Informatica® Intelligent Cloud Services
April 2024

Runtime Environments

Informatica Intelligent Cloud Services Runtime Environments
April 2024

Table of Contents

Preface

Use *Runtime Environments* to learn how to create and configure runtime environments and serverless runtime environments to use with Informatica Intelligent Cloud Services℠. Learn how to use the Informatica Intelligent Cloud Services Hosted Agent, download and install Secure Agents, create and configure Secure Agent groups, and troubleshoot Secure Agents.

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:

https://network.informatica.com/community/informatica-network/products/cloud-integration

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

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

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

https://marketplace.informatica.com/

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, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can 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 Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

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.

CHAPTER 1

Runtime environments

A runtime environment is the execution platform that runs Informatica Intelligent Cloud Services assets such as tasks and taskflows. You must have at least one runtime environment in each organization so that users in the organization can run tasks.

A runtime environment consists of one or more Secure Agents. A Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services.

You can set up runtime environments in the following ways:

Use the Informatica Cloud Hosted Agent.

When you use the Hosted Agent, you run tasks within the Informatica Cloud hosting facility. Informatica maintains the Hosted Agent runtime environment and agents. For more information about the Informatica Cloud Hosted Agent, see Chapter 2, "Hosted Agent" on page 9.

Create one or more Secure Agent groups.

You can install one or more Secure Agents to run within your network or in a cloud computing services environment such as AWS, Google Cloud, Microsoft Azure, or Oracle Cloud Infrastructure. You can install one Secure Agent on each physical or virtual machine.

When you install a Secure Agent, it is added to its own group by default. You can add multiple agents to one Secure Agent group. For more information about Secure Agent groups, see Chapter 3, "Secure Agent groups" on page 11.

Configure a serverless runtime environment.

If your cloud environment is AWS, you can configure a serverless runtime environment. This environment is hosted by Informatica, so you don't need to configure a Secure Agent or Secure Agent group. For more information about serverless runtime environments, see Chapter 8, "Serverless runtime environments" on page 77.

When you configure a connection or some types of tasks, you specify the runtime environment to use. The runtime environment determines which agent runs the tasks at run time. If the runtime environment is the Hosted Agent, the Hosted Agent runs the tasks. If the runtime environment is a Secure Agent group, any available agent in the group can run the tasks.

To run a mapping in advanced mode, the agent can create a default local cluster on the agent machine so that you can begin developing and running advanced functionality on small data sets to test mapping logic. For more information, see *Advanced Clusters*.

Before you run mappings in advanced mode on a local cluster, make sure that the agent has enough resources so that it can create a cluster and run jobs successfully, especially if the agent is already running other jobs. If the agent doesn't have enough resources, the jobs that are already running on the agent and the mappings in advanced mode will fail. It's recommended to have at least 8 cores and 32 GB of memory on the agent machine.

CHAPTER 2

Hosted Agent

The Hosted Agent can run synchronization, mapping, and replication tasks that use certain connectors.

Informatica Intelligent Cloud Services manages the Hosted Agent runtime environment, so you cannot add, delete, or configure a Hosted Agent.

The Hosted Agent can run synchronization, mapping, and replication tasks that use the following connectors:

- Amazon Athena Connector
- Amazon Aurora Connector
- Amazon Redshift Connector
- Amazon Redshift V2 Connector
- Amazon S3 Connector
- Amazon S3 V2 Connector
- Box Connector
- Box Oauth Connector
- Cloud Integration Hub
- Concur V2 Connector
- Coupa Connector
- Coupa V2 Connector
- Cvent Connector
- Databricks Delta Connector
- DB2 Warehouse on Cloud Connector
- Eloqua Bulk API Connector
- Google Analytics Connector
- Google Big Query Connector
- Google Big Query V2 Connector
- Google Cloud Spanner Connector
- Google Cloud Storage Connector
- Google Cloud Storage V2 Connector
- JIRA Connector
- Marketo V3 Connector
- Microsoft Azure Blob Storage V2 Connector
- Microsoft Azure Blob Storage V3 Connector

- Microsoft Azure Cosmos DB SQL API Connector
- Microsoft Azure Data Lake Storage Gen1 V2 Connector
- Microsoft Azure Data Lake Storage Gen1 V3 Connector
- Microsoft Azure Data Lake Storage Gen2 Connector
- Microsoft Azure SQL Data Warehouse V2 Connector
- Microsoft Azure Synapse SQL Connector
- Microsoft CDM Folders V2 Connector
- Microsoft Dynamics 365 for Operations Connector
- Microsoft Dynamics 365 for Sales Connector
- NetSuite Connector
- Microsoft SQL Server Connector
- MySQL Connector
- OData Connector
- Oracle Connector
- PostgreSQL Connector
- REST V2 Connector
- Salesforce Connector
- Salesforce Marketing Cloud Connector
- Salesforce Oauth Connector
- ServiceNow Connector
- Snowflake Cloud Data Warehouse V2 Connector
- SuccessFactors ODATA Connector
- UltiPro Connector
- Workday V2 Connector
- Xactly Connector
- Zendesk V2 Connector
- Zuora AQuA Connector

Note: The Hosted Agent support is specific to connectors. For more information, see the help for the relevant connector.

CHAPTER 3

Secure Agent groups

Use a Secure Agent group as the runtime environment when you need to access data on-premises or when you want to access data in a cloud computing services environment without using the Hosted Agent. When you select a Secure Agent group as the runtime environment for a connection or task, a Secure Agent within the group runs the tasks.

Create Secure Agent groups to accomplish the following goals:

Prevent the activities of one department from affecting another department.

To prevent the activities of one department from impacting a different department, create separate Secure Agent groups for each department. For example, users in the sales department run 10 times as many tasks as users in the finance department, but the finance tasks are more time critical. To prevent the sales tasks from impacting the finance tasks, create separate Secure Agent groups for each department. Then assign the sales tasks to one runtime environment and the finance tasks to the other runtime environment.

Separate tasks by environment.

You can create different Secure Agent groups for test and production environments. When you configure a connection, you can associate it with the test or production database by choosing the appropriate Secure Agent group as the runtime environment.

When you create a Secure Agent group, all users in the organization can select the Secure Agent group as the runtime environment.

You can perform the following actions on a Secure Agent group:

- You can add and remove Secure Agents from a group.
- You can add multiple agents to a Secure Agent group.

  Note: If you use the runtime environment to run a mapping task that is based on a mapping in advanced mode, the Secure Agent group must have only one Secure Agent.

- You can share a Secure Agent group with your sub-organizations.

If you need to access output files on the Secure Agent machine, you can view the **All Jobs** page in Monitor or the **My Jobs** page in Data Integration to determine where a task ran.

Secure Agent groups with multiple agents

When you create a Secure Agent, it is added to its own group by default. You can add multiple agents to one Secure Agent group. All agents within a group must be of the same type, for example, all agents that run within your network or all agents that run on Amazon EC2 machines.

Add multiple agents to a group to achieve the following goals:

Balance the workload across machines.

Add multiple agents to a group to balance the distribution of tasks across machines. When the runtime environment is a Secure Agent group with multiple agents, the group dispatches tasks and background processes such as metadata calls to the available agents in a round-robin fashion.

Improve scalability for connections and tasks.

When you create a connection or task, you select the runtime environment to use. If the runtime environment is a Secure Agent group with multiple agents, the tasks can run if any Secure Agent in the group is up and running. You do not need to change connection or task properties when you add or remove an agent or if an agent in the group stops running.

When you add multiple agents to a group, ensure that all of the Secure Agents are of the same type. For example, your organization installs four Secure Agents on physical machines within your network and two Secure Agents on Amazon EC2 machines. You can create a Secure Agent group that contains some or all of the local agents and a different group that contains the EC2 agents. Do not create a group that contains both a local agent and an EC2 agent.

If you need to access output files on the Secure Agent machine, you can view the job details to determine which Secure Agent ran the task. To view job details, open Monitor, select **All Jobs**, and click the job name.

Service and connector assignment for Secure Agent groups

Your organization can enable and disable specific Informatica Intelligent Cloud Services and connectors that your organization is licensed to use, for a Secure Agent group.

You can perform the following actions:

Enable or disable Informatica Intelligent Cloud Services for a Secure Agent group.

You can enable services such as Data Integration or Application Integration when you want the agents in the group to run the tasks, processes, and product features associated with the service. By default, when you create a Secure Agent group, all services and connectors that your organization is licensed to use are disabled. When you enable a service, the service starts on each agent in the Secure Agent group.

Some services require other services or connectors. If you enable a service that requires other services, Informatica Intelligent Cloud Services automatically enables the required services. For example, you enable Data Quality on a Secure Agent group. Data Quality requires Data Integration. When you enable Data Quality, Informatica Intelligent Cloud Services automatically enables Data Integration as well.

Disable services when you do not want the agents in the group to run the tasks, processes, or product features associated with the service. When you disable a service, the service stops on each agent in the Secure Agent group. Any task, process, or product feature that uses the Secure Agent group as the runtime environment no longer runs.

When you enable a service, you also enable the required Secure Agent services. For more information about the Secure Agent services that each service requires, see *Secure Agent Services*.

Enable or disable connectors for a Secure Agent group.

You can enable specific connectors when you want the agents in the group to be able to communicate with cloud and on-premise applications, platforms, databases and flat files. When you enable a connector, all agents in the group download the packages associated with the connector.

Disable connectors when you do not want the agents in the group to download the packages associated with the connectors. When you disable a connector, any connection that uses the Secure Agent group as the runtime environment no longer runs.

Enable or disable additional services for a Secure Agent group.

You can enable or disable additional services such as Self-Hosted Git Repo or EDC Integration.

You can also enable or disable Secure Agent services for individual Secure Agents within the Secure Agent group. For more information, see "Stopping and starting services on a Secure Agent" on page 23.

After you make service assignments for a Secure Agent group, you might add or remove agents. When you add a Secure Agent to a group, the agent inherits the service assignments of the group that you add it to.

Enable or disable services and connectors for a Secure Agent group on the **Runtime Environments** page:

Service assignment guidelines

Use the following guidelines when you enable and disable services for a Secure Agent group:

- Before you disable a service, verify that no connection, task, or process that uses the group as the runtime environment requires the service.

- Before you disable a service, verify that no feature that uses the group as the runtime environment requires the service.
  If a feature has a Secure Agent group selected as the runtime environment and you disable a required service, the feature cannot be used. For example, the runtime environment for Enterprise Data Catalog integration is set to RuntimeEnv2. If you disable EDC Search Service on RuntimeEnv2, you can no longer perform data catalog discovery.

- When you create a connection, select a runtime environment in which the required services are enabled. For example, you want to create an Advanced SFTP connection for a file ingestion task target. When you create the connection, select a runtime environment in which the Mass Ingestion service is enabled.

- If you configure your organization to store connection properties locally, the Data Integration service must be enabled for the Secure Agent group.

Enabling or disabling services and connectors for a Secure Agent group

You can enable or disable Informatica Intelligent Cloud Services and connectors for a Secure Agent group. By default, all services and connectors are disabled in newly-created Secure Agent groups. Enable the services and connections you want to run on the group.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group and select **Enable or Disable Services and Connectors**.

   A dialog box listing all the services and connectors for the Secure Agent group is displayed.
3. On the **Services** tab, choose the Informatica Intelligent Cloud Services to enable or disable.

   Certain services may be listed in the **Additional Services** tab.
4. On the **Connectors** tab, choose the connectors to enable or disable.
5. On the **Additional Services** tab, select the Secure Agent services to enable or disable.

   For example, if your organization uses source control, and you want to disable it on your Secure Agent group, disable the GitRepoConnectApp service.

   The services that appear in this list vary based on your licenses. You might not see any services listed here.
6. Click **OK**.

   The changes affect every Secure Agent in the group.

Service and connector assignment example

Your organization uses Data Integration and has licenses for mass ingestion and for Enterprise Data Catalog data discovery.

The organization uses the following Secure Agent groups:

- Group 1: Secure Agent 1, Secure Agent 2 , Secure Agent 3
- Group 2: Secure Agent 4
- Group 3: Secure Agent 5

By default, users in your organization can select any group as the runtime environment for any connection or any task, including file ingestion tasks. An administrator can also select any group as the runtime environment for integration with Enterprise Data Catalog.

To balance the load across Secure Agent groups, you want might want to reserve Group 1 for Data Integration tasks except file ingestion tasks, Group 2 for file ingestion tasks, and Group 3 for data catalog discovery.

Therefore, you enable and disable the following Secure Agent services:

Secure Agent Group	Enabled Services	Disabled Services
Group 1	Data Integration Server	Mass Ingestion, EDC Search Agent
Group 2	Mass Ingestion	Data Integration Server, EDC Search Agent
Group 3	EDC Search Agent	Data Integration Server, Mass Ingestion

To avoid task and feature failures, you must also verify the following settings:

- All Data Integration tasks except file ingestion tasks use Group 1 as the runtime environment. All connections that these tasks use also use Group 1 as the runtime environment.
- All file ingestion tasks use Group 2 as the runtime environment. All connections that these tasks use also use Group 2 as the runtime environment.
- On the **Organization** page in Administrator, the Enterprise Data Catalog integration properties use Group 3 as the runtime environment.

Shared Secure Agent groups

If you are the administrator of a parent organization, you can share a Secure Agent group with the sub-organizations. When you share a Secure Agent group, all sub-organizations can run data integration jobs on the Secure Agents within the group.

Note: Share a Secure Agent group when all agents in the group run only the Data Integration Server service and Mass Ingestion Files. For other agent services, you cannot run jobs on a shared Secure Agent group.

Share a Secure Agent group to optimize the use of available Secure Agent resources. For example, your organization contains separate sub-organizations for departments in different time zones. Each sub-organization runs data integration tasks at different times of the day. If you create one Secure Agent group for each sub-organization, some Secure Agent groups might be used heavily at certain times of the day while others remain idle. To distribute the tasks more evenly, add the Secure Agents to a Secure Agent group, and share the Secure Agent group with the sub-organizations.

To share a Secure Agent group, you must have the appropriate license.

When you share a Secure Agent group, the group appears on the **Runtime Environments** page in all sub-organizations. The sub-organization administrators cannot view the Secure Agents within the group. They cannot perform management tasks on the group such as adding or deleting Secure Agents, renaming, deleting, or unsharing the group, or changing the group permissions.

When a user in the sub-organization creates a connection or task, the user can select the shared Secure Agent group as the runtime environment.

Flat file connections in shared Secure Agent groups

If a shared Secure Agent group contains multiple Secure Agents and the group is used as the runtime environment for a flat file connection, the directory used in the connection must be accessible by all Secure Agents in the group.

If the directory is not accessible by all Secure Agents, tasks that use the connection fail if they are assigned to a Secure Agent that cannot access the directory.

Working with Secure Agent groups

Create Secure Agent groups on the **Runtime Environments** page. After you create a Secure Agent group, you can rename or delete the group, add and remove Secure Agents, and change group permissions. You can also enable services and connectors for the group.

Tip: Click the refresh icon next to **New Runtime Environment** to refresh the page before performing any actions on Secure Agent groups.

You can complete the following tasks:

Create a Secure Agent group.

> To create a Secure Agent group, click **New Runtime Environment** and enter a name and optionally a description for the group. After you create a group, you can add Secure Agents to the group.
>
> **Note:** If you use multi-byte characters in the Secure Agent group name and you create the group in a cloud-hosted environment, verify that the environment also supports these characters.

Edit Secure Agent group properties.

> To rename a Secure Agent group or to add or update the description, expand the Actions menu, select **Edit Environment Properties**, and complete the fields in the dialog box. Informatica Intelligent Cloud Services updates the group name in all services that use the group.

Enable or disable specific Informatica Intelligent Cloud Services and connectors for a Secure Agent group.

> To enable or disable services for a Secure Agent group, expand the Actions menu and select **Enable or Disable Services, Connectors**. On the **Services** tab, select the services to enable or disable. You can enable or disable any service that your organization is licensed to use.
>
> **Note:** Before you disable a service, verify that no connection, task, or process that uses the group as the runtime environment requires the service. If a connection, task, or process has a Secure Agent group selected as the runtime environment and you disable a required service, the task or process cannot run. Similarly, if a feature has a Secure Agent group selected as the runtime environment and you disable a required service, the feature cannot be used.
>
> To enable or disable connectors, expand the Actions menu and select **Enable or Disable Services, Connectors**. On the **Connectors** tab, select the connectors to enable or disable. You can enable or disable any connector that you organization is licensed to use.
>
> To enable or disable additional services such as Self-Hosted Git Repo, expand the Actions menu and select **Enable and Disable Services and Connectors.** On the **Additional Services** tab, select the services to enable or disable. You can enable or disable any service that your organization is licensed to use.

Add Secure Agents to a group.

> To add Secure Agents to a group, expand the Actions menu and select **Add or Remove Secure Agents**. You can add any agent that is in the Unassigned Agents group on the **Runtime Environments** page.
>
> Alternatively, you can add a new Secure Agent to an existing group by setting the InfaAgent.GroupName property in the infaagent.ini file before you register the agent. When you add a Secure Agent to a Secure Agent group, the Secure Agent inherits the services and connectors that are configured for the Secure Agent groups.
>
> When you add more than one Secure Agent to a Secure Agent group, all agents must meet the following requirements:
>
> - All of the agents must be of the same type, for example, all local agents or all agents that run on Amazon EC2 machines.

- Each Secure Agent must be configured to connect to the same external systems and have access to files such as libraries, initialization files, and JAR files.
- Each Secure Agent must have access to the files used in tasks. Ensure that all files used in a task are available in a shared location.

Remove Secure Agents from a group.

To remove Secure Agents from a group, expand the Actions menu and select **Add or Remove Secure Agents**. When you remove an agent from a group, Informatica Intelligent Cloud Services adds it to a group named "Unassigned Agents."

You can remove an agent from a Secure Agent group if the group is not used as the runtime environment for a connection or task. If the group is used, you can remove an agent if it is not the only agent in the group.

Delete a Secure Agent group.

To delete Secure Agent group, expand the Actions menu and select **Delete**. You can delete a Secure Agent group if it does not contain any Secure Agents.

If the Secure Agent group is associated with an advanced configuration and the advanced cluster is running, you must stop the cluster and associate the configuration with a different runtime environment before you can delete the group.

Share or unshare a Secure Agent group.

If you are the administrator of a parent organization, you can share a Secure Agent group so that the sub-organizations can use it. You can unshare a group if it is not used in a connection or task. From the Actions menu associated with the group, choose **Share Secure Agent Group** or **Unshare Secure Agent Group**.

Change permissions for a Secure Agent group.

To change permissions for a Secure Agent group, expand the Actions menu and select **Permissions**. You can define permissions for a Secure Agent group for each user group in your organization.

You can set the following permissions:

Permission	Description
Read	View details about the Secure Agent group and use the Secure Agent group in a task.
Update	Edit the Secure Agent group.
Delete	Delete the Secure Agent group.
Change	Change permissions for the Secure Agent group.

Adding a Secure Agent to a group

You can add any available Secure Agent to a Secure Agent group. Available agents appear in the "Unassigned Agents" group on the **Runtime Environments** page. You cannot add a Secure Agent to a group if the agent has already been added to another group. When you add a Secure Agent to a group, the Secure Agent inherits all the services and connectors that are enabled for the group.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group, and select **Add or Remove Secure Agents**.

3. In the **Secure Agents** list, enable the checkbox for the Secure Agents that you want to add to the group.

    If the agent you want isn't listed, that means it is currently assigned to another group. You must remove an agent from a group before you can add it to a different group.

    If there are many agents in the list, use the **Find** box to quickly locate an agent.
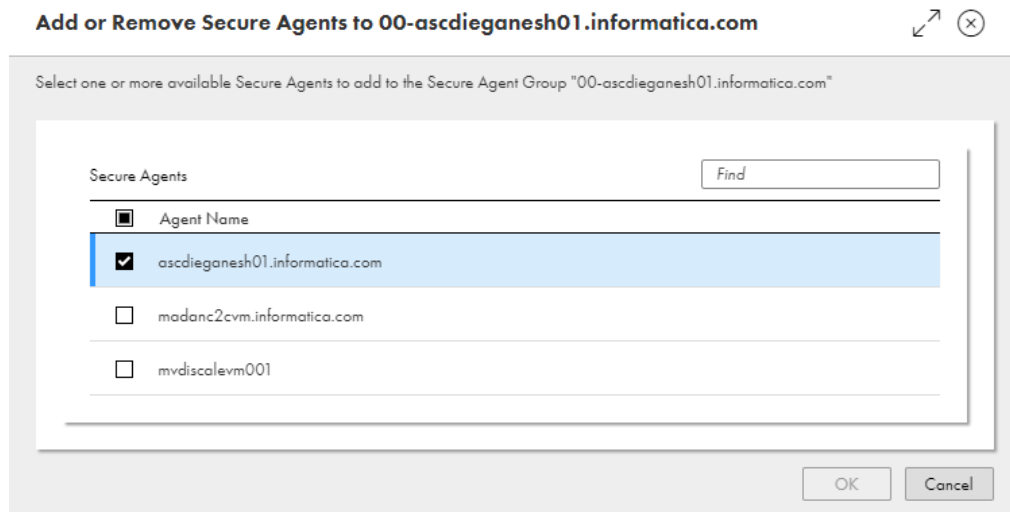
4. Click **OK.**

Adding a new Secure Agent to an existing group

You can add a Secure Agent to an existing Secure Agent group when you install the agent. To add a Secure Agent to an existing group, add the InfaAgent.GroupName property to the infaagent.ini file before you register the agent. When you add a Secure Agent to a group, the Secure Agent inherits all the services and connectors that are enabled for the group.

1. Install the Secure Agent.
2. On Windows, when you are prompted to register the agent, open Windows Services and stop the agent.

    On Linux, when the installation program finishes, do not start the agent.
3. Open `<Secure Agent installation directory>/apps/agentcore/conf/infaagent.ini` in a text editor.
4. Add the following property and save the file:

    `InfaAgent.GroupName=<Secure Agent group name>`
5. Start the agent.
6. Register the agent.

    Informatica Intelligent Cloud Services adds the Secure Agent to the group you specify in the InfaAgent.GroupName property instead of a new group.

Removing a Secure Agent from a group

You can remove an agent from a Secure Agent group if the group is not used in a connection or task. If the group is used in a connection or task, you can remove an agent if it is not the only agent in the group. When

you remove a Secure Agent from a group, Informatica Intelligent Cloud Services adds it to a group named "Unassigned Agents."

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group, and select **Add or Remove Secure Agents**.
3. In the list of **Secure Agents**, clear the check mark next to the agents that you want to remove from the group.
4. Click **OK.**

The Secure Agents that were removed appear in the "Unassigned Agents" group on the **Runtime Environments** page.
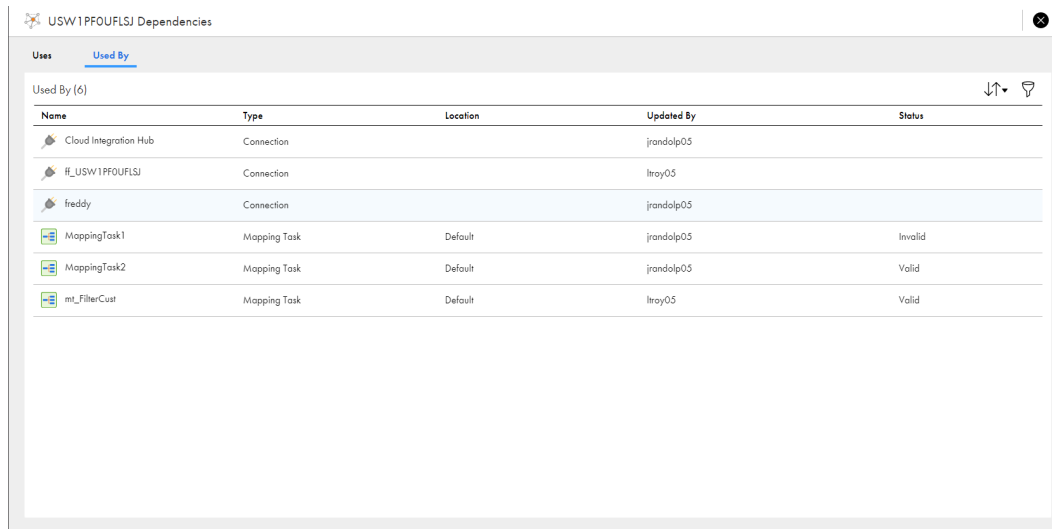
Viewing Secure Agent group dependencies

You can view object dependencies for Secure Agent groups.

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.

To view object dependencies for a Secure Agent Group, expand the Actions menu and select **Show Dependencies**.

The following image shows the **Dependencies** page for a Secure Agent group:

To sort the objects that appear on the page, click the sort icon and select the column name for the property you want to sort by.

To filter the objects that appear on the dependencies page, click the Filter icon. Use filters to find specific objects. To apply a filter, click **Add Field**, select the property to filter by, and then enter the property value. You can specify multiple filters. For example, to find connections with Oracle in the name, add the Type filter and specify Connection. Then add the Name filter and enter "Oracle."

CHAPTER 4

Secure Agents

The Informatica Cloud Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. When the Secure Agent runs a task, it connects to the Informatica Cloud hosting facility to access task information. It connects directly and securely to sources and targets, transfers data between them, orchestrates the flow of tasks, runs processes, and performs any additional task requirement.

If the Secure Agent loses connectivity to Informatica Intelligent Cloud Services, it tries to reestablish connectivity to continue the task. If it cannot reestablish connectivity, the task fails.

The Secure Agent uses pluggable microservices for data processing. For example, the Data Integration Server runs all data integration jobs, and Process Server runs application integration and process orchestration jobs. Each Secure Agent service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings. For more information about Secure Agent services, see *Secure Agent Services*.

You can install and run one Secure Agent on a physical or virtual machine. After you install a Secure Agent, all users in the organization share the Secure Agent. You can configure the Secure Agent properties and move it to a different Secure Agent group. To improve scalability, you can also add multiple agents to a Secure Agent group.

Working with Secure Agents

After you create a Secure Agent, you might need to perform management tasks such as viewing and configuring agent properties, checking the host information, viewing audit logs, or refreshing the agent status. You can also delete a Secure Agent if it is no longer used.

You perform most management tasks for Secure Agents on the agent details page. To access the agent details page, click a Secure Agent on the **Runtime Environments** page.

The following image shows the agent details page:
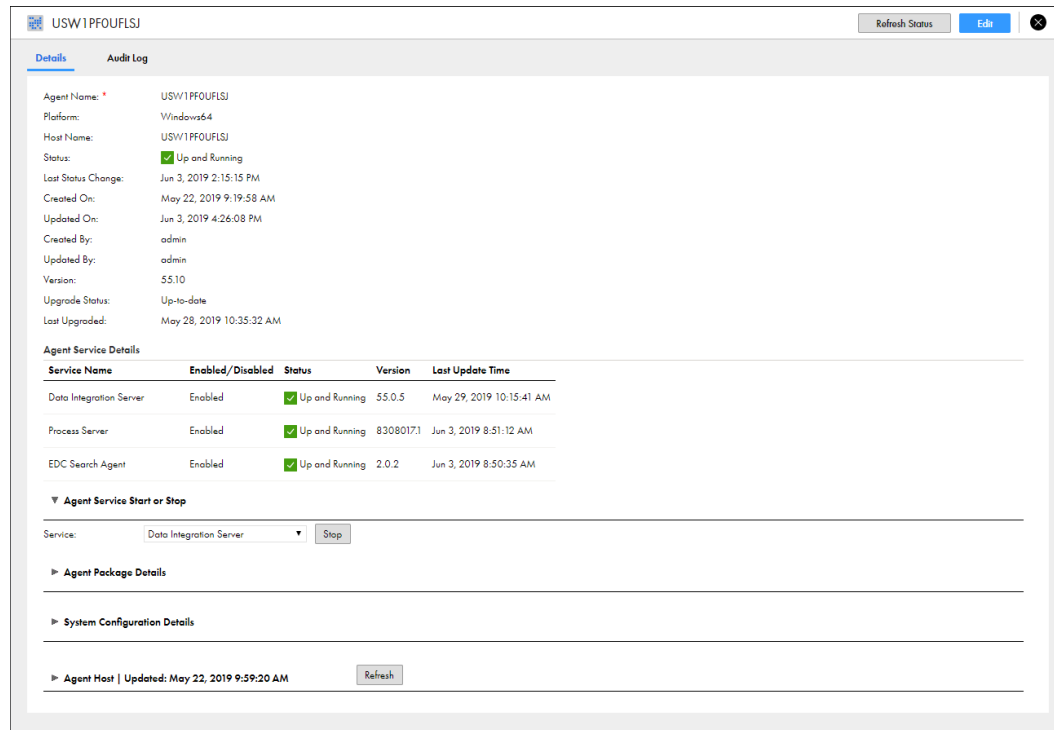
You can complete the following tasks:

View the Secure Agent details.

View details such as the host name, the current status, the last date and time that the agent was updated, and the agent version.

The Secure Agent can have any of the following statuses:

Status	Description
Agent Core is not running.	The Secure Agent is not available, but one or more of the services is running.
Not all the services are running.	The Secure Agent is available, but one or more of the services is not available.
Agent Core Upgrading	The Secure Agent is upgrading to a new version.
Stopped	The Secure Agent is not available.
Up and Running	The Secure Agent and all of the services that the agent runs are available.

View the Secure Agent service details.

View details for Secure Agent services that run on the Secure Agent such as the service name, status, version, and last update time.

A Secure Agent service can have any of the following statuses:

Status	Description
Error	The process failed.
Restarting Due to Error	The service is starting due to a failure.
Shutting Down	The service is shutting down.
Standby	The service is running, but it is not compatible with Informatica Intelligent Cloud Services.
Starting Up	The service is starting up.
Stopped	The service is not available.
Up and Running	The service is running.
User Stopped	The service was stopped by a user.
Warning	The service is running, but it cannot accept work.

The version number changes each time you modify the service. The Secure Agent retains the directories for the old version of the service for seven days. For example, if you update the NetworkTimeoutPeriod for version 55.0.2 of the Data Integration Server, the agent increments the version number to 55.0.3 and creates the following directory:

`<Secure Agent installation directory>/apps/Data_Integration_Server/55.0.3.1`

It deletes the `<Secure Agent installation directory>/apps/Data_Integration_Server/55.0.2.x` directories after seven days.

Stop and start Secure Agent services.

Stop and start the services that run on a Secure Agent to perform troubleshooting, optimize resources on the agent machine, or make service configuration changes. When you stop or start a Secure Agent service, other services that run on the agent are not affected.

View the Secure Agent package details.

Expand the **Agent Package Details** section to see the name and version number for the packages in each service that runs on the Secure Agent. You can filter the packages by service.

View and edit Secure Agent service properties.

Expand the **System Configuration Details** section to see the Secure Agent service properties. You can filter the properties by service and type.

To configure the properties, click **Edit**. You can configure properties for each service that runs on the Secure Agent. You can also add and remove custom properties, which are used by connectors. For more information about Secure Agent services and service properties, see *Secure Agent Services*. For more information about custom properties, see the help for the appropriate connector.

View the Secure Agent host properties.

Expand the **Agent Host** section to see information about the machine that hosts the Secure Agent. For example, you can view the machine name, operating system, and available disk space.

To refresh the information, click **Refresh**. The last date and time that the information was refreshed appears next to the **Agent Host | Updated** heading.

View the Audit Log.

To view audit information such as start and stop times, server connections, and upgrade messages, click **Audit Log**.

Refresh the Secure Agent status.

To refresh the status of the Secure Agent, click **Refresh Status** in the upper right corner of the page.

To view the status on Linux, you can also navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

Then run one of the following commands:

```
./consoleAgentManager.sh getstatus
```

```
./consoleAgentManager.sh updatestatus
```

Stopping and starting services on a Secure Agent

By default, each Secure Agent in an organization runs all microservices that are used for data processing in the organization. You can stop and start the microservices to perform troubleshooting, optimize resources on the agent machine, or make configuration changes. When you stop or start a Secure Agent microservice, other microservices that run on the agent are not affected.

The microservices that you stop and start on a Secure Agent are the Secure Agent services, which are different from the Informatica Intelligent Cloud Services. For example, if you want to stop the services associated with Operational Insights, you must stop the OI Data Collector service on the agent. For more information about Secure Agent services, see *Secure Agent Services*.

You might need to stop and restart a Secure Agent service in the following circumstances:

You need to troubleshoot issues with a specific Secure Agent service.

If a Secure Agent service shows an error state, you can stop the service, troubleshoot the problem, and then restart the service.

You are running memory or CPU intensive jobs, and you want to optimize computing resources on the Secure Agent machine.

For example, your organization runs Data Integration and Application Integration jobs. You want to optimize computing resources so that the Data Integration jobs run during the day and the Application Integration jobs run at night. To do this, stop Process Server during the day and restart it in the evening, and stop the Data Integration Server at night and restart it in the morning.

You update service configuration properties for the File Integration Service.

After you change configuration properties for the File Integration Service, you must restart the service. If the Secure Agent runs other services, you can stop and restart the File Integration Service without affecting the other services.

To start or stop a service on a Secure Agent, you must have update permission on the Secure Agent.

If you are the administrator of a sub-organization, you can start and stop services on the agents in the sub-organization. However, you cannot start and stop services on a Secure Agent that is in a shared Secure Agent group.

Each time you start and restart a service, the Secure Agent creates a new subdirectory for the service-related files. For example, if the Secure Agent uses version 64.0.38 of the Data Integration Server, the Secure Agent installation directory contains the following subdirectory:

`<Secure Agent installation directory>/apps/Data_Integration_Server/64.0.38.1`

When you stop and restart the Data Integration Server, the Secure Agent creates the following directory:

`<Secure Agent installation directory>/apps/Data_Integration_Server/64.0.38.2`

The Secure Agent does not delete the `.../64.0.38.1` directory.

Example

Your organization uses Data Integration and has licenses for Enterprise Data Catalog integration, file integration, and mass ingestion.

Your Secure Agent runs the following Secure Agent services:

- Data Integration Server
- EDC Search Agent
- File Integration Service
- Mass Ingestion

If you have issues with Enterprise Data Catalog search, you can stop the EDC Search Agent service while you perform troubleshooting. When you stop the EDC Search Agent service, you cannot perform data catalog discovery in Data Integration. However, jobs processed by the other services on this agent such as mappings, tasks, taskflows, and AS2 file transfers continue to run.

Guidelines for stopping and starting Secure Agent services

Use the following guidelines when you stop and start services on a Secure Agent:

- Use caution when you stop Secure Agent services because this can cause job failures.

    When you stop a Secure Agent service, any job that requires the service and is currently running on the agent stops. If there are no other agents in the group, the job can no longer run. If there are other agents in the group, you can restart the job and it will run on a different agent.

- Do not stop the Data Integration Server on an agent if you store connection properties with the agent.

    If you store connection properties with a local Secure Agent and you stop the Data Integration Server on the agent, users will not be able to access any connections or run tasks in the organization. Any job that is currently running on the agent also fails.

- Do not stop and start services to reserve a Secure Agent group for certain types of jobs.

    If you want to reserve a Secure Agent group for certain types of jobs, you can enable the required services for the Secure Agent group and disable other services. For more information about enabling and disabling services for a Secure Agent group, see "Service and connector assignment for Secure Agent groups" on page 12.

Stopping a Secure Agent service

You can stop a Secure Agent service that is in the "Up and Running" or "Error" state. Stopping a Secure Agent service stops all versions of the service that are running. After a service stops, you can start the latest version of the service.

Note: If you stop a Secure Agent service and then restart the Secure Agent, the service remains stopped until you start it.

1. In Administrator, select **Runtime Environments**.

2. On the **Runtime Environments** page, click the name of the Secure Agent.

   Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.

3. Click the **Details** tab.

4. In the **Agent Service Start or Stop** area, select the service that you want to stop.

5. Click **Stop**.

The Secure Agent service stops, and Informatica Intelligent Cloud Services adds an entry in the audit log indicating that the service was stopped by a user.

Starting a Secure Agent service

You can start a Secure Agent service that is in the "Stopped" state. Starting a Secure Agent service starts the latest version of the service.

1. In Administrator, select **Runtime Environments**.

2. On the **Runtime Environments** page, click the name of the Secure Agent.

   Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.

3. Click the **Details** tab.

4. In the **Agent Service Start or Stop** area, select the service that you want to start.

5. Click **Start**.

Informatica Intelligent Cloud Services attempts to start the Secure Agent service. After the service starts, the status changes to "Up and Running." If the Secure Agent service fails to start, check the audit log to find the cause of the error.

Configuring 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 period. Configure an agent blackout period to configure specific hours, days, or intervals in which no data integration jobs can run on the agent.

Agent blackout periods stop the Data Integration Server service from running jobs on a Secure Agent during the blackout period. They do not prevent other types of jobs from running on the agent. Configure an agent blackout period in the following circumstances:

- The Data Integration Server is the only service enabled on the agent and you want to stop all data integration jobs from running during a certain period.

- The Secure Agent runs multiple services and you want to stop only the data integration jobs from running during a certain period.

Note: The agent blackout period is different than the schedule blackout period for the organization. During an organization's schedule blackout period, no jobs can run on any agent. For more information about schedule blackout periods, see *Organization Administration*.

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

For example, the following blackout file contains two blackout periods: one blackout period from July 27, 2021, 5:00 AM through July 28, 2021, 11:00 PM and a second blackout period that repeats on Fridays from 2:00-4:00 PM:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
    <BlackoutWindow>
        <RepeatFrequency>OneTime</RepeatFrequency>
        <Start>2021-07-27 5:00:00</Start>
        <End>2021-07-28 23:00:00</End>
    </BlackoutWindow>
    <BlackoutWindow>
        <RepeatFrequency>Friday</RepeatFrequency>
        <Start>14:00:00</Start>
        <End>16:00:00</End>
    </BlackoutWindow>
</BlackoutWindows>
```

To configure one or more blackout periods, create a file named "blackoutWindows.dat" in the following directory on the Secure Agent machine:

```
<Secure Agent Installation Directory>\apps\Data_Integration_Server\conf\
```

If the Secure Agent is in a Secure Agent group, copy the blackout file to the `...\conf\` directory on each agent machine in the group.

If you want to use a different file name and directory, you can override the file name and file path.

After you create a blackout file, restart the Data Integration Server service on the Secure Agent so that the blackout periods take effect.

Overriding the blackout file name and directory

You can override the blackout file name and directory by setting the BlackoutWindowsFile Tomcat custom property for the Data Integration Server.

Set the following custom property for the Data Integration Server on the agent details page:

Service	Type	Name	Value
Data Integration Server	Tomcat	BlackoutWindowsFile	File path and file name for the blackout file. For example: `C:/AgentBlackouts/Agent001Blackouts.dat` **Note:** Use forward slashes (/) in the file path on both Windows and UNIX machines because the Secure Agent interprets backslashes (\) as escape characters. The file path must be accessible by the Secure Agent.

For more information about configuring custom properties for a Secure Agent service, see *Secure Agent Services*.

Blackout file structure

The blackout file is an XML file that contains elements that define each blackout period and the frequency, start time, and end time for each blackout period.

The blackout file has the following structure:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
    <BlackoutWindow>
        <RepeatFrequency></RepeatFrequency>
        <Start></Start>
        <End></End>
    </BlackoutWindow>
    <BlackoutWindow>
        <RepeatFrequency></RepeatFrequency>
        <Start></Start>
        <End></End>
    </BlackoutWindow>
    …
</BlackoutWindows>
```

The file contains the following elements:

Element	Required/ Optional	Description
BlackoutWindows	Required	Contains a BlackoutWindow element for each blackout period. Must contain one or more BlackoutWindow elements.
BlackoutWindow	Required	Defines one blackout period. Must contain one RepeatFrequency element, one Start element, and one End element.
RepeatFrequency	Required	Repeat frequency for the blackout period. Must contain one of the following values: - `OneTime` - `Daily` - `Weekdays` - `Sunday` - `Monday` - `Tuesday` - `Wednesday` - `Thursday` - `Friday` - `Saturday`
Start	Required	Blackout period start time in the format yyyy-mm-dd hh24:mi:ss. For example, `2019-07-25 10:26:55`. The time zone is the Secure Agent time zone.
End	Required	Blackout period end time in the format yyyy-mm-dd hh24:mi:ss. For example, `2019-07-26 11:45:00`. The time zone is the Secure Agent time zone.

Do not enclose element values in quotation marks.

Renaming a Secure Agent

By default, the name of a Secure Agent is the same as the name of the machine where you installed the agent. You can change the agent name.

1. On the **Runtime Environments** page, click the name of the Secure Agent.

    Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
2. Click the **Details** tab.
3. In the upper right corner, click **Edit**.
4. Enter a new name in the **Agent Name** field.

    Note: If you use multi-byte characters in the Secure Agent name and the agent is in a cloud-hosted environment, verify that the environment also supports these characters.
5. Click **Save**.

Deleting a Secure Agent

Delete a Secure Agent if you no longer need it to run tasks. Delete a Secure Agent on the **Runtime Environments** page.

Note: You cannot delete a Secure Agent if it is used in a connection or a task. For example, if the Secure Agent is the only agent in a group, and the group is used as the runtime environment for a connection or task, you cannot delete the agent.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent and select **Delete Secure Agent**.

    If the Secure Agent is running, a warning message appears. Stopping an active Secure Agent prevents scheduled tasks associated with the Secure Agent from running. Ignore the warning if you do not need the Secure Agent.

If you no longer need the Secure Agent, uninstall the Secure Agent after you delete it.

Upgrading a Secure Agent

The Secure Agent upgrades automatically the first time that you access a new Informatica Intelligent Cloud Services release. The upgrade process installs a new version of the Secure Agent, updates connector packages, and applies configuration changes for the microservices that run on the agent. You do not need to upgrade the Secure Agent manually.

However, to prepare for an upgrade, you might need to perform tasks such as ensuring that each Secure Agent machine has enough disk space available for the upgrade. For more information about preparing for an upgrade, see *Administrator What's New*.

Note: A Secure Agent can upgrade only if the agent version is the current major release and the agent is running. For example, the new major release upgrades the Secure Agent to version 65.x. To be upgraded, an agent must be version 64.x and must be running.

Secure Agent data encryption

The Secure Agent encrypts sensitive data that is stored in the Secure Agent directory, preventing an attacker from copying and running the Secure Agent on another machine. You can change the key that it is used to encrypt this data.

When you install a Secure Agent, some of the files in the Secure Agent directory contain sensitive data such as agent credentials, agent proxy credentials, and JDK keystore passwords. If you store connections on the Secure Agent, files on the Secure Agent machine also store the connection credentials.

To encrypt all the information stored within the Secure Agent, Informatica uses AES 256 as the encryption method. This method uses a key that is unique to the Secure Agent. The encryption key is generated using some machine-specific information and can be found in this location: `<Secure Agent installation directory>/apps/agentcore/conf`.

By default, the encryption key is generated using the following properties:

- Operating system of the Secure Agent machine

- Machine architecture, for example, 32-bit, 64-bit, or 64-bit ARM

- Host name of the machine

- Hardware MAC address

You can prevent some of these properties from being used to generate the encryption key. For example, if you plan to back up the agent on one machine and restore it on a different machine, you might want to exclude the host name and hardware MAC address. You can also add other properties to make the encryption even more secure. For example, if the Secure Agent is installed on Amazon Web Services, you might add the instance ID or the AMI ID.

You can change the encryption key at any time. To do this, you use the consoleAgentManager rotateDeviceKey command.

The command performs the following actions:

- Re-encrypts the infaagent.ini and proxy.ini files.

- Re-encrypts the connection master key.

- Forces the redeployment of the Secure Agent services on the next startup.

After you run the command, you must also configure the following environment variables:

Environment variable	Description
INFA_AGENT_EXCLUDE_SEC_PROPS	Specifies the properties to exclude. Set the value to the same values you excluded in the rotateDeviceKey command.
INFA_AGENT_ADDITIONAL_SEC_PROPS	Specifies the properties to add. Set the value to the same values you added in the rotateDeviceKey command.

Changing the data encryption key on Windows

To change the Secure Agent data encryption key, use the consoleAgentManager rotateDeviceKey command.

Back up the Secure Agent installation directory before you change the data encryption key.

The user account you use to change the encryption key must have privileges to delete files in the Secure Agent installation directory and its subdirectories.

Note: During upgrade, there can be two versions of the Data Integration Server running within the maintenance window. Do not change the encryption key until the upgrade has completed and the newer version of the Data Integration Server is the only version that is running.

1. Stop the Secure Agent.

2. Open a command prompt as an administrator, and navigate to the following directory:

   `<Secure Agent installation directory>/apps/agentcore`

3. Run the following command:

   `consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<excluded security properties> INFA_AGENT_ADDITIONAL_SEC_PROPS=<additional security properties>`

   You can exclude the following properties: `OS_TYPE`, `OS_ARCH`, `HOSTNAME`, and `HWD_MAC_ADDR`. Separate multiple properties with a comma.

   Additional properties can be any key=value pair. For example, `instanceId=<AWS instance ID>,amiId=<AWS AMI ID>`. Separate multiple properties with a comma.

   For example, to exclude the Secure Agent machine hostname and hardware MAC address from the encryption key and include the AWS instance ID, run the following command:

   `consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS instance ID>`

4. When the command completes successfully, if you excluded security properties, create the system environment variable INFA_AGENT_EXCLUDE_SEC_PROPS, and set the value to the same values that you set in the rotateDeviceKey command.

5. If you added security properties, create the system environment variable INFA_AGENT_ADDITIONAL_SEC_PROPS, and set the value to the same values that you set in the rotateDeviceKey command.

6. Restart the machine.

7. If the Secure Agent doesn't start automatically, restart the Secure Agent.

Changing the data encryption key on Linux

To change the Secure Agent data encryption key, use the consoleAgentManager rotateDeviceKey command.

Back up the Secure Agent installation directory before you change the data encryption key.

Note: During upgrade, there can be two versions of the Data Integration Server running within the maintenance window. Do not change the encryption key until the upgrade has completed and the newer version of the Data Integration Server is the only version that is running.

1. Stop the Secure Agent.

2. Navigate to the following directory:

   `<Secure Agent installation directory>/apps/agentcore`

3. Run the following command:

   `./consoleAgentManager.sh rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<excluded security properties> INFA_AGENT_ADDITIONAL_SEC_PROPS=<additional security properties>`

   You can exclude the following properties: `OS_TYPE`, `OS_ARCH`, `HOSTNAME`, and `HWD_MAC_ADDR`. Separate multiple properties with a comma.

   Additional properties can be any key=value pair. For example, `instanceId=<AWS instance ID>,amiId=<AWS AMI ID>`. Separate multiple properties with a comma.

For example, to exclude the Secure Agent machine hostname and hardware MAC address from the encryption key and include the AWS instance ID, run the following command:

```
./consoleAgentManager.sh rotateDeviceKey
INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR
INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS instance ID>
```

4. When the command completes successfully, if you excluded security properties, create the environment variable INFA_AGENT_EXCLUDE_SEC_PROPS in the source bash profile, and set the value to the same values that you set in the rotateDeviceKey command.

5. If you added security properties, create the environment variable INFA_AGENT_ADDITIONAL_SEC_PROPS in the soource bash profile, and set the value to the same values that you set in the rotateDeviceKey command.

6. Restart the Secure Agent.

Secure Agent Manager

When you install the Secure Agent on Windows, you also install the Informatica Cloud Secure Agent Manager. The Secure Agent runs as a Windows service. You can launch the Secure Agent Manager from the Windows Start menu or the desktop icon.

Use the Secure Agent Manager to perform the following tasks:

- View the status of the Secure Agent and the services that the Secure Agent runs.

- Stop and restart the Secure Agent.

- Configure Windows settings such as proxy settings and a Windows Secure Agent service login.

The Secure Agent Manager displays the status of the Secure Agent and the services that the Secure Agent runs. If the Secure Agent or one of the services that the Secure Agent runs is not starting or not running, the Secure Agent Manager displays an alert message and a link that you can click to view details.

When you close the Secure Agent Manager, it minimizes to the Windows taskbar for quick access. Closing the Secure Agent Manager does not stop the Secure Agent. When the Secure Agent Manager is minimized, you can view the Secure Agent status by hovering over the Secure Agent Manager icon.

Using a proxy server for the Secure Agent

A proxy server allows indirect connection to network services for security and performance reasons. For example, you can use a proxy server to get through a firewall, and some proxies provide caching mechanisms.

When you configure a proxy server for the Informatica Cloud Secure Agent, you define the minimum required settings in the Secure Agent Manager. Informatica Intelligent Cloud Services updates the following file and adds other properties that you can edit manually:

```
<Secure Agent installation directory>/apps/agentcore/conf/proxy.ini
```

The following code shows the default contents of `proxy.ini`:

```
InfaAgent.ProxyPassword=ZU8KjIzgtVrVmfRMUPzPMw\=\=
InfaAgent.ProxyNtDomain=
InfaAgent.ProxyHost=foo.bar.com
```

```
InfaAgent.ProxyPasswordEncrypted=true
InfaAgent.NonProxyHost=localhost|127.*|[\:\:1]
InfaAgent.ProxyUser=
InfaAgent.ProxyPort=12345
InfaAgent.AuthenticationOrder=
```

When you configure a proxy server for the Informatica Cloud Secure Agent, you can set InfaAgent.NonProxyHost to exclude certain IP addresses and host names from the proxy. For example, when you use managed identity authentication to connect to an Azure source or target in a mapping that runs in advanced mode, exclude the IP address of the metadata service, 169.254.169.254.

Configuring a proxy to exclude non-proxy hosts

In the `proxy.ini` file, set the property InfaAgent.NonProxyHost to exclude IP addresses or host names. By default, Informatica Intelligent Cloud Services adds localhost as the value for InfaAgent.NonProxyHost when you initially configure the proxy server.

1. Open `<Secure Agent installation directory>/apps/agentcore/conf/proxy.ini`.

2. Update the value for InfaAgent.NonProxyHost to specify the IP addresses or host names that you want to exclude.

    For example:

    - Local IP addresses:

      `InfaAgent.NonProxyHost=localhost|127.`**`|[\:\:1]|123.432.`**

    - Host names:

      `InfaAgent.NonProxyHost=localhost|127.`**`|[\:\:1]|`**`.foo.com`

    Note: You can combine a list of host names and IP addresses using the pipe character (|) as a delimiter. You can also enter a wildcard to the left for host names or to the right for IP addresses.

3. Restart the Secure Agent so that the changes take effect.

Stopping and restarting the Secure Agent on Windows

The Secure Agent Manager displays the Secure Agent status. You can use the Secure Agent Manager to stop or restart the Secure Agent.

Launch the Secure Agent Manager from the Windows **Start** menu. If the Secure Agent Manager is active, you can click the Informatica Cloud Secure Agent Manager icon in the Windows taskbar notification area to open the Secure Agent Manager.

To stop the Secure Agent from the Secure Agent Manager, click **Stop**. To restart the Secure Agent, click **Restart**. The Secure Agent Manager displays a message when the action is complete.

When you close the Secure Agent Manager, it minimizes to the Windows taskbar notification tray. Closing the Secure Agent Manager does not stop the Secure Agent.

Starting and stopping the Secure Agent on Linux

After you download the Secure Agent program files on a Linux machine, you can run the Secure Agent as a Linux process. Manually start the Secure Agent process on Linux.

1. From the command line, navigate to the following directory:

   `<Secure Agent installation directory>/apps/agentcore`

2. To start the Secure Agent, enter the following command:

   `./infaagent.sh startup`

3. To stop the Secure Agent, enter the following command:

   `./infaagent.sh shutdown`

You can view the Secure Agent status from Informatica Intelligent Cloud Services or from a Linux command line.

Note: Effective in the October 2022 release, the `infaagent startup` and `infaagent shutdown` commands are deprecated. Informatica intends to drop support for these commands in a future release.

Deprecated functionality is supported, but Informatica intends to drop support in a future release. Informatica requests that you transition to different functionality before the functionality is dropped.

Secure Agent logs

The different Secure Agent services generate their own logs. Use these logs to help you troubleshoot issues.

Tip: In the file paths below, "<install>" represents the directory in which the Secure Agent is installed.

General

The following table describes the general Secure Agent log files and shows the \apps subdirectory where you can find the files.

File	Description
<install>\apps\agentcore\agentcore.log	Tracks all operations managed by the Secure Agent for agent applications such as upgrade or opening tunnels for communications.
<install>\apps\agentcore\infaagent.log	Contains logs related to bootstrapping the agent.
<install>\apps\agentcore\agentUpgrLog.txt	Keeps agent core upgrade timestamps.
<install>\apps\agentcore\consoleAgentManager.log	Contains logs related to agent registrations.
<install>\apps\Administrator\logs\tomcat\tomcat.log	Contains logs related to pre-downloading packages.

B2B Processor

File	Description
\<install\>\apps\B2BProcessor \<version\>\logs\b2b-aaap.log	Contains information about main execution entry points, failure messages and B2B Processor service status.

CIHProcessor

The CIHProcessor logs are generated when you use a private repository with Cloud Integration Hub.

File	Description
\<install\>\apps \CIHProcessor \<version\>\logs\cih-aaap.log	Contains information about the following items: - Logs on the start and stop of the Cloud Integration Hub agent application. - Logs about CRUD runtime operations on the private staging database. For example, logging create, read, update, and delete actions for CIH topics. Also, logging read or write operations for Cloud Integration Hub publications and subscriptions.
\<install\>\apps \CIHProcessor \<version\>\log\prs-audit.log	Contains entry and exit access logs of the APIs exposed by the CIHProcessor.

Common Integration Components

File	Description
\<install\>\apps\Common_Integration_Components\logs \<version\>\app.log	Contains information about the Common Integration Components services.
\<install\>\apps\Common_Integration_Components\logs \<version\>\tomcat.out	Contains log information about the Common Integration Components service stdout.

Data Integration Server

File	Description
\<install\>\apps\agentcore	See the log files described in the General section.
\<install\>\apps\Data_Integration_Server \logs\tomcat	Contains information about the Tomcat server.
\<install\>\apps\Data_Integration_Server \logs\tomcat\tomcat\<version\>.log	Contains information about the Data Integration Server service.
\<install\>\apps\Data_Integration_Server \<version\>\tomcat.out	Contains information about the Data Integration Server stdout logs.

File	Description
<install>\apps\Data_Integration_Server\<version>\scripts.log	Contains information about the Data Integration Server life cycle scripts, for example: deploy, start, status, and stop scripts.
<install>\apps\Data_Integration_Server\logs\session logs	Contains information about the Data Integration Server task session.

File Integration service

File	Description
<install>\apps\FileIntegrationService\logs\FileIntegrationService.log	Contains logs related to the File Integration service, which includes the following information: - Logs related to the file servers, such as AS2, HTTPs, SFTP, MLLP - Transfer tasks such as encrypt, decrypt, compress, decompress. - API-triggered jobs, such as sendFiles to SFTP/AS2/FTPs. - Filer server users - Connectivity to fis-proxy

Mass Ingestion runtime

File	Description
<install>\apps\MassIngestionRuntime\logs\informaticamft.log	Contains log information related to File Mass Ingestion and File Listener logs running the MassIngestionRuntime service. Also contains logs related to the startup and status of this service.

Operational Insights Data Collector

File	Description
<install>\apps\OpsInsightsDataCollector\logs\App.log	Contains startup information for the Operational Insights Data Collector (also known as the "OI Data Collector").
<install>\apps\OpsInsightsDataCollector\logs\datacollector.log	Contains information about on-premises and cloud data collections. Also contains information about the publishing performed by the Operational Insights Data Collector service.

Process Server

File	Description
<install>\apps\process-engine\logs\catalina.log	Contains logging information from the Process Server. This is useful for diagnosing runtime errors.
<install>\apps\process-engine\logs\scripts.log	Contains logging from scripts executed by agentcore to start or stop the components of the Process Server, including the database and server itself.

File	Description
<install>\apps\process-engine\logs\localhost-access.log	Contains information associated with a request, for example: IP address, time, request method such as GET or POST, and the resource from which the request is coming.
<install>\apps\process-engine\logs\PostGreSql\upgrade.log	Contains logging that captures information about if or when the database version is upgraded.
<install>\apps\process-engine\logs\PostGreSql\postgresql.log	Contains logs for the PostgreSQL database, which is useful for diagnosing database-related issues.

Troubleshooting a Secure Agent

The Secure Agent did not install or start correctly.

If the Secure Agent does not install or start correctly, complete the following tasks:

1. Review the following logs:

File	Description
<Secure Agent installation directory>\apps\agentcore\infaagent.log	Contains startup and shutdown information about the Secure Agent.
<Secure Agent installation directory>\apps\agentcore\agentcore.log	Contains information about the activities related to the Secure Agent, including details of all the services enabled for the agent.
<Secure Agent installation directory>\apps\Data_Integration_Server\logs\tomcat\tomcat<version>.log	Contains details related to the Tomcat process for the Data Integration Server. It records the task execution details, including the start time, end time, and statistics for the tasks. Also includes design time and metadata-related activities for the Data Integration assets.
<Secure Agent installation directory>\apps\Data_Integration_Server\<version>\tomcat.out	Contains basic information about the Tomcat process for the Data Integration Server, including when the Tomcat process started and stopped. Also includes Secure Agent connection details, such as certificate and SSL-related information.
<Secure Agent installation directory>\apps\Data_Integration_Server\<version>\scripts.log	Contains information about the Data Integration Server, including details about how the script used by the Data Integration Server was run. Use this log if there is an issue with the Data Integration Server.

2. For Secure Agents that run on Windows, view the application logs in the Windows Event Viewer.

I started the Secure Agent, but the status is inactive.

The Secure Agent might take a few minutes to start. The status refreshes every 5 seconds. If the Secure Agent does not become active, complete the following tasks:

- If your organization uses a proxy server to access the internet, verify that the proxy settings are set correctly.
- View the details in infaagent.log in the directory where you installed the Secure Agent.

I installed the Secure Agent, but I want to install another on a different machine. How do I do that?

On the new machine, use your login to connect to Informatica Intelligent Cloud Services. Then, download and install the Secure Agent.

One of my services shows an error status after I restarted the service successfully.

If a service fails with an error status, the error status for the service might continue to display in the Agent Service Details after the service starts up successfully. The error stays on the page until an internal job that cleans up obsolete messages runs. You can ignore the error.

I am trying to uninstall the Secure Agent, but the Secure Agent status still shows "Up and Running."

When you uninstall the Secure Agent without first stopping the Secure Agent, the Agent Core and other services might continue to run for several minutes. To avoid this issue, stop the Secure Agent before you uninstall it.

Why does my Secure Agent always display "Agent Core Upgrading" in Administrator?

On the **Runtime Environments** page in Administrator, the status of an agent always displays "Agent Core Upgrading". You see the following message in the `agentcore.log` file:

```
2022-10-11 17:02:57,560 GMT tid="21" tn="Agent Core State Machine Thread" ERROR
[com.informatica.saas.infaagent.agentcore.AgentCoreStateMachine] - Authentication failed
due to IO error: [cannot decrypt null or empty string].
```

This issue occurs when the agent missed one or more previous major upgrades. For example, you stopped an agent that was on version 62.x and the current version is 65.x when you restart it. The automatic upgrade only supports upgrading from the previous major version, 64.x. Since your version is older than version 64.x, the automatic upgrade fails.

To resolve the issue, either reregister or reinstall the Secure Agent.

You can see the agent version in the Details tab of a Secure Agent:

Details	Audit Log

Agent Name: *	asCDIEHQILABS01
Platform:	Linux64
Host Name:	asCDIEHQILABS01
Status:	✅ Up and Running
Last Status Change:	Mar 1, 2023 10:14:27 AM
Created On:	Feb 6, 2023 10:23:46 AM
Updated On:	Mar 1, 2023 1:24:07 PM
Created By:	admin
Updated By:	agent
Version:	65.04
Upgrade Status:	Up-to-date
Last Upgraded:	Feb 15, 2023 7:29:53 AM

CHAPTER 5

Secure Agent installation in a cloud environment

You have several ways install a Secure Agent and installing to a cloud environment is a common scenario. The Runtime Environments page provides an installation wizard to streamline the installation for AWS or Microsoft Azure.

You can install a Secure Agent in the following ways:

In an AWS or Microsoft Azure cloud environment

In AWS, you are redirected to the AWS Marketplace to continue the installation.

In Azure, you first log in using your Azure credentials and then you enter essential configuration details for the Secure Agent.

When installing in these environments, you do not need to download the Secure Agent installer separately.

In different cloud environment

If you are not using AWS or Azure, you first set up a VM in your cloud environment and then follow the steps described in Chapter 6, "Secure Agent installation in a local environment" on page 44.

In a local environment

To install on a local machine running Windows or Linux, you first ensure that your system meets the prerequisites, then you download the Secure Agent installer. For more information, see Chapter 6, "Secure Agent installation in a local environment" on page 44.

Installing in AWS

The Secure Agent installer can help you create a runtime environment on Amazon Web Services (AWS). The runtime environment you create is a Secure Agent group that contains one Secure Agent.

When you create a runtime environment on AWS, you create a new stack where the Secure Agent is deployed. You can create the stack in a new or existing virtual private cloud (VPC). The installer creates an Amazon Elastic Compute Cloud (EC2) instance within the VPC.

To create a runtime environment, you must have a subscription with AWS that includes create, modify, and delete privileges for the following resource types:

- AWS CloudFormation templates
- EC2 instances

- Elastic IP addresses
- Elastic network interfaces
- Internet gateways
- Route tables
- Security groups
- Subnets
- VPCs

You must also have read and launch permissions for machine images and AWS CloudFormation templates.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Manage Cloud Secure Agents**.
3. Click **New Cloud Secure Agent**.
4. Select **Amazon Web Services**.
5. Click **Next**.
6. On the **Environment Configuration** page, copy the install token.

   The install token is valid for 24 hours and can't be reused.
7. Choose whether to create the runtime environment on an existing or new VPC.
8. Click **Continue Configuration in AWS**.

   The AWS **Sign in** screen opens in a new browser tab.
9. Sign in to your AWS account.

   The **Quick create stack** page opens.
10. In the **Stack name** area, enter a stack name.
11. In the **Parameters** area, under **Network Configuration**, configure the following properties based on whether you're using an existing VPC or a new VPC.
    - For an existing VPC, configure the following properties:

Property	Value
VPC ID	Select the ID for the VPC where you want to deploy the Secure Agent.
Subnet ID	Enter or select a subnet within the VPC.
Allowed Remote Access CIDR	Enter the CIDR block that specifies the IP addresses where the Secure Agent can be installed. CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses. It configures a network rule to allow remote access to the Secure Agent. The "/x" portion of the address determines how many IP addresses are available in the subnet, for example: 108.124.81.10/32

• For a new VPC, configure the following properties:

Property	Value
Availability Zones	Select the availability zone for your region.
VPC CIDR	Enter the CIDR block that specifies the IP addresses where you want to create the VPC.
Subnet CIDR	Enter the CIDR block that specifies the IP addresses for the subnet in the availability zone that you selected.
Allowed Remote Access CIDR	Enter the CIDR block that specifies the IP addresses where the Secure Agent can be installed.

12. Under **Amazon EC2 Configuration**, configure the following properties:

Property	Value
Key Pair Name	Enter the name of an existing EC2 key pair to enable external access to the EC2 instance. Corresponding key pair files are required for SSH access to the server.
Instance Type	Select the instance type for the EC2 instance or accept the default. Default is m5.xlarge.
Enable Elastic IP Addressing	Choose whether to assign elastic IP addresses to the EC2 instance or accept the default. Default is no.

13. Under **Informatica Intelligent Data Management Cloud (IDMC) Account Details**, configure the following properties:

Property	Value
IDMC POD Master URL	Accept the default value for the IDMC POD Master URL. This is the URL that you use to access Informatica Intelligent Cloud Services. **Warning:** Changing this URL can result in stack deployment failure.
IDMC User Name	Enter your Informatica Intelligent Cloud Services user name.
IDMC User Token	Paste the install token that you copied. If you forgot to copy the install token, you can switch back to Informatica Intelligent Cloud Services and generate a new one.
Secure Agent Group Name	Accept the default value for the Secure Agent group name. This is the name of the runtime environment that you're creating.

14. Click **Create stack**.

It takes a few minutes to create the stack. Be sure to monitor the stack creation and address any issues that might occur. For more information about troubleshooting CloudFormation stacks, see the AWS documentation.

When the stack is created successfully, the EC2 Instance status changes from CREATE_IN_PROGRESS to CREATE_COMPLETE.

15. In Informatica Intelligent Cloud Services, on the **Environment Configuration** page, click **Finish**.

    IICS creates your runtime environment and displays it on the **Runtime Environments** page.

    Tip: To see the progress of your pending Secure Agents, click **Manage Cloud Secure Agents** on the **Runtime Environments** page. The status appears at the top of the page.

It takes a few minutes for the Secure Agent services to start. When the Secure Agent is ready to use, the status changes from "Pending Environment Set Up" to "Up and Running." You might need to refresh the page to see the updated status.

Installing in Azure

The Secure Agent installer can configure a runtime environment on Microsoft Azure. Note that running data integration tasks on Azure incurs costs based on the workload and the VM size.

Note: You need a Microsoft Azure subscription with permissions that allow you to deploy resources. If admin consent is enabled at your organization, reach out to the Azure administrator for app consent approvals. For more information about admin consent requests, see the Microsoft documentation.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Manage Cloud Secure Agents**.
3. Click **New Cloud Secure Agent**.
4. Select **Microsoft Azure**.
5. Click **Next**.
6. Select the Microsoft account to use.
7. Enter the following properties:

Property	Description
Subscription	Select your Microsoft Azure subscription. The subscription must include permissions to deploy the following resources: - Network security group - Virtual network (including subnet) - Network interface - Public IP address - OS disk - Virtual machine Be sure to grant permission to the Hyperscalar Azure Integration App when prompted. **Note:** If you do not have an Azure subscription, exit the installer and sign up for one with Microsoft. You cannot sign up from within Informatica Intelligent Cloud Services.
Resource Group	A resource group is a container that holds related resources for your runtime environment. Informatica Intelligent Cloud Services uses one resource group for each Secure Agent to simplify management of the VM resources for that agent. You typically create new resource groups, but you can use any existing group that is empty. **Tip:** Use the same or similar name as the Secure Agent to more easily identify which resource group belongs with each agent.

Property	Description
Resource Group Name	Name of the resource group. Enter the name of a new group or select an existing group.
	Ensure that any existing resource group is empty, otherwise this message appears: *"API Input validation failed."*
Location	Select the region to deploy the Secure Agent. Choose the Azure region that's appropriate for your organization and your customers. Not every resource is available in every region.
VM Name	Enter a name for the virtual machine (VM) that will be created.
VM User Name	Enter your name as the virtual machine user.
VM Password	Enter a password to access the virtual machine.
Secure Agent Name	Enter a name for your Secure Agent. By default, the runtime environment has the same name as the agent.
	Tip: Use the same or similar name as the resource group, to more easily identify which resource group belongs with each agent.
VM Size	Select a size for your virtual machine. If you are unfamiliar with Azure image sizing, start with a size with at least 4 cores and 16 GB of memory.
	Note that your Azure hourly charges are affected by the VM size.
Virtual Network	Select an existing virtual network based on your Microsoft Azure subscription and location or create a new virtual network.
Virtual Network Name	Select an existing virtual network or enter the name for a new virtual network.
	When you select an existing virtual network, this associates the newly created VM with the existing VNet.
Virtual Network Address	Select an existing virtual network address or enter a new address.
Subnet Name	Select the subnet to use or enter a name for a new subnet.
	The subnet holds all the Azure resources that are deployed to the virtual network.
Subnet Address	Select the subnet address that includes all the resources or enter a new subnet address.
	Subnet addressing allows a system made up of multiple networks to share the same Internet address.
CIDR IP Address Range	Enter the CIDR IP address range.
	CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses. It configures a network rule to allow remote access to the Secure Agent. The "/x" portion of the address determines how many IP addresses are available in the subnet, for example: 108.124.81.10/32

Tip: For more information, refer to "Explore Azure Virtual Networks" in the Microsoft documentation.

8. Click **Create**. Administrator creates your runtime environment and displays it on the **Runtime Environments** page.

   Tip: To see the progress of your pending Secure Agents, click **Manage Cloud Secure Agents** on the **Runtime Environments** page. The status appears at the top of the page.

CHAPTER 6

Secure Agent installation in a local environment

Install a Secure Agent in a local environment when you can't use the Hosted Agent or you're not installing an agent on AWS or Microsoft Azure.

You can install a Secure Agent in a local environment in the following ways:

On a local machine or VM running Windows

On Windows, the Secure Agent runs as a Windows service. Ensure that your Windows environment meets the Secure Agent requirements before downloading the Secure Agent installer.

On a local machine or VM running Linux

On Linux, the Secure Agent runs as a process. Ensure that your Linux environment meets the Secure Agent requirements before downloading the Secure Agent installer.

Secure Agent installation on Windows

On Windows, the Secure Agent runs as a Windows service. When you install the Secure Agent, you also install the Informatica Cloud Secure Agent Manager.

By default, the Secure Agent starts when you start Windows. You can stop and restart the Secure Agent using the Secure Agent Manager or Windows Services. If you install the Secure Agent on a different volume than you use to run the installation program, you must start and stop the Secure Agent from Windows Services.

You can also use the Secure Agent Manager to check the Secure Agent status and configure proxy information. The Secure Agent works with BASIC, DIGEST, and NTLMv2 proxy authentication.

You can launch the Secure Agent Manager from the Start menu or desktop icon. When you close the Secure Agent Manager, it minimizes to the Windows taskbar notification area for quick access.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.
2. Download the Secure Agent installer files.
3. Install and register the Secure Agent.

Secure Agent requirements on Windows

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services.

Verify the following requirements before you install the Secure Agent on Windows:

- The Secure Agent machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the
  Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on the Knowledge Base.
- The Secure Agent machine has the Microsoft Visual C++ 2015 Redistributable.
- The Secure Agent machine has at least 4 CPU cores, 16 GB RAM, and at least 5 GB of free disk space.
- The Secure Agent machine is on a volume with at least 250GB disk space, with at least 5 GB free space or three times the size of the Secure Agent installation, whichever is greater.
- The account you use to install the Secure Agent has access to all remote directories that contain flat source or target files.
- No other Secure Agent is installed on the machine. If another Secure Agent is installed on the machine, uninstall it first.

For more information about Secure Agent requirements, see this article:
https://knowledge.informatica.com/s/article/526096

Configure the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. To ensure that the Secure Agent can perform all necessary tasks through the firewall, enable the port that the Secure Agent uses.

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

Secure Agent permissions on Windows

A Secure Agent requires certain permissions to transfer data between sources and targets.

When you install a Secure Agent on Windows, the Secure Agent must be part of the local Administrators group.

Configure Windows settings

Before you use the Secure Agent on Windows, configure proxy settings and a Windows Secure Agent service login.

You can configure proxy settings in Secure Agent Manager. Configure a login for the Windows Secure Agent service on Windows.

Note: If you use the Secure Agent for Informatica Cloud Data Wizard, you do not need to configure proxy settings or a Windows service login for the Secure Agent.

Downloading and installing the Secure Agent on Windows

To install the Secure Agent on a Windows machine, you must download and run the Secure Agent installation program and then register the agent.
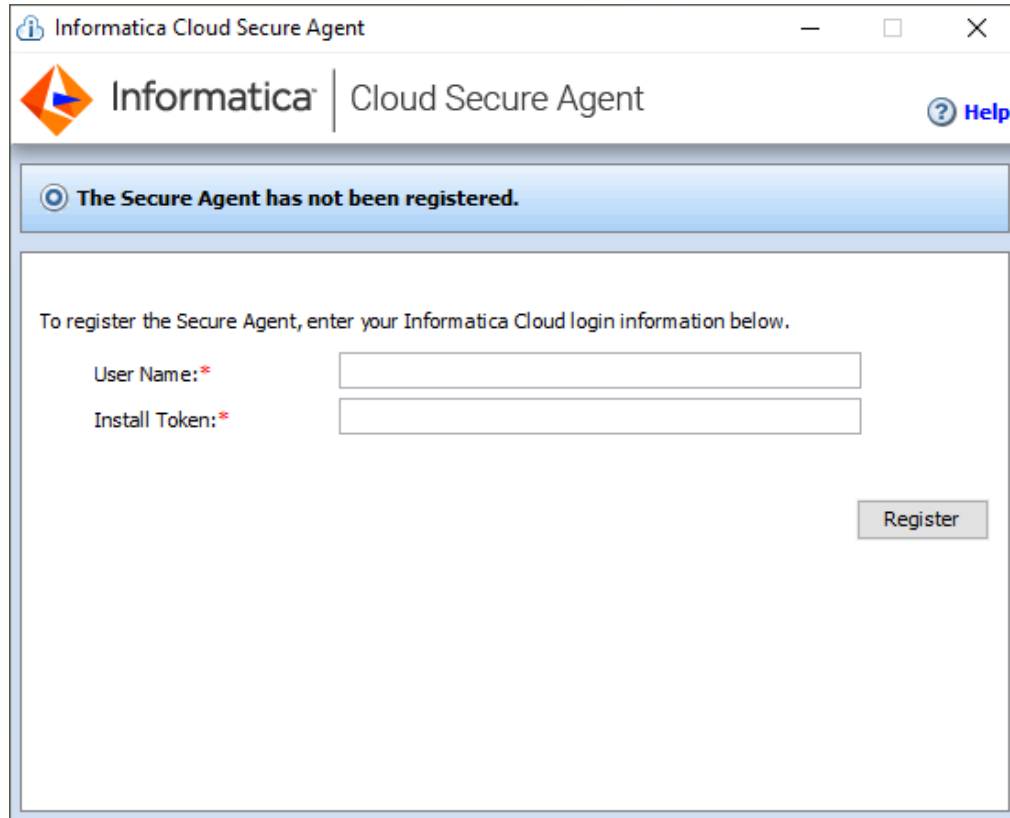
Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine. If any other Secure Agent exists, you must uninstall it.

Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.

2. On the **Runtime Environments** page, click **Download Secure Agent**.

3. Select the Windows 64-bit operating system platform, copy the install token, and then click **Download**.

   The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.exe`.

4. Run the installation program as an Administrator:

   a. Specify the Secure Agent installation directory, and click **Next**.

   b. Click **Install** to install the agent.

The **Cloud Secure Agent** dialog box opens and prompts you to register the agent as shown in the following image:

5. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.

6. In the Secure Agent Manager, enter the following information, and then click **Register**:

Option	Description
User Name	User name that you use to access Informatica Intelligent Cloud Services.
Install Token	Token that you copied.

The Secure Agent Manager displays the status of the Secure Agent. It takes a minute for all of the services to start.

7. If your organization uses an outgoing proxy server to connect to the internet, enter the proxy server information.

8. Close the Secure Agent Manager.

The Secure Agent Manager minimizes to the taskbar and continues to run as a service until stopped.

Configure the proxy settings on Windows

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server. The Secure Agent installer configures the

proxy server settings for the Secure Agent based on settings configured in the browser. You can change the proxy server settings through the Secure Agent Manager.

Contact your network administrator for the correct proxy settings.

1. In the Secure Agent Manager, click **Proxy**.

2. To enter proxy server settings, click **Use a Proxy Server**.

3. Enter the following information:

Field	Description
Proxy Host	Required. Host name of the outgoing proxy server that the Secure Agent uses.
Proxy Port	Required. Port number of the outgoing proxy server.
User Name	User name to connect to the outgoing proxy server.
Password	Password to connect to the outgoing proxy server.

4. Click **OK**.

The Secure Agent Manager restarts the Secure Agent to apply the settings.

Configure a login for a Windows Secure Agent Service

On Windows, configure a network login for the Secure Agent service. The Secure Agent can access the network with the privileges and permissions associated with the login.

Configure a login for the Secure Agent machine to allow the Secure Agent to access directories to configure and run tasks. When you configure connections, configure tasks, and run tasks that use flat file or FTP/SFTP connection types, the Secure Agent might require read and write permissions on the related directories.

For example, to browse to a directory to configure a flat file or FTP/SFTP connection, the Secure Agent login might require permission to access the directory. Without a Secure Agent login with the appropriate permissions, Informatica Intelligent Cloud Services cannot display the directory in the **Browse for Directory** dialog box.

1. Go to the **Services** window from the Windows Administrative tools.

2. In the **Services** window, right-click the Informatica Cloud Secure Agent service and choose **Properties**.

3. In the **Properties** dialog box, click the **Log On** tab.

4. To configure a login, select **This Account**.

5. Enter an account and password.

    Use an account with the required privileges and permissions for the network security defined for the domain. By default, the account format is <domain name>\<user name>.

6. Click **OK**.

7. In the **Services** window, restart the Secure Agent service for the changes to take effect.

Uninstalling the Secure Agent on Windows

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. Click **Start** > **All Programs** > **Informatica Cloud Secure Agent** > **Uninstall Informatica Cloud Secure Agent**.

    The Secure Agent uninstaller launches.

2. Click **Uninstall**.

3. When the uninstall completes, click **Done**.

4. Delete any remaining files in the installation directory.

    After you uninstall the Secure Agent, delete all files and directories associated with the Secure Agent installation.

Note: Uninstalling the Secure Agent does not delete log files from the Secure Agent directory. If you want to reinstall a Secure Agent on the machine, you must delete all files and directories associated with the Secure Agent installation or reinstallation will fail. If you want to save the log files, copy them to a different directory, and then delete the Secure Agent installation directory.

Secure Agent installation on Linux

On Linux, the Secure Agent runs as a process. You can use a shell command line to install, register, start, stop, and uninstall the Secure Agent.

You can also use the shell command line to check the Secure Agent status.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.

2. Download the Secure Agent installer files.

3. Install and register the Secure Agent.

Consider the following guidelines:

*   Create a specific user profile to install the Secure Agent with full access to all folders from the Secure Agent installation directory. Don't install the Secure Agent as the root user.

*   You can't install more than one Secure Agent on the same machine under the same user account. Multiple agents may exist under different user accounts.

*   Don't install the Secure Agent on any node within the Informatica domain.

For more information about Secure Agent requirements, see this KB article:
IICS Minimum requirements and best practices when installing Informatica Cloud Secure Agent.

Secure Agent requirements on Linux

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services. Before you install the Secure Agent on Linux, verify the system requirements.

Verify the following requirements before you install the Secure Agent on Linux:

- Verify that the machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on the Knowledge Base.

- Verify that the machine has at least 11 GB free disk space.

- Verify that the `libidn.x86_64` package is installed.
  If the package isn't present, install it using the following command: `sudo yum install libidn.x86_64`

  Note: The command to install the package might vary based on your Linux distribution.

- Verify that the `libidn.so.*` libraries are installed.
  If the libraries aren't present, install them using the following commands:

  - For 64-bit systems: `cd /usr/lib/x86_64-linux-gnu`

  - For 32-bit systems: `cd /usr/lib/i386-linux-gnu`

  After installing the libraries, create a symbolic link using the following command:

  ```
  sudo ln -s libidn.so.12 libidn.so.11
  ```

- The account that you use to install the Secure Agent must have access to all remote directories that contain flat source or target files.

- If you use PowerCenter, install the Secure Agent using a different user account than the account you used to install PowerCenter.
  Informatica Intelligent Cloud Services and PowerCenter use some common environment variables. If the environment variables are not set correctly for Informatica Intelligent Cloud Services, your jobs might fail at run time.

For more information about Secure Agent requirements, see this article:
https://knowledge.informatica.com/s/article/526096

Configure the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. To ensure that the Secure Agent can perform all necessary tasks through the firewall, enable the port that the Secure Agent uses.

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

Secure Agent permissions on Linux

A Secure Agent requires certain permissions to transfer data between sources and targets.

When you install a Secure Agent on Linux, the Secure Agent must have read/write/execute permissions for the installation directory.

Downloading and installing the Secure Agent on Linux

To install the Secure Agent on a Linux machine, you must download and run the Secure Agent installation program and then register the agent.

Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

When you register the agent, it is added to its own Secure Agent group by default. You can add the agent to a different Secure Agent group.

Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine using the same Linux user account. If there is, you must uninstall it.

Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.

2. On the **Runtime Environments** page, click **Download Secure Agent**.

3. Select the Linux 64-bit operating system platform, copy the install token, and then click **Download**.

    The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.bin`.

4. Save the installation program to a directory on the machine where you want to run the Secure Agent.

    Note: If the file path contains spaces, the installation might fail.

5. From a shell command line, navigate to the directory where you downloaded the installation program and enter the following command:

    `./agent64_install_ng_ext.bin -i console`

6. When the installer completes, navigate to the following directory:

    `<Secure Agent installation directory>/apps/agentcore`

7. To start the Secure Agent, enter the following command:

    `./infaagent startup`

    The Secure Agent Manager starts. You must register the agent using the user name that you use to access Informatica Intelligent Cloud Services. You must also supply the install token.

8. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.

9. To register the agent, in the `<Secure Agent installation directory>/apps/agentcore` directory, enter one of the following commands using your Informatica Intelligent Cloud Services user name and the token that you copied:

    *   To add the agent to its own Secure Agent group, use the following command:

        `./consoleAgentManager.sh configureToken <user name> <install token>`

- To add the agent to an existing Secure Agent group, use the following command:

```
./consoleAgentManager.sh configureTokenWithRuntime <user name> <install token>
<Secure Agent group name>
```

Note: If the command includes a Secure Agent group name that doesn't exist, the Secure Agent is not assigned to a group. Be sure to use a valid Secure Agent group name.

The following table lists the command options:

Option	Description
User Name	Required. Informatica Intelligent Cloud Services user name of the user installing the Secure Agent.
Install Token	Required. The install token that you copied.
Secure Agent group name	Optional. Include when you want to add the agent to an existing Secure Agent group instead. If this option isn't included in the command, the agent will be in its own Secure Agent group.

You can check the registration status of a Secure Agent using the following command:

```
./consoleAgentManager.sh isConfigured
```

Configure the proxy settings on Linux

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

The Secure Agent installer configures the proxy server settings for the Secure Agent based on settings configured in the browser. You can update the proxy server settings defined for the Secure Agent from the command line. The Secure Agent works with BASIC, DIGEST, and NTLMv2 proxy authentication.

To configure the proxy server settings for the Secure Agent on a Linux machine, use a shell command that updates the `proxy.ini` file. Contact the network administrator to determine the proxy settings.

1. Navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

2. To update the `proxy.ini` file, enter the following command:

```
./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name>
<proxy password>
```

3. Restart the Secure Agent.

Uninstalling the Secure Agent on Linux

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. From the command line, navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

2.   Stop the Secure Agent Linux process by entering the following command:

```
./infaagent shutdown
```

3.   To uninstall the Secure Agent, run rm -rf on the directory where you installed the Secure Agent to remove Secure Agent files.

Troubleshooting a Secure Agent installation

The Secure Agent download failed.

If you receive a download failure after clicking **Download Secure Agent**, add the following domain to your allowlist: `https://global-package.dm.informaticacloud.com` and then try the download again.

For more information, see this KB article:
[Change in Package Dependency Manager IP Addresses and Domain for IDMC](#)

CHAPTER 7

Serverless runtime environment setup in AWS

A serverless runtime environment is an advanced serverless deployment solution that doesn't require downloading, installing, configuring, or maintaining a Secure Agent or Secure Agent group. You can use a serverless runtime environment in the same way that you use a runtime environment when you configure a connection or tasks in Data Integration.

Note: For information on creating a serverless runtime environment in Azure Native ISV Services, see Configure serverless runtime environment on Azure Native ISV. You can't create a serverless runtime environment in Google Cloud.

Before you can create a serverless runtime environment, you must create or connect an existing VPC to your AWS account. You can either do this manually or by using the AWS CloudFormation template provided by Informatica.

Note: Your cloud environment must be on the AWS cloud platform and your VPC must have default tenancy. A serverless runtime environment can't connect to a VPC with dedicated instance tenancy.

You can set up your cloud environment using one of the following methods:

- Manually create and configure AWS resources in your VPC to connect to the serverless runtime environment in Informatica's VPC. For more information about this method, see "Create and configure your environment manually" on page 55.

- Use a template provided by Informatica to create a VPC in your AWS account. If you have an existing VPC, you can connect that to a serverless runtime environment. For more information, see "Create a VPC using a template" on page 57.

Create and configure your environment manually

Create and configure AWS resources in your VPC to connect to the serverless runtime environment in Informatica's VPC.

The following image shows the resources in a sample environment:
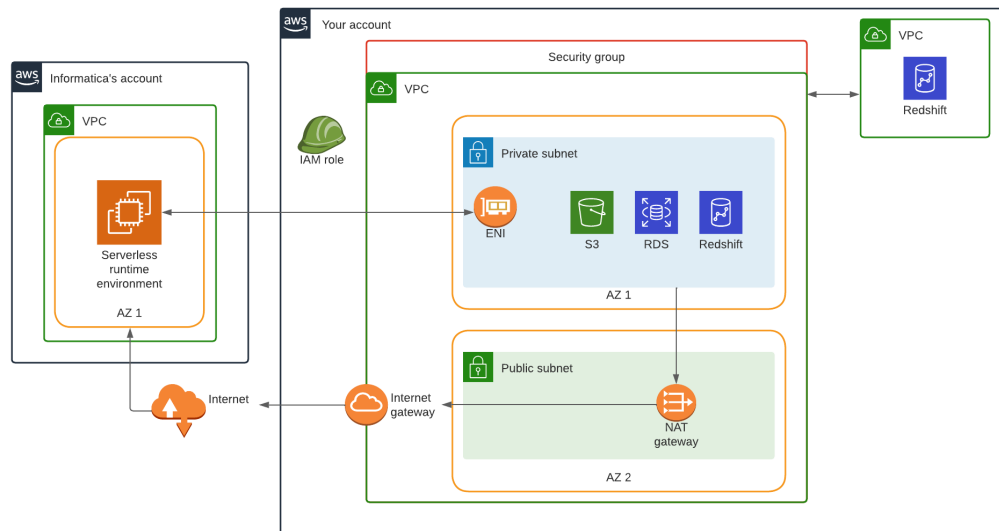
Use the following guidelines to create and configure each resource:

VPC

A VPC contains the data to process in the serverless runtime environment.

Create a VPC in your AWS account. Enable DNS hostnames and DNS resolution for the VPC.

Also, ensure that at least one of the following scenarios apply to you:

- Your VPC's DHCP option is set with AmazonProvidedDNS.
- If you have custom DNS servers in your DHCP option set, ensure that AmazonProvidedDNs is part of the option set or that the DNS servers can resolve EC2 internal hostnames. To ensure that the DNS servers can resolve EC2 internal hostnames, internally redirect the DNS query to AmazonProvidedDNS.

Security group

A security group controls the traffic flow from the serverless runtime environment.

Create a security group in the VPC. The security group is associated with all ENIs that the serverless runtime environment creates. You specify this security group in the serverless runtime environment properties.

Leave the inbound rules empty to restrict all incoming traffic. The outbound rules can either allow all traffic or limit traffic to all Amazon S3 resources and all source and target systems that the serverless runtime environment accesses.

Private subnet to host the ENI

A private subnet hosts the ENI that the serverless runtime environment uses to connect to your VPC.

Create a private subnet and configure a CIDR range to determine the maximum number of IP addresses and therefore, the scalability, of the serverless runtime environment. Configure the CIDR range to have at least 25 IP addresses per serverless runtime environment so that the serverless runtime environment can scale effectively when developers run concurrent workloads.

After your organization administrator creates a serverless runtime environment in Administrator, the serverless runtime environment creates a ENI in your private subnet.

Public subnet for internet access

A public subnet provides internet access through a NAT gateway.

Create a public subnet using any availability zone in the region where you created the VPC. The CIDR range must be within the VPC CIDR range. Choose a range based on the number of IP addresses that you want to have within the subnet.

VPC to VPC connectivity

VPC to VPC connectivity is used to access data in a different VPC than the VPC that connects to the serverless runtime environment. For example, a mapping might read data from an Amazon Redshift cluster in a VPC and write data to a different Amazon Redshift cluster in another VPC.

If you process data across VPCs, configure VPC to VPC connectivity. AWS provides several ways to configure VPC to VPC connectivity, such as VPC peering or AWS Transit Gateway. Use AWS PrivateLink wherever it's applicable. For more information, refer to the AWS documentation.

NAT gateway for internet access from the private subnet

A NAT gateway allows outbound traffic to the internet from private instances. All compute instances in the serverless runtime environment that are associated with the ENI are private.

Create a NAT gateway to route outbound traffic from the private subnet to the internet. AWS provides several ways to configure subnet routing rules, such as route tables and NACL. For more information, refer to the AWS documentation.

IAM role

An IAM role defines a minimal policy that the serverless runtime environment and advanced cluster worker nodes use to create, attach, detach, and delete the ENI that's associated with the private subnet in your VPC.

The IAM role must be able to access the S3 location for supplementary files as well as the sources and targets you use in mappings. You can use the following template:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachNetworkInterface",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:AttachNetworkInterface",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets",
```

```
                    "ec2:DescribeNetworkAcls"
                ],
                "Resource": "*"
            },
            {
                "Sid": "VisualEditor1",
                "Effect": "Allow",
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl"
                ],
                "Resource": "arn:aws:s3:::<S3 bucket name>"
            },
            {
                "Sid": "VisualEditor2",
                "Effect": "Allow",
                "Action": [
                    "s3:PutObject",
                    "s3:GetObject",
                    "s3:DeleteObject"
                ],
                "Resource": [
                    "arn:aws:s3:::<Supplementary file location>/*"
                ]
            }
        ]
    }
```

In the trust relationship, specify the Informatica account number as a trusted entity and create an external ID. To find the Informatica account number, create a serverless runtime environment in Administrator and check the environment properties. You can use the following template:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<Informatica account>:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "<External ID>"
        }
      }
    }
  ]
}
```

Create a VPC using a template

Use an AWS CloudFormation template provided by Informatica to create a VPC in your AWS account. If you have an existing VPC, you can connect that to a serverless runtime environment.

1. Ask your organization administrator for an email containing the AWS CloudFormation template for Informatica Intelligent Cloud Services.

    Organization administrators can generate the email by requesting a serverless configuration file in Administrator. For more information, see "Requesting a serverless configuration file" on page 82.

2. Use the AWS CloudFormation template to create a stack in AWS CloudFormation.

For more information, see or .

3. Navigate to the S3 location for the JSON file that you specified in the template.

4. Download the JSON file from the S3 location to the `iics-sre-config` folder.

5. Share the JSON file with your organization administrator.

   The organization administrator will import the file into Informatica Intelligent Cloud Services to let Informatica know that your VPC is ready to connect to the serverless runtime environment in Informatica's VPC.

6. Optionally, create the supplementary file location.

   The supplementary file location stores supplementary files, such as JAR files and external libraries that developers can use to access and process data. For more information, see .

Creating a new VPC using the AWS CloudFormation template

When you use the AWS CloudFormation template to create a new VPC, the stack creates a VPC and all required resources and configurations to connect to the serverless runtime environment in Informatica's VPC, including subnets and an IAM role with minimal policies.

To create the stack in AWS CloudFormation, specify the stack name and configure stack parameters.

The following table describes the stack parameters:

| Parameter	Description
VPC CIDR	CIDR block that specifies where to create the VPC.
Public Subnet CIDR	CIDR block that specifies where to create the public subnet. The IP range of the public subnet must be within the IP range of the VPC.
Availability Zone for Public Subnet	Availability zone where you want to create the public subnet. You can select any availability zone in the current region.
Private Subnet CIDR	CIDR block that specifies where to create the private subnet. The IP range of the private subnet must be within the IP range of the VPC.
Availability Zone for Private Subnet	Availability zone where you want to create the private subnet. You can select any availability zone in the current region.
VPC Deployment Type	Select the NAT Gateway.
Informatica Cloud Region	Region where the Informatica POD resides. You can identify the region through the URL that appears when you open any service in Informatica Intelligent Cloud Services. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, the POD resides in the US region.
External ID	External ID to associate with the IAM role.
AWS Tags	AWS tags to label the ENI.

Parameter	Description
Supplementary File Location	Location on Amazon S3 to store supplementary files, such as JAR files and external libraries that developers can use to access and process data.
S3 Location for JSON File	Location on Amazon S3 to generate the serverless configuration file.

Note: The stack is not created if the parameters are not valid.

AWS resources created by the stack

When you use the AWS CloudFormation template to create a VPC, the stack creates various AWS resources for you.

The following image shows the resources that the stack creates in your AWS account:
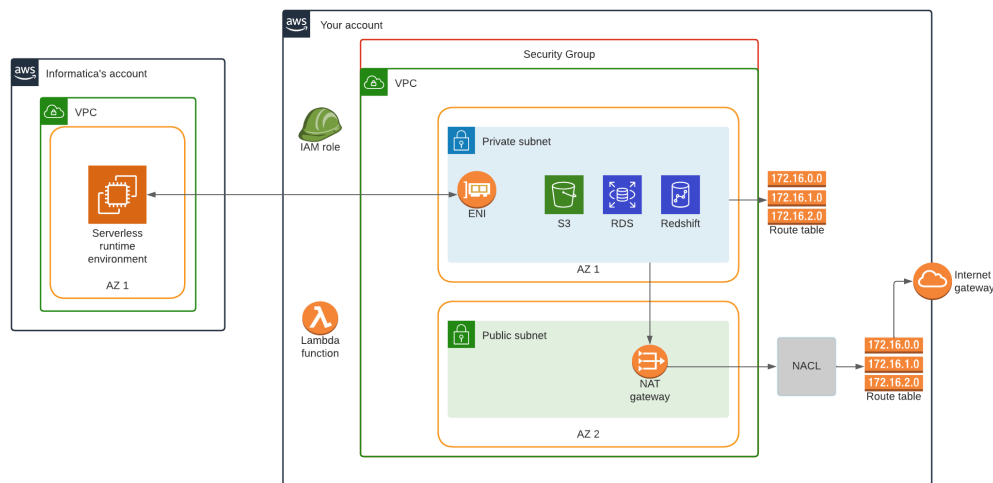
The following table summarizes the AWS resources and resource counts that the stack creates:

AWS resource	Number of resources created
VPC	1
Security group	1
Subnets	2 1 public subnet and 1 private subnet
NAT gateway	1
Elastic IP address	1 elastic IP address attached to the NAT gateway
NACL	1
Route tables	2 1 public route table and 1 private route table

AWS resource	Number of resources created
Internet gateway	1
IAM role	1

Configurations performed by the stack

When you use the AWS CloudFormation template to create a VPC, the stack performs various configurations.

The stack performs the following configurations:

- Associates the security group with the VPC and defines inbound and outbound rules.
- Adds routes to the private route table and makes the private route table the default route table for the VPC.
- Associates the NAT gateway with the public subnet for outbound traffic to the internet and assigns an elastic IP to the gateway.
- Updates the NACL inbound rules that are associated with the public subnet.
- Attaches the internet gateway to the VPC.
- Assigns the following policy to the IAM role:

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"VisualEditor0",
            "Effect":"Allow",
            "Action":[
                "ec2:DetachNetworkInterface",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:AttachNetworkInterface",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkAcls"
            ],
            "Resource":"*"
        },
        {
            "Sid":"VisualEditor1",
            "Effect":"Allow",
            "Action":[
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetBucketAcl"
            ],
            "Resource":[
                "arn:aws:s3:::<S3 location for supplementary files>",
                "arn:aws:s3:::<S3 location for supplementary files>/*"
            ]
        }
```

```
            ]
        }
```

- Creates the following trust relationship in the IAM role:

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::<Informatica's account number>:root"
            },
            "Action":"sts:AssumeRole",
            "Condition":{
                "StringEquals":{
                    "sts:ExternalId":"<external ID>"
                }
            }
        }
    ]
}
```

Connecting to an existing VPC using the AWS CloudFormation template

You specify a template in AWS CloudFormation, and then AWS CloudFormation creates a stack based on this template.

When you log in to AWS CloudFormation, you can create a new stack. When you create the stack, you specify a template to use. This template populates the stack parameters that you need to fill in. Once the parameters are complete, AWS CloudFormation creates the stack based on the parameter values.

The following table describes the stack parameters:

Parameter	Description
VPC ID	ID of the VPC. For example, vpc-2f09a348. The stack assumes that the VPC is in the same AWS region where the stack is created.
Subnet ID	ID of the subnet within the VPC. For example, subnet-b46032ec.
Security Group ID	Optional. ID of the security group. For example, sg-e1fb8c9a.
Should Security Group be created if it does not exist?	Indicates whether the stack will create a security group if a security group doesn't exist. Select **Yes** or **No**.
Informatica Cloud Region	Region where the Informatica POD resides. You can identify the region through the URL that appears when you open any service in Informatica Intelligent Cloud Services. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, the POD resides in the US region.
AWS Tags	AWS tags to label the ENI.
Supplementary File Location	Location on Amazon S3 to store supplementary files, such as JAR files and external libraries for certain transformations and connectors.
S3 Location for JSON File	Location on Amazon S3 to generate the serverless configuration file.

Note: If the parameters are not valid, the stack fails to be created.

Configurations that the stack performs

The stack performs the following configurations:

- Detects the region based on the VPC ID and checks if a serverless runtime environment can connect to the region.
- Checks if the subnet exists.
- Fetches the availability zone ID from the subnet ID.
- Checks the inbound and outbound rules in the security group. If a security group is not provided or does not exist, the stack creates a security group.
- Creates an IAM role and assigns the following policy to the role:

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"VisualEditor0",
            "Effect":"Allow",
            "Action":[
                "ec2:DetachNetworkInterface",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:AttachNetworkInterface",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkAcls"
            ],
            "Resource":"*"
        },
        {
            "Sid":"VisualEditor1",
            "Effect":"Allow",
            "Action":[
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetBucketAcl"
            ],
            "Resource":[
                "arn:aws:s3:::<S3 location for supplementary files>",
                "arn:aws:s3:::<S3 location for supplementary files>/*"
            ]
        }
    ]
}
```

- Creates the following trust relationship in the IAM role:

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::<Informatica's account number>:root"
            },
            "Action":"sts:AssumeRole",
            "Condition":{
```

```
                        "StringEquals":{
                          "sts:ExternalId":"<external ID>"
                        }
                      }
                    }
                  ]
               }
```

Troubleshooting the stack

How do I troubleshoot errors during stack creation in AWS CloudFormation?

Perform the following tasks:

1. In AWS CloudFormation, go to the **Home** page.
2. Select the stack that you created.
3. On the **Events** tab, review the messages in the **Status reason** column.
4. On the **Parameters** tab, review the messages in the **Status reason** column.

How do I view the AWS resources that the stack created?

Perform the following tasks:

1. In AWS CloudFormation, go to the **Home** page.
2. Select the stack that you created.
3. Navigate to the **InfaVPCStack** nested stack.
4. On the **Resources** tab, view the resources that the stack created.

How do I delete the AWS resources that the stack created?

Perform the following tasks:

1. In AWS CloudFormation, go to the **Home** page.
2. Select the stack that you created.
3. Click **Delete**.

I tried deleting the stack that created the VPC but deletion is taking too long.

You can force deletion by deleting the VPC. Perform the following tasks:

1. In AWS CloudFormation, go to the **Home** page.
2. Select the stack that you created.
3. Navigate to the **InfaVPCStack** nested stack.
4. On the **Resources** tab, click the VPC link in the **Physical ID** column.

   You're redirected to the VPC home page.
5. Select the VPC to delete.
6. Click **Actions > Delete VPC**.

   If there is a warning message stating that other AWS resources need to be deleted first, manually delete
   the specified resources before deleting the VPC.
7. Return to the stack in AWS CloudFormation and try to delete the stack again.

The serverless runtime environment in Administrator doesn't start or takes too long to start.

The parameters might not be set correctly. Verify the parameters that you input to the stack during creation. Perform the following tasks:

1. In AWS CloudFormation, go to the **Home** page.
2. Select the stack that you created.
3. On the **Parameters** tab, click **Events**.
4. Review the **Status reason** column.

Common tasks for VPC configuration

When you set up your cloud environment, you can add safe IP addresses for IP filtering, set up a system disk, set up a location for JAR files and external libraries, and configure TLS to authenticate REST APIs. These apply whether you set up your VPC manually or through a template.

Perform the following tasks as necessary:

- Add trusted IP addresses. If your organization filters based on IP addresses, add the safe Informatica addresses so that they won't get blocked by the firewall. For more information, see "Adding trusted Informatica IP addresses" on page 64.
- Configure a system disk. A system disk can help improve mapping performance. For guidelines on setting up a system disk, see "Configuring a system disk" on page 66. For directions on setting up the system disk, see "System Disk" on page 81.
- Create a supplementary file location. If your mappings use JAR files and external libraries, set up a location on Amazon S3 to store the files. For more information, see "Creating the supplementary file location" on page 69.
- Configure TLS to authenticate REST APIs. If you use a REST V3 Connector, you can configure TLS to authenticate REST APIs. For more information, see "Configuring TLS to authenticate REST APIs" on page 69.

Adding trusted Informatica IP addresses

If your organization uses trusted IP address ranges, edit the ranges in your organization properties and add the appropriate trusted IP addresses.

US

The following table lists trusted IP addresses for US regions:

Region	Trusted IP addresses
US East (N. Virginia) us-east-1	- 54.160.9.90 - 54.221.247.69
US East (Ohio) us-east-2	- 18.220.76.98 - 3.131.176.232

Region	Trusted IP addresses
US West (N. California) us-west-1	- 52.52.220.198 - 13.56.74.27
US West (Oregon) us-west-2	- 44.239.8.148 - 44.242.20.143

APJ

The following table lists trusted IP addresses for APJ regions:

Region	Trusted IP addresses
Asia Pacific (Hong Kong) ap-east-1	- 18.167.71.151 - 18.163.244.73
Asia Pacific (Mumbai) ap-south-1	- 65.1.80.5 - 13.234.141.216
Asia Pacific (Osaka) ap-northeast-3	- Not available
Asia Pacific (Seoul) ap-northeast-2	- 52.79.244.47 - 3.34.56.248
Asia Pacific (Singapore) ap-southeast-1	- 52.76.184.230 - 18.140.193.120
Asia Pacific (Sydney) ap-southeast-2	- 3.24.111.61 - 54.253.179.190
Asia Pacific (Tokyo) ap-northeast-1	- 35.72.149.44 - 13.112.143.134

Canada

The following table lists trusted IP addresses for Canada regions:

Region	Trusted IP addresses
Canada (Central) ca-central-1	- 3.96.182.201 - 3.97.103.68

EMEA

The following table lists trusted IP addresses for EMEA regions:

Region	Trusted IP addresses
Europe (Frankfurt) eu-central-1	- 3.125.185.124 - 3.64.66.226
Europe (Ireland) eu-west-1	- 54.76.54.130 - 54.78.183.88
Europe (London) eu-west-2	- 35.176.60.118 - 18.135.50.152
Europe (Milan) eu-south-1	- 35.152.49.63 - 35.152.45.151
Europe (Paris) eu-west-3	- 15.237.157.126 - 15.237.97.211
Europe (Stockholm) eu-north-1	- 13.49.61.89 - 13.53.141.231

UK

The following table lists trusted IP addresses for UK regions:

Region	Trusted IP addresses
Europe (Frankfurt) eu-central-1	- 18.157.124.91
Europe (Ireland) eu-west-1	- 34.250.251.16
Europe (London) eu-west-2	- 18.170.170.192
Europe (Milan) eu-south-1	- 15.161.184.93 - 15.160.41.209
Europe (Paris) eu-west-3	- 13.37.37.71
Europe (Stockholm) eu-north-1	- 13.53.147.238

Configuring a system disk

The serverless runtime environment can use system disks for improved performance.

Configure a system disk to improve mapping performance in Data Integration.

You can configure system disks in Amazon EFS (Elastic File System) and NFS (Network File System) formats. File system connections in EFS are TLS-enabled by default. File system connections in NFS use NFSv4 (Network File System Version 4).

When you use a system disk, the serverless runtime environment creates a folder with the name `<organization ID>/<serverless environment Id>` on the system disk. This folder stores job metadata and logs.

Rules and guidelines for the EFS file system

Use the following guidelines when you configure system disks in the Amazon EFS format:

- Set the file system to the ID of the EFS file system.

- Allow the subnet in the serverless runtime environment to access to the Amazon EFS file system.

- Configure the EFS security group to allow inbound access from the security group configured in the serverless runtime environment.

- Configure the IAM role in the serverless environment with full access to the EFS file system. You can grant full access in the file system policy or in the IAM role. For example, the following file system policy allows root access to ServerlessRole (SREIICS) for file system fs-12345 and allows SecureTransport only:

```
"Version": "2012-10-17",
    "Id": "efs-policy-wizard-<efs policy wizard ID>",
    "Statement": [
        {
            "Sid": "efs-statement-<efs statement ID>",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<arn ID>:role/SREIICS"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientRootAccess"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-west-2: <arn ID>:file-system/
fs-12345",
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
        },
        {
            "Sid": "efs-statement-<efs statement ID>",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": "arn:aws:elasticfilesystem:us-west-2: 123456789:file-system/
fs-12345",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

The following table describes the actions in the sample policy:

Action	Description
elasticfilesystem:ClientMount	Provides read-only access to a file system.
elasticfilesystem:ClientWrite	Provides write permissions on a file system.
elasticfilesystem:ClientRootAccess	Provides use of the root user when accessing a file system.

- Create any folder required by an access point before creating the access point itself. For example, if the access point refers to the folder `/my-company/dev`, then define this folder first before you set up the access point.
- Configure the IAM role to restrict access to specific access points on the file system. For more information, see https://docs.aws.amazon.com/efs/latest/ug/efs-access-points.html

Rules and guidelines for the NFS file system

Use the following guidelines when you configure system disks in the NFS format.

- Set the file system to the DNS of the NFS server.
- Configure the subnet in the serverless runtime environment to allow access to the NFS file server.
- Configure the file server security group to allow inbound access from the security group configured in the serverless runtime environment.

Using EFS or NFS directories as data disks

To use existing EFS or NFS directories as data disks in a serverless runtime environment, perform some setup steps so that the serverless runtime environment has permissions to access these directories. When the setup is complete, the serverless runtime environment can read existing files and write new files to these directories.

1. Mount the EFS or NFS directories in an EC2 instance that you have.
2. Log in to the EC2 instance.
3. Locate a user with ID=501. If one doesn't exist, create a new user with this ID.

   User ID 501 is the user `cldagnt`, which the serverless runtime environment uses to access mounted EFS or NFS directories.
4. Assign read and write permissions to the mounted directories for user 501.

   For more information, see the following topic in the AWS documentation: Working with users, groups, and permissions at the Network File System Level.

Configuring a data disk

Create a data disk in your serverless runtime environment if you have files in EFS or NFS directories that you want to use in the environment, without updating all your mappings.

Once you mount your EFS or NFS locations in a data disk, you have access to the following features:

- Flat file support. You can use flat files from the mounted EFS or NFS locations in your mappings.
- Parameter file support. You can use parameter files stored in the mounted EFS or NFS locations. This simplifies migrating jobs from a Secure Agent group to a serverless runtime environment, since you do not need to modify your mappings.

Tip: If you create data disks, ensure that you've set up the correct user and permissions to use the mounted directories as data disks. For more information, see "Using EFS or NFS directories as data disks" on page 68.

For information on configuring data disks, see "Data Disk" on page 82.

Creating the supplementary file location

If mappings use JAR files and external libraries, dedicate a location on Amazon S3 to store the files and create folders for each file type.

To create the supplementary file location:

1. Create the following file structure on Amazon S3:

```
<Supplementary file location>
├── ext
├── odbc
│   └── lib
└── serverless_agent_config
    ├── jars
    ├── SSL
    ├── j_depends
    └── py_depends
```

2. Create a `serverlessUserAgentConfig.yml` file. For a template, see "Populating the serverlessUserAgentConfig.yml File" on page 71.

3. Add the `serverlessUserAgentConfig.yml` file directly under the `serverless_agent_config` directory.

The following table lists the file types that you can store in each location:

Location	Files
<Supplementary file location>/ext	JDBC JAR files
<Supplementary file location>/odbc	The following files: - odbc.ini - odbcinst.ini - exports.ini
<Supplementary file location>/odbc/lib	ODBC shared libraries for a Linux operating system
<Supplementary file location>/serverless_agent_config	The following files: - serverlessUserAgentConfig.yml - JDBC V2 Connector JAR files - REST V3 Connector truststore and keystore certificates - JAR files for the Java transformation - Installation and resource files for the Python transformation You can customize the directory structure under the serverless_agent_config folder and specify the relative path to each file in the serverlessUserAgentConfig.yml file.

Configuring TLS to authenticate REST APIs

If you use REST V3 Connector with an API collection or Machine Learning transformation that runs in a serverless runtime environment, you can configure TLS to establish one-way or two-way secure communication to authenticate REST APIs.

Contact Informatica Global Customer Support to request the required custom properties. Make sure that truststore and keystore certificates are in JKS format.

1. Navigate to the supplementary file location on Amazon S3.

2. In the `serverless_agent_config` folder, create a subfolder called `SSL`.

3. Add the truststore and keystore certificates to the `SSL` folder.

For one-way secure communication, add the truststore certificates. For two-way secure communication, add both the truststore and keystore certificates.

4. Copy the following code snippet to a text editor and add the relative path to each certificate in the supplementary file location:

```
version: 1
agent:
  agentAutoApply:
    general:
        sslStore:
          - fileCopy:
                sourcePath: SSL/<REST V3 truststore certificate name>.jks
          - fileCopy:
                sourcePath: SSL/<REST V3 keystore certificate name>.jks
```

5. In the `serverless_agent_config` folder, open the `serverlessUserAgentConfig.yml` file.

6. Add the code snippet to the `serverlessUserAgentConfig.yml` file and save the file.

   The serverless runtime environment will copy the certificates from the supplementary file location to its own reference directory so that it can use the certificates at run time.

7. In the REST V3 connection properties, use the following format to specify each truststore and keystore file path in the serverless runtime environment: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<certificate name>.jks`

Provide the custom properties to your developer. Developers enter the custom properties in mapping tasks that run in the serverless runtime environment.

Configuring the serverlessUserAgentConfig.yml file

When you create a supplementary file location, you need to create and configure the `serverlessUserAgentConfig.yml` file.

Select a task to perform:

- To create the `serverlessUserAgentConfig.yml` file, use the template listed in "Populating the serverlessUserAgentConfig.yml File" on page 71 and adjust accordingly.

  To configure which files to copy from the supplementary file location to the serverless runtime environment, specify the file paths within the `serverlessUserAgentConfig.yml` file.

- To copy files for the Elastic Server, use the code snippet provided in "Copying files for the Elastic Server" on page 72.

- To copy JAR files for the JDBC V2 Connector, use the code snippet provided in "Copying JDBC V2 Connector JAR files" on page 73.

- To copy JAR files for the Java transformation, use the code snippet provided in "Copying Java transformation JAR files" on page 73.

- To copy resource files for the Python transformation, use the code snippet provided in "Copying Python transformation resource files" on page 74

- To add files to the supplementary file location while the serverless runtime environment is running, see "Adding files while the environment is running" on page 74.

Note: Escape any spaces or special characters that appear in paths entered in the `serverlessUserAgentConfig.yml` file.

Populating the serverlessUserAgentConfig.yml File

Use the following template to create your `serverlessUserAgentConfig.yml` file:

```
# The Secure Agent is the root element, and configurations are applied to the agent.
# Under the agent, there are three levels:
#1: apps : Application where you need to apply configurations.
#2: event: Event relating to the life cycle of application.
   #autoDeploy: Configurations that need the agent app to restart. Configurations are
applied and minor versions of the app are upgraded. An upgrade event will detect the
difference between the configuration that was last applied and the current request and
apply only those configuration changes. Note that Administrator does not show
notifications during minor version upgrades.
   #autoApply: Configuration that takes effect immediately, such as copying Swagger files.
#3: section: Contains configurations based on connectors.

# How do I apply the YML file?
# Create a serverlessUserAgentConfig.yml file with these contents in
<supplementary_file_location>/serverless_agent_config.
# The path in the serverlessUserAgentConfig.yml file is relative to
<supplementary_file_location>/serverless_agent_config/.

# fileCopy section : Provide the source location of the file that needs to be copied.

version: 1
agent: # At the agent level, provide general configurations that are not specific to the
application.
  agentAutoApply:
    general: # General section for common configurations across applications and
connectors.
      sslStore: # Use this to copy SSL files to the instance machine. You can provide a
list of fileCopy.
        - fileCopy:
            sourcePath: SSL/RESTV2_JWTpyn.jks
  # Data Integration Server app
  dataIntegrationServer:
    autoApply: # Apply configurations that don't need to upgrade the minor version or a
restart of the app. For example, you can copy files.
      restv2: # Connector section
        swaggers: # List of Swaggers files to copy to the instance machine.
          - fileCopy:
              sourcePath: restv2/<swagger_file_name>.json
        keystores: # List of keystore files to copy to the instance machine.
          - fileCopy:
              sourcePath: restv2/key
        truststores: # List of truststore files to copy to the instance machine.
          - fileCopy:
              sourcePath: restv2/key.ext
      wsconsumer:
        wsdls:
          - fileCopy:
              sourcePath: s3/
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: s3/file
    autoDeploy:
    # A change in this event will trigger a minor version upgrade with the new
configurations.
    # In this case, the Data Integration Server app will get a minor version upgrade.
      general: # General section for Data Integration Server app autoDeploy event.
        ssls:
          - fileCopy:
              sourcePath: SSL/RESTV2_JWTpyn.jks
            importCerts:
              certName: cname
              alias: IICS
        sap:
          jcos: # List of jco related files to copy.
            - fileCopy:
                sourcePath: sap/jco/libsapjco3.so
```

```
            - fileCopy:
                 sourcePath: sap/jco/sapjco3.jar
           nwrfcs: # List of nwrfc related files to copy.
              - fileCopy:
                  sourcePath: sap/nwrfc/libicudata.so.50
              - fileCopy:
                  sourcePath: sap/nwrfc/libicudecnumber.so
           hanas: # List of hana related files to copy.
              - fileCopy:
                  sourcePath: sap/hana/libicudata.so.50
       odbc:
         # Specify ODBC configurations.
         # This section can be used to configure multiple drivers.
         drivers: # Specify drivers to copy.
            - fileCopy:
                 sourcePath: ODBC/DWdb227.so
            - fileCopy:
                 sourcePath: ODBC/DWdb227.so
         dns:
            # Specify DNS entries. These entries will be updated in odbc.ini file.
            # If the file is not present, a new odbc.ini file will be created.
            # Make sure to give a name as a unique entry for the ini file configuration.
  The file will be read and updated using the name.
            - name: "SQL server" # Section name in ini file unique key.
              entries:
                 - key: Driver # Only provide the driver file name without the path.
                   value: DWsqls227.so # Because the file is copied, the path to attach
  during odbc entry is already known.
                 - key: Description
                   value: "SQL Server 2014 Connection for ODL"
                 - key: HostName
                   value: INVW16SQL19
                 - key: PortNumber
                   value: 1433
                 - key: Database
                   value: adapter_semantic
                 - key: QuotedId
                   value: No
                 - key: AnsiNPW
                   value: Yes
```

For more information about populating connector information in the `serverlessUserAgentConfig.yml` file, see the help for the appropriate connector.

Copying files for the Elastic Server

In the `serverlessUserAgentConfig.yml` file, you can specify files to copy from the supplementary file location to the serverless runtime environment. When you run mappings in advanced mode in the serverless runtime environment, the Elastic Server and the advanced cluster can use the files to access and process data.

You can copy the following file types for the Elastic Server:

- JDBC V2 Connector JAR files

- JAR files for the Java transformation

- Installation and resource files for the Python transformation

You can customize file paths by specifying the relative path to the file in the supplementary file location. For example, you might store JDBC V2 Connector JAR files in the following locations:

```
<Supplementary file location>/serverless_agent_config/jdbc_v2_jars/common/

<Supplementary file location>/serverless_agent_config/jdbc_v2_jars/spark/
```

You can specify the following relative paths in the `serverlessUserAgentConfig.yml` file:

```
agent:
  elasticServer:
    autoApply:
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: jdbc_v2_jars/common/driver.jar
        spark:
          - fileCopy:
              sourcePath: jdbc_v2_jars/spark/driver.jar
```

Copying JDBC V2 Connector JAR files

To copy JAR files for JDBC V2 Connector, use the following code snippet as a template:

```
agent:
  elasticServer:
    autoApply:.
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: jars/connectors/thirdparty/informatica.jdbc_v2/common/
driver.jar
          - fileCopy:
              sourcePath: jars/connectors/thirdparty/informatica.jdbc_v2/common/
driver.jar
        spark:
          - fileCopy:
              sourcePath: jars/connectors/thirdparty/informatica.jdbc_v2/spark/driver.jar
          - fileCopy:
              sourcePath: jars/connectors/thirdparty/informatica.jdbc_v2/spark/driver.jar
```

Copying Java transformation JAR files

To copy JAR files, native libraries, and/or native binaries for the Java transformation, use the following code snippet as a template:

```
agent:
  elasticServer:
    autoApply:
      javaTx:
        resources:
          - fileCopy:
              sourcePath: j_depends/sapjco3.jar
          - fileCopy:
              sourcePath: j_depends/chilkat.jar
          - fileCopy:
              sourcePath: j_depends/chilkatLoader.jar
          - fileCopy:
              sourcePath: j_depends/NativeBinExecutor.jar
      nativeLib:
        resources:
          - fileCopy:
              sourcePath: native-lib/libchilkat.so
          - fileCopy:
              sourcePath: native-lib/libsapjco3.so
      nativeBin:
        resources:
          - fileCopy:
              sourcePath: native-bin/printEnvVariables.sh
          - fileCopy:
              sourcePath: native-bin/printProcess.sh
```

Copying Python transformation resource files

To copy resource files for the Python transformation, use the following code snippet as a template:

```
agent:
  elasticServer:
    autoApply:
      pythonTx:
        resources:
        - fileCopy:
            sourcePath: py_depends/res1.txt
        - fileCopy:
            sourcePath: py_depends/res2.txt
```

Adding files while the environment is running

You can add files for the Elastic Server to the supplementary file location while the serverless runtime environment is running. Files for the Elastic Server include JDBC V2 Connector JAR files, Java transformation JAR files, and Python transformation resource files.

To add a file while the environment is running, complete the following steps:

1. Add the file to the appropriate location in `<Supplementary file location>/serverless_agent_config/`.

2. Specify the file in the `serverlessUserAgentConfig.yml` file. For information about the `serverlessUserAgentConfig.yml` file, see "Creating the supplementary file location" on page 69 or the help for the appropriate connector.

It may take up to 10 minutes for the file to synchronize to the serverless runtime environment.

You must redeploy the serverless runtime environment after you perform any of the following tasks:

- Update an existing file.

  To update an existing file while the serverless runtime environment is running, you must add the file to the supplementary file location and to the `serverlessUserAgentConfig.yml` file using a different name.

- Add other file types, such as ODBC shared libraries.

- Add a new folder or directory, such as a Python installation directory for the Python transformation.

- Remove files from the serverless runtime environment.

Using a proxy server

If your organization uses an outgoing proxy server to connect to the internet, you can configure the serverless runtime environment to connect to Informatica Intelligent Cloud Services through the proxy server.

When you configure a proxy server for the serverless runtime environment, you define the required proxy server settings in the `serverlessUserAgentConfig.yml` file before you can import metadata or design your mappings. Data Integration copies the proxy entries in the file to the serverless runtime environment.

To apply the proxy when you run mappings, set the proxy configurations on the **Serverless Environments** page in Administrator.

You can configure proxy settings for the serverless runtime environment in certain connectors. To see if the proxy applies in a connector, see the help for the appropriate connector.

Configure the proxy in the serverlessUserAgentConfig.yml file

To apply proxy server settings when you design mappings and import metadata, add the proxy server details to the `serverlessUserAgentConfig.yml` file.

Use the following code snippet as a template to provide the values for the proxy server in the `serverlessUserAgentConfig.yml` file:

```
agent:
  agentAutoDeploy:
    general:
        proxy:
            proxyHost: <Host_name of proxy server>
            proxyPort: <Port number of the proxy server>
            proxyUser: <User name of the proxy server>
            proxyPassword: <Password to access the proxy server>
            nonProxyHost: <Non-proxy host>
```

Configure the proxy in the JVM options

To apply proxy server settings when you run mappings or tasks, configure JVM options in Administrator.

1. On the **Serverless Environments** page, click the name of the serverless runtime environment.

2. Click **Edit**.

3. In the **Runtime Configuration Properties** section, select the **Service** as **Data Integration Server** and the **Type** as **DTM**.

4. Edit any of the JVMOption fields and specify appropriate values for each parameter based on whether you use an HTTPS or HTTP proxy server.

   The following table describes the parameters:

Parameter	Description
-Dhttp.proxySet=	Determines if the serverless runtime environment must use the proxy settings when the outgoing proxy server is HTTP. Select -Dhttp.proxySet=True to use the proxy.
-Dhttps.proxySet=	Determines if the serverless runtime environment must use the proxy settings when the outgoing proxy server is HTTPS. Select -Dhttps.proxySet=True to use the proxy.
-Dhttp.proxyHost=	Host name of the outgoing HTTP proxy server.
-Dhttp.proxyPort=	Port number of the outgoing HTTP proxy server.
-Dhttp.proxyUser=	Authenticated user name for the HTTP proxy server.
-Dhttp.proxyPassword=	Password for the authenticated user.
-Dhttps.proxyHost=	Host name of the outgoing HTTPS proxy server.
-Dhttps.proxyPort=	Port number of the outgoing HTTPS proxy server.
-Dhttps.proxyUser=	Authenticated user name for the HTTPS proxy server.
-Dhttps.proxyPassword=	Password for the authenticated user.

5. Click **Save**.

Allow domains in the proxy server

To run a mapping successfully, the proxy server must allow traffic from the AWS endpoints that are required to process the data in the mapping.

Allow traffic from the following domains:

```
s3.<region>.amazonaws.com
s3.amazonaws.com
ec2.<region>.amazonaws.com
sts.<region>.amazonaws.com
efs.<region>.amazonaws.com
elasticfilesystem.<region>.amazonaws.com
```

Specify the region that contains the VPC that connects to the serverless runtime environment.

CHAPTER 8

Serverless runtime environments

A serverless runtime environment is an advanced serverless deployment solution that uses an isolated, single-tenant model, unlike the multi-tenant model on the Hosted Agent.

The single-tenant model provides a dedicated server with virtual machine resources to run tasks for your organization. The serverless runtime environment auto-scales with the size of the workload while your data remains in your cloud environment.

A serverless runtime environment can be hosted on these cloud platforms:

- Azure Virtual Network (VNet)
- Amazon Virtual Private Cloud (VPC). The serverless runtime environment creates an elastic network interface (ENI) to connect to your cloud environment.

A serverless runtime environment supports local regions in each geo-location. For example, an AWS cloud platform in the United States (US) supports all US regions and an AWS cloud platform in Asia-Pacific (APAC) supports all APAC regions.

Users who require access to the Serverless Environments configuration page require the PRIVILEGES.VIEW_AGENT_GROUP permission.

Running mappings in advanced mode

When you use a serverless runtime environment to run mappings in advanced mode, the advanced serverless deployment fulfills the prerequisites to create an advanced cluster and to run jobs on the cluster.

The serverless runtime environment manages the advanced cluster while the cluster adapts to workload changes by provisioning and de-provisioning resources. Worker nodes in the advanced cluster are highly available. High availability mitigates job failures and maintains job performance when a worker node crashes.

Creating a serverless runtime environment in Azure

Create a serverless runtime environment and configure properties in the Azure portal. You can view properties for a serverless runtime environment by expanding the **Actions** menu for the environment in the Azure portal and selecting **View properties**.

For instructions on creating and maintaining serverless runtime environments in Azure Native ISV Services, see Configure serverless runtime environment on Azure Native ISV.

Creating a serverless runtime environment in AWS

Create a serverless runtime environment and configure properties on the **Serverless Environments** page. You can view properties for a serverless runtime environment by expanding the **Actions** menu for the environment and selecting **View**.

The following image shows the **Serverless Environments** page:
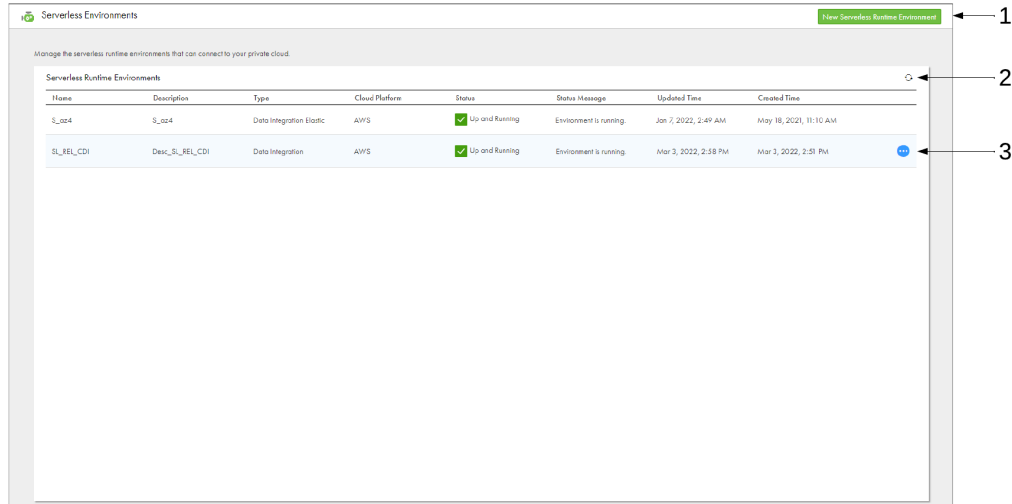
1. Option to create a serverless runtime environment
2. Refresh icon
3. Actions menu

To create a serverless runtime environment, you can enter the serverless runtime environment properties, or you can import a serverless configuration file to populate the properties. It takes at least five minutes for the serverless runtime environment to become available. Use the **Serverless Environments** page to track the status of the environment and review any status messages.

You can create a maximum of 10 serverless runtime environments in your organization. If you have a trial license, you can create a maximum of two environments.

Serverless runtime environment properties

Configure properties for the serverless runtime environment. The basic properties define the serverless runtime environment. The platform configuration properties describe the AWS resources in your VPC that connect to the serverless runtime environment.

Basic Configuration

The Basic Configuration section of a serverless runtime environment contains general information about the environment, including its Informatica Account Number and its current status.

The following table describes the basic properties:

Property	Description
Name	Name of the serverless runtime environment.
Description	Description of the serverless runtime environment.
Task Type	Type of tasks that run in the serverless runtime environment. - Select **Data Integration** to run mappings outside of advanced mode. - Select **Advanced Data Integration** to run mappings in advanced mode.
Cloud Platform	Cloud platform to host the serverless runtime environment. You can use only Amazon Web Services (AWS).
Max Compute Units Per Task	Maximum number of serverless compute units corresponding to machine resources that a task can use.
Task Timeout	Amount of time in minutes to wait for a task to complete before it is terminated. The timeout ensures that serverless compute units are not unproductive when a task hangs. By default, the timeout is 2880 minutes (48 hours). You can set the timeout to a value that is less than 2880 minutes.
Informatica Account Number	Informatica's account number on the cloud platform where the serverless runtime environment will be created. The account number is populated automatically.
External ID	External ID to associate with the role that you create for the serverless runtime environment. You can use the generated external ID or specify your own external ID.

Platform Configuration

The Platform Configuration section of a serverless runtime environment contains technical information about the platform, including the region, subnet, and security group.

The following table describes the platform properties:

Property	Description
Configuration Name	Name of the resource configuration.
Configuration Description	Description of the resource configuration. The description can be up to 256 characters and can contain alphanumeric characters and the following special characters: ._-:/()#,@[]+=&;{}!$"*
Account Number	Your account number on the cloud platform.
Region	Region of your cloud environment. The sources and targets that you use in mappings should either reside in or be accessible from this region.

Property	Description
AZ ID	Identifier for the availability zone. The sources and targets that you use in mappings must either reside or be accessible from the availability zone.
VPC ID	ID of the Amazon Virtual Private Cloud (VPC). The VPC must be configured with an endpoint to access the sources and targets that you use in mappings. For example, `vpc-2f09a348`.
Subnet ID	ID of the subnet within the VPC. The subnet must be have an entry point to access the sources and targets that you use in mappings. For example, `subnet-b46032ec`.
Security Group ID	ID of the security group that the serverless runtime environment will attach to the ENI. The security group allows access to the sources and targets that you use in tasks. For example, `sg-e1fb8c9a`.
Role Name	Name of the IAM role that the serverless runtime environment can assume on your AWS account. The role must have permissions to create, read, delete, list, detach, and attach an ENI. It also requires read and write permissions on supplementary file location. Use the Informatica account number and the external ID when you create a policy for the role.
AWS Tags	AWS tags to label the ENI that is created in your AWS account. Each tag must be a key-value pair in the format: `Key=string,Value=string` where `Key` and `Value` are case-sensitive. Use a space to separate tags. Follow the rules and guidelines for tagging that AWS specifies. For more information, refer to the AWS documentation.
Supplementary File Location	Location on Amazon S3 to store supplementary files, such as JAR files and external libraries for certain transformations and connectors. Use the format: `s3://<bucket name>/<folder name>`. You must put script files in a folder named `command_scripts`. This folder can have subfolders. Informatica Intelligent Cloud Services synchronizes files at regular intervals within the `command_scripts` directory to the Secure Agent, specifically to the agent install directory `apps/Common_Integration_Components/data/command/serverless/command_scripts`. If you update files in Amazon S3, Informatica Intelligent Cloud Services automatically synchronizes them to the Secure Agent.

Runtime Configuration Properties

The Runtime Configuration Properties section of a serverless runtime environment determines how the environment behaves.

Note: Set the variables for the default directories, but don't change any other variables or properties unless directed by your system administrator or by Informatica Global Customer Support.

The following table lists the system variables that the serverless runtime environment uses for locations such as the source and target directories and temp files. Review the system defaults and update them as necessary.

Directory names can't contain these special characters: * ? < > " | ,

Tip: Filter the list to show "Service = Data_Integration_Server" and "Type = PMRDTM_CFG" to find the default directory variables more easily.

System Variable Name	Description
$PMLookupFileDir	Directory for lookup files. Default is $PMRootDir
$PMBadFileDir	Directory for reject files. Default is $PMRootDir/error
$PMCacheDir	Directory for index and data cache files. Default is $PMRootDir/cache
$PMStorageDir	Directory for state of operation files. The Data Integration Service uses these files for recovery if you have the high availability option or if you enable a workflow for recovery. These files store the state of each workflow and session operation. Default is $PMRootDir
$PMTargetFileDir	Directory for target files. Default is $PMRootDir
$PMSourceFileDir	Directory for source files. Default is $PMRootDir
$PMExtProcDir	Directory for external procedures. Default is $PMRootDir
$PMTempDir	Directory for temporary files. Default is $PMRootDir/temp

System Disk

Configuring a system disk can in the serverless runtime environment can improve mapping performance in Data Integration.

For rules and guidelines about configuring a system disk, see "Configuring a system disk" on page 66.

The following table describes the properties for a system disk:

Property	Description
Type	System disk type, either EFS or NFS.
File System	For EFS disks, the file system is the file system ID of the EFS disk. For NFS disks, the file system is the DNS of the file system.
Source Mount	File system path to be mounted in the serverless runtime environment.
Access Point	The ID of the Amazon EFS file system access point. The access point ensures isolation for tenants in a multi-tenant EFS file system. Once an access point is set up, you can configure the file system policy to allow access only to the access point for the serverless IAM role.

Data Disk

Configuring a data disk in your serverless runtime environment allows you to access files in EFS or NFS directories.

For more information, see "Using EFS or NFS directories as data disks" on page 68 and "Configuring a data disk" on page 68.

The following table describes the properties for a data disk:

Property	Description
Type	Data disk type, either EFS or NFS.
File System	For EFS disks, the file system is the file system ID of the EFS disk. For NFS disks, the file system is the DNS of the file system.
Source Mount	File system path to be mounted in the serverless runtime environment.
Target Mount	File system to be mounted on the Secure Agent.
Access Point	The ID of the Amazon EFS file system access point. The access point ensures isolation for tenants in a multi-tenant EFS file system. Once an access point is set up, you can configure the file system policy to allow access only to the access point for the serverless IAM role.

Using a serverless configuration file

You can use a serverless configuration file to populate the serverless runtime environment properties.

Request the configuration file from your cloud administrator and import it in Administrator when you create a serverless runtime environment.

Requesting a serverless configuration file

Request the serverless configuration file from your cloud administrator.

1. On the **Serverless Environments** page, click **New Serverless Runtime Environment**.

2. Select **Request a configuration file from your cloud administrator**.

    The **Configuration File Request** dialog box appears.

3. Select the cloud region.

    The dialog box generates an email template.

4. Click **Copy to Clipboard**.

5. Using your preferred email service, use the template to compose an email and send it to your cloud administrator.

    The email contains URLs to the AWS CloudFormation templates that your cloud administrator can use to create a VPC or connect an existing VPC to a serverless runtime environment and generate the serverless configuration file. For more information, see "Create a VPC using a template" on page 57.

Importing a serverless configuration file

Import a serverless configuration file to populate serverless runtime environment properties.

1. On the **Serverless Environments** page, click **New Serverless Runtime Environment**.

2. Select **Create a serverless runtime environment**.

3. Enter the basic properties.

4. For the platform properties, click **Import Configuration**.

   The **Import a Configuration File** dialog box appears.

5. Click **Choose File** and navigate to the serverless configuration file on your local machine.

6. Click **Import**.

Serverless runtime validation

The validation process validates the AWS resource configuration properties and some network settings on the serverless runtime environment when you perform specific tasks.

The validation process connects to your AWS account using the IAM role to verify and list the resource properties, such as the subnet ID, availability zone ID, and role name. The IAM role establishes trust between your AWS account and the Informatica AWS account so that the serverless runtime environment can create an ENI and securely connect to data sources in your cloud environment. The IAM role must have permission to view the resource. For more information about setting up the IAM role, see "Create and configure your environment manually" on page 55.

The following role permissions are required for validation:

- ec2:DescribeRegions

- ec2:DescribeAvailabilityZones

- ec2:DescribeVpcs

- ec2:DescribeSubnets

- ec2:DescribeSecurityGroups

If validation fails for any resource, the serverless runtime environment fails to start. You can download the detailed validation messages using the download option on the **Serverless Environments** page or the specific serverless runtime environment configuration page. Validation results and messages are available for failed environments only.

In addition to the serverless runtime environment properties, the validation process also checks for the number of IP addresses available on the subnet. The serverless runtime environment creation fails if there are insufficient IP addresses available on the subnet.

Note: The validation process does not validate the Amazon Virtual Private Cloud (VPC) ID if the subnet ID does not exist in your Amazon account.

Serverless runtime environment properties and network settings are validated when you perform the following tasks on a serverless runtime environment:

- Create a new serverless runtime environment.

- Edit a failed serverless runtime environment and save the updates.

- Clone a serverless runtime environment and save the configurations.

- Redeploy a failed serverless runtime environment.

Managing a serverless runtime environment

After you create a serverless runtime environment, you can perform management tasks such as editing, redeploying, or cloning the serverless runtime environment.

Except where noted, management actions described in this section apply to both AWS and Azure serverless runtime environments.

Editing a serverless runtime environment

The properties that you can edit in a serverless runtime environment vary, depending on the environment's status.

You can edit the following properties, based on the status of the serverless runtime environment:

- Up and Running. You can only update the following fields: **Max Compute Units Per Task** and **Task Timeout**. The updated values take effect for subsequent task runs.

- Failed. You can update all the properties. The updated properties take effect once you use the **Redeploy** (AWS) or **Start environment** action (Azure).

If the serverless runtime environment shows any other status, you must delete the serverless runtime environment and create a new one.

To edit a serverless runtime environment, expand the **Actions** menu for the serverless runtime environment and select **Edit**. This works for both Azure and AWS serverless runtime environments.

For serverless runtime environments created in Azure Native ISV Services, you can also use the Azure portal to edit the properties.

Redeploying a serverless runtime environment (AWS)

The redeploy action restarts the serverless runtime environment, either after a change in the environment or if the environment shuts down for a specific reason.

You might redeploy the serverless runtime environment in the following situations:

- You change your organization's licenses.

- The serverless runtime environment shuts down because the organization ran out of serverless compute units. You can add more compute units to your organization and redeploy the serverless runtime environment.

- You update the configuration in your cloud environment. For example, you update files in the supplementary file location, or you update the policy that is attached to the IAM role.

Before you redeploy a serverless runtime environment, in Monitor, be sure that no jobs are running in the runtime environment. Then, in Administrator, expand the **Actions** menu for the serverless runtime environment and click **Redeploy**.

Note: Wait until the redeployment completes before you run a mapping. Any jobs running during redeployment will fail.

Cloning a serverless runtime environment

You might clone a serverless runtime environment to create another environment that has a similar configuration. For example, you want to create a similar serverless runtime environment that connects to a different subnet in your cloud environment or uses a different security group.

Note: To clone serverless runtime environments created in Azure Native ISV Services, use the Azure portal.

To clone a serverless runtime environment, expand the **Actions** menu for the serverless runtime environment and select **Clone**.

Deleting a serverless runtime environment

Delete a serverless runtime environment when it's no longer required.

Note: To delete serverless runtime environments created in Azure Native ISV Services, use the Azure portal.

Before you delete a serverless runtime environment, perform the following tasks:

- Use Monitor to make sure that the environment is not running any jobs.
- Use the **Show Dependencies** action to see if the environment is being used by any tasks, mappings, or connections. If dependencies exist, remove them before deleting the environment.

To delete a serverless runtime environment, expand the **Actions** menu for the serverless runtime environment and select **Delete**.

Metering serverless compute units

Serverless compute units represent CPUs and memory that a serverless runtime environment can use to run tasks.

When you create a serverless runtime environment, you configure a maximum number of serverless compute units that each task can request from the serverless runtime environment. When you create a mapping task, you can override the maximum number of compute units that the task can request. In Monitor, you can view the number of compute units that the task requested and consumed.

If the task runs longer than the task timeout that you specify, the serverless runtime environment terminates the task.

For information about the meter, see *Organization Administration*.

Disaster recovery (AWS)

If a disaster impacts the region or the availability zone that hosts a serverless runtime environment, redirect jobs to a temporary serverless runtime environment in a stable region or availability zone as part of your organization's disaster recovery plan.

Disaster recovery procedure

During a disaster, all virtual machines in the serverless runtime environment shut down and jobs can no longer run in the environment.

To minimize data loss and downtime, complete the following tasks:

1. Create a temporary serverless runtime environment in a stable region or availability zone.

2. Make sure that the connections used in jobs are available in the stable region or availability zone.

3. Clean up data related to incomplete job runs. If data was partially loaded to a target, manually delete the data or update the mapping to truncate the target before writing new rows.

4. Redirect jobs to the temporary environment.

Restoring the primary environment

When the region or availability zone that hosts the primary serverless runtime environment has recovered, you can restore the primary environment.

To restore the primary environment, complete the following tasks:

1. Clean up the ENIs that were created in your AWS account for the primary environment.

2. Redeploy the primary environment.

3. Redirect jobs to the primary environment.

4. Delete the temporary environment.

Connectors in a serverless runtime environment

When you create a connection, you can specify a serverless runtime environment configured in AWS or Azure.

The list of connectors applicable to the serverless runtime environment configured on Azure and AWS might vary.

AWS serverless runtime environment

You can use the serverless runtime environment configured in AWS for the following connectors:

Amazon Athena Connector	MongoDB Connector
Amazon Aurora Connector	Microsoft SQL Server Connector
Amazon Redshift V2 Connector	MongoDB V2 Connector*
Amazon DynamoDB V2 Connector*	MySQL Connector
Amazon S3 V2 Connector	NetSuite RESTlet V2
BigMachines Connector	OData Connector
Box Connector	OData Consumer Connector
Concur V2 Connector	OData V2 Protocol Reader Connector
Coupa V2 Connector	ODBC Connector
Cvent Connector	Oracle Connector
Databricks Delta Connector	PostgreSQL Connector
Dropbox Connector	REST V2 Connector
Eloqua Bulk API Connector	REST V3 Connector
Google Analytics Connector	Salesfore Oauth Connector
Google BigQuery V2 Connector	Salesforce Connector
Google Cloud Storage V2 Connector	Salesforce Marketing Cloud Connector
JDBC (JDBC_IC) Connector	SAP ADSO Writer Connector
JDBC V2 Connector	SAP BAPI Connector
JIRA Connector	SAP BW Bex Query Connector
Kafka Connector*	SAP Table Connector
Marketo REST Connector	SAP ODP Extractor Connector
Marketo V3 Connector	SAP HANA Connector
Microsoft Azure Blob Storage V3 Connector	ServiceNow Connector
Microsoft Azure Cosmos DB SQL API Connector	Snowflake Data Cloud Connector
Microsoft Azure Data Lake Storage Gen1 V3 Connector	SuccessFactors ODATA Connector
Microsoft Azure Data Lake Storage Gen2 Connector	Web Service Consumer Connector
Microsoft Azure Synapse SQL Connector	Workday V2 Connector
Microsoft CDM Folders V2 Connector	Xero Connector
Microsoft Dynamics 365 for Operations Connector	Xactly Connector
Microsoft Dynamics 365 for Sales Connector	Zendesk V2 Connector

*Serverless runtime environment in AWS applies for the connector in mappings in advanced mode only.

Azure serverless runtime environment

You can use the serverless runtime environment configured in Azure for the following connectors:

Amazon Athena Connector	Microsoft Dynamics 365 for Operations Connector
Amazon Aurora Connector	Microsoft Dynamics 365 for Sales Connector
Amazon Redshift V2 Connector	Microsoft SQL Server Connector
Amazon S3 V2 Connector	MongoDB V2 Connector*
BigMachines Connector	MySQL Connector
Concur V2 Connector	OData Connector
Coupa V2 Connector	OData Consumer Connector
Cvent Connector	OData V2 Protocol Reader Connector
Databricks Delta Connector	ODBC Connector
DB2 Warehouse on Cloud Connector	Oracle Connector
Dropbox Connector	PostgreSQL Connector
Eloqua Bulk API Connector	REST V2 Connector
Google Analytics Connector	REST V3 Connector
Google BigQuery V2 Connector	Salesforce Connector
Google Cloud Spanner Connector	Salesforce Marketing Cloud Connector
Google Cloud Storage V2 Connector	SAP ADSO Writer Connector
JDBC (JDBC_IC) Connector	SAP BAPI Connector
JDBC V2 Connector	SAP ODP Extractor Connector
JIRA Connector	SAP HANA Connector
Kafka Connector*	ServiceNow Connector
Marketo V3 Connector	Snowflake Data Cloud Connector
Microsoft Azure Blob Storage V3 Connector	SuccessFactors ODATA Connector
Microsoft Azure Cosmos DB SQL API Connector	Web Service Consumer Connector
Microsoft Azure Data Lake Storage Gen1 V3 Connector	Workday V2 Connector
Microsoft Azure Data Lake Storage Gen2 Connector	Xero Connector
Microsoft Azure Synapse SQL Connector	Xactly Connector
Microsoft CDM Folders V2 Connector	Zendesk V2 Connector

*Serverless runtime environment in Azure applies for the connector in mappings in advanced mode only.

INDEX