Structure Parser transformation

Intelligent Structure Discovery and Structure Parser transformation include the following new features:

- **Simplified method for applying unique names to data fields**
  When the model contains fields with identical names, you can apply unique naming to the entire structure by performing an action on the root element. Intelligent Structure Discovery uses suffixes to rename identical names to unique names.

- **Update existing intelligent structures**
  You can apply the update sample functionality to additional file types, including XML, ORC, AVRO, and PARQUET sample files.

- **Document identifier port**
  When a model includes a document identifier, a document identifier output port appears in the Structure Parser transformation for each output group in the model.

- **Structured view of JSON sample files**
  When you select a JSON sample file, the file that appears in the input data panel is structured. You can expand and collapse nodes in the data tree.

- **Handling of Excel files**
  Intelligent Structure Discovery improved the accuracy of models that are based on Excel files.

For more information, see Components.
Changed behavior

The Summer 2019 September release of Informatica Intelligent Cloud Services™ Data Integration includes the following changed behaviors:

Integration At Scale

Integration At Scale includes the following behavior changes:

aws.properties file

Effective in the Summer 2019 September release, the Secure Agent reads the `aws.properties` file from the following directory on the Secure Agent machine:

   `<Secure Agent installation directory>/apps/At_Scale_Server/conf`

Previously, the agent read the `aws.properties` from the following directory on the Secure Agent machine:

   `<Secure Agent installation directory>/apps/At_Scale_Server/<version>/conf`

If the Secure Agent uses a kops role to access AWS, make sure that the `aws.properties` file is in the correct directory. For more information, see "Integration At Scale post-upgrade tasks" on page 32.

postscript.sh

To help you configure a kops role or a kops user to access AWS, the setup script `postscript.sh` is packaged with the Secure Agent installation.

If you configure a kops role, you run the script to create the `aws.properties` file and generate an SSH key pair on the Secure Agent machine.

If you configure a kops user, you run the script to populate the `~/.aws/credentials` and the `~/.aws/config` files and generate an SSH key pair on the Secure Agent machine.

Previously, you manually configured the `aws.properties`, `~/.aws/credentials`, and `~/.aws/config` files and generated the SSH key pair.

For more information, see the Administrator help.

Tagged AWS resources

If you specify AWS tags in an at-scale configuration, the Secure Agent propagates the tags to the following additional AWS resources:

- Load balancer
- Security group
- Subnet
- VPC

Note: Tags are propagated to VPCs and subnets that the Secure Agent creates.

Previously, tags were propagated only to the following AWS resources:

- Auto Scaling group
- EC2 instance
Intelligent Structure Discovery and Structure Parser Transformation

Intelligent Structure Discovery includes the following behavior changes:

Handling of fields with identical names
When a mapping that uses the Structure Parser transformation contains fields with identical names in different groups, the transformation retains the original field names in the output fields.
Previously, the Structure Parser transformation added a suffix to output field names of fields with identical names.

Working with repeating groups
The options Select as Primary Key and Deselect as Primary Key are renamed to Select as Record ID and Deselect as Record ID, respectively.

Connectors

The Summer 2019 September release includes the following new connectors and enhanced connectors.

New Connectors
This release includes the following new connector.

Ariba V2 Connector
You can use Ariba V2 Connector to connect to Ariba from Data Integration and read from or write hierarchical data to Ariba. Ariba V2 Connector integrates with Ariba using inbound SOAP web services and Ariba ITK support. You can create an Ariba V2 connection and use the connection in mappings and mapping tasks.

Enhanced Connectors
This release includes enhancements to the following connectors.

Google Drive Connector
You can read data from the following additional Google Drive objects:

- Files_GetAll
- Files_ExportAll

Litmos Connector
You can set the waiting time to re-attempt an API call after the number of calls to the Litmos API exceeds the API limit.

Microsoft Azure Data Lake Store Gen2 Connector
You can read and write the flat structure Avro, ORC, and Parquet files.
NetSuite Connector
This release includes the following enhancements for NetSuite Connector:

- You can use NetSuite Connector with the WSDL 2019.1 version.
- From WSDL 2019.1 version, if your NetSuite account does not use the default NetSuite WSDL URL, you can enter the WSDL URL used by your NetSuite account.
- You can write a NULL value to a NetSuite record reference or custom segment field.

Teradata Connector
You can override source and target connection and object parameters at runtime if the source or target uses a Teradata connection. Specify the value to use at runtime in the parameter file.

Snowflake Connector
When you configure a mapping to write data to a Snowflake target, you can specify the filename and path of the file that the Secure Agent can use to write the rejected records. You can specify the Rejected File Path in the Snowflake advanced target properties. For example, you can specify the following path and name in the rejected file path: `\rejectedfiles\reject7`

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

NetSuite Connector
This release includes the following change in NetSuite Connector:

- Version 2010_2 of the NetSuite WSDL URL is not supported.
The following topics provide information about new features, enhancements, and behavior changes in the Summer 2019 July release of Informatica Intelligent Cloud Services Data Integration.

New features and enhancements

The Summer 2019 July release of Informatica Intelligent Cloud Services℠ Data Integration includes the following new features and enhancements.

Integration At Scale

Effective in the Summer 2019 July release, you can use Integration At Scale to run data integration jobs in a serverless infrastructure that automatically scales as you increase or decrease your workload.

To begin using Integration At Scale, you must have an AWS account. First, you install a Secure Agent on an Amazon EC2 instance. Then you use Administrator to create an at-scale configuration to define how the Secure Agent provisions resources on the AWS cloud platform to host an at-scale cluster.

An at-scale cluster is an ephemeral Kubernetes cluster that provides the Serverless Spark engine with the computing power to run at-scale jobs. An at-scale job is an instance of an at-scale mapping or an associated mapping task that you create in Data Integration.

When you run an at-scale job, the Secure Agent starts the at-scale cluster and pushes the job to the cluster for processing. You can use Monitor to monitor both the running job and the cluster. As you run additional jobs, the cluster is scaled up or scaled down accordingly.

When all jobs have completed, the Secure Agent shuts down the cluster so that you pay only for the resources that you use.

Intelligent Structure Discovery

Intelligent Structure Discovery includes the following new features:

Add prefixes and suffixes to field names in intelligent structures

You can add a prefix or a suffix to a field name or to multiple field names in an intelligent structure. For example, add a suffix to field names that you want to identify easily when you use an intelligent structure model in a Big Data Management mapping.

For more information about adding prefixes and suffixes to a structure, see Components.
Mapping Designer

The Mapping Designer includes the following new features:

**CLAIRE transformation recommendations**

You can enable Informatica's AI engine CLAIRE™ for transformation recommendations during mapping design. The CLAIRE engine uses metadata from Informatica Intelligent Cloud Services organizations to recommend transformation to include in a mapping flow.

For more information about transformation recommendations, see *Mappings*.

**Mapping canvas enhancements**

Click the Add Transformation icon to add transformations to a mapping directly on the mapping canvas. The Add Transformation icon appears when you hover over the link between transformations or when you select an unconnected transformation. If your organization has CLAIRE recommendations enabled, you will see recommended transformations in the Add Transformation menu.

The following image shows the Add Transformation icon and the Add Transformation menu:

![Add Transformation Icon and Menu](image)

**Transformations**

This release includes the following enhancements to transformations.

**Lookup transformation**

In a dynamic Lookup transformation, you can configure how the mapping task handles inserts and updates to the cache for insert rows. To update existing rows in the dynamic lookup cache when the row type is insert, enable the **Insert Else Update** advanced property for the transformation.

When you enable this property, the mapping task inserts rows in the cache and updates existing rows. When you disable this property, the mapping task does not update existing rows. This property is disabled by default.

For more information about the Lookup transformation **Insert Else Update** property, see *Transformations*. 
SQL transformation

You can configure the SQL transformation to execute a query that you define in a query editor or to execute a saved query that you create in Data Integration. The SQL transformation processes the query and returns rows and database errors.

The following image shows the SQL tab when a user-entered query is selected as the query type:

![SQL Transformation Tab](image)

For more information about entering user-defined queries or selecting saved queries for an SQL transformation, see Transformations.

Structure Parser transformation

Manage the intelligent structure model that is associated with a Structure Parser transformation

When you use a Structure Parser transformation in a mapping, you can view the associated intelligent structure model, or create a model to associate with the transformation, from the Mapping Designer.

For more information about using a Structure Parser transformation in a mapping, see Transformations.

Update an intelligent structure model in a mapping

When you open a mapping that contains a Structure Parser transformation in the Mapping Designer, and the associated intelligent structure model changed after it was associated with the transformation, a message shows in the Mapping Designer. You can click the link that is provided in the message to update the model so that it complies with the mapping.

For more information about using a Structure Parser transformation in a mapping, see Transformations.

Mapping parameters

When you configure a connection or data object parameter, you can override the parameter values at runtime. You define the new value to use in the parameter file.

You can override source or target connections and objects that use flat file, relational database or FTP/SFTP connections. You can also override complete source queries in relational database connections.

For more information about overriding parameter values in mapping tasks, see Mappings.
Parameter files

You can reuse parameter files across tasks when you define local and global parameters within a parameter file. You can create global sections that apply to all tasks and also create sections that apply only to the specified task.

You can save a parameter file in any location that is accessible by the Secure Agent. When you configure a task, you can enter the absolute path for the directory that contains the parameter file.

For more information about configuring parameter files, see Mappings.

Masking tasks

The masking task includes the following new features:

Refresh metadata

You can refresh the source and target metadata in a masking task without updating the task. The refresh runs as a separate job. You can view the status and progress of the job from the My Jobs page.

For more information about refreshing the metadata in a masking task, see Masking tasks.

Reset task

You can reset a masking task that fails if you want to restart the task from the first step. Reset a failed masking task that has different source and target connections and contains data filters. When you reset the task, the status returns to the start step. When you restart the job, the job performs all the steps of staging data, estimation, load to target, and drop staging tables. If you restart a failed task without resetting the task, it continues from the point of failure. The task might reuse previously created staging tables and estimation data that might not be accurate.

For more information about resetting a masking task, see Masking tasks.

Mass ingestion tasks

The mass ingestion task includes the following new features:

Mass ingestion sources and targets

The following table lists additional connectors that you can use in mass ingestion tasks:

<table>
<thead>
<tr>
<th>Connector</th>
<th>Source</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Azure Data Lake Store Gen2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Azure Data Lake Store V3</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Snowflake Cloud Data Warehouse V2</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

File processing actions

You can configure a mass ingestion task to process files. You can add one or more of the following file processing actions:

- Encrypt
- Decrypt
• Compress
• Decompress
• Flatten File Structure

For more information about file processing actions, see Tasks.

Configuration options for source types

In addition to the file pattern, you can filter the source files using the following options:

• File modification date
• File size

For more information about configuring source options, see Tasks.

Interrupted state for file transfers

The mass ingestion task goes into an interrupted state when a file transfer interrupts because of network issues or you change credentials during the transfer. To resume the transfer of interrupted files, run the mass ingestion task again. The interrupted state is applicable when you transfer files from the advanced FTP, advanced SFTP, or advanced FTPS connectors.

For more information about the interrupted state, see Tasks.

File transfer events

You can view the file transfer events for the following mass ingestion task scenarios in a mass ingestion job:

• File is downloaded from source.
• File is uploaded to target.
• The mass ingestion task is performing file processing actions.
• The file is transferred from a local directory to another local directory.

You can view the events as file transfer types in the mass ingestion job and in the log.

For more information about the file transfer events, see Monitor.

Integration of Mass Ingestion with Enterprise Data Catalog

You can use the assets that you discover in Enterprise Data Catalog as sources in new mass ingestion tasks.

For more information about discovering Enterprise Data Catalog assets and using them as sources in a mass ingestion task, see Tasks.

Taskflows

Taskflows include the following enhancement:

Support for File Listeners

You can invoke a taskflow through a file listener. Within the taskflow, define the binding type as event and select the file listener. When you publish the taskflow, the taskflow subscribes to the file listener that is defined in it. When a file event occurs, the file listener invokes the taskflow.

For example, if you configure the file listener to listen for new files on a folder, the file listener invokes the associated taskflow each time a new file arrives in the specified folder.

For more information about invoking a taskflow through a file listener, see Taskflows.
View asset dependencies

You can view asset dependencies on the Explore page.

When you view dependencies for an asset, Informatica Intelligent Cloud Services lists the objects in your organization that the asset uses as well as the objects that use the selected asset.

For more information about viewing asset dependencies, see Asset Management.

Administrator

The Administrator service includes the following enhancements.

Agent blackout periods

You can configure blackout periods for a Secure Agent. Blackout periods prevent data integration jobs from running on the agent during a certain time period.

To configure a blackout period on a Secure Agent, you create an XML file that specifies the repeat frequency, start date, and end date for each blackout period.

For more information about agent blackout periods, see Administrator in the Administrator help.

Assign and unassign services to a user

You can assign and unassign services to a user on the Users page in Administrator.

When you assign a service to a user, the service is visible on the My Services page. The user can access and use the service as long as the user’s role allows this.

When you unassign a service, the user cannot see the service on the My Services page. The user cannot access or use the service regardless of the user’s role.

For more information about assigning and unassigning services, see Administrator in the Administrator help.

CLAIRE recommendation preferences

You can enable or disable CLAIRE recommendations for your organization. CLAIRE recommendations allow in-product recommendations for mapping design based on analysis of metadata from your organization’s assets and assets from other Informatica Intelligent Cloud Services organizations. CLAIRE recommendations are enabled by default.

For more information about CLAIRE recommendation preferences, see Administrator in the Administrator help.

Disable a user

You can disable a user on the Users page in Administrator. When you disable a user, the user can no longer log in to Informatica Intelligent Cloud Services, but the user account remains in the organization. If you need to reactivate a user account after you disable it, you can reset the user.

For more information about disabling a user, see Administrator in the Administrator help.

File server configuration

You can configure file servers such as AS2 to run on each agent that uses the File Integration Service. You can also configure partner users so that they can connect to the servers to send files.

Configure file servers and partner users on the File Servers page in Administrator.

Salesforce user activation

When you create a user account that uses Salesforce authentication, you can choose whether to activate the user account using a verification code or using Salesforce OAuth authentication.
For more information about account activation methods for Salesforce users, see Administrator in the Administrator help.

Stop and start services that run on a Secure Agent

You can stop and start the microservices that run on a Secure Agent to perform troubleshooting, to optimize resources on the agent machine, or when a service configuration changes. Start and stop Secure Agent services on the agent details page in Administrator. When you stop or start a Secure Agent service, other services that run on the agent are not impacted.

For example, if you encounter a problem with the Data Integration Server that runs on a Secure Agent, you can stop the service to perform troubleshooting and restart it without affecting the other services that run on the agent.

For more information about stopping and starting Secure Agent services, see Administrator in the Administrator help.

View object dependencies

You can view object dependencies for Secure Agent groups and connections. When you view dependencies for a Secure Agent group, Administrator lists the connections and assets in each service that use the group as the runtime environment. When you view dependencies for a connection, Administrator lists the runtime environments that the connection uses as well as the assets in each service that use the connection.

For more information about displaying dependencies for a Secure Agent group, see Administrator in the Administrator help. For more information about displaying dependencies for a connection, see Connections in the Administrator help.

REST API

The Informatica Intelligent Cloud Services REST API includes the following enhancements.

User management resources

New user management resources provide the ability to create users, user groups, and custom roles. The following REST API version 3 resources were added in this release:

users

Use to create Informatica Intelligent Cloud Services users and get the details for all users in your organization or details for a particular user.

Note: To leverage full user management capabilities, use this resource instead of the version 2 user resource. The version 2 user resource does not support user groups and roles.

userGroups

Use to create user groups and get the details for all user groups in the organization or the details for a particular user group.

roles

Use to create custom roles and get a list of all the roles that your organization uses.

privileges

Use to get a list of privileges that you can use for custom roles.

agentservice resource

Use the agentservice resource to start or stop a Secure Agent service. You can stop or start a Secure Agent service without affecting other services that run on the agent.
**Updated sendfiles resource**

When you send a sendfiles POST request, you can specify whether to delete or save the source files after the request completes successfully. By default, source files are deleted when a sendfiles POST request is successful.

**RunAJob utility**

You can run a published taskflow using the RunAJob utility.

To use the utility, your organization must have the RunAJobCli package. When the package is enabled, the utility can be found in the following location:

```bash
<Secure Agent installation directory>\apps\runAJobCli
```

For more information, see *RunAJob utility* in REST API Reference.

**Changed behavior**

The Summer 2019 July release of Informatica Intelligent Cloud Services℠ Data Integration includes the following changed behaviors:

**Intelligent Structure Discovery**

Intelligent Structure Discovery includes the following behavior changes:

**Exporting an intelligent structure model**

You can export an intelligent structure model only if your organization has the *Informatica Cloud Intelligent Structure Discovery for Big Data Management* license.

Previously, you could export intelligent structure models regardless of the type of Intelligent Structure Discovery license your organization has.

**Viewing data about intelligent structure model nodes**

When you view data about a node in an intelligent structure model that is based on an Excel spreadsheet, Intelligent Structure Discovery shows the names of the numeric data types in the data.

Previously, numeric data types were denoted by single characters. For example, decimal was denoted by the letter f.

**Transformations**

This release includes the following behavior changes for transformations.

**Java transformation**

Effective in the Summer 2019 August release, you no longer need to install a Java Development Kit (JDK) to compile the Java code and generate byte code for the Java transformation. Azul OpenJDK is now installed with the Secure Agent.

When you download and install a Secure Agent, Azul OpenJDK is installed automatically. The upgrade process also updates existing Secure Agents so that they include Azul OpenJDK.
You do not have to update the Java transformation to use Azul OpenJDK. Mappings that include the Java transformation will continue to run after the upgrade.

Previously, you had to install a JDK manually to compile the Java code and generate byte code for the Java transformation. If you installed a JDK during a previous release, you do not have to uninstall it.

For more information about the Java transformation, see Transformations.

Taskflows

Taskflows include the following behavior changes:

Deletion of taskflows

You cannot delete a taskflow that was published, previously run from the taskflow designer, or associated with a schedule. You must first unpublish the taskflow, and then delete it.

Previously, you could delete a taskflow that was published, previously run from the taskflow designer page, or associated with a schedule without unpublishing it.

For more information about deleting taskflows, see Asset Management.

Reordering of GET response fields for the status resource

The GET response fields for the status resource now appear in alphabetical order.

Previously, the GET response fields for the status resource were not ordered.

For more information about the GET response fields for the status resource, see Taskflows.

Masking tasks

The masking task has the following updates:

The Estimate option on the masking task view page is available in the Actions menu.

Previously, the option was available as a separate button on the masking task view page.

For more information about estimating a subset, see Masking tasks in the Data Integration help.

AS2 file servers

Configure AS2 file servers on the File Servers page in Administrator.

The following image shows the File Servers page:

Previously, you configured the AS2 file server by configuring the File Integration Service on the Runtime Environments page.
Note: All AS2 file server settings are removed during the upgrade. If you configured the File Integration Service for an AS2 file server, you need to configure the AS2 file server on the File Servers page in Administrator after the upgrade.

Monitor

The Monitor service includes the following behavior changes.

Viewing details for running jobs

You can now view job details and download a session log while a job is running so that you can more easily monitor long-running jobs.

Previously, you could only view job details and download a session log after a job completed or failed.

Note: You cannot monitor an at-scale job while the job is running.

Connectors

The Summer 2019 July release includes the following new connectors and enhanced connectors.

New Connectors

This release includes the following new connectors.

CDM Folders Connector

You can use CDM Folders Connector to connect to the Microsoft Azure Data Lake Storage Gen2 (ADLS Gen2) storage and Power BI from Data Integration. Use CDM Folders Connector to read data from or write data in the .csv file format to the common data model folder present in the ADLS Gen2 storage. You can also use CDM Folders Connector to create an external dataflow on Power BI workspace to access the data from the common data model folder in the ADLS Gen2 storage.

You can create a CDM Folders connection and use the connection in mappings or mapping tasks.

Note: Effective in Cloud Data Integration Summer 2019, CDM Folder Connector is available for 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.

Snowflake Cloud Data Warehouse V2

You can use Snowflake Cloud Data Warehouse V2 Connector to connect to Snowflake from Data Integration. Use Snowflake Cloud Data Warehouse V2 Connector to securely read data from and write data to Snowflake.

You can create a Snowflake Cloud Data Warehouse V2 connection and use the connection in mass ingestion tasks, mappings, or mapping tasks. You can use a mass ingestion task to transfer files from any source that mass ingestion task supports to a Snowflake target.

When you configure a mass ingestion task to load files to a Snowflake target, you must specify the file format and the copy options for the data files. To write data from sources such as Microsoft Azure Blob
Storage to Snowflake, you must specify the external stage location on Snowflake to load the files. You can choose to specify an external stage location for Amazon S3 on Snowflake.

**Zendesk V2 Connector**

You can use Zendesk V2 Connector to connect to Zendesk from Data Integration. Use Zendesk V2 Connector to read data from and write data to Zendesk.

Zendesk V2 Connector uses REST call to connect to Zendesk. You can create a Zendesk V2 connection and use the connection in synchronization tasks, mapping and mapping tasks.

When you run a synchronization task or a mapping task, the Secure Agents uses the Zendesk API to read data from and write data to Zendesk. You can use Zendesk objects, such as Users, Tickets, or Organizations in a task.

### 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 specify a new schema name and override the default schema name.
- You can specify a new SQL query and override the default SQL query.
- You can replace the null values in an Amazon Redshift source table with the string that you specify using the NULL Unload command option.
  
  **Note:** Does not apply to at-scale mappings.

**Amazon S3 V2 Connector**

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

- You can use the temporary security credentials using AssumeRole to access the AWS resources.
- You can apply the Informatica Encryption method using Informatica Crypto Libraries to encrypt or decrypt data of a binary or flat file target.
- You can use Amazon S3 V2 objects in a cached Lookup transformation.
- You can read or write Double data types in an at-scale mapping that uses a JSON file.

**Concur V2 Connector**

You can use OAuth 2.0 authentication to implement token-based authentication for Concur V2 Connector.

**Cvent Connector**

You can use the `Survey_AssociatedEvents` object as source in Cvent mappings and synchronization tasks.

**Greenplum Connector**

When you configure a Source transformation for a Greenplum source, you can specify the source type as multiple object to read from multiple Greenplum source tables.

**Google BigQuery Connector**

You can configure the HTTPS proxy server authentication settings for the Secure Agent to connect to Google BigQuery.
Google BigQuery V2 Connector

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

- You can read data from and write data to a table in a Google BigQuery dataset available in a specific region. Specify the Google BigQuery region in the **Region ID** connection property.
- You can configure the HTTPS proxy server authentication settings for the Secure Agent to connect to Google BigQuery.

Google Cloud Storage Connector

You can configure the HTTPS proxy server authentication settings for the Secure Agent to connect to Google Cloud Storage.

Google Cloud Storage V2 Connector

You can configure the HTTPS proxy server authentication settings for the Secure Agent to connect to Google Cloud Storage.

Google Drive Connector

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

- You can configure simple data filters to fetch specific data from the **Files_List** object.
- You can use the following additional fields when you select the **Files_List** object in a mapping:
  - createTime
  - explicitlyTrashed
  - hasThumbnail
  - iconLink
  - lastModifyingUser
  - lastModifyingUser.displayName
  - lastModifyingUser.emailAddress
  - lastModifyingUser.kind
  - lastModifyingUser.me
  - lastModifyingUser.permissionId
  - modifiedByMe
  - modifiedByMeTime
  - ownedByMe
  - shared
  - spaces
  - thumbnailLink
  - thumbnailVersion
  - version
  - viewedByMe
  - webContentLink
  - webViewLink
Hadoop Files V2 Connector

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

- When you run a mapping to read data from a complex file data object, you can use the asterisk (*) wildcard character to specify the source directory name or the source file name.
- When you run a mapping to read data from or write data to a complex file data object, you can specify the input or output file format in the advanced source or target properties.
- You can use Hadoop Files V2 Connector to create a target object at runtime.
- You can use Hadoop Files V2 Connector to read data from and write data to files in Avro file format.
- When you run a mapping to write data to a complex file data object, you can overwrite the data in the target. The Secure Agent deletes the existing data in the target before writing data.

Hive Connector

You can use a Hive connection to connect to Amazon S3, Azure Data Lake Storage, and Windows Azure Storage Blob storage systems.

JD Edwards EnterpriseOne Connector

This release includes the following enhancements for JD Edwards EnterpriseOne Connector:

- The following .jar files are the new JD Edwards EnterpriseOne API libraries and .ini files that JD Edwards EnterpriseOne Connector uses:
  - commons-codec.jar
  - commons-lang-2.6.jar
  - jmxremote_optional.jar
  - log4j-core.jar
  - ojdbc6.jar
  - tnsnames.ora

Marketo V3 Connector

This release includes the following enhancements for Marketo V3 Connector:

- When you configure a synchronization task or mapping task with the lead source object to read lead data from Marketo, you can specify the required filter values in the Filter Values field directly instead of adding the filter values in a CSV file and specifying the location. To filter a lead source object, specify the values in the Filter Values field in the advanced lead source properties on the Schedule page in a synchronization or mapping task. You can specify more than one filter value for the lead object fields and separate each value by a comma.
  
  You can continue to specify the filter values in a CSV file and specify the location of the file in the Filter Values CSV File field in the advanced lead source properties. If you specify both the Filter Values CSV File and the Filter Values field, the Secure Agent considers the Filter Values CSV File field and uses the values in the CSV file to filter the lead data.

- When you configure a synchronization task or mapping task to read data from a custom object fields in Marketo, you can specify the required filter values in the Custom Object Filter String Values field directly instead of adding the filter values in a CSV file and specifying the location.
  
  To filter a custom source object, specify the values in the Custom Object Filter String Values field in the advanced source properties in a synchronization or mapping task. When you specify the filter values,
enter the column name of the custom object, followed by the filter string values on consecutive lines similar to the following format as in a CSV file:

```
<custom_object_column_name>
<filter_value1>
<filter_value2>
<filter_value3>
```

You can continue to specify the filter values in a CSV file and specify the location of the file in the Custom Object Values Filter field in the advanced lead source properties. If you specify both the Custom Object Filter String Values and the Custom Object Values Filter field, the Secure Agent considers the Values Filter field and uses the values in the CSV file to filter data from the custom object.

- The field names in the Marketo V3 source and target properties are changed. The following table lists the changed Marketo V3 advanced source property names:

<table>
<thead>
<tr>
<th>Previous Names</th>
<th>Current Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead - Filter Field</td>
<td>Filter Field</td>
</tr>
<tr>
<td>Lead - Filter Values CSV File</td>
<td>Filter Values CSV File</td>
</tr>
<tr>
<td>Lead - List Id</td>
<td>List Id for Leads</td>
</tr>
<tr>
<td>Lead - Partition Name</td>
<td>Partition Name</td>
</tr>
<tr>
<td>Lead - Program Id</td>
<td>Program Id</td>
</tr>
<tr>
<td>Lead - Activity Type Id</td>
<td>Activity Type Id</td>
</tr>
<tr>
<td>Lead Activity - Activity Type Id</td>
<td>Lead Activity - Activity Type Id</td>
</tr>
<tr>
<td>Lead Activity - List Id</td>
<td>List Ids for Activity Type Ids</td>
</tr>
<tr>
<td>Lead Activity - Lead Id</td>
<td>Lead Ids for Activity Type Ids</td>
</tr>
<tr>
<td>List - List Id</td>
<td>List Id for List Details</td>
</tr>
<tr>
<td>List - List Name</td>
<td>List Name</td>
</tr>
<tr>
<td>List - Program Name</td>
<td>Program Name</td>
</tr>
<tr>
<td>Program - Program ID</td>
<td>Program - Program ID</td>
</tr>
<tr>
<td>Program - Program Name</td>
<td>Program - Program Name</td>
</tr>
<tr>
<td>Program - Tag Type</td>
<td>Program - Tag Type</td>
</tr>
<tr>
<td>Program - Tag Value</td>
<td>Program - Tag Value</td>
</tr>
<tr>
<td>Channel - Channel Name</td>
<td>Channel - Channel Name</td>
</tr>
<tr>
<td>Email - Email Id</td>
<td>Email - Email Id</td>
</tr>
<tr>
<td>Tag - Tag Name</td>
<td>Tag - Tag Name</td>
</tr>
</tbody>
</table>
The following table lists the changed Marketo V3 advanced target property names:

<table>
<thead>
<tr>
<th>Advanced Target Properties Names</th>
<th>Current Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead - Type of API to be used</td>
<td>Type of API to be used</td>
</tr>
<tr>
<td>Lead - Staging Folder for Bulk Load API</td>
<td>Staging Folder for Bulk Load API</td>
</tr>
<tr>
<td>Lead - Create Duplicate</td>
<td>Create Duplicate</td>
</tr>
<tr>
<td>Lead - List ID for Leads</td>
<td>List ID for Leads</td>
</tr>
<tr>
<td>Lead - Lookup Field</td>
<td>Lookup Field</td>
</tr>
<tr>
<td>Lead - Partition Name</td>
<td>Partition Name</td>
</tr>
<tr>
<td>Custom Obj / Oppty (Role) / Company / Sales Per - Dedupe Fields</td>
<td>Custom Object Dedupe Fields</td>
</tr>
<tr>
<td>Success File Directory</td>
<td>Success File Directory</td>
</tr>
<tr>
<td>Error File Directory</td>
<td>Error File Directory</td>
</tr>
</tbody>
</table>

Microsoft Azure Cosmos DB SQL API Connector

You can write data in bulk mode when you perform an Insert, Upsert, Update, or Delete operation.
Microsoft Azure Data Lake Store Gen2 Connector

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

- The Secure Agent can connect to Informatica Intelligent Cloud Services through the proxy server.
- You can import source and target objects from subfolders of the specified directory.
- You can specify the following settings when you select Create Target:
  - Include the period (.), the underscore (_), @, $, and % special characters in the object name.
  - Append the timestamp in the object name.
  - Parameterize the object name.
- You can read multiple source files from a directory.
- You can use a Microsoft Azure Data Lake Store Gen2 connection as a source or as a target in mass ingestion tasks.
- Microsoft Azure Data Lake Store Gen2 Connector supports storage accounts on which secure transfer is enabled.

Microsoft Azure Data Lake Store V3 Connector

This release includes the following enhancements for Microsoft Azure Data Lake Store V3 Connector:

- You can import Microsoft Azure Data Lake Store source and target objects from subfolders of the specified directory.
- You can use mass ingestion tasks to read data from Microsoft Azure Data Lake Store.

Microsoft Azure SQL Data Warehouse V3 Connector

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

- You can configure advance target properties to honor the flagged rows coming from an update strategy or any other custom transformation.
- You can connect to Microsoft Azure SQL Data Warehouse endpoints that reside in a virtual network (VNet).
- You can read data from and write data to Microsoft Azure SQL Data Warehouse case-sensitive databases when you use a Microsoft Azure SQL Data Warehouse V3 connection or an ODBC connection.
- You can read and write a datetimeoffset field in passthrough mappings when you use a Microsoft Azure SQL Data Warehouse V3 connection or an ODBC connection.

Microsoft Dynamics 365 for Operations Connector

You can use Microsoft Dynamics 365 for Operations Connector to write data to a Microsoft Dynamics 365 for Operations target. You can use Microsoft Dynamics 365 for Operations objects as targets in synchronization tasks, mappings, and mapping tasks.

Microsoft SQL Server Connector

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

- You can connect to Azure SQL Database managed instance using Microsoft SQL Server Connector from Data Integration.
- The DataDirect Microsoft SQL Server JDBC and ODBC drivers are upgraded to the latest versions.
MongoDB Connector
This release includes the following enhancements for MongoDB Connector:

- You can use the MongoDB connector to read data from or write data to collections in a MongoDB Atlas database.
- You can use the Data Integration Hosted Agent as a runtime environment for MongoDB Connector.

NetSuite Connector
You can use NetSuite Connector with the WSDL 2018.2 version.

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

- You can connect to an Oracle Advanced Security Option enabled instance using an Oracle connection. You can configure the advanced security encryption level options in the metadata and runtime properties in the Oracle connection.
- The DataDirect Oracle JDBC and ODBC drivers are upgraded to the latest versions.

PostgreSQL Connector
This release includes the following enhancements for PostgreSQL Connector:

- You can specify a target table name and schema in a mapping to create a new PostgreSQL target at runtime. The agent creates the table in the specified schema in the PostgreSQL database when you run the task.

  To create a target at runtime, select the Create New at Runtime in the PostgreSQL target object properties and then specify the table name in the Object Name field and the schema in the Path field. You must specify the path in the following format: `<Schema_Name>/<TableType>`, where the value for TableType is TABLE. If you do not specify a value in the Path field, the target table is created in the public schema.

- You can read or write data of the CITEXT data type to PostgreSQL. CITEXT is a case-insensitive extension to the PostgreSQL database. When you read or write the CITEXT data type, the Secure Agent maps the CITEXT data type to the Text transformation data type and the allowed precision is up to 104857600.

- You can configure a custom query as the source type for a PostgreSQL source object. In the mapping, select Query as the Source Type and then define the SQL query to select the source columns that you want to use.

- You can specify an SQL override statement to override the default query used to read data from the PostgreSQL source. In the mapping, specify the SQL statement to override in the advanced properties of the Source transformation.

- You can configure an SQL override in a Lookup transformation in which cache is enabled. To configure an SQL override, open the Advanced tab of the Lookup transformation, and enter the SQL override statement in the SQL Override field.

REST V2 Connector
This release includes the following enhancements for REST V2 Connector:

- You can configure the connection delay time as an advance field in the connection properties.
- You can define the response header and response cookies in the swagger file and parse them.
- You can define security definitions in the swagger file. REST V2 Connector supports the basic and apiKey security definition types.
- You can define default values for request input parameters except for the body and securityDefinitions parameters.
Salesforce Connector
You can use version 45.0 and 46.0 of the Salesforce API to create a Salesforce connection and access Salesforce objects.

Salesforce Marketing Cloud Connector
You can configure OAuth 2.0 for Salesforce Marketing Cloud connections.

ServiceNow Connector
This release includes the following enhancements for ServiceNow Connector:

- You can configure the HTTP proxy server authentication settings for the Secure Agent to connect to ServiceNow.
- When you configure a lookup in a task, you can enter multiple lookup conditions to return values from a ServiceNow record. The task evaluates the lookup conditions using the AND logical operator to join the conditions and returns rows that match all of the lookup conditions.
- You can use the BETWEEN operator in a data filter to filter data between two different SYSDATE values in a record. Use the following format to filter the SYSDATE values: field BETWEEN SYSDATE-<value>,SYSDATE-<value>.

Web Service Consumer Connector
You can use Web Service Consumer Connector to connect to web services that support SOAP version 1.2.

Xactly Connector
You can use the following additional objects when you create an Xactly connection:

- BusinessGroupWSO
- CurrencyRateWSO
- EmployeeStatusWSO
- UnitTypeWSO

Zuora REST V2 Connector
You can read data from and write data to custom fields in a Zuora object. In a Zuora REST V2 connection, specify the Zuora object or comma separated Zuora objects for which you want to configure custom fields.

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

Client-Side Encryption Support for Amazon Connectors
This release includes the following changes in Amazon Redshift, Amazon Redshift V2, Amazon S3, and Amazon S3 V2 Connectors:

- To enable client-side encryption, you do not have to update the local_policy.jar and US_export_policy.jar files.
  Previously, you had to update the existing local_policy.jar and US_export_policy.jar files in the following directory: <Secure Agent installation directory>\lib\security
Runtime Support Changes for Hadoop Connectors

This release includes the following changes in Hadoop, Hive, and Hadoop Files V2 Connectors:

• To access the Kerberos enabled Hadoop cluster, you must copy the krb5.conf configuration file to the following directory: <Secure Agent installation directory>/jdk/jre/lib/security

  Previously, you used to copy the krb5.conf configuration file to the following directory: <Secure Agent installation directory>/jre/lib/security

• If the cluster is SSL enabled, you must manually import the SSL certificate alias file to the following directory:

  <Secure Agent installation directory>/jdk/jre/lib/security/cacerts

  Previously, you used to manually import the SSL certificate alias file to the following directory: <Secure Agent installation directory>/jre/lib/security/cacerts

LDAP Connector

This release includes the following change in LDAP Connector:

• If you choose to copy the server certificate to configure the TLS authentication using one-way SSL, you must copy the server certificates to the following directory: <Secure Agent installation directory>\%jdk\%jre\lib\security\cacerts

  Previously, you used to copy the server certificate in the following directory: <Secure Agent installation directory>\%jre\lib\security\cacerts

Microsoft Azure SQL Data Warehouse V3 Connector

This release includes the following change in Microsoft Azure SQL Data Warehouse V3 Connector:

• If you choose to copy the server certificate to configure the TLS authentication using one-way SSL, you must copy the server certificates to the following directory: <Secure Agent installation directory>\%jdk\%jre\lib\security\cacerts

  Previously, you used to copy the server certificate in the following directory: <Secure Agent installation directory>\%jre\lib\security\cacerts

Microsoft Dynamics CRM Connector

This release includes the following change in Microsoft Dynamics CRM Connector:

• To configure Java security for Microsoft Dynamics CRM instances that use Active Directory and self-signed certificates, you must navigate to the following directory: <Secure Agent installation directory>/jdk/jre/bin/

  Previously, you used to configure Java security for Microsoft Dynamics CRM instances in the following directory: <Secure Agent installation directory>/jre/bin/

REST V2 Connector

This release includes the following change in REST V2 Connector:

• If you choose to copy the server certificate to configure the TLS authentication using one-way SSL, you must copy the server certificates to the following directory: <Secure Agent installation directory>\%jdk\%jre\lib\security\cacerts

  Previously, you used to copy the server certificate in the following directory: <Secure Agent installation directory>\%jre\lib\security\cacerts
Enhancements in previous releases

You can find information on enhancements and changed behavior in previous Data Integration releases on Informatica Network.

What's New guides for releases occurring within the last year of the current release are included in the following community article: https://network.informatica.com/docs/DOC-17912
Chapter 3

Upgrading to Summer 2019

The following topics provide information about tasks that you might need to perform before or after an upgrade to Summer 2019.

Preparing for the upgrade

The Secure Agent upgrades the first time that you access the Informatica Intelligent Cloud Services Summer 2019 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)

After you upgrade

Perform the following tasks after you upgrade to the Summer 2019 release.

Secure Agent post-upgrade tasks

Effective in the Summer 2019 release, the provider for the Java Runtime Environment that is installed with the Secure Agent is changed from Oracle to Azul. If you modified the java.security files in the Secure Agent
directory to change the disabled algorithms or to configure strong encryption support, you might need to update the files after the upgrade.

The following table summarizes the security configuration differences between Oracle and Azul Java:

<table>
<thead>
<tr>
<th></th>
<th>Oracle Java</th>
<th>Azul Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled algorithms</td>
<td>jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize &lt; 768</td>
<td>jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize &lt; 1024, \ EC keySize &lt; 224, 3DES_EDE_CBC, anon, NULL</td>
</tr>
<tr>
<td></td>
<td>jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize &lt; 1024</td>
<td>jdk.certpath.disabledAlgorithms=MD2, MD5, SHA1, dkCA &amp; usage TLSServer, \ RSA keySize &lt; 1024, DSA keySize &lt; 1024, EC keySize &lt; 224</td>
</tr>
<tr>
<td>Strong encryption</td>
<td>Strong encryption algorithms such AES192 and AES256 are disabled by default.</td>
<td>Strong encryption algorithms are enabled by default.</td>
</tr>
<tr>
<td>support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Amazon Redshift V2 Connector post-upgrade tasks

After you upgrade, you cannot edit the metadata of the target object fields using the Create Target option for the existing mappings with source type as custom query.

Cvent Connector post-upgrade tasks

After you upgrade, the existing Cvent mappings might fail or the Secure Agent may read data incorrectly, you must refresh the metadata and map the fields again to run the mappings successfully.

Integration At Scale post-upgrade tasks

Effective in the Summer 2019 September release, the Secure Agent reads the aws.properties file from the following directory on the Secure Agent machine:

<Secure Agent installation directory>/apps/At_Scale_Server/conf

Previously, the agent read the aws.properties from the following directory on the Secure Agent machine:

<Secure Agent installation directory>/apps/At_Scale_Server/<version>/conf

If the Secure Agent uses the kops role to access your AWS account, perform one of the following tasks to make sure that the aws.properties is in the correct directory:

- Move the aws.properties file to the new directory.
- Run the setup script postscript.sh.
  The script is located in the following directory on the Secure Agent machine:
  <Secure Agent installation directory>/apps/At_Scale_Server/<version>
  For more information about the setup script, see the Administrator help.

Microsoft Azure Data Lake Store V3 Connector post-upgrade tasks

After you upgrade to Summer 2019, ensure to use the existing connections without any modifications to run the existing mappings. Create new connections to use with new mappings.
Do not enable the Show Subfolders property in connections used in the existing mappings. If you enable Show Subfolders in the existing connections, import the objects again before running the existing mappings.

If you enable Show Subfolders in connections used in the existing mappings and do not import the objects again, the underlying mappings start to fail with the following error:

[ERROR] com.informatica.powercenter.sdk.SDKException: Invalid operation field name.

The data preview fails with the following error:

Cannot get data preview for the selected Connection and object. Please verify connection and object details. ([Exception : class com.informatica.adapter.sdkadapter.metadata.semantic lwconsumer.MetadataExceptionImpl occurred in createDataOperation.])

Microsoft Azure SQL Data Warehouse V3 Connector post-upgrade tasks

After you upgrade to Summer 2019, perform the following steps if a datetimeoffset field is used in your existing mappings:

- If the source or target objects in the existing mappings have a connected field of type datetimeoffset, reimport the objects.
- Configure field mapping after reimporting the objects.
- If you do not reimport the objects and remap the fields, the mappings that read a datetimeoffset field and write a datetimeoffset field fail.
- Reimporting the objects works only for the passthrough mappings that read from a Microsoft Azure SQL Data Warehouse V3 source and write to a Microsoft Azure SQL Data Warehouse V3 target. If a datetimeoffset field has been used in other transformations to define the mapping logic, make sure to redesign the mapping as required.

You must modify the existing mappings by reimporting the source or target objects before you re-run the existing mappings.

Tableau V2 Connector post-upgrade tasks

After you upgrade, you must perform the following tasks for Tableau V2 Connector to run the mappings successfully:

- Install Red Hat Enterprise Linux version 7 or higher for the Secure Agents installed on Linux operating systems.
- Assign the read, write, and execute permissions to the third-party libraries manually. To assign permissions, perform the following steps:
  1. From the command prompt, go to the following directory:
     `<INFRA_AGENT_INSTALLED_LOCATION>/downloads/package-tableauV2.<latest_version>/package/rdtm`
  2. Enter the following command:
     `chmod 777 *`

Tableau V3 Connector post-upgrade tasks

After you upgrade, you must assign the read, write, and execute permissions to the third-party libraries manually to run the mappings successfully:
To assign permissions, perform the following steps:

1. From the command prompt, go to the following directory:
   `<INFA_AGENT_INSTALLED_LOCATION>downloads/package-TableauV3.5/package/tableauv3/libs`

2. Enter the following command:
   ```
   chmod 777 *
   ```

**Taskflows post-upgrade tasks**

After you upgrade, when you open an existing taskflow or import a taskflow that was exported before the Winter 2019 March release, a message appears stating that the taskflow definition has been upgraded and that you must verify the taskflow for possible upgrade errors.

You must verify the taskflow for possible upgrade errors and manually save the taskflow. Otherwise, the upgrade message appears each time you open the taskflow and you cannot run or publish the taskflow.

Scheduled taskflows will continue to run as is. However, if you open and edit a scheduled taskflow, you must verify the scheduled taskflow for possible upgrade errors and manually save the taskflow. Otherwise, the upgrade message appears each time you open the scheduled taskflow.

**AS2 file servers**

All AS2 file server settings configured for the Secure Agent File Integration Service in Administrator will be removed during the upgrade. After the upgrade, reconfigure your AS2 file server settings on the **File Servers** page in Administrator.
INDEX

C
Cloud Application Integration community
URL 5
Cloud Developer community
URL 5
connections
viewing dependencies 16

D
Data Integration community
URL 5

I
Informatica Global Customer Support
contact information 6
Informatica Intelligent Cloud Services
web site 5
Intelligent Structure Discovery
enhancements 7, 11

J
Java transformation
behavior changes 18

L
Lookup transformation
enhancements 12

M
maintenance outages 6
Monitor
changed behavior 20

R
REST API
enhancements 17

S
Secure Agent groups
viewing dependencies 16
Secure Agents
blackout periods 16
Oracle vs. Azul Java 32
post-upgrade tasks 32
starting and stopping services 16
upgrade preparation 31
SQL transformation
enhancements 12
status
Informatica Intelligent Cloud Services 6
Structure Parser transformation
enhancements 12
system status 6

T
transformations
behavior changes 18
enhancements 12
trust site
description 6

U
upgrade notifications 6
upgrade preparation
Secure Agent preparation 31
users
assigning and unassigning services 16
disabling 16

W
web site 5