Informatica®

Informatica® Intelligent Cloud Services
October 2022

ランタイム環境

Informatica Intelligent Cloud Services ランタイム環境
October 2022

発行日: 2022-12-01

目次

序文

*ランタイム環境*の説明を使用して、Informatica Intelligent Cloud Services℠で使用するランタイム環境とサーバーレスランタイム環境を作成および構成する方法を確認してください。Informatica Intelligent Cloud Services ホステッドエージェントの使用方法、Secure Agent のダウンロードとインストール、Secure Agent グループの作成と設定、および Secure Agent のトラブルシューティングの方法を確認します。

Informatica のリソース

Informatica は、Informatica Network やその他のオンラインポータルを通じてさまざまな製品リソースを提供しています。リソースを使用して Informatica 製品とソリューションを最大限に活用し、その他の Informatica ユーザーや各分野の専門家から知見を得ることができます。

Informatica マニュアル

Informatica マニュアルポータルでは、最新および最近の製品リリースに関するドキュメントの膨大なライブラリを参照できます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

製品マニュアルに関する質問、コメント、ご意見については、Informatica マニュアルチーム（infa_documentation@informatica.com）までご連絡ください。

Informatica Intelligent Cloud Services Web サイト

Informatica Intelligent Cloud Services Web サイト（http://www.informatica.com/cloud）にアクセスできます。このサイトには、Informatica Cloud 統合サービスに関する情報が含まれます。

Informatica Intelligent Cloud Services コミュニティ

Informatica Intelligent Cloud Services コミュニティを使用して、技術的な問題について議論し、解決します。また、技術的なヒント、マニュアルの更新情報、FAQ（よくある質問）への答えを得ることもできます。

次の Informatica Intelligent Cloud Services コミュニティにアクセスします。

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

開発者は、次の Cloud 開発者コミュニティで詳細情報を確認したり、ヒントを共有したりできます。

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

Informatica Intelligent Cloud Services マーケットプレース

Informatica マーケットプレイスにアクセスすると、データ統合コネクタ、テンプレート、およびマップレットを試用したり購入したりできます。

https://marketplace.informatica.com/

データ統合コネクタのドキュメント

データ統合コネクタのドキュメントには、マニュアルポータルからアクセスできます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

Informatica ナレッジベース

Informatica ナレッジベースを使用して、ハウツー記事、ベストプラクティス、よくある質問に対する回答など、製品リソースを見つけることができます。

ナレッジベースを検索するには、https://search.informatica.com にアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム（KB_Feedback@informatica.com）です。

Informatica Intelligent Cloud Services Trust Center

Informatica Intelligent Cloud Services Trust Center は、Informatica のセキュリティポリシーおよびリアルタイムでのシステムの可用性について情報を提供します。

Trust Center（https://www.informatica.com/trust-center.html）にアクセスします。

Informatica Intelligent Cloud Services Trust Center にサブスクライブして、アップグレード、メンテナンス、およびインシデントの通知を受信します。Informatica Intelligent Cloud Services Status ページには、すべての Informatica Cloud 製品の実稼働ステータスが表示されます。メンテナンスの更新はすべてこのページに送信され、停止中は最新の情報が表示されます。更新と停止の通知がされるようにするには、Informatica Intelligent Cloud Services の 1 つのコンポーネントまたはすべてのコンポーネントについて更新の受信をサブスクライブします。すべてのコンポーネントにサブスクライブするのが、更新を逃さないようにするための最良の方法です。

登録するには、https://status.informatica.com/に移動し、**[更新を購読登録]** をクリックします。その後、電子メール、SMS テキストメッセージ、Webhook、RSS フィードとして、またはこの 4 つを任意に組み合わせて送信された通知を受信することを選択ができます。

Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

オンラインサポートについては、Informatica Intelligent Cloud Services の **[サポート要求の送信]** をクリックしてください。またオンラインサポートを使用して問題を記録することもできます。オンラインサポートを利用するには、ログインが必要です。https://network.informatica.com/welcome でログイン要求できます。

Informatica グローバルカスタマサポートの電話番号は、Informatica の Web サイト https://www.informatica.com/services-and-training/support-services/contact-us.html に掲載されています。

第 1 章

ランタイム環境

ランタイム環境は、タスクやタスクフローなどの Informatica Intelligent Cloud Services アセットを実行する実行プラットフォームです。組織内のユーザーがタスクを実行できるように、各組織に少なくとも 1 つのランタイム環境が必要です。

ランタイム環境は、1 つ以上の Secure Agent で構成されます。Secure Agent は、すべてのタスクを実行し、組織と Informatica Intelligent Cloud Services 間でのファイアウォールを越えた安全な通信を可能にする軽量プログラムです。

ランタイム環境は、次の方法で設定できます。

Informatica Cloud Hosted Agent **のライセンスを取得します。**

Hosted Agent のライセンスを取得する場合は、Informatica Cloud ホスティングファシリティ内でタスクを実行します。Informatica は、Hosted Agent のランタイム環境とエージェントを保持します。Informatica Cloud Hosted Agent の詳細については、第 2 章, 「Hosted Agent」 (ページ 9)を参照してください。

1 **つ以上の** Secure Agent **グループを作成します。**

1 つ以上の Secure Agent をダウンロードしてインストールし、ネットワーク内または Amazon Web Services や Google Cloud、Microsoft Azure などのクラウドコンピューティングサービス環境で実行することができます。1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールできます。

Secure Agent をインストールすると、デフォルトでは独自のグループに追加されます。Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。Secure Agent グループの詳細については、第 3 章, 「Secure Agent グループ」 (ページ 11)を参照してください。

サーバーレスランタイム環境を設定します。

クラウド環境が AWS の場合は、サーバーレスランタイム環境を設定できます。この環境は Informatica によってホストされるため、Secure Agent または Secure Agent グループを設定する必要はありません。サーバーレスランタイム環境の詳細については、第 6 章, 「サーバーレスランタイム環境」 (ページ 45)を参照してください。

接続または一部のタイプのタスクを構成するときは、使用するランタイム環境を指定します。ランタイム環境により、実行時にタスクを実行するエージェントが決まります。ランタイム環境が Hosted Agent である場合は、Hosted Agent がタスクを実行します。ランタイム環境が Secure Agent グループである場合、グループ内の使用可能なすべてのエージェントがタスクを実行できます。

詳細モードのマッピングを実行するため、エージェントは、エージェントマシン上にデフォルトのローカルクラスタを作成し、小さなデータセットで高度な機能の開発と実行を開始して、マッピングロジックをテストできます。詳細については、*詳細クラスタ*の説明を参照してください。

ローカルクラスタの詳細モードでマッピングを実行する前に、特にエージェントがすでに他のジョブを実行している場合には、クラスタを作成してジョブを正常に実行できるように、エージェントに十分なリソースがあることを確認してください。エージェントに十分なリソースがない場合、エージェントですでに実行されてい

るジョブと詳細モードのマッピングは失敗します。エージェントマシンには少なくとも 8 つのコアと 32GB のメモリを搭載することをお勧めします。

第 2 章

Hosted Agent

組織に Cloud Runtime ライセンスがある場合は、Hosted Agent を使用してタスクを実行できます。Hosted Agent は、特定のコネクタを使用する同期タスクおよびマッピングタスクを実行できます。

データ統合で Hosted Agent のランタイム環境が管理されるため、Hosted Agent を追加、削除、または構成することはできません。

Hosted Agent は、特定のコネクタを使用する同期タスク、マッピングタスク、およびレプリケーションタスクを実行できます。

- Amazon Athena コネクタ
- Amazon Aurora コネクタ
- Amazon Redshift コネクタ
- Amazon Redshift V2 コネクタ
- Amazon S3 コネクタ
- Amazon S3 V2 コネクタ
- Box コネクタ
- Box Oauth コネクタ
- Cloud 統合ハブ
- Concur V2 コネクタ
- Coupa コネクタ
- Coupa V2 コネクタ
- Cvent コネクタ
- Databricks Delta コネクタ
- DB2 Warehouse on Cloud コネクタ
- Eloqua Bulk API コネクタ
- Google Analytics コネクタ
- Google Big Query コネクタ
- Google Big Query V2 コネクタ
- Google Cloud Spanner コネクタ
- Google Cloud Storage コネクタ
- Google Cloud Storage V2 コネクタ
- JIRA コネクタ
- Marketo V3 コネクタ

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

注: Hosted Agent のサポートはコネクタ固有です。詳細については、関連するコネクタのヘルプを参照してください。

第 3 章

Secure Agent グループ

オンプレミスのデータにアクセスする必要がある場合や、Hosted Agent を使用せずにクラウドコンピューティングサービス環境内のデータにアクセスする場合は、Secure Agent をランタイム環境として使用します。接続またはタスクのランタイム環境として Secure Agent グループを選択すると、グループ内の Secure Agent エージェントがタスクを実行します。

次の目標を達成するために、Secure Agent エージェントグループを作成します。

ある部門の活動が別の部門に影響を与えないようにします。

ある部門の活動が別の部門に影響を与えないようにするため、部門ごとに別々の Secure Agent グループを作成します。例えば、営業部門のユーザーが、財務部門のユーザーと同じ数のタスクを 10 回実行するとしても、財務タスクは時間が非常に重要です。営業タスクが財務タスクに影響を与えないようにするため、部門ごとに別々の Secure Agent エージェントグループを作成します。次に、一方のランタイム環境に営業タスクを割り当て、もう一方のランタイム環境に対して財務タスクを実行します。

環境ごとにタスクを分離する。

テストおよび運用環境では、異なる Secure Agent グループを作成できます。接続を構成するとき、ランタイム環境として適切な Secure Agent グループを選択することで、その接続をテスト用または本稼働用のデータベースに関連付けることができます。

Secure Agent グループを作成すると、組織内のすべてのユーザーが、ランタイム環境として Secure Agent グループを選択できます。

グループから Secure Agent を追加および削除できます。ライセンスに基づいて、次の操作を実行することもできます。

- Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。
- 組織階層ライセンスがある場合は、Secure Agent グループをサブ組織と共有できます。

注: ランタイム環境を使用して、詳細モードのマッピングに基づくマッピングタスクを実行するには、Secure Agent グループに含まれる Secure Agent が 1 つのみであることが必要です。

Secure Agent マシン上の出力ファイルにアクセスする必要がある場合は、モニタで **［すべてのジョブ］** ページを表示するか、データ統合で **［マイジョブ］** ページを表示してタスクの実行場所を決定します。

複数のエージェントを含む Secure Agent グループ

Secure Agent を作成すると、デフォルトでは独自のグループに追加されます。Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。グループ内のすべてのエージェントは、ネットワーク内で実行されるすべてのエージェントや Amazon EC2 マシンで実行されるすべてのエージェントなど、同じ種類である必要があります。

グループに複数のエージェントを追加して、次の目標を達成します。

負荷をマシン間で分散する。

複数のエージェントをグループに追加して、マシン間のタスクの分散を調整します。ランタイム環境が複数のエージェントを持つ Secure Agent グループである場合、グループは使用可能なエージェントにタスクとメタデータ呼び出しなどのバックグラウンドプロセスをラウンドロビン方式でディスパッチします。

接続とタスクの拡張性を向上させる。

接続またはタスクを作成するときは、使用するランタイム環境を選択します。ランタイム環境が複数のエージェントを持つ Secure Agent グループである場合、グループ内に稼働している Secure Agent があれば、そのタスクを実行できます。エージェントを追加または削除するとき、またはグループ内のエージェントが実行を停止したときに、接続またはタスクのプロパティを変更する必要はありません。

グループに複数のエージェントを追加する場合は、すべての Secure Agent が同じタイプであることを確認します。例えば、組織で、ネットワーク内の物理マシンに 4 つの Secure Agent、Amazon EC2 マシン上に 2 つの Secure Agent をインストールしているとします。ローカルエージェントの一部またはすべてを含む Secure Agent グループ、および EC2 エージェントを含む別のグループを作成できます。ローカルエージェントと EC2 エージェントの両方を含むグループを作成しないでください。

Secure Agent マシン上の出力ファイルにアクセスする必要がある場合は、ジョブの詳細を表示して、どの Secure Agent がタスクを実行したかを確認できます。ジョブの詳細を表示するには、モニタを開いて **[すべてのジョブ]** を選択し、ジョブ名をクリックします。

Secure Agent グループに対するサービスとコネクタの割り当て

組織で複数のサービスを使用している場合、Secure Agent グループが使用される頻度が高くなる可能性があります。Secure Agent グループが使用される頻度を減らすために、グループに対して特定の Secure Agent サービスを有効または無効にできます。または、組織がランタイム環境選択ライセンスを持っている場合は、組織にライセンスされている特定の Informatica Intelligent Cloud Services およびコネクタを有効または無効にすることができます。

組織のライセンスに応じて、次の操作を実行できます。

Secure Agent **グループに対して** Secure Agent **サービスを有効または無効にする。**

グループのエージェントに、サービスまたはサービスセットに関連付けられた接続、タスク、プロセス、または製品機能を実行させる場合は、Secure Agent サービスを有効にします。Secure Agent サービスを有効にすると、Secure Agent グループの各エージェントでサービスが起動します。

グループのエージェントに、サービスまたはサービスセットに関連付けられた接続、タスク、プロセス、または製品機能を実行させない場合は、Secure Agent サービスを無効にします。Secure Agent サービスを無効にすると、Secure Agent グループの各エージェントでサービスが停止します。Secure Agent グループをランタイム環境として使用する接続、タスク、プロセス、または製品機能は実行されなくなります。

Secure Agent **グループの** Informatica Intelligent Cloud Services **を有効または無効にします。**

組織がランタイム環境選択ライセンスを持っている場合は、グループ内のエージェントに、サービスに関連付けられたタスク、プロセス、および製品機能を実行させるときに、データ統合やアプリケーションの統合などのサービスを有効にできます。デフォルトでは、Secure Agent グループを作成すると、組織が使用ライセンスを持っているすべてのサービスとコネクタが無効になります。サービスを有効にすると、Secure Agent グループの各エージェントでサービスが起動します。

一部のサービスには、他のサービスまたはコネクタが必要です。他のサービスを必要とするサービスを有効にすると、Informatica Intelligent Cloud Services では必要なサービスが自動的に有効になります。例

えば、Secure Agent グループで Data Quality が有効になります。Data Quality にはデータ統合が必要です。Data Quality を有効にすると、Informatica Intelligent Cloud Services では自動的にデータ統合が有効になります。

グループ内のエージェントに、サービスに関連付けられたタスク、プロセス、または製品機能を実行させない場合は、サービスを無効にします。サービスを無効にすると、Secure Agent グループの各エージェントでサービスが停止します。Secure Agent グループをランタイム環境として使用する接続、タスク、プロセス、または製品機能は実行されなくなります。

Secure Agent **グループに対して接続を有効または無効にする。**

組織がランタイム環境選択ライセンスを持っている場合は、グループ内のエージェントに、クラウドおよびオンプレミスのアプリケーション、プラットフォーム、データベース、およびフラットファイルと通信できるようにするときに、特定のコネクタを有効にできます。コネクタを有効にすると、グループ内のすべてのエージェントで、コネクタに関連付けられたパッケージがダウンロードされます。

グループ内のエージェントに、コネクタに関連付けられたパッケージをダウンロードさせない場合は、コネクタを無効にします。コネクタを無効にすると、ランタイム環境として Secure Agent グループを使用する接続は実行されなくなります。

Secure Agent **グループに対して追加のサービスを有効または無効にする。**

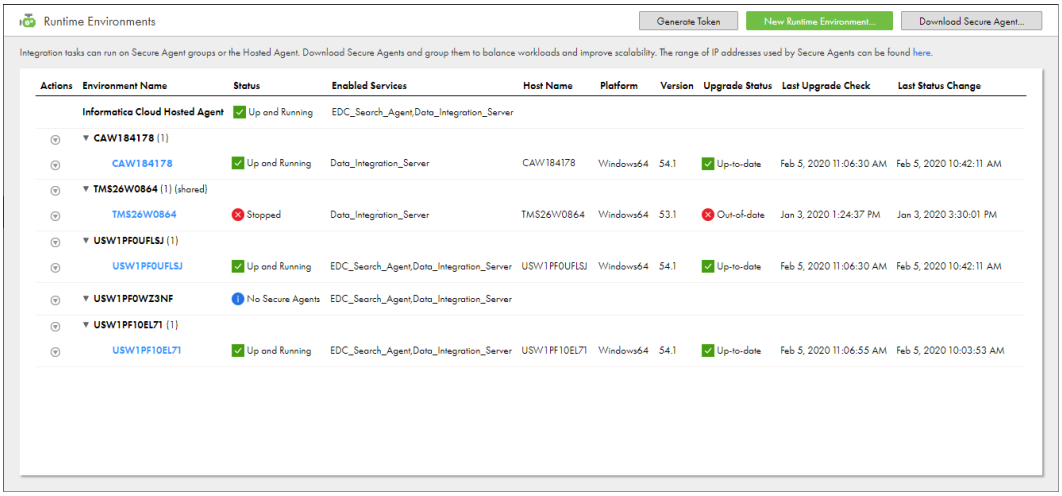
組織がランタイム環境選択ライセンスを持っている場合は、Self-Hosted GitRepo や EDC Integration などの追加サービスを有効または無効にできます。

また、Secure Agent グループ内の個々の Secure Agent に対して Secure Agent サービスを有効または無効にすることもできます。詳細については、「Secure Agent でのサービスの停止と開始」 (ページ 24)を参照してください。

Secure Agent サービスの詳細については、「*Secure Agent サービス*」を参照してください。

［ランタイム環境］ページで、Secure Agent グループに対してサービスと接続を有効または無効にします。

次の図は、**［ランタイム環境］**ページを示しています。



［有効なサービス］カラムに、Secure Agent グループに対して有効になっている Secure Agent サービスが示されます。Hosted Agent の［有効なサービス］カラムには、組織が使用ライセンスを持っているすべての Secure Agent サービスが一覧表示されます。

組織のライセンスに基づいて、次の方法で Secure Agent サービスを有効または無効にできます。

- Secure Agent グループの**［アクション］**メニューを展開し、**［サービスの有効化または無効化］**を選択します。

- 組織がランタイム環境選択ライセンスを持っている場合は、Secure Agent グループのサービスを有効にすると、サービスに関連付けられているすべての Secure Agent サービスがグループ内のすべての Secure Agent で自動的に開始されます。それぞれのエージェントで Secure Agent サービスを開始または停止します。詳細については、「*Secure Agent サービス*」を参照してください。

Secure Agent グループにサービス割り当てを行った後、エージェントを追加または削除できます。グループに Secure Agent を追加すると、エージェントは追加先グループのサービス割り当てを継承します。

例

組織はデータ統合を使用しており、一括取り込みおよび Enterprise Data Catalog データ検出のライセンスを持っています。組織では、次の Secure Agent グループを使用しています。

- グループ 1: Secure Agent 1、Secure Agent 2、Secure Agent 3
- グループ 2: Secure Agent 4
- グループ 3: Secure Agent 5

デフォルトでは、組織のユーザーは任意のグループを接続またはタスク（ファイル取り込みタスクを含む）のランタイム環境として選択できます。管理者は、任意のグループを Enterprise Data Catalog との統合のランタイム環境として選択することもできます。

Secure Agent グループ間の負荷を分散するために、グループ 1 をファイル取り込みタスクを除くデータ統合タスクに予約し、グループ 2 をファイル取り込みタスクに予約し、グループ 3 をデータカタログ検出に予約することができます。

そのために、次の Secure Agent サービスを有効または無効にすることができます。

Secure Agent **グループ**	**有効なサービス**	**無効なサービス**
グループ 1	データ統合サーバー	一括取り込み、EDC 検索エージェント
グループ 2	一括取り込み	データ統合サーバー、EDC 検索エージェント
グループ 3	EDC 検索エージェント	データ統合サーバー、一括取り込み

タスクおよび機能の失敗を回避するために、次の設定も確認する必要があります。

- データ統合タスクを除くすべてのデータ統合タスクが、グループ 1 をランタイム環境として使用している。これらのタスクで使用する接続もすべて、グループ 1 をランタイム環境として使用している。
- すべてのファイル取り込みタスクが、グループ 2 をランタイム環境として使用している。これらのタスクで使用する接続もすべて、グループ 2 をランタイム環境として使用している。
- 管理者の **[組織]** ページで、Enterprise Data Catalog 統合プロパティがグループ 3 をランタイム環境として使用している。

サービス割り当てのガイドライン

Secure Agent グループに対してサービスまたは Secure Agent サービスを有効または無効にする場合は、次のガイドラインを使用します。

- サービスを無効にする前に、グループをランタイム環境として使用する接続、タスク、またはプロセスでサービスが使用されていないことを確認します。

  接続、タスク、またはプロセスで Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、そのタスクまたはプロセスは実行できません。例えば、マッピングソースの接続でランタイム環境 RuntimeEnv1 を使用しているとします。RuntimeEnv1 でデータ統合サーバーを無効にすると、マッピングタスクは実行時に失敗します。
- サービスを無効にする前に、グループをランタイム環境として使用する機能がサービスを必要としていないことを確認します。

  機能で Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、その機能は使用できません。例えば、Enterprise Data Catalog 統合のランタイム環境が RuntimeEnv2 に設定されているとします。RuntimeEnv2 で EDC 検索サービスを無効にすると、データカタログ検索を実行できなくなります。
- 接続を作成する際は、必要なサービスが有効化されているランタイム環境を選択します。

  例えば、ファイル取り込みタスクターゲットに高度な SFTP 接続を作成するとします。接続を作成する際は、一括取り込みサービスが有効化されているランタイム環境を選択します。
- Secure Agent では、サービスを無効にして一時的に停止する事はしないでください。Secure Agent でのサービスの一時的な停止に関する詳細については、「Secure Agent でのサービスの停止と開始」 (ページ 24)を参照してください。
- 接続プロパティをローカルに保存するように組織を設定する場合は、Secure Agent グループに対してデータ統合サービスを有効にする必要があります。

Secure Agent グループの共有

親組織の管理者は、Secure Agent グループをサブ組織と共有できます。Secure Agent グループを共有すると、すべてのサブ組織がグループ内の Secure Agent でデータ統合ジョブを実行出来るようになります。

注: グループ内のすべてのエージェントでデータ統合サーバーのサービスのみを実行する場合は、Secure Agent グループを共有します。Secure Agent グループの共有で非データ統合ジョブを実行する事は出来ません。

Secure Agent グループを共有すると、使用可能な Secure Agent リソースを最大限に活用できます。例えば、タイムゾーンが異なる部門の別々のサブ組織が組織に含まれているとします。各サブ組織は、1 日の中の異なる時間にデータ統合タスクを実行します。サブ組織ごとに 1 つの Secure Agent グループを作成すると、時間帯によっては、使用負荷が高い Secure Agent グループと、アイドル状態の Secure Agent グループが混在する場合があります。タスクをより均等に分散するには、Secure Agent を Secure Agent グループに追加して、その Secure Agent グループをサブ組織と共有します。

Secure Agent グループを共有するには、適切なライセンスが必要です。

Secure Agent グループを共有すると、そのグループがすべてのサブ組織の［**ランタイム環境**］ページに表示されます。サブ組織の管理者が、グループ内の Secure Agent を表示することはできません。また、Secure Agent の追加や削除、グループの名前変更、削除、共有解除、グループ権限の変更などのグループ管理タスクを行うこともできません。

サブ組織のユーザーが接続またはタスクを作成すると、そのユーザーはランタイム環境に Secure Agent グループの共有を選択出来ます。

共有された Secure Agent グループでのフラットファイル接続

共有された Secure Agent グループに複数の Secure Agent が含まれている場合、このグループをフラットファイル接続用のランタイム環境として使用するときは、グループ内のすべての Secure Agent が、接続で使用されるディレクトリにアクセスできる必要があります。

すべての Secure Agent がこのディレクトリにアクセスできない場合は、Secure Agent に割り当てられている、その接続を使用するタスクが失敗します。

Secure Agent グループの操作

［ランタイム環境］ページで Secure Agent グループを作成します。Secure Agent グループの作成後は、グループの名前変更または削除、Secure Agent の追加と削除、およびグループ権限の変更を行うことができます。組織がランタイム環境選択ライセンスを持っている場合は、グループに対するサービスとコネクタを有効にすることもできます。

次のタスクを実行できます。

Secure Agent **グループを作成する。**

Secure Agent グループを作成するには、**［新しいランタイム環境］**をクリックし、グループの名前を入力します。グループを作成した後、グループに Secure Agent を追加できます。

Secure Agent **グループの名前を変更する。**

Secure Agent グループの名前を変更するには、［アクション］メニューを展開して**［Secure Agent グループの名前変更］**を選択し、グループの新しい名前を入力します。Informatica Intelligent Cloud Services は、そのグループを使用するすべてのサービスでグループ名を更新します。

Secure Agent **グループに対して** Secure Agent **サービスを有効または無効にする。**

組織がランタイム環境選択ライセンスを持っている場合は使用できません。

Secure Agent グループに対して Secure Agent サービスを有効または無効にするには、［アクション］メニューを展開して**［サービスの有効化または無効化］**を選択し、有効または無効にするサービスを選択します。組織が使用ライセンスを持っているサービスを有効または無効にできます。

注: サービスを無効にする前に、グループをランタイム環境として使用する接続、タスク、またはプロセスでサービスが使用されていないことを確認します。接続、タスク、またはプロセスで Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、そのタスクまたはプロセスは実行できません。同様に、機能で Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、その機能は使用できません。

Secure Agent **グループの特定の** Informatica Intelligent Cloud Services **およびコネクタを有効または無効にします。**

組織がランタイム環境選択ライセンスを持っている場合に使用できます。

Secure Agent グループに対してサービスを有効または無効にするには、［アクション］メニューを展開し、**［サービスおよびコネクタの有効化または無効化］**を選択します。**［サービス］**タブで、有効または無効にするサービスを選択します。組織が使用ライセンスを持っているサービスを有効または無効にできます。

注: サービスを無効にする前に、グループをランタイム環境として使用する接続、タスク、またはプロセスでサービスが使用されていないことを確認します。接続、タスク、またはプロセスで Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、そのタスクまたは

プロセスは実行できません。同様に、機能で Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、その機能は使用できません。

コネクタを有効または無効にするには、［アクション］メニューを展開し、**［サービスおよびコネクタの有効化または無効化］**を選択します。**［コネクタ］**タブで、有効または無効にするコネクタを選択します。組織が使用ライセンスを持っているコネクタを有効または無効にできます。

Self-Hosted Git Repo などの追加サービスを有効または無効にするには、［アクション］メニューを展開し、**［サービスおよびコネクタの有効化または無効化］**を選択します。**［追加サービス］**タブで、有効または無効にするサービスを選択します。組織が使用ライセンスを持っているサービスを有効または無効にできます。

Secure Agent **をグループに追加する。**

Secure Agent をグループに追加するには、［アクション］メニューを展開し、**［Secure Agent の追加または削除］**を選択します。**［ランタイム環境］**ページの［未割り当て状態のエージェント］グループにある任意のエージェントを追加できます。

または、エージェントを登録する前に infaagent.ini ファイルの InfaAgent.GroupName プロパティを設定することで、既存のグループに新しい Secure Agent を追加できます。Secure Agent を Secure Agent グループに追加すると、Secure Agent は Secure Agent グループ用に設定されたサービスとコネクタを継承します。

Secure Agent グループに複数の Secure Agent を追加する場合、すべてのエージェントは次の要件を満たしている必要があります。

- すべてのエージェントは、すべてローカルエージェントである、またはすべて Amazon EC2 マシンで実行されているなど、同じ種類である必要がある。
- 各 Secure Agent は、同じ外部システムに接続し、ライブラリ、初期化ファイル、および JAR ファイルなどのファイルへのアクセス権を持つように設定されている。
- 各 Secure Agent は、タスクで使用するファイルにアクセスできる必要がある。タスクで使用されるファイルが共有場所でも使用可能なことを確認する。

Secure Agent **をグループから削除する。**

Secure Agent をグループから削除するには、［アクション］メニューを展開し、**［Secure Agent の追加または削除］**を選択します。グループからエージェントを削除すると、Informatica Intelligent Cloud Services で「Unassigned Agents（未割り当て状態のエージェント）」という名前のグループにエージェントが追加されます。

グループが接続またはタスクでランタイム環境として使用されていない場合は、Secure Agent グループからエージェントを削除できます。グループが使用されている場合、そのグループ内の唯一のエージェントでない場合は、エージェントを削除できます。

Secure Agent **グループを削除する。**

Secure Agent グループを削除するには、［アクション］メニューを展開し、**［Secure Agent グループの削除］**を選択します。Secure Agent グループは、Secure Agent が含まれていない場合には削除できます。

Secure Agent グループが詳細設定に関連付けられており、詳細クラスタが実行されている場合は、グループを削除する前にクラスタを停止し、この構成を別のランタイム環境に関連付ける必要があります。

Secure Agent **グループを共有または共有解除する。**

親組織の管理者が Secure Agent グループを共有すると、サブ組織は、その Secure Agent グループを使用できるようになります。接続またはタスクで使用されていないグループは、共有解除できます。グループに関連付けられている［アクション］メニューから、**［Secure Agent グループの共有］**または**［Secure Agent グループの共有解除］**を選択します。

Secure Agent **グループの権限を変更する。**

Secure Agent グループの権限を変更するには、［アクション］メニューを展開し、**［権限の変更］**を選択します。組織のユーザーグループごとに Secure Agent グループの権限を定義できます。

次の権限を設定することができます。

権限	説明
読み取り	Secure Agent グループに関する詳細を表示し、タスクで Secure Agent グループを使用します。
更新	Secure Agent グループを編集します。
削除	Secure Agent グループを削除します。
変更	Secure Agent グループの権限を変更します。

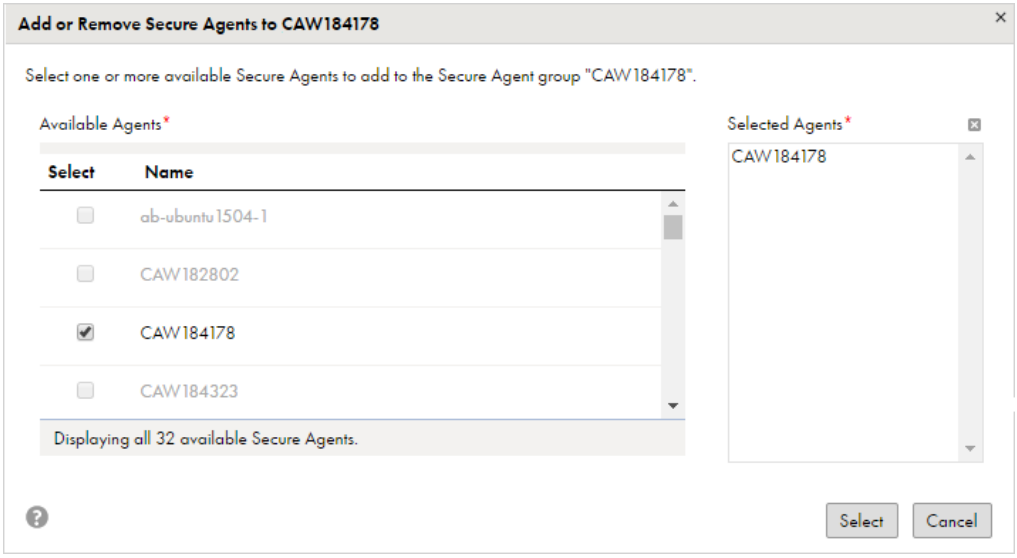
グループへの Secure Agent の追加

Secure Agent グループに、使用可能な任意の Secure Agent を追加できます。使用可能なエージェントは、**［ランタイム環境］**ページの「未割り当て状態のエージェント」グループに表示されます。Secure Agent がすでに別のグループに追加されている場合は、グループにエージェントを追加することはできません。

1. 管理者で、**［ランタイム環境］**を選択します。
2. Secure Agent グループの［アクション］メニューを展開し、**［Secure Agent の追加または削除］**を選択します。
3. **［使用可能なエージェント］**リストで、グループに追加する Secure Agent のチェックボックスをオンにします。

   ［使用可能なエージェント］リストでエージェント名が有効になっていない場合は、すべてのエージェントが他のグループに追加されます。エージェントを別のグループに追加するには、まずはグループからエージェントを削除する必要があります。

   チェックボックスを有効にすると、次の図に示すように、Secure Agent が **［選択したエージェント］**リストに示されます。



4. **［選択］**をクリックします。

既存のグループへの新規 Secure Agent の追加

エージェントをインストールしている場合、Secure Agent グループに Secure Agent を追加できます。既存のグループに Secure Agent を追加するには、エージェントを登録する前に infaagent.ini ファイルに InfaAgent.GroupName プロパティを追加します。

1. Secure Agent をインストールします。
2. Windows では、エージェントの登録を求められたときに Windows の[サービス]を開き、エージェントを停止します。

   Linux では、インストールプログラムが完了したときに、エージェントを起動しないようにします。
3. テキストエディタで<Secure Agent インストールディレクトリ>/apps/agentcore/conf/infaagent.ini を開きます。
4. 次のプロパティを追加してファイルを保存します。

   InfaAgent.GroupName=<Secure Agent グループ名>
5. エージェントを開始します。
6. エージェントを登録します。

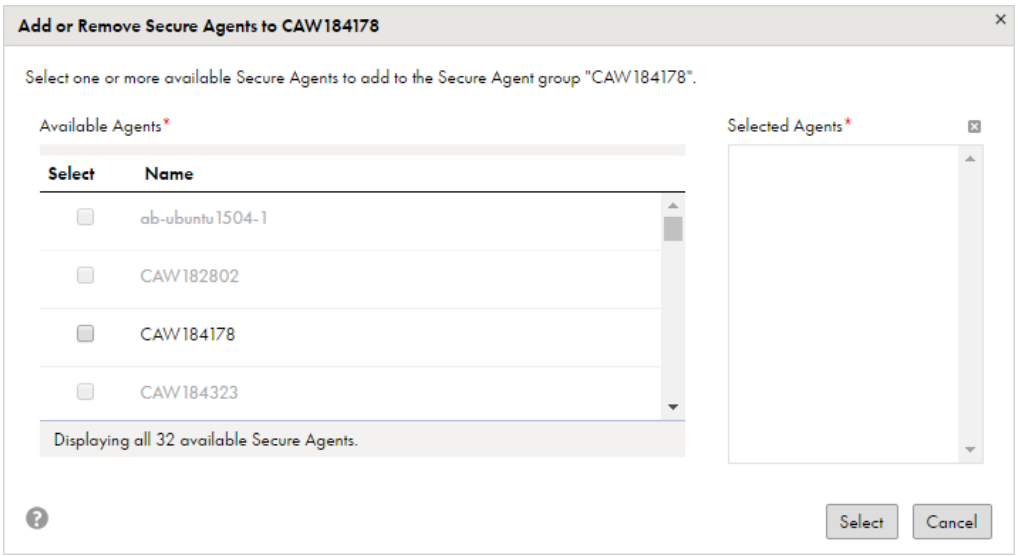
   Informatica Intelligent Cloud Services によって、新規グループではなく InfaAgent.GroupName プロパティで指定したグループに Secure Agent が追加されます。

グループからの Secure Agent の削除

グループが接続またはタスクで使用されていない場合は、Secure Agent グループからエージェントを削除できます。グループが接続またはタスクで使用されている場合、そのグループ内の唯一のエージェントでない場合は、エージェントを削除できます。グループから Secure Agent を削除すると、Informatica Intelligent Cloud Services によって Secure Agent が「未割り当て状態のエージェント」という名前のグループに追加されます。

1. 管理者で、**［ランタイム環境］**を選択します。
2. Secure Agent グループの［アクション］メニューを展開し、**［Secure Agent の追加または削除］**を選択します。
3. **［選択したエージェント］**の一覧で、グループから削除するエージェントを選択し、**［X］**をクリックします。

   次の図に示すように、削除した各エージェントのチェックボックスは無効になり、Secure Agent は **［選択したエージェント］**の一覧に表示されなくなります。



4. **［選択］**をクリックします。

［ランタイム環境］ページの「未割り当て状態のエージェント」グループに、Secure Agent が表示されます。

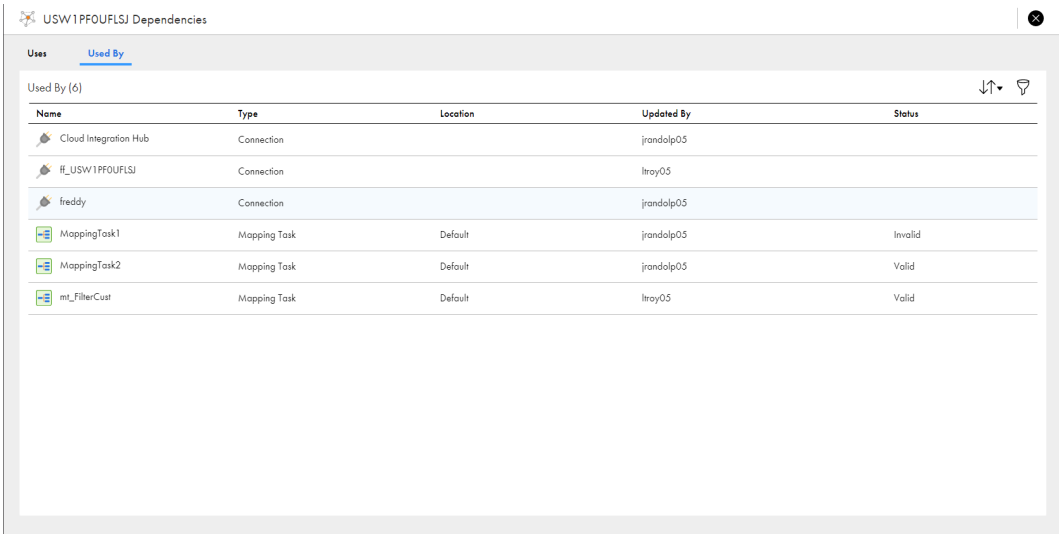
Secure Agent グループの依存関係の表示

Secure Agent グループのオブジェクトの依存関係を表示する事ができます。

Secure Agent グループの依存関係を表示する場合、管理者はランタイム環境としてグループを使用する各サービスの接続およびアセットのリストを表示します。

Secure Agent グループのオブジェクトの依存関係を表示するには、［アクション］メニューを展開し、**［依存関係の表示］**を選択します。

次の図に、Secure Agent グループの **［依存関係］**ページを示します。



ページに表示されるオブジェクトをソートするには、ソートアイコンをクリックし、ソート基準のプロパティのカラム名を選択します。

依存関係ページに表示されるオブジェクトをフィルタ処理するには、［フィルタ］アイコンをクリックします。フィルタを使用して特定のオブジェクトを見つけます。フィルタを適用するには、**［フィールドの追加］**をクリックし、フィルタ対象のプロパティを選択し、プロパティ値を入力します。複数のフィルタを指定できます。例えば、Oracle の接続を名前で見つけるには、［タイプ］フィルタを追加し、［接続］を指定します。次に、［名前］フィルタを追加し、「Oracle」と入力します。

第 4 章

Secure Agent

Informatica Cloud Secure Agent は、すべてのタスクを実行し、組織と Informatica Intelligent Cloud Services の間でファイアウォールを越えた安全な通信を可能にする軽量プログラムです。Secure Agent は、タスクを実行する場合、Informatica Cloud ホスティング機能に接続してタスク情報にアクセスします。ソースとターゲットに直接かつ安全に接続し、それらの間でデータを転送し、タスクのフローを調整し、プロセスを実行して、追加のタスク要件を実行します。

Secure Agent で Informatica Intelligent Cloud Services への接続が失われると、接続を再確立してタスクの継続を試みます。接続を再確立できない場合、タスクは失敗します。

Secure Agent は、データ処理にプラガブルサービスを使用します。例えば、データ統合サーバーはすべてのデータ統合ジョブを実行し、プロセスサーバーはアプリケーション統合を実行してオーケストレーションジョブを処理します。それぞれの Secure Agent サービスには、Tomcat 設定や Tomcat JRE 設定などの一意の設定プロパティセットがあります。Secure Agent サービスの詳細については、「*Secure Agent サービス*」を参照してください。

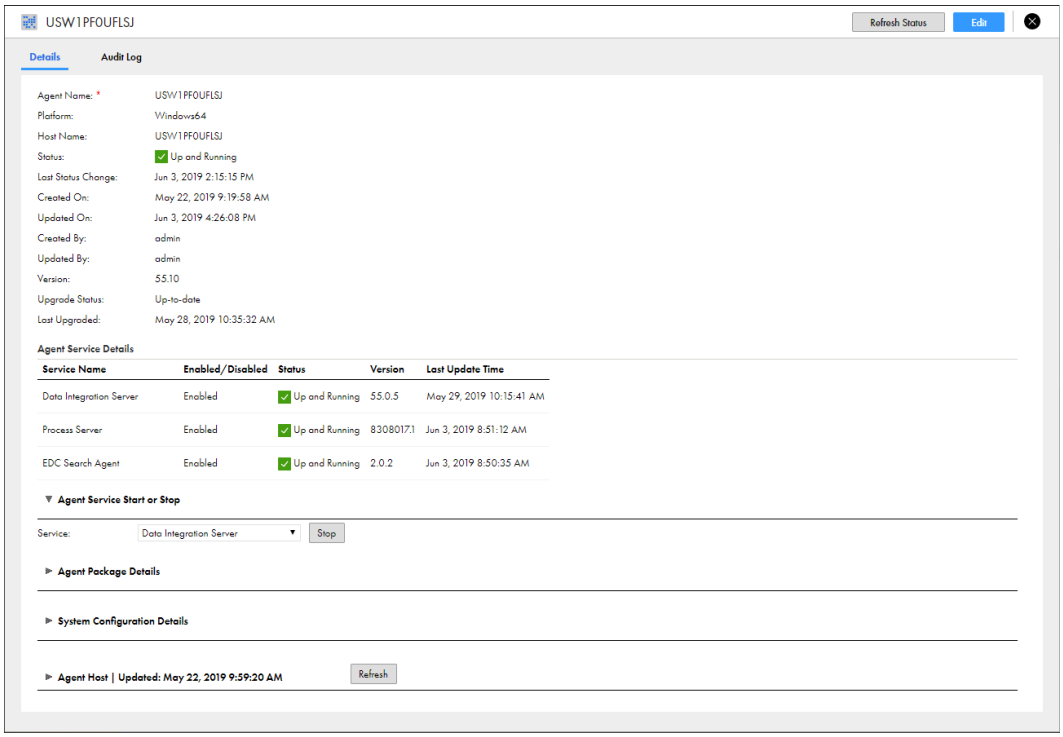
1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールして実行できます。Secure Agent をインストールすると、組織内のすべてのユーザーがその Secure Agent を共有します。Secure Agent のプロパティを設定し、別の Secure Agent グループに移動することができます。また、拡張性を向上させるために、Secure Agent グループに複数のエージェントを追加することもできます。

Secure Agent の操作

Secure Agent を作成したら、エージェントのプロパティの表示および構成、ホスト情報の確認、監査ログの表示、エージェントの状態の更新などの管理タスクを実行する必要があります。また、Secure Agent が使用されなくなった場合は、削除できます。

Secure Agent のほとんどの管理タスクは、エージェントの詳細ページで実行します。エージェントの詳細ページにアクセスするには、**［ランタイム環境］**ページで Secure Agent をクリックします。

次の図に、エージェントの詳細ページを示します。



次のタスクを実行できます。

Secure Agent **の詳細を表示する。**

ホスト名、現在のステータス、エージェントの最終更新日時、およびエージェントバージョンなどの詳細を表示します。

Secure Agent は、次のいずれかのステータスを持つことができます。

ステータス	説明
Agent Core は実行されていません。	Secure Agent は使用できませんが、1 つ以上のサービスが実行されています。
実行されていないサービスがあります。	Secure Agent は使用可能ですが、使用できないサービスが 1 つ以上あります。
Agent Core のアップグレード中	Secure Agent は新しいバージョンにアップグレード中です。
停止	Secure Agent を使用できません。
稼働中	Secure Agent、およびそのエージェントが実行するすべてのサービスが使用可能です。

Secure Agent **サービスの詳細を表示する。**

Secure Agent サービス名、状態、バージョン、最終更新時刻など、Secure Agent で実行されるサービスの詳細を表示します。

Secure Agent サービスのステータスには、次のようなものがあります。

ステータス	説明
エラー	プロセスが失敗しました。
エラーによる再起動中	サービスはエラーが発生したため起動中です。
シャットダウン中	サービスがシャットダウンしています。
スタンバイ	サービスは実行中ですが、Informatica Intelligent Cloud Services と互換性がありません。
起動中	サービスは起動中です。
停止	サービスは使用できません。
稼働中	サービスは実行中です。
ユーザーが停止	サービスがユーザーによって停止されました。
警告	サービスは実行中ですが、操作を受け付けることができません。

サービスを変更するたびにバージョン番号が変更されます。Secure Agent では、旧バージョンのサービスのディレクトリが 7 日間維持されます。例えば、バージョン 55.0.2 のデータ統合サーバーの NetworkTimeoutPeriod を更新すると、エージェントはバージョン番号を 55.0.3 に上げ、次のディレクトリを作成します。

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

7 日間後、<Secure Agent installation directory>/apps/Data_Integration_Server/55.0.2.x ディレクトリは削除されます。

Secure Agent **サービスを停止および開始する。**

Secure Agent で実行するサービスを停止および開始し、トラブルシューティングの実行、エージェントマシンでのリソースの最適化、またはサービス設定の変更を行います。Secure Agent サービスを停止または開始しても、エージェントで実行されている他のサービスは影響を受けません。

Secure Agent **パッケージを表示する。**

[エージェントパッケージの詳細] セクションを展開して、Secure Agent で実行する各サービスのパッケージの名前とバージョン番号を確認します。サービスごとにパッケージをフィルタ処理できます。

Secure Agent **サービスプロパティを表示および編集します。**

[システム構成の詳細] セクションを展開すると、Secure Agent サービスプロパティが表示されます。プロパティは、サービスとタイプでフィルタリングできます。

プロパティを構成するには、**[編集]** をクリックします。Secure Agent で実行される各サービスのプロパティを設定できます。コネクタで使用されるカスタムプロパティを追加および削除することもできます。Secure Agent サービスとサービスプロパティの詳細については、「*Secure Agent サービス*」を参照してください。カスタムプロパティの詳細については、該当するコネクタのヘルプを参照してください。

Secure Agent **ホストのプロパティを表示する。**

[エージェントホスト] セクションを展開し、Secure Agent をホストするマシンに関する情報を表示します。例えば、マシン名、オペレーティングシステム、および使用可能なディスク領域を表示できます。

情報を更新するには、**[更新]** をクリックします。情報が更新された最後の日時が、**[エージェントホスト | 更新済み]** 見出しの横に表示されます。

監査ログを表示する。

開始時間と終了時間、サーバー接続、およびアップグレードメッセージなどの監査情報を表示するには、**[監査ログ]** をクリックします。

Secure Agent **のステータスを更新する。**

Secure Agent の状態を更新するには、ページの右上隅にある **[状態の更新]** をクリックします。

Linux では、次のディレクトリに移動してステータスを表示することもできます。

<Secure Agent のインストールディレクトリ>/apps/agentcore

次に、次のコマンドのいずれかを実行します。

- consoleAgentManager.sh getstatus
- consoleAgentManager.sh updatestatus

Secure Agent でのサービスの停止と開始

デフォルトでは、組織内の各 Secure Agent は、組織内のデータ処理で使用するすべてのマイクロサービスを実行します。トラブルシューティングの実行、エージェントマシンのリソースの最適化、または設定の変更を行う場合は、マイクロサービスを停止および開始します。Secure Agent マイクロサービスを停止または開始しても、エージェントで実行されている他のマイクロサービスは影響を受けません。

Secure Agent で停止および開始するマイクロサービスは Secure Agent サービスであるため、Informatica Intelligent Cloud Services とは異なります。例えば、オペレーションインサイトに関連するサービスを停止する場合、OI データコレクタサービスをエージェントで停止する必要があります。Secure Agent サービスの詳細については、「*Secure Agent サービス*」を参照してください。

次の状況での Secure Agent サービスの停止および再起動が必要になる場合があります。

特定の Secure Agent **サービスの問題をトラブルシューティングする必要があります。**

Secure Agent サービスでエラー状態が表示された場合は、サービスを停止し、問題をトラブルシューティングしてから、サービスを再開します。

メモリまたは CPU **負荷の高いジョブを実行する場合、**Secure Agent **マシンの計算リソースを最適化します。**

例えば、組織でデータ統合ジョブおよびアプリケーションの統合ジョブを実行します。データ統合ジョブを昼間に、アプリケーションの統合ジョブを夜間に実行するように、計算リソースを最適化します。このためには、プロセスサーバーを昼間停止し、夜間に再起動して、データ統合サーバーを夜間に停止し、早朝再起動します。

ファイル統合サービスのサービス設定プロパティを更新します。

ファイル統合サービスの設定プロパティを変更すると、サービスを再起動する必要があります。Secure Agent が他のサービスを実行している場合、他のサービスに影響を与えずにファイル統合サービスを停止および再起動できます。

Secure Agent のサービスを開始または停止するには、Secure Agent で権限を更新しておく必要があります。

下位組織の管理者である場合は、下位組織のエージェントでサービスを開始および停止できます。ただし、Secure Agent 共有グループ内の Secure Agent でサービスを開始および停止する事は出来ません。

サービスを開始および再起動するたびに、Secure Agent はサービス関連ファイルの新しいサブディレクトリを作成します。例えば、Secure Agent がバージョン 12.1 の B2B Processor Service を使用する場合、Secure Agent のインストールディレクトリには次のサブディレクトリが含まれます。

<Secure Agent インストールディレクトリ>/apps/B2BProcessor/12.1.1

B2B Processor Service を停止および再起動すると、Secure Agent は次のディレクトリを作成します。

<Secure Agent インストールディレクトリ>/apps/B2BProcessor/12.1.2

Secure Agent はディレクトリ .../12.1.1 を削除しません。

例

組織でデータ統合を使用し、Enterprise Data Catalog 統合、ファイル統合、および一括取り込みのライセンスを使用します。

Secure Agent は、次の Secure Agent サービスを実行します。

- データ統合サーバー
- EDC 検索エージェント
- ファイル統合サービス
- 一括取り込み

Enterprise Data Catalog 検索に問題がある場合、トラブルシューティングを実行しながら EDC Search Agent サービスを停止する事ができます。EDC Search Agent サービスを停止すると、データ統合でデータカタログ検索を実行出来ません。ただし、マッピング、タスク、タスクフローなど、このエージェントの他のサービスで処理されるジョブ、および AS2 ファイルの転送は継続されます。

Secure Agent サービスを停止および開始するためのガイドライン

Secure Agent でサービスを停止および開始する際は、次のガイドラインを使用します。

- Secure Agent サービスを停止する場合は、ジョブの失敗を引き起こす可能性があるため、注意が必要です。

  Secure Agent サービスを停止すると、そのサービスを必要とするジョブ、およびエージェント上で現在実行中のジョブがすべて停止します。グループ内に他のエージェントがない場合、ジョブを実行出来なくなります。グループ内に他のエージェントがある場合、そのジョブを再開すると別のエージェントで実行されるようになります。
- エージェントに接続プロパティを保存している場合は、そのエージェント上のデータ統合サーバーを停止しないでください。

  ローカルの Secure Agent に接続プロパティを保存している場合にそのエージェント上のデータ統合サーバーを停止すると、ユーザーが組織内の接続にアクセスする事もタスクを実行する事も出来なくなります。また、エージェント上で現在実行中のジョブも失敗します。
- 特定のタイプのジョブの Secure Agent グループを保持するためにサービスを開始したり停止したりしないでください。

  特定のタイプのジョブの Secure Agent グループを保持する場合は、Secure Agent グループで必要なサービスを有効にし、その他のサービスを無効にできます。Secure Agent グループのサービスの有効化および無効化に関する詳細については、「Secure Agent グループに対するサービスとコネクタの割り当て」 (ページ 12)を参照してください。

Secure Agent サービスの停止

「稼働中」または「エラー」状態の Secure Agent サービスを停止できます。Secure Agent サービスを停止すると、稼働中のすべてのバージョンのサービスが停止します。サービスの停止後、最新バージョンのサービスを開始する事ができます。

注: Secure Agent サービスを停止してから Secure Agent を再開した場合、サービスはユーザーが開始するまで停止状態となります。

1. 管理者で、**［ランタイム環境］**を選択します。
2. **［ランタイム環境］**ページで、Secure Agent の名前をクリックします。

   注: Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
3. **［詳細］**タブをクリックします。
4. **［Agent Service の開始または停止］**領域で、停止するサービスを選択します。
5. **［停止］**をクリックします。

Secure Agent サービスが停止し、Informatica Intelligent Cloud Services では、サービスがユーザーによって停止されたことを示すエントリが監査ログに追加されます。

Secure Agent サービスの開始

「停止」状態の Secure Agent サービスを開始できます。Secure Agent サービスを開始すると、サービスの最新バージョンが開始されます。

1. 管理者で、**［ランタイム環境］**を選択します。
2. **［ランタイム環境］**ページで、Secure Agent の名前をクリックします。

   注: Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
3. **［詳細］**タブをクリックします。
4. **［エージェントサービスの開始または停止］**領域で、起動するサービスを選択します。
5. **［開始］**をクリックします。

Informatica Intelligent Cloud Services は、Secure Agent サービスの開始を試行します。サービスが起動すると、ステータスが「稼働中」に変わります。Secure Agent サービスでの開始が失敗する場合は、監査ログを確認してエラーの原因を特定します。

エージェントのブラックアウト期間の設定

Secure Agent のブラックアウト期間を設定できます。ブラックアウト期間によって、一定期間中にデータ統合ジョブがエージェント上で実行されないようにします。エージェントのブラックアウト期間を設定し、エージェント上でデータ統合ジョブを実行出来ないようにする具体的な時間、日数、または間隔を指定します。

エージェントのブラックアウト期間によって、データ統合サーバーサービスでは当該期間中の Secure Agent 上でのジョブの実行が停止します。エージェント上のその他のタイプのジョブが実行されなくなる事はありません。エージェントのブラックアウト期間は、以下のような状況の場合に設定します。

- データ統合サーバーがエージェント上で唯一有効になっているサービスであり、一定期間中のすべてのデータ統合ジョブの実行を停止する必要がある。

- Secure Agent で複数のサービスを実行しているが、一定期間データ統合ジョブの実行のみを停止する必要がある。

注: エージェントのブラックアウト期間は、組織のスケジュールブラックアウト期間とは異なります。組織のスケジュールブラックアウト期間中は、いずれのエージェント上でもジョブを実行する事は出来ません。スケジュールのブラックアウト期間の詳細については、「*組織の管理*」を参照してください。

Secure Agent 上でブラックアウト期間を設定するには、ブラックアウトファイルを作成する必要があります。ブラックアウトファイルは、各ブラックアウト期間の繰り返し頻度、および開始日と終了日を指定する XML ファイルです。

例えば、以下のブラックアウトファイルには、2021 年 7 月 27 日午前 5 時～2021 年 7 月 28 日午後 11 時というブラックアウト期間と、金曜日の午後 2 時～4 時に繰り返すというブラックアウト期間が含まれています。

```
<?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>
```

1 つ以上のブラックアウト期間を設定するには、Secure Agent を実行するマシンの次のディレクトリに「blackoutWindows.dat」という名前のファイルを作成します。

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

Secure Agent が Secure Agent グループに含まれている場合は、ブラックアウトファイルをグループ内の各エージェントマシンの...\conf\ディレクトリにコピーします。

別のファイル名やディレクトリを使用する場合は、このファイル名とファイルパスを上書きしてください。

ブラックアウトファイルを作成すると、Secure Agent 上のデータ統合サーバーサービスが再開され、ブラックアウト期間が有効になります。

ブラックアウトファイル名およびディレクトリの上書き

ブラックアウトファイル名およびディレクトリを上書きできます。

上書きするには、エージェントの詳細ページでデータ統合サーバーの以下のカスタムプロパティを設定します。

サービス	タイプ	名前	値
データ統合サーバー	Tomcat	BlackoutWindowsFile	ブラックアウトファイルのファイルパスとファイル名。以下に例を示します。 C:/AgentBlackouts/Agent001Blackouts.dat **注:** Secure Agent ではバックスラッシュ（\）をエスケープ文字と解釈するため、Windows マシンでも UNIX マシンでもファイルパスにはスラッシュ（/）を使用してください。 Secure Agent からアクセスできるファイルパスにする必要があります。

Secure Agent サービスのカスタムプロパティの構成の詳細については、「*Secure Agent サービス*」を参照してください。

ブラックアウトファイルの構造

ブラックアウトファイルは、各ブラックアウトの期間とその頻度、および各ブラックアウト期間の開始時刻と終了時刻を定義する要素が含まれた XML ファイルです。

ブラックアウトファイルの構造は次のとおりです。

```
<?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>
```

ファイルには、以下の要素が含まれます。

要素	必須/オプション	説明
BlackoutWindows	必須	ブラックアウト期間ごとに BlackoutWindow 要素が含まれています。 BlackoutWindow 要素は 1 つ以上含まれている必要があります。
BlackoutWindow	必須	ブラックアウト期間を 1 つ定義します。 RepeatFrequency 要素、Start 要素、End 要素を 1 つずつ含める必要があります。
RepeatFrequency	必須	ブラックアウト期間の繰り返し頻度。 次のいずれかの値を含める必要があります。 - 1 回 - 日次 - 平日 - 日曜日 - 月曜日 - 火曜日 - 水曜日 - 木曜日 - 金曜日 - 土曜日
Start	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の開始時刻。例: 2019-07-25 10:26:55。 タイムゾーンは Secure Agent ゾーンです。
End	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の終了時刻。例: 2019/07/26 11:45:00。 タイムゾーンは Secure Agent ゾーンです。

要素値は引用符で囲まないで下さい。

Secure Agent の名前変更

デフォルトでは、Secure Agent の名前はエージェントをインストールしたマシンの名前と同じです。エージェント名は変更できます。

1. **［ランタイム環境］**ページで、Secure Agent の名前をクリックします。

   注: Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
2. **［詳細］**タブをクリックします。
3. 右上隅の **［編集］**をクリックします。
4. **［エージェント名］**フィールドに新しい名前を入力します。
5. **［保存］**をクリックします。

Secure Agent の削除

タスクを実行するのに必要ではなくなった場合は、Secure Agent を削除します。**［ランタイム環境］**ページで、Secure Agent を削除します。

注: 接続またはタスクで使用されている場合は、Secure Agent を削除することはできません。例えば、Secure Agent がグループ内の唯一のエージェントであり、そのグループが接続またはタスクの実行時環境として使用されている場合、エージェントを削除することはできません。

1. 管理者で **［ランタイム環境］**を選択します。
2. Secure Agent の［アクション］メニューを展開し、**［Secure Agent の削除］**を選択します。

   Secure Agent が実行中の場合には、警告メッセージが表示されます。アクティブな Secure Agent を停止すると、その Secure Agent に関連付けられているスケジュール済みタスクの実行が阻まれます。Secure Agent が不要な場合は、警告を無視します。

Secure Agent が不要になった場合は、削除した後、Secure Agent をアンインストールします。

Secure Agent のアップグレード

Secure Agent は、新しい Informatica Intelligent Cloud Services リリースに初めてアクセスしたときに自動でアップグレードされます。アップグレードプロセスは、Secure Agent の新しいバージョンをインストールし、コネクタパッケージを更新し、エージェント上で実行されるマイクロサービスの構成の変更を適用します。Secure Agent を手動でアップグレードする必要はありません。

ただし、アップグレードを準備するため、アップグレードに利用可能なディスク空き容量が各 Secure Agent マシンにあることを確認するなどのタスクを実行する必要があります。アップグレードの準備の詳細については、『*管理者の新機能*』を参照してください。

Secure Agent のデータ暗号化

Secure Agent は、Secure Agent ディレクトリに保存されている機密データを暗号化します。このデータの暗号化に使用されるキーを変更できます。

Secure Agent をインストールすると、Secure Agent ディレクトリ内の一部のファイルには、エージェントの資格情報、エージェントプロキシの資格情報、JDK キーストアパスワードなどの機密データが含まれます。Secure Agent に接続を保存すると、Secure Agent マシン上のファイルにも接続資格情報が保存されます。この情報は、Secure Agent に固有のキーを使用して暗号化されます。

暗号化キーにはマシン固有の情報がいくつか使用されます。これにより、攻撃者がマシン上の Secure Agent ディレクトリを別のマシンにコピーしても、そのマシンでエージェントを起動することはできません。

デフォルトでは、暗号化キーは次のプロパティを使用して生成されます。

- Secure Agent マシンのオペレーティングシステム
- マシンアーキテクチャ（32 ビット、64 ビット、64 ビット ARM など）
- マシンのホスト名
- ハードウェア MAC アドレス

これらのプロパティの一部が暗号化キーの生成に使用されないようにすることができます。例えば、あるマシンでエージェントをバックアップして別のマシンでリストアする予定がある場合、ホスト名とハードウェア MAC アドレスを除外することができます。また、他のプロパティを追加して、暗号化の安全性を高めることもできます。例えば、Secure Agent が Amazon Web Services にインストールされている場合、インスタンス ID または AMI ID を追加できます。

暗号化キーはいつでも変更できます。変更するには、consoleAgentManager rotateDeviceKey コマンドを使用します。

このコマンドは次のアクションを実行します。

- infaagent.ini ファイルと proxy.ini ファイルを再暗号化します。
- 接続マスタキーを再暗号化します。
- 次回の起動時に Secure Agent サービスを強制的に再デプロイします。

コマンドの実行後に、次の環境変数も設定する必要があります。

環境変数	説明
INFA_AGENT_EXCLUDE_SEC_PROPS	除外するプロパティを指定します。rotateDeviceKey コマンドで除外した同じ値を設定します。
INFA_AGENT_ADDITIONAL_SEC_PROPS	追加するプロパティを指定します。rotateDeviceKey コマンドで追加した同じ値を設定します。

Windows でのデータ暗号化キーの変更

Secure Agent のデータ暗号化キーを変更するには、consoleAgentManager rotateDeviceKey コマンドを使用します。

データ暗号化キーを変更する前に、Secure Agent のインストールディレクトリをバックアップしてください。

暗号化キーの変更に使用するユーザーアカウントには、Secure Agent のインストールディレクトリとそのサブディレクトリ内のファイルを削除する特権が必要です。

注: アップグレード中は、2 つのバージョンのデータ統合サーバーが実行される可能性があります。アップグレードが完了し、新しいバージョンのデータ統合サーバーのみが実行されている状態になるまでは、暗号化キーを変更しないでください。

1. Secure Agent を停止します。
2. 管理者としてコマンドプロンプトを開き、次のディレクトリに移動します。

   <Secure Agent のインストールディレクトリ>/apps/agentcore
3. 次のコマンドを実行します。

   consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<除外するセキュリティプロパティ> INFA_AGENT_ADDITIONAL_SEC_PROPS=<追加のセキュリティプロパティ>

   OS_TYPE、OS_ARCH、HOSTNAME、および HWD_MAC_ADDR の各プロパティは除外できます。複数のプロパティはカンマで区切ります。

   プロパティを追加する場合は、任意のキーと値のペアを指定できます。例えば、instanceId=<AWS インスタンス ID>,amiId=<AWS AMI ID>のように指定します。複数のプロパティはカンマで区切ります。

   例えば、Secure Agent マシンのホスト名とハードウェア MAC アドレスを暗号化キーから除外し、AWS インスタンス ID を追加するには、次のコマンドを実行します。

   consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS インスタンス ID>
4. コマンドが正常に完了したら、セキュリティプロパティを除外した場合は、システム環境変数 INFA_AGENT_EXCLUDE_SEC_PROPS を作成し、rotateDeviceKey コマンドで設定した値に設定します。
5. セキュリティプロパティを追加した場合は、システム環境変数 INFA_AGENT_ADDITIONAL_SEC_PROPS を作成し、rotateDeviceKey コマンドで設定した値に設定します。
6. マシンを再起動します。
7. Secure Agent が自動的に起動しない場合は、Secure Agent を再起動します。

Linux でのデータ暗号化キーの変更

Secure Agent のデータ暗号化キーを変更するには、consoleAgentManager rotateDeviceKey コマンドを使用します。

データ暗号化キーを変更する前に、Secure Agent のインストールディレクトリをバックアップしてください。

注: アップグレード中は、2 つのバージョンのデータ統合サーバーが実行される可能性があります。アップグレードが完了し、新しいバージョンのデータ統合サーバーのみが実行されている状態になるまでは、暗号化キーを変更しないでください。

1. Secure Agent を停止します。
2. 次のディレクトリに移動します。

   <Secure Agent のインストールディレクトリ>/apps/agentcore
3. 次のコマンドを実行します。

   。/consoleAgentManager.sh rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<除外するセキュリティプロパティ> INFA_AGENT_ADDITIONAL_SEC_PROPS=<追加のセキュリティプロパティ>

   OS_TYPE、OS_ARCH、HOSTNAME、および HWD_MAC_ADDR の各プロパティは除外できます。複数のプロパティはカンマで区切ります。

   プロパティを追加する場合は、任意のキーと値のペアを指定できます。例えば、instanceId=<AWS インスタンス ID>,amiId=<AWS AMI ID>のように指定します。複数のプロパティはカンマで区切ります。

例えば、Secure Agent マシンのホスト名とハードウェア MAC アドレスを暗号化キーから除外し、AWS インスタンス ID を追加するには、次のコマンドを実行します。

。/consoleAgentManager.sh rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS インスタンス ID>

4. コマンドが正常に完了したら、セキュリティプロパティを除外した場合は、ソース bash プロファイルに環境変数 INFA_AGENT_EXCLUDE_SEC_PROPS を作成し、rotateDeviceKey コマンドで設定した値に設定します。
5. セキュリティプロパティを追加した場合は、ソース bash プロファイルに環境変数 INFA_AGENT_ADDITIONAL_SEC_PROPS を作成し、rotateDeviceKey コマンドで設定した値に設定します。
6. Secure Agent を再起動します。

Secure Agent Manager

Windows に Secure Agent をインストールするときには、Informatica Cloud Secure Agent Manager もインストールします。Secure Agent が Windows サービスとして実行されます。Secure Agent Manager は、Windows の［スタート］メニューまたはデスクトップアイコンから起動できます。

Secure Agent Manager を使用すると、次のタスクを実行できます。

- Secure Agent の状態と、Secure Agent で実行されるサービスを表示します。
- Secure Agent を停止および再起動します。
- プロキシ設定や Windows の Secure Agent サービスログインなどの Windows 設定を構成します。

Secure Agent Manager には、Secure Agent のステータスと、Secure Agent が実行するサービスのステータスが表示されます。Secure Agent、または Secure Agent が実行するいずれかのサービスが起動または稼働していない場合、Secure Agent Manager には、警告メッセージとリンクが表示されます。このリンクをクリックすると、詳細を確認できます。

Secure Agent Manager を閉じると、Windows タスクバーが最小化され、即座にアクセスできる状態で表示されます。Secure Agent Manager を閉じても、Secure Agent は停止しません。Secure Agent Manager を最小化する場合は、Secure Agent Manager アイコンにカーソルを合わせると Secure Agent の状態を表示できます。

Secure Agent でのプロキシサーバーの使用

プロキシサーバーでは、セキュリティとパフォーマンス上の理由から、ネットワークサービスへの間接接続が許可されています。例えば、プロキシサーバーを使用してファイアウォールを通過できます。一部のプロキシではキャッシュメカニズムが提供されています。

Informatica Cloud Secure Agent にプロキシサーバーを設定するときは、Secure Agent Manager で必要最低限の設定を定義します。Informatica Intelligent Cloud Services は、次のファイルを更新して、手動で編集できる他のプロパティを追加します。

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

次のコードは、proxy.ini のデフォルトの内容を示しています。

```
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=
```

Informatica Cloud Secure Agent のプロキシサーバーを設定するときは、InfaAgent.NonProxyHost を設定して、プロキシから特定の IP アドレスとホスト名を除外できます。例えば、詳細モードで実行されるマッピングで、マネージド ID 認証を使用して Azure のソースまたはターゲットに接続する場合は、メタデータサービスの IP アドレスである 169.254.169.254 を除外します。

非プロキシホストを除外するためのプロキシの設定

proxy.ini ファイルで、InfaAgent.NonProxyHost プロパティを設定して、IP アドレスまたはホスト名を除外しますプロキシサーバーを最初に設定するとき、Informatica Intelligent Cloud Services はデフォルトで InfaAgent.NonProxyHost の値として localhost を追加します。

1. <Secure Agent installation directory>/apps/agentcore/conf/proxy.ini を開きます。
2. 除外する IP アドレスまたはホスト名を指定して、InfaAgent.NonProxyHost の値を更新します。

   例:

   - ローカル IP アドレス:

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

   - ホスト名:

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

   注: 区切り文字としてパイプ文字（|）を使用して、ホスト名と IP アドレスのリストを結合できます。ホスト名の左または IP アドレスの右に、ワイルドカードを入力することもできます。
3. 変更が有効になるように、Secure Agent を再起動します。

Windows での Secure Agent の停止および再起動

Secure Agent Manager に Secure Agent のステータスが表示されます。Secure Agent Manager を使用して、Secure Agent を停止または再起動することができます。

Windows の **[スタート]** メニューから Secure Agent Manager を起動します。Secure Agent Manager がアクティブである場合は、Windows タスクバーの通知領域にある Informatica Cloud Secure Agent Manager のアイコンをクリックして Secure Agent Manager を開くことができます。

Secure Agent Manager から Secure Agent を停止するには、**[停止]** をクリックします。Secure Agent を再起動するには、**[再起動]** をクリックします。アクションが完了すると、Secure Agent Manager にメッセージが表示されます。

Secure Agent Manager を閉じると、Windows タスクバーの通知トレイが最小化されます。Secure Agent Manager を閉じても、Secure Agent は停止しません。

Linux での Secure Agent の起動および停止

Linux マシンに Secure Agent プログラムをダウンロードした後は、Secure Agent を Linux プロセスとして実行できます。Linux で、Secure Agent プロセスを手動で起動します。

1. コマンドラインから次のディレクトリに移動します。

   `<Secure Agent installation directory>/apps/agentcore`
2. Secure Agent を起動するには、次のいずれかのコマンドを入力します。
   - 2022 年 10 月のリリースより前に Secure Agent のインストールプログラムをダウンロードした場合は、次のコマンドを入力します。

     `./infaagent startup`
   - 2022 年 10 月のリリースの期間中またはその後に Secure Agent のインストールをダウンロードした場合は、次のコマンドを入力します。

     `./infaagent.sh startup`
3. Secure Agent を停止するには、次のいずれかのコマンドを入力します。
   - 2022 年 10 月のリリースより前に Secure Agent のインストールプログラムをダウンロードした場合は、次のコマンドを入力します。

     `./infaagent shutdown`
   - 2022 年 10 月のリリースの期間中またはその後に Secure Agent のインストールをダウンロードした場合は、次のコマンドを入力します。

     `./infaagent.sh shutdown`

Secure Agent の状態は、Informatica Intelligent Cloud Services または Linux コマンドラインから確認できます。

注: 2022 年 10 月のリリース以降、`infaagent startup` コマンドと `infaagent shutdown` コマンドは非推奨となっています。これらのコマンドは、今後のリリースで削除される予定です。

廃止された機能はサポートされていますが、今後のリリースではサポートも廃止される予定です。この機能が廃止される前に、別の機能に移行するようお願いいたします。

Secure Agent のトラブルシューティング

Secure Agent をインストールしましたが、別のマシンにも Secure Agent をインストールしたいと考えています。どのようにすればよいでしょうか？

新しいマシンで、自分のログイン情報を使用してデータ統合に接続します。次に、Secure Agent をダウンロードしてインストールします。

Secure Agent のエラー

Secure Agent を開始しましたが、そのステータスが非アクティブになっています。

Secure Agent の開始には数分かかることがあります。ステータスは 5 秒ごとに更新されます。Secure Agent がアクティブにならない場合は、次のタスクを実行します。

- 組織がプロキシサーバーを使用してインターネットにアクセスする場合は、プロキシ設定が正しく設定されていることを確認します。

- Secure Agent をインストールしたディレクトリにある infaagent.log の詳細情報を表示します。

Secure Agent が正常にインストールされない、または開始されません。

Secure Agent が正常にインストールされないか開始されない場合は、次のタスクを実行します。

1. Secure Agent をインストールしたディレクトリにある infaagent.log で、インストールの詳細情報を確認します。
2. Windows で実行されている Secure Agent のイベントビューアで、アプリケーションログを表示します。

サービスの 1 つを正常に再起動した後に、エラーステータスが表示されます。

サービスがエラーステータスで失敗すると、サービスが正常に起動された後でも、サービスのエラーステータスが引き続き［エージェントサービスの詳細］に表示されることがあります。古いメッセージをクリーンアップする内部ジョブが実行されるまで、エラーはページに表示されます。このエラーは無視してかまいません。

Secure Agent をアンインストールしようとしていますが、Secure Agent のステータスは「稼動中」のままです。

最初に Secure Agent を停止せずに Secure Agent をアンインストールすると、Agent Core と他のサービスの実行が数分間継続することがあります。この問題を回避するには、Secure Agent を停止してからアンインストールします。

第 5 章

Secure Agent のインストール

Secure Agent は Windows または Linux にインストールできます。また、マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

インストールとアンインストールの手順は、オペレーティングシステムによって異なります。

Secure Agent を使用して、詳細モードのマッピングに基づくマッピングタスクを実行する場合は、Secure Agent をクラウドプラットフォームの Linux 仮想マシンにインストールするか、サーバーレスランタイム環境を使用します。

Windows での Secure Agent のインストール

Windows 上では、Secure Agent が Windows サービスとして実行されます。Secure Agent をインストールするときには、Informatica Cloud Secure Agent Manager もインストールします。

Secure Agent Manager または Windows サービスを使用して Secure Agent を停止および再起動できます。インストールプログラムの実行に使用するボリュームとは異なるボリュームに Secure Agent をインストールする場合は、Windows サービスから Secure Agent を起動および停止する必要があります。

また、Secure Agent Manager を使用して、Secure Agent のステータスをチェックし、プロキシ情報を設定することもできます。

Secure Agent Manager は、［スタート］メニューまたはデスクトップアイコンから起動できます。Secure Agent Manager を閉じると、最小化されて Windows タスクバーの通知領域に表示され、すぐにアクセスできるようにされます。

Secure Agent をインストールするときには、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。

Windows での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。

Windows で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポートされているオペレーティングシステムのリストについては、ナレッジベースの Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。
- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されていることを確認します。
- マシンに他の Secure Agent がインストールされていないことを確認します。マシンに別の Secure Agent がインストールされている場合は、まずそのエージェントをアンインストールする必要があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent がファイアウォールを介して必要なすべてのタスクを実行できるようにするには、Secure Agent が使用するポートを有効にします。

Secure Agent はインターネットに接続するためにポート 443（HTTPS）を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

Windows での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Windows に Secure Agent をインストールする場合、その Secure Agent はローカル管理者グループの一部になっている必要があります。

Windows の設定の実行

Windows で Secure Agent を使用する前に、プロキシ設定と Windows Secure Agent サービスログインを設定します。

プロキシ設定は、Secure Agent Manager で設定できます。Windows で Windows Secure Agent サービスのログインを設定します。

注: Informatica Cloud Data ウィザードで Secure Agent を使用する場合、Secure Agent に対してプロキシ設定または Windows サービスログインを設定する必要はありません。

Windows での Secure Agent のダウンロードおよびインストール

Windows マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **［インストールトークンの生成］** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

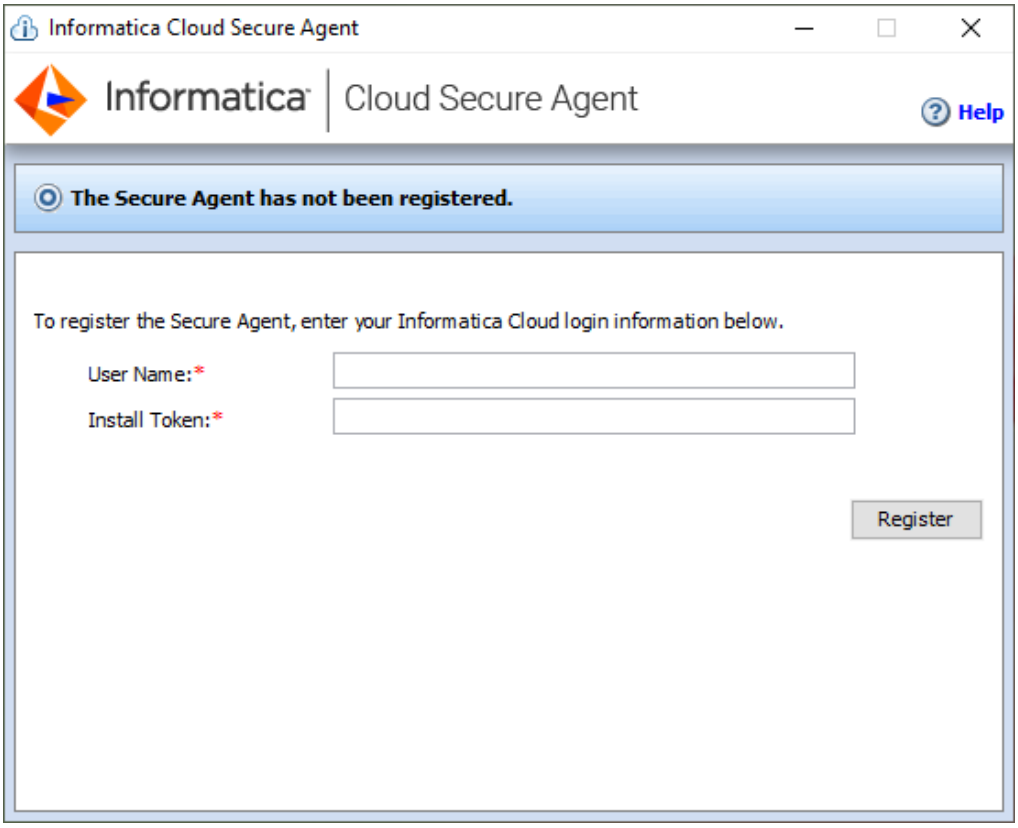
Secure Agent をダウンロードしてインストールする前に、そのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

ヒント: Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

1. 管理者を開いて［**ランタイム環境**］を選択します。
2. ［**ランタイム環境**］ページで、［**Secure Agent のダウンロード**］をクリックします。
3. Windows 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから［**ダウンロード**］をクリックします。

   インストールプログラムがご使用のマシンにダウンロードされます。このインストールプログラムの名前は `agent64_install_ng_ext.<Agent Core バージョン>.exe` です 。
4. インストールプログラムの実行:
   a. Secure Agent インストールディレクトリを指定し、［**次へ**］をクリックします。
   b. ［**インストール**］をクリックしてエージェントをインストールします。

   Secure Agent Manager が開き、次の図に示すようにエージェントを登録するように求めるプロンプトが表示されます。



5. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の［**ランタイム環境**］ページで［**インストールトークンの生成**］をクリックし、トークンをコピーします。

6. Secure Agent Manager で、次の情報を入力し、**[登録]** をクリックします。

オプション	説明
ユーザー名	Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名。
インストールトークン	コピーしたトークン。

Secure Agent Manager が Secure Agent のステータスを表示します。すべてのサービスが起動するまで 1 分かかります。

7. お客様の組織で送信プロキシサーバーを使用してインターネットに接続している場合は、プロキシサーバー情報を入力します。
8. Secure Agent Manager を閉じます。

Secure Agent Manager は、最小化されてタスクバーに表示され、停止されるまでサービスとして実行し続けます。

Windows でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。プロキシサーバーの設定は、Secure Agent Manager から変更できます。

正しいプロキシ設定については、ネットワーク管理者にお問い合わせください。

1. Secure Agent Manager で、**[プロキシ]** をクリックします。
2. プロキシサーバーの設定値を入力するには、**[プロキシサーバーを使用]** をクリックします。
3. 次の情報を入力します。

フィールド	説明
プロキシホスト	必須。Secure Agent が使用する送信プロキシサーバーのホスト名。
プロキシポート	必須。送信プロキシサーバーのポート番号。
ユーザー名	送信プロキシサーバーに接続するユーザー名。
パスワード	送信プロキシサーバーに接続するためのパスワード。

4. **[OK]** をクリックします。

Secure Agent Manager によって Secure Agent が再起動され、設定が適用されます。

Windows Secure Agent サービスへのログインの設定

Windows では、Secure Agent サービスのネットワークログインを設定します。Secure Agent は、ログインに関連付けられている特権と権限によってネットワークにアクセスできます。

Secure Agent がディレクトリにアクセスしてタスクを設定および実行できるように、Secure Agent がインストールされているマシンのログインを設定します。接続を設定する、タスクを設定する、およびフラットファ

イルまたは FTP/SFTP 接続タイプを使用するタスクを実行する場合、Secure Agent には、関連するディレクトリでの読み取りおよび書き込み権限が必要です。

例えば、ディレクトリを参照してフラットファイルまたは FTP/SFTP 接続を設定するには、Secure Agent のログインでそのディレクトリへのアクセス権限を必要とする場合があります。Secure Agent のログインに適切な権限が付与されていないと、Informatica Intelligent Cloud Services では、**［ディレクトリの参照］**ダイアログボックスにディレクトリを表示できません。

1. Windows の［管理ツール］から、**［サービス］**ウィンドウに移動します。
2. **［サービス］**ウィンドウで、Informatica Cloud Secure Agent サービスを右クリックし、**［プロパティ］**を選択します。
3. **［プロパティ］**ダイアログボックスで、**［ログオン］**タブをクリックします。
4. ログインを設定するには、**［このアカウント］**を選択します。
5. アカウントとパスワードを入力します。

   ドメインで定義されているネットワークセキュリティに応じて、必須の特権と権限が付与されているアカウントを使用します。デフォルトのアカウント形式は、<ドメイン名>\<ユーザー名>です。
6. **［OK］**をクリックします。
7. **［サービス］**ウィンドウで、Secure Agent サービスを再起動して変更を有効にします。

Windows での Secure Agent のアンインストール

Secure Agent をアンインストールできます。マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

Secure Agent をアンインストールする前に、接続またはタスクがそれを使用するように構成されていないことを確認します。

1. **［スタート］** > **［すべてのプログラム］** > **［Informatica Cloud Secure Agent］** > **［Informatica Cloud Secure Agent のアンインストール］**をクリックします。

   Secure Agent のアンインストーラが起動します。
2. **［アンインストール］**をクリックします。
3. アンインストールが完了したら、**［完了］**をクリックします。
4. インストールディレクトリに残されているすべてのファイルを削除します。

   Secure Agent をアンインストールした後は、Secure Agent のインストールに関連付けられているすべてのファイルとディレクトリを削除します。

注: Secure Agent をアンインストールしても、Secure Agent ディレクトリからログファイルは削除されません。マシンに Secure Agent を再インストールする場合は、Secure Agent のインストールに関連付けられているすべてのファイルとディレクトリを削除する必要があります。そうしないと、再インストールは失敗します。ログファイルを保存する場合は、別のディレクトリにコピーしてから、Secure Agent のインストールディレクトリを削除してください。

Linux での Secure Agent のインストール

Linux の場合、Secure Agent はプロセスとして実行されます。シェルコマンドラインを使用して、Secure Agent をインストール、登録、起動、停止、およびアンインストールすることができます。

また、シェルコマンドラインを使用して Secure Agent のステータスをチェックすることもできます。

Secure Agent をインストールするときには、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。

Linux での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。Linux で Secure Agent をインストールする前に、システム要件を確認してください。

Linux で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポートされているオペレーティングシステムのリストについては、ナレッジベースの Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。
- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されている必要があります。
- PowerCenter を使用する場合は、PowerCenter のインストールに使用したアカウントとは別のユーザーアカウントを使用して、Secure Agent をインストールします。

  Informatica Intelligent Cloud Services と PowerCenter は、いくつかの共通の環境変数を使用します。Informatica Intelligent Cloud Services に対して環境変数が正しく設定されていない場合、ジョブは実行時に失敗する可能性があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent がファイアウォールを介して必要なすべてのタスクを実行できるようにするには、Secure Agent が使用するポートを有効にします。

Secure Agent はインターネットに接続するためにポート 443（HTTPS）を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

Linux での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Linux に Secure Agent をインストールする場合、その Secure Agent には、インストールディレクトリに対する読み取り/書き込み/実行権限が必要です。

Linux での Secure Agent のダウンロードおよびインストール

Linux マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **［インストールトークンの生成］** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

エージェントを登録すると、デフォルトで独自の Secure Agent グループに追加されます。エージェントは別の Secure Agent グループに追加することもできます。

Secure Agent をダウンロードしてインストールする前に、同じ Linux ユーザーアカウントを使用してそのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

ヒント: Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

1. 管理者を開いて **［ランタイム環境］** を選択します。
2. **［ランタイム環境］** ページで、**［Secure Agent のダウンロード］** をクリックします。
3. Linux 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから **［ダウンロード］** をクリックします。

   インストールプログラムがご使用のマシンにダウンロードされます。このインストールプログラムの名前は agent64_install_ng_ext.<Agent Core バージョン>.bin です。
4. Secure Agent を実行するマシン上のディレクトリにインストールプログラムを保存します。

   注: ファイルパスにスペースが含まれていると、インストールに失敗します。
5. シェルコマンドラインから、インストールプログラムをダウンロードしたディレクトリに移動し、次のコマンドを入力します。

   。/agent64_install_ng_ext.bin –i console
6. インストーラが終了したら、次のディレクトリに移動します。

   <Secure Agent のインストールディレクトリ>/apps/agentcore
7. Secure Agent を起動するには、次のコマンドを入力します。

   。/infaagent startup

   Secure Agent Manager が起動します。Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名を使用してエージェントを登録する必要があります。また、インストールトークンを指定する必要もあります。
8. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の **［ランタイム環境］** ページで **［インストールトークンの生成］** をクリックし、トークンをコピーします。
9. エージェントを登録するには、<Secure Agent のインストールディレクトリ>/apps/agentcore ディレクトリで、Informatica Intelligent Cloud Services のユーザー名とコピーしたトークンを使用して、次のいずれかのコマンドを入力します。
   - エージェントを独自の Secure Agent グループに追加するには、次のコマンドを使用します。

     ./consoleAgentManager.sh configureToken <user name> <install token>
   - エージェントを既存の Secure Agent グループに追加するには、次のコマンドを使用します。

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

注: 存在しない Secure Agent グループ名がコマンドに含まれている場合、Secure Agent はグループに割り当てられません。有効な Secure Agent グループ名を使用するようにしてください。

以下の表にコマンドのオプションの一覧を示します。

オプション	説明
ユーザー名	必須。Secure Agent をインストールするユーザーの Informatica Intelligent Cloud Services ユーザー名。
インストールトークン	必須。コピーしたインストールトークン。
Secure Agent グループ名	オプション。既存の Secure Agent グループにエージェントを追加する場合、代わりに含めます。このオプションがコマンドに含まれていない場合、エージェントは独自の Secure Agent グループに追加されます。

Secure Agent の登録ステータスは、次のコマンドを使用して確認できます。

。/consoleAgentManager.sh isConfigured

Linux でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。

Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。Secure Agent に定義されているプロキシサーバーの設定は、コマンドラインから更新できます。

Linux マシンで Secure Agent のプロキシサーバーを設定するには、proxy.ini ファイルを更新するシェルコマンドを使用します。 ネットワーク管理者に問い合わせて、プロキシの設定項目を決めてください。

1. 次のディレクトリに移動します。

   <Secure Agent installation directory>/apps/agentcore
2. proxy.ini ファイルを更新するには、次のコマンドを入力します。

   ./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name> <proxy password>
3. Secure Agent を再起動します。

Linux での Secure Agent のアンインストール

Secure Agent をアンインストールできます。マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

Secure Agent をアンインストールする前に、接続またはタスクがそれを使用するように構成されていないことを確認します。

1. コマンドラインから次のディレクトリに移動します。

   <Secure Agent installation directory>/apps/agentcore
2. 次のコマンドを入力して、Secure Agent Linux プロセスを停止します。

   ./infaagent shutdown

3. Secure Agent をアンインストールするには、Secure Agent をインストールしたディレクトリで rm -rf を実行して Secure Agent のファイルを削除します。

第 6 章

サーバーレスランタイム環境

サーバーレスランタイム環境は、Secure Agent や Secure Agent グループのダウンロード、インストール、設定、管理が必要ない高度なサーバーレスデプロイメントソリューションです。サーバーレスランタイム環境は、データ統合で接続や一部のタイプのタスクを設定するときにランタイム環境を使用する場合と同じ方法で使用できます。

Hosted Agent 上のマルチテナントモデルと比較して、サーバーレスランタイム環境は、分離されたシングルテナントモデルを使用します。このモデルでは、組織のタスクを実行する仮想マシンリソースを備えた専用サーバー 1 台があります。サーバーレスランタイム環境は、負荷の規模に合わせて自動スケールしますが、データはクラウド環境内に残ります。

サーバーレスランタイム環境は、AWS クラウドプラットフォームの Informatica の Amazon Virtual Private Cloud（VPC）にホストされます。サーバーレスランタイム環境は、アカウント間エラスティックネットワークインタフェース（ENI）を作成してクラウド環境に接続します。

注: サーバーレスランタイム環境を使用するには、クラウド環境が AWS クラウドプラットフォームにあり、VPC がデフォルトテナンシを使用する必要があります。サーバーレスランタイム環境は、専用インスタンステナンシを使用する VPC に接続できません。

サーバーレスランタイム環境は、各ジオロケーションのローカルリージョンをサポートします。例えば、米国（US）の AWS クラウドプラットフォームはすべての米国リージョンをサポートし、アジア太平洋（APAC）の AWS クラウドプラットフォームはすべての APAC リージョンをサポートします。

サーバーレス環境の設定ページへのアクセスが必要なユーザーには、PRIVILEGES.VIEW_AGENT_GROUP 権限が必要です。

詳細モードのマッピングの実行

サーバーレスランタイム環境を使用して詳細モードのマッピングを実行する場合、詳細クラスタを作成し、クラスタでジョブを実行するための前提条件を満たすのは、詳細なサーバーレスデプロイメントです。

サーバーレスランタイム環境は詳細クラスタを管理しますが、クラスタはリソースのプロビジョニングとプロビジョニング解除によって負荷の変化に適応します。詳細クラスタのワーカーノードは高い可用性を実現します。高可用性によって、ワーカーノードがクラッシュした場合のジョブのエラーが軽減され、ジョブのパフォーマンスが維持されます。

始める前に

サーバーレスランタイム環境を作成する前に、サーバーレスランタイム環境に接続するクラウド環境をセットアップします。

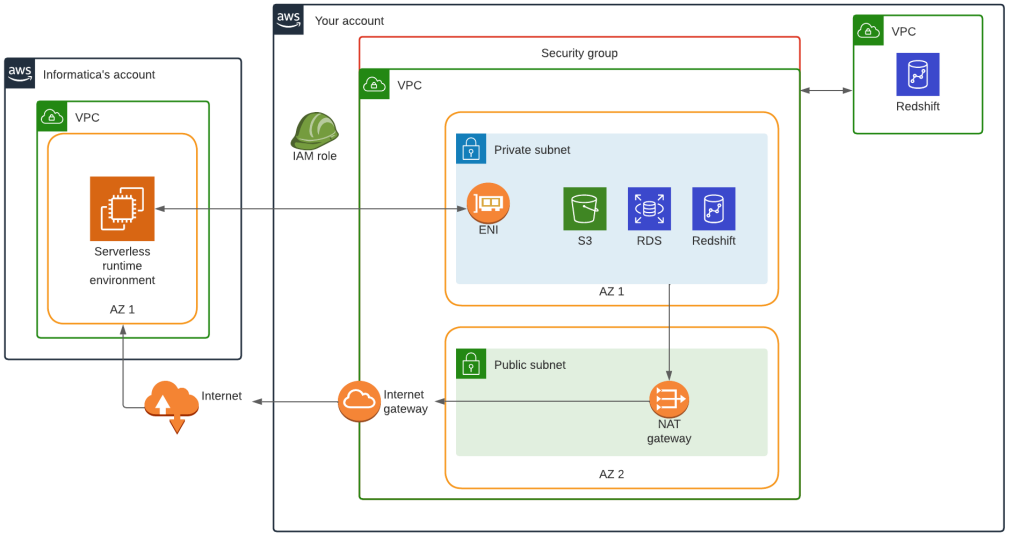
クラウド環境は、次のいずれかのオプションを使用して設定できます。

- VPC で AWS リソースを手動で作成し、Informatica の VPC のサーバーレスランタイム環境に接続するように設定する。
- Informatica が提供するテンプレートを使用して、AWS アカウントに VPC を作成する。既存の VPC がある場合は、それをサーバーレスランタイム環境に接続できます。

手動による VPC の作成および設定

VPC で AWS リソースを作成し、Informatica の VPC のサーバーレスランタイム環境に接続するように設定します。

次の図は、サンプル環境のリソースを示しています。



次のガイドラインを使用して、各リソースを作成および設定します。

VPC

VPC には、サーバーレスランタイム環境で処理するデータが含まれています。

AWS アカウントで VPC を作成します。VPC の DNS ホスト名と DNS 解決を有効にします。

セキュリティグループ

セキュリティグループは、サーバーレスランタイム環境からのトラフィックフローを制御します。

VPC にセキュリティグループを作成します。セキュリティグループは、サーバーレスランタイム環境が作成するすべての ENI に関連付けられています。このセキュリティグループは、サーバーレスランタイム環境のプロパティで指定します。

すべての受信トラフィックを制限するには、受信ルールを空のままにします。送信ルールは、すべてのトラフィックを許可するか、すべての Amazon S3 リソースおよびサーバーレスランタイム環境がアクセスするすべてのソースシステムとターゲットシステムへのトラフィックを制限するかのいずれかです。

ENI をホストするプライベートサブネット

プライベートサブネットは、サーバーレスランタイム環境が VPC への接続に使用する ENI をホストします。

プライベートサブネットを作成し、IP アドレスの最大数を決める CIDR 範囲を設定してサーバーレスランタイム環境のスケーラビリティを決定します。サーバーレスランタイム環境ごとに少なくとも 25 個の IP アドレスを持つように CIDR 範囲を設定して、開発者が同時ワークロードを実行するときにサーバーレスランタイム環境を効果的にスケーリングできるようにします。

組織の管理者が Administrator でサーバーレスランタイム環境を作成した後に、サーバーレスランタイム環境ではプライベートサブネットにアカウント間 ENI が作成されます。

インターネットアクセス用のパブリックサブネット

パブリックサブネットは、NAT ゲートウェイを介したインターネットアクセスを提供します。

VPC を作成したリージョンの任意の可用性ゾーンを使用して、パブリックサブネットを作成します。CIDR の範囲は、VPC CIDR の範囲内である必要があります。サブネット内に含める IP アドレスの数に基づいて範囲を選択します。

VPC から VPC への接続

VPC から VPC への接続は、サーバーレスランタイム環境に接続する VPC とは異なる VPC 内のデータにアクセスするために使用されます。例えば、マッピングが、VPC の Amazon Redshift クラスタからデータを読み取り、別の VPC にある別の Amazon Redshift クラスタにデータを書き込む場合があります。

VPC 間でデータを処理する場合は、VPC から VPC への接続を設定します。AWS には、VPC ピアリングや AWS Transit Gateway など、VPC から VPC への接続を設定する方法がいくつかあります。該当する場合は、AWS PrivateLink を使用してください。詳細については、AWS のマニュアルを参照してください。

プライベートサブネットからのインターネットアクセス用の NAT ゲートウェイ

NAT ゲートウェイは、プライベートインスタンスからインターネットへの送信トラフィックを許可します。アカウント間 ENI に関連付けられているサーバーレスランタイム環境のすべてのコンピューティングインスタンスはプライベートです。

プライベートサブネットからインターネットへの送信トラフィックをルーティングするには、NAT ゲートウェイを作成します。AWS には、ルートテーブルや NACL など、サブネットルーティングルールを設定する方法がいくつか用意されています。詳細については、AWS のマニュアルを参照してください。

IAM ロール

IAM ロールは、サーバーレスランタイム環境と詳細クラスタのワーカーノードが、VPC のプライベートサブネットに関連付けられているアカウント間 ENI を作成、アタッチ、デタッチ、および削除するために使用する、最小限のポリシーを定義します。

IAM ロールは、マッピングで使用するソースとターゲットだけではなく、補足ファイルの S3 ロケーションにアクセスできる必要があります。次のテンプレートを使用できます。

```
{
    "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>/*"
            ]
        }
    ]
}
```

信頼関係で、Informatica アカウント番号を信頼済みのエンティティとして指定し、外部 ID を作成します。Informatica アカウント番号を見つけるには、Administrator でサーバーレスランタイム環境を作成し、環境のプロパティを確認します。次のテンプレートを使用できます。

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

テンプレートを使用した VPC の作成

Informatica が提供する AWS CloudFormation テンプレートを使用して、AWS アカウントに VPC を作成できます。既存の VPC がある場合は、それをサーバーレスランタイム環境に接続できます。

1. Informatica Intelligent Cloud Services の AWS CloudFormation テンプレートを含む電子メールを組織の管理者に依頼してください。

   組織の管理者は、Administrator でサーバーレス設定ファイルを要求することで電子メールを生成できます。詳細については、「サーバーレス設定ファイルの要求」 (ページ 68)を参照してください。

2. AWS CloudFormation テンプレートを使用して、AWS CloudFormation にスタックを作成します。

詳細については、「AWS CloudFormation テンプレートを使用した VPC の作成」 (ページ 49)または「AWS CloudFormation テンプレートを使用した既存の VPC への接続」 (ページ 52)を参照してください。

3. テンプレートで指定した JSON ファイルの S3 の場所に移動します。
4. `iics-sre-config` フォルダに、JSON ファイルをダウンロードします。
5. JSON ファイルを組織の管理者と共有します。

   組織の管理者は、このファイルを Informatica Intelligent Cloud Services にインポートし、VPC が Informatica の VPC のサーバーレスランタイム環境に接続する準備ができていることを Informatica に通知します。
6. 必要に応じて、補足ファイルの場所を作成します。

   補足ファイルの場所には、開発者がデータにアクセスして処理するために使用できる JAR ファイルや外部ライブラリなどの補足ファイルが格納されます。詳細については、「補足ファイルの場所の作成」 (ページ 59)を参照してください。

AWS CloudFormation テンプレートを使用した VPC の作成

CloudFormation テンプレートを使用して VPC を作成する場合、スタックは VPC と、サブネットおよび最小限のポリシーを持つ IAM ロールを含む、Informatica の VPC のサーバーレスランタイム環境に接続するために必要なすべてのリソースと設定を作成します。

AWS CloudFormation でスタックを作成するには、スタック名を指定し、スタックパラメータを設定します。以下の表に、スタックパラメータを示します。

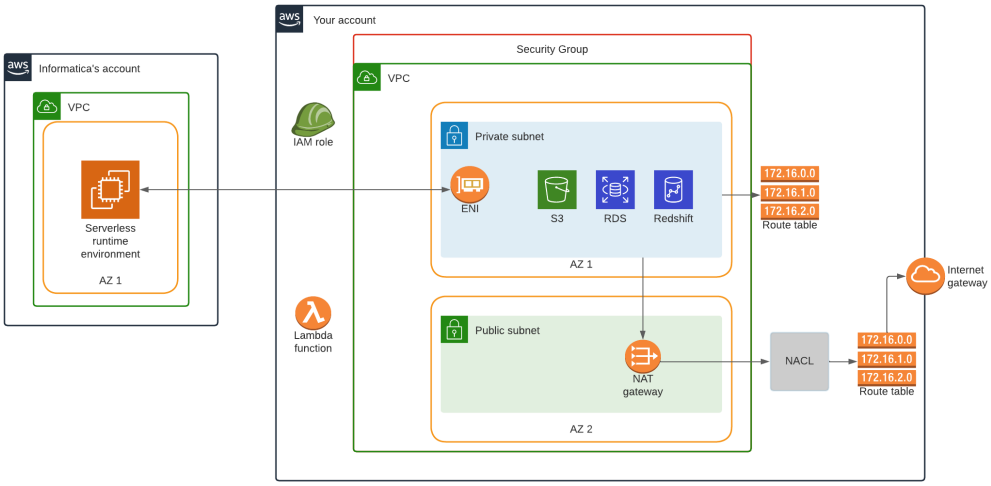
パラメータ	説明
VPC CIDR	VPC を作成する場所を指定する CIDR ブロック。
パブリックサブネット CIDR	パブリックサブネットを作成する場所を指定する CIDR ブロック。パブリックサブネットの IP 範囲は、VPC の IP 範囲内にある必要があります。
パブリックサブネットの可用性ゾーン	パブリックサブネットを作成する可用性ゾーン。現在のリージョンの任意の可用性ゾーンを選択できます。
プライベートサブネット CIDR	プライベートサブネットを作成する場所を指定する CIDR ブロック。プライベートサブネットの IP 範囲は、VPC の IP 範囲内にある必要があります。
プライベートサブネットの可用性ゾーン	プライベートサブネットを作成する可用性ゾーン。現在のリージョンの任意の可用性ゾーンを選択できます。
VPC デプロイメントタイプ	[NAT ゲートウェイ] を選択します。
Informatica Cloud リージョン	Informatica POD が存在するリージョン。 このリージョンは、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は米国リージョンに存在します。
External ID	IAM ロールに関連付ける外部 ID。
AWS タグ	ENI のラベルを付ける AWS タグ。

パラメータ	説明
補足ファイルの場所	開発者がデータにアクセスして処理するために使用できる JAR ファイルや外部ライブラリなど補足ファイルを格納するための Amazon S3 の場所。
JSON ファイルの S3 の場所	サーバーレス設定ファイルを生成するための Amazon S3 の場所。

注: パラメータが有効でない場合、スタックは作成されません。

スタックが作成する AWS リソース

次の図は、スタックによって AWS アカウントで作成されるリソースを示しています。



次の表は、スタックによって作成される AWS リソースとリソース数をまとめたものです。

AWS リソース	作成されるリソースの数
VPC	1
セキュリティグループ	1
サブネット	2 1 つのパブリックサブネットと 1 つのプライベートサブネット
NAT ゲートウェイ	1
エラスティック IP アドレス	NAT ゲートウェイに接続された 1 つのエラスティック IP アドレス
NACL	1
ルートテーブル	2 1 つのパブリックルートテーブルと 1 つのプライベートルートテーブル

AWS リソース	作成されるリソースの数
インターネットゲートウェイ	1
IAM ロール	1

スタックが実行する設定

スタックは次の設定を実行します。

- セキュリティグループを VPC に関連付け、受信ルールと送信ルールを定義します。
- ルートをプライベートルートテーブルに追加し、そのプライベートルートテーブルを VPC のデフォルトルートテーブルにします。
- インターネットへの送信トラフィック用に NAT ゲートウェイをパブリックサブネットに関連付け、そのゲートウェイにエラスティック IP を割り当てます。
- パブリックサブネットに関連付けられた NACL 受信ルールを更新します。
- インターネットゲートウェイを VPC に接続します。
- 次のポリシーを IAM ロールに割り当てます。

```
{
   "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>/*"
         ]
      }
   ]
}
```

- IAM ロールで次の信頼関係を作成します。

```
{
   "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>"
            }
         }
      }
   ]
}
```

AWS CloudFormation テンプレートを使用した既存の VPC への接続

AWS CloudFormation でテンプレートを指定すると、AWS CloudFormation によって、このテンプレートに基づいたスタックが作成されます。

AWS CloudFormation にログインすると、新しいスタックを作成できます。スタックを作成する際は、使用するテンプレートを指定します。このテンプレートでは、入力する必要があるスタックパラメータが取り込まれます。パラメータの入力が完了すると、AWS CloudFormation によって、パラメータ値に基づいたスタックが作成されます。

以下の表に、スタックパラメータを示します。

パラメータ	説明
VPC ID	VPC の ID。例えば、vpc-2f09a348 です。 スタックでは、VPC がスタックの作成場所と同じ AWS リージョンにあると想定されます。
サブネット ID	VPC 内のサブネットの ID。例えば、subnet-b46032ec です。
セキュリティグループ ID	オプション。セキュリティグループの ID。例えば、sg-e1fb8c9a です。
セキュリティグループが存在しない場合に作成する必要がありますか?	セキュリティグループが存在しない場合にスタックでセキュリティグループを作成するかどうかを示します。**[はい]** または **[いいえ]** を選択します。
Informatica Cloud リージョン	Informatica POD が存在するリージョン。 このリージョンは、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。例えば、URL が usw3.dm-us.informaticacloud.com で始まる場合、POD は米国リージョンに存在します。
AWS タグ	ENI のラベルを付ける AWS タグ。
補足ファイルの場所	特定のトランスフォーメーションおよびコネクタ用の JAR ファイルや外部ライブラリなど補足ファイルを格納するための Amazon S3 の場所。
JSON ファイルの S3 の場所	サーバーレス設定ファイルを生成するための Amazon S3 の場所。

注: パラメータが有効でない場合、スタックは作成されません。

スタックが実行する設定

スタックは次の設定を実行します。

- VPC ID に基づいてリージョンを検出し、サーバーレスランタイム環境がそのリージョンに接続できるかどうかを確認します。
- サブネットが存在するかどうかを確認します。
- サブネット ID から可用性ゾーン ID を取得します。
- セキュリティグループの受信ルールと送信ルールを確認します。セキュリティグループが指定されていないか存在しない場合、スタックはセキュリティグループを作成します。
- IAM ロールを作成し、そのロールに次のポリシーを割り当てます。

```
{
   "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>/*"
         ]
      }
   ]
}
```

- IAM ロールで次の信頼関係を作成します。

```
{
   "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>"
            }
         }
      }
   ]
}
```

スタックのトラブルシューティング

AWS CloudFormation でスタック作成中のエラーをトラブルシューティングする方法

以下のタスクを実行します。

1. AWS CloudFormation で、**[Home]** ページに移動します。
2. 作成したスタックを選択します。
3. **[Events]** タブで、**[Status reason]** カラムのメッセージを確認します。
4. **[Parameters]** タブで、**[Status reason]** カラムのメッセージを確認します。

スタックによって作成された AWS リソースを表示する方法

以下のタスクを実行します。

1. AWS CloudFormation で、**[Home]** ページに移動します。
2. 作成したスタックを選択します。
3. ネストされたスタック **[InfaVPCStack]** に移動します。
4. **[Resources]** タブで、スタックによって作成されたリソースを表示します。

スタックによって作成された AWS リソースを削除する方法

以下のタスクを実行します。

1. AWS CloudFormation で、**[Home]** ページに移動します。
2. 作成したスタックを選択します。
3. **[Delete]** をクリックします。

VPC を作成したスタックを削除しようとしたが、削除に時間がかかりすぎている

VPC を削除することで強制的に削除できます。以下のタスクを実行します。

1. AWS CloudFormation で、**[Home]** ページに移動します。
2. 作成したスタックを選択します。
3. ネストされたスタック **[InfaVPCStack]** に移動します。
4. **[Resources]** タブで、**[Physical ID]** カラムの VPC リンクをクリックします。

   VPC ホームページにリダイレクトされます。
5. 削除する VPC を選択します。
6. **[Actions] > [Delete VPC]** をクリックします。

   他の AWS リソースを最初に削除する必要があることを示す警告メッセージが表示された場合は、VPC を削除する前に、指定されたリソースを手動で削除してください。
7. AWS CloudFormation のスタックに戻り、スタックの削除を再試行します。

Administrator のサーバーレスランタイム環境が起動しないか、起動に時間がかかりすぎている

パラメータが正しく設定されていない可能性があります。作成中にスタックに入力したパラメータを確認します。以下のタスクを実行します。

1. AWS CloudFormation で、**[Home]** ページに移動します。
2. 作成したスタックを選択します。
3. **[Parameters]** タブで、**[Events]** をクリックします。
4. **[Status reason]** カラムを確認します。

クラウド環境を設定する際の一般的な情報

クラウド環境を設定する際は、IP フィルタリング用の安全な IP アドレスを追加し、システムディスクを設定し、JAR ファイルと外部ライブラリの場所を設定し、REST API を認証するように TLS を設定できます。

必要に応じて、次のタスクを実行します。

- IP アドレスに基づいたフィルタリングを行う組織の場合は、安全な Informatica アドレスを追加します。詳細については、「信頼済みの Informatica IP アドレス」 (ページ 55)を参照してください。
- パフォーマンスを向上するには、システムディスクの設定を検討してください。詳細については、「システムディスクの設定」 (ページ 57)を参照してください。
- マッピングで JAR ファイルと外部ライブラリを使用する場合は、ファイルを保存する場所を Amazon S3 に設定します。詳細については、「補足ファイルの場所の作成」 (ページ 59)を参照してください。
- REST V3 コネクタを使用する場合は、REST API を認証するように TLS を設定できます。詳細については、「REST API を認証するための TLS の設定」 (ページ 60)を参照してください。

信頼済みの Informatica IP アドレス

組織で信頼済み IP アドレス範囲を使用する場合は、組織のプロパティでその範囲を編集し、適切な信頼済み IP アドレスを追加します。

米国

次の表に、米国リージョンの信頼済み IP アドレスを示します。

領域	信頼済み IP アドレス
米国東部（バージニア北部）us-east-1	- 54.160.9.90 - 54.221.247.69
米国東部（オハイオ）us-east-2	- 18.220.76.98 - 3.131.176.232
米国西部（北カリフォルニア）us-west-1	- 52.52.220.198 - 13.56.74.27
米国西部（オレゴン）us-west-2	- 44.239.8.148 - 44.242.20.143

APJ

次の表に、APJ リージョンの信頼済み IP アドレスを示します。

領域	信頼済み IP アドレス
アジアパシフィック（香港）ap-east-1	- 18.167.71.151 - 18.163.244.73
アジアパシフィック（ムンバイ）ap-south-1	- 65.1.80.5 - 13.234.141.216
アジアパシフィック（大阪）ap-northeast-3	- 該当なし
アジアパシフィック（ソウル）ap-northeast-2	- 52.79.244.47 - 3.34.56.248
アジアパシフィック（シンガポール）ap-southeast-1	- 52.76.184.230 - 18.140.193.120
アジアパシフィック（シドニー）ap-southeast-2	- 3.24.111.61 - 54.253.179.190
アジアパシフィック（東京）ap-northeast-1	- 35.72.149.44 - 13.112.143.134

カナダ

次の表に、カナダリージョンの信頼済み IP アドレスを示します。

領域	信頼済み IP アドレス
カナダ（中部）ca-central-1	- 3.96.182.201 - 3.97.103.68

EMEA

次の表に、EMEA リージョンの信頼済み IP アドレスを示します。

領域	信頼済み IP アドレス
ヨーロッパ（フランクフルト）eu-central-1	- 3.125.185.124 - 3.64.66.226
ヨーロッパ（アイルランド）eu-west-1	- 54.76.54.130 - 54.78.183.88
ヨーロッパ（ロンドン）eu-west-2	- 35.176.60.118 - 18.135.50.152
ヨーロッパ（ミラノ）eu-south-1	- 35.152.49.63 - 35.152.45.151

領域	信頼済み IP アドレス
ヨーロッパ（パリ）eu-west-3	- 15.237.157.126 - 15.237.97.211
ヨーロッパ（ストックホルム）eu-north-1	- 13.49.61.89 - 13.53.141.231

英国

次の表に、英国リージョンの信頼済み IP アドレスを示します。

領域	信頼済み IP アドレス
ヨーロッパ（フランクフルト）eu-central-1	- 18.157.124.91
ヨーロッパ（アイルランド）eu-west-1	- 34.250.251.16
ヨーロッパ（ロンドン）eu-west-2	- 18.170.170.192
ヨーロッパ（ミラノ）eu-south-1	- 15.161.184.93 - 15.160.41.209
ヨーロッパ（パリ）eu-west-3	- 13.37.37.71
ヨーロッパ（ストックホルム）eu-north-1	- 13.53.147.238

システムディスクの設定

サーバーレスランタイム環境では、システムディスクを使用してパフォーマンスを向上させることができます。

データ統合でのマッピングのパフォーマンスが向上するように、システムディスクを設定します。

システムディスクは、Amazon EFS（Elastic File System）および NFS（Network File System）形式で設定できます。EFS のファイルシステム接続は、デフォルトで TLS が有効になっています。NFS のファイルシステム接続は、NFSv4（Network File System Version 4）を使用します。

サーバーレスランタイム環境でシステムディスクを使用すると、そのシステムディスク上に<組織 ID>/<サーバーレス環境 ID>という名前のフォルダが作成されます。このフォルダには、ジョブのメタデータとログが保存されます。

EFS ファイルシステムのルールとガイドライン

システムディスクを Amazon EFS 形式で設定する場合は、次のガイドラインに従ってください。

- ファイルシステムを EFS ファイルシステムの ID に設定します。
- サーバーレスランタイム環境のサブネットに Amazon EFS ファイルシステムへのアクセスを許可します。
- サーバーレスランタイム環境内に設定されたセキュリティグループからのインバウンドアクセスを許可するように、EFS のセキュリティグループを設定します。
- サーバーレス環境内の IAM ロールに、EFS ファイルシステムへのフルアクセスを設定します。フルアクセスはファイルシステムポリシーまたは IAM ロールで許可できます。例えば、次のファイルシステムポリシ

ーは、ServerlessRole（SREIICS）にファイルシステム fs-12345 に対するルートアクセスを許可し、SecureTransport のみを許可します。

```
"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"
                }
            }
        }
    ]
}
```

以下の表に、サンプルポリシーのアクションを示します。

アクション	説明
elasticfilesystem:ClientMount	ファイルシステムへの読み取り専用アクセスを許可します。
elasticfilesystem:ClientWrite	ファイルシステムに対する書き込み権限を許可します。
elasticfilesystem:ClientRootAccess	ファイルシステムにアクセスする時にルートユーザーの使用を許可します。

- アクセスポイント自体を作成する前に、アクセスポイントに必要なフォルダを作成します。例えば、アクセスポイントがフォルダ/my-company/dev を参照する場合は、アクセスポイントを設定する前に、まずこのフォルダを定義します。
- ファイルシステム上の特定のアクセスポイントにアクセスを制限するように IAM ロールを設定します。詳細については、 https://docs.aws.amazon.com/efs/latest/ug/efs-access-points.html を参照してください。

NFS ファイルシステムのルールとガイドライン

システムディスクを NFS 形式で設定する場合は、次のガイドラインに従ってください。

- ファイルシステムを NFS サーバーの DNS に設定します。

- NFS ファイルサーバーへのアクセスを許可するようにサーバーレスランタイム環境のサブネットを設定します。
- サーバーレスランタイム環境内に設定されたセキュリティグループからのインバウンドアクセスを許可するように、ファイルサーバーのセキュリティグループを設定します。

補足ファイルの場所の作成

マッピングで JAR ファイルと外部ライブラリを使用する場合は、Amazon S3 にファイルを保存する専用の場所を確保し、ファイルタイプごとにフォルダを作成します。

補足ファイルの場所を作成するには、次のタスクを完了します。

1. Amazon S3 に次のファイル構造を作成します。

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

2. serverlessUserAgentConfig.yml ファイルを作成します。テンプレートについては、「serverlessUserAgentConfig.yml ファイルへの入力」 (ページ 61)を参照してください。
3. serverlessUserAgentConfig.yml ファイルを serverless_agent_config ディレクトリ直下に追加します。

次の表に、それぞれの場所に保存できるファイルの種類を示します。

場所	ファイル
<Supplementary file location>/ext	JDBC JAR ファイル
<Supplementary file location>/odbc	次のファイル - odbc.ini - odbcinst.ini - exports.ini
<Supplementary file location>/odbc/lib	Linux オペレーティングシステム用の ODBC 共有ライブラリ
<Supplementary file location>/serverless_agent_config	次のファイル - serverlessUserAgentConfig.yml - JDBC V2 コネクタ JAR ファイル - REST V3 コネクタのトラストストア証明書とキーストア証明書 - Java トランスフォーメーション用の JAR ファイル - Python トランスフォーメーション用のインストールファイルとリソースファイル serverless_agent_config フォルダのディレクトリ構造をカスタマイズし、serverlessUserAgentConfig.yml ファイルで各ファイルへの相対パスを指定できます。

REST API を認証するための TLS の設定

サーバーレスランタイム環境で実行される API コレクションまたは機械学習トランスフォーメーションで REST V3 コネクタを使用する場合、一方向または双方向の安全な通信を確立して REST API を認証するように TLS を設定できます。

Informatica グローバルカスタマサポートに連絡して、必要なカスタムプロパティを要求してください。トラストストア証明書とキーストア証明書が JKS 形式であることを確認してください。

1. Amazon S3 の補足ファイルの場所に移動します。
2. serverless_agent_config フォルダに、SSL というサブフォルダを作成します。
3. SSL フォルダにトラストストア証明書とキーストア証明書を追加します。

   一方向の安全な通信を行うには、トラストストア証明書を追加します。双方向の安全な通信を行うには、トラストストア証明書とキーストア証明書の両方を追加します。
4. 次のコードスニペットをテキストエディタにコピーし、補足ファイルの場所にある各証明書への相対パスを追加します。

```
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. serverless_agent_config フォルダで、serverlessUserAgentConfig.yml ファイルを開きます。
6. コードスニペットを serverlessUserAgentConfig.yml ファイルに追加し、ファイルを保存します。

   サーバーレスランタイム環境は、実行時に証明書を使用できるように、証明書を補足ファイルの場所から固有の参照ディレクトリにコピーします。
7. REST V3 接続プロパティで、/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<証明書名>.jks という形式を使用して、サーバーレスランタイム環境の各トラストストアファイルパスおよびキーストアファイルパスを指定します。

開発者にカスタムプロパティを提供します。開発者は、このカスタムプロパティを、サーバーレスランタイム環境で実行されるマッピングタスクに入力します。

serverlessUserAgentConfig.yml の参考資料

補足ファイルの場所を作成する際は、serverlessUserAgentConfig.yml ファイルを作成および設定する必要があります。

次のアクションを実行します。

- serverlessUserAgentConfig.yml ファイルに入力するには、ここで提供されるテンプレートを使用し、必要に応じて調整します。詳細については、「serverlessUserAgentConfig.yml ファイルへの入力」 (ページ 61)を参照してください。

  補足ファイルの場所からサーバーレスランタイム環境にコピーするファイルを設定するには、serverlessUserAgentConfig.yml ファイル内でファイルパスを指定します。
- エラスティックサーバーのファイルをコピーするには、ここで提供されるコードスニペットを使用します。詳細については、「エラスティックサーバーのファイルのコピー」 (ページ 62)を参照してください。
- JDBC V2 コネクタの JAR ファイルをコピーするには、ここで提供されるコードスニペットを使用します。詳細については、「JDBC V2 コネクタ JAR ファイルのコピー」 (ページ 63)を参照してください。

- Java トランスフォーメーションの JAR ファイルをコピーするには、ここで提供されるコードスニペットを使用します。詳細については、「Java トランスフォーメーション JAR ファイルのコピー」 (ページ 63)を参照してください。
- Python トランスフォーメーションのリソースファイルをコピーするには、ここで提供されるコードスニペットを使用します。詳細については、「Python トランスフォーメーションのインストールファイルとリソースファイルのコピー」 (ページ 63)を参照してください。

serverlessUserAgentConfig.yml ファイルへの入力

次のテンプレートを使用して、serverlessUserAgentConfig.yml ファイルにデータを入力します。

```
# 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/swg.ext
        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
```

serverlessUserAgentConfig.yml ファイルへの入力の詳細については、適切なコネクタのヘルプを参照してください。

エラスティックサーバーのファイルのコピー

serverlessUserAgentConfig.yml ファイルで、補足ファイルの場所からサーバーレスランタイム環境にコピーするファイルを指定できます。サーバーレスランタイム環境で詳細モードのマッピングを実行する際、エラスティックサーバーと詳細クラスタはそのファイルを使用して、データにアクセスし処理することができます。

次のタイプのエラスティックサーバー用ファイルをコピーできます。

- JDBC V2 コネクタ JAR ファイル
- Java トランスフォーメーション用の JAR ファイル
- Python トランスフォーメーション用のインストールファイルとリソースファイル

補足ファイルの場所にあるファイルへの相対パスを指定することにより、ファイルパスをカスタマイズできます。例えば、JDBC V2 コネクタ JAR ファイルを次の場所に保存するとします。

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

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

serverlessUserAgentConfig.yml ファイルで次の相対パスを指定できます。

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

JDBC V2 コネクタ JAR ファイルのコピー

JDBC V2 コネクタ用の JAR ファイルをコピーするには、次のコードスニペットをテンプレートとして使用します。

```
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
```

Java トランスフォーメーション JAR ファイルのコピー

Java トランスフォーメーション用の JAR ファイルをコピーするには、次のコードスニペットをテンプレートとして使用します。

```
agent:
  elasticServer:
    autoApply:
      javaTx:
        resources:
        - fileCopy:
            sourcePath: j_depends/Helper.jar
        - fileCopy:
            sourcePath: j_depends/Student.jar
```

Python トランスフォーメーションのインストールファイルとリソースファイルのコピー

Python トランスフォーメーション用のリソースファイルをコピーするには、次のコードスニペットをテンプレートとして使用します。

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

Python インストールを補足ファイルの場所からサーバーレスランタイム環境にコピーするには、Python インストールディレクトリへの相対パスを指定します。

例えば、補足ファイルの場所の Python3_8_with_sklearn_panda/というフォルダに Python インストールが保存されている場合は、次のコードスニペットを使用します。

```
agent:
  elasticServer:
    autoApply:
      pythonTx:
        resources:
        - fileCopy:
            sourcePath: py_depends/Python3_8_with_sklearn_panda/
```

サーバーレスランタイム環境の実行中に Python インストールディレクトリを補足ファイルの場所に追加した場合、インストールが使用可能になるには、環境を再デプロイする必要があります。

環境の実行中におけるファイルの追加

サーバーレスランタイム環境の実行中に、エラスティックサーバーのファイルを補足ファイルの場所に追加できます。エラスティックサーバーのファイルには、JDBC V2 コネクタ JAR ファイル、Java トランスフォーメーション JAR ファイル、および Python トランスフォーメーションリソースファイルが含まれます。

環境の実行中にファイルを追加するには、次の手順を実行します。

1. <Supplementary file location>/serverless_agent_config/.の適切な場所にファイルを追加します。
2. serverlessUserAgentConfig.yml ファイルでファイルを指定します。ファイルへの入力の詳細については、「serverlessUserAgentConfig.yml ファイルへの入力」 (ページ 61)または適切なコネクタのヘルプを参照してください。

ファイルがサーバーレスランタイム環境に同期するのに 10 分かかります。

次のタスクの実行後に、サーバーレスランタイム環境を再デプロイする必要があります。

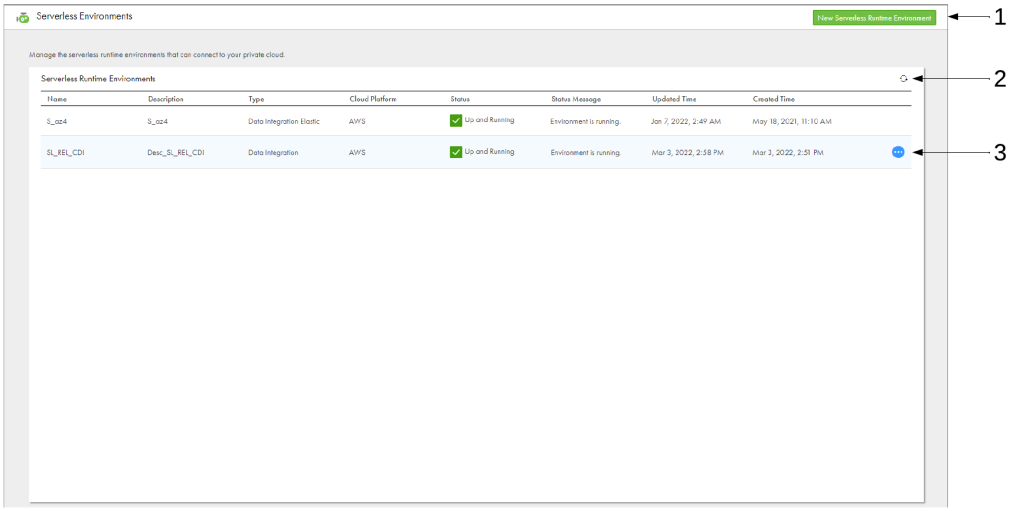
- 既存のファイルを更新します。

  サーバーレスランタイム環境の実行中に既存のファイルを更新するには、別の名前を使用してファイルを補足ファイルの場所と serverlessUserAgentConfig.yml ファイルに追加する必要があります。
- ODBC 共有ライブラリなどの他のファイルタイプを追加します。
- Python トランスフォーメーション用の Python インストールディレクトリなど、新しいフォルダまたはディレクトリを追加します。
- サーバーレスランタイム環境からファイルを削除します。

サーバーレスランタイム環境の作成

[サーバーレス環境] ページで、サーバーレスランタイム環境を作成し、プロパティを設定します。ーバーレスランタイム環境のプロパティを表示するには、環境の **[アクション]** メニューを展開し、**[表示]** を選択します。

次の図は、**[サーバーレス環境]** ページを示しています。



1. サーバーレスランタイム環境を作成するためのオプション
2. [更新] アイコン
3. アクション

サーバーレスランタイム環境を作成するには、サーバーレスランタイム環境のプロパティを入力するか、サーバーレス設定ファイルをインポートしてプロパティを取り込みます。サーバーレスランタイム環境が使用可能になるには少なくとも 5 分かかります。**[サーバーレス環境]** ページを使用して、環境のステータスを追跡し、ステータスメッセージを確認します。

組織には最大で 10 のサーバーレスランタイム環境を作成できます。トライアルライセンスでは、最大で 2 つの環境を作成できます。

サーバーレスランタイム環境のプロパティ

サーバーレスランタイム環境のプロパティを設定します。基本プロパティでは、サーバーレスランタイム環境を定義します。プラットフォーム設定プロパティでは、サーバーレスランタイム環境に接続する VPC 内の AWS リソースを記述します。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	サーバーレスランタイム環境の名前
説明	サーバーレスランタイム環境の説明。

プロパティ	説明
タスクタイプ	サーバーレスランタイム環境で実行されるタスクのタイプ。 - 詳細モード外のマッピングを実行するには、データ統合を選択します。 - 詳細クラスタで全面的に実行できる、詳細モードのマッピングを実行するには、Data Integration Elastic を選択します。
クラウドプラットフォーム	サーバーレスランタイム環境をホストするクラウドプラットフォーム。 使用できるのは Amazon Web Services（AWS）のみです。
最大コンピューティングユニットタスクごと	タスクが使用できる、マシンリソースに対応するサーバーレスコンピューティングユニットの最大数。
タスクのタイムアウト	タスクを終了する前に、タスクが完了するまで待機する時間の長さ。タイムアウトにより、タスクがハングしたときにサーバーレスコンピューティングユニットが無応答にならないようにします。 デフォルトでは、タイムアウトは 2880 分（48 時間）です。タイムアウトは 2880 分未満の値に設定できます。
Informatica アカウント番号	サーバーレスランタイム環境が作成されるクラウドプラットフォームの Informatica のアカウント番号。アカウント番号は自動的に取り込まれます。
External ID	サーバーレスランタイム環境用に作成するロールに関連付ける外部 ID。生成された外部 ID を使用することも、固有の外部 ID を指定することもできます。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
設定名	リソース設定の名前。
設定の説明	リソース設定の説明。
アカウント番号	クラウドプラットフォームでのアカウント番号。
リージョン	クラウド環境のリージョン。マッピングで使用するソースおよびターゲットは、このリージョンに存在するか、このリージョンからアクセスできる必要があります。
AZ ID	可用性ゾーンの識別子。マッピングで使用するソースおよびターゲットは、リージョンに存在するか、可用性ゾーンからアクセスできる必要があります。
VPC ID	Amazon Virtual Private Cloud（VPC）の ID。VPC ではマッピングで使用するソースおよびターゲットにアクセスするためのエンドポイントが設定されている必要があります。 例えば、`vpc-2f09a348` です。
サブネット ID	VPC 内のサブネットの ID。サブネットにはマッピングで使用するソースおよびターゲットにアクセスするためのエンドポイントが含まれている必要があります。 例えば、`subnet-b46032ec` です。

プロパティ	説明
セキュリティグループ ID	サーバーレスランタイム環境が ENI にアタッチするセキュリティグループの ID。タスクで使用するソースおよびターゲットにアクセスできるセキュリティグループ。 例えば、sg-e1fb8c9a です。
ロール名	サーバーレスランタイム環境が AWS アカウントで想定できる IAM ロールの名前。 このロールには、ENI を作成、読み取り、削除、リスト、デタッチおよびアタッチする権限が必要です。補足ファイルの場所に対する読み取りおよび書き込み権限も必要です。 ロールのポリシーを作成するときに、Informatica アカウント番号および外部 ID を使用します。
AWS タグ	AWS アカウントで作成される ENI のラベルを付ける AWS タグ。 各タグは、Key=string,Value=string というフォーマットのキーと値のペアにする必要があります。Key と Value は大文字小文字の区別があります。 複数のタグはスペースで区切ります。タグにスペースを含めることはできません。 AWS によって指定されたタグ付けのルールとガイドラインに従います。詳細については、AWS のマニュアルを参照してください。
補足ファイルの場所	特定のトランスフォーメーションおよびコネクタ用の JAR ファイルや外部ライブラリなど補足ファイルを格納するための Amazon S3 の場所。 s3://<bucket name>/<folder name>の形式を使用します。 スクリプトファイルは、command_scripts という名前のフォルダに配置する必要があります。このフォルダにはサブフォルダを含めることができます。Informatica Intelligent Cloud Services は、command_scripts ディレクトリ内のファイルを Secure Agent のエージェントインストールディレクトリ apps/Common_Integration_Components/data/command/serverless/command_scripts に定期的に同期します。Amazon S3 でファイルを更新すると、Informatica Intelligent Cloud Services はそれらのファイルを Secure Agent へ自動的に同期します。

システムディスク

以下の表に、システムディスクのプロパティを示します。システムディスクの設定に関するガイドラインについては、「システムディスクの設定」 (ページ 57)を参照してください。

プロパティ	説明
タイプ	システムディスクタイプ。EFS または NFS です。
ファイルシステム	EFS ディスクの場合、ファイルシステムは EFS ディスクのファイルシステム ID です。 NFS ディスクの場合、ファイルシステムはファイルシステムの DNS です。
ソースマウント	サーバーレスランタイム環境でマウントするファイルシステムパス。
アクセスポイント	Amazon EFS ファイルシステムのアクセスポイントの ID。 アクセスポイントをしようすると、マルチテナント型の EFS ファイルシステム内で確実にテナントを分離できます。 アクセスポイントを設定したら、サーバーレス IAM ロールに対してそのアクセスポイントへのアクセスのみを許可するようにファイルシステムポリシーを設定できます。

サーバーレス設定ファイルの使用

サーバーレス設定ファイルを使用して、サーバーレスランタイム環境のプロパティを取り込むことができます。

サーバーレスランタイム環境を作成するときに、クラウド管理者に設定ファイルを要求し、それを Administrator にインポートします。

サーバーレス設定ファイルの要求

クラウド管理者にサーバーレス設定ファイルを要求します。

1. **[サーバーレス環境]** ページで、**[新しいサーバーレスランタイム環境]** をクリックします。
2. **[クラウド管理者から設定ファイルを要求]** を選択します。

   [設定ファイルの要求] ダイアログボックスが表示されます。
3. クラウドリージョンを選択します。

   電子メールテンプレートが生成されます。
4. **[クリップボードにコピー]** をクリックします。
5. 希望する電子メールサービスを使用して、テンプレートを使用して電子メールを作成し、クラウド管理者に送信します。

   この電子メールには、クラウド管理者が VPC を作成するか、既存の VPC をサーバーレスランタイム環境に接続してサーバーレス設定ファイルを生成するために使用できる AWS CloudFormation テンプレートへの URL が含まれています。詳細については、「テンプレートを使用した VPC の作成」 (ページ 48)を参照してください。

サーバーレス設定ファイルのインポート

サーバーレス設定ファイルをインポートして、サーバーレスランタイム環境のプロパティを取り込みます。

1. **[サーバーレス環境]** ページで、**[新しいサーバーレスランタイム環境]** をクリックします。
2. **[サーバーレスランタイム環境を作成]** を選択します。
3. 基本プロパティを入力します。
4. プラットフォームプロパティについては、**[インポート構成]** をクリックします。

   [設定ファイルのインポート] ダイアログボックスが表示されます。
5. **[ファイルを選択]** をクリックし、ローカルマシン上のサーバーレス設定ファイルに移動します。
6. **[インポート]** をクリックします。

サーバーレスランタイムの検証

検証プロセスは特定のタスクの実行時に、サーバーレスランタイム環境で AWS リソース構成プロパティと一部のネットワーク設定を検証します。

検証プロセスは IAM ロールを使用して AWS アカウントに接続し、サブネット ID、可用性ゾーン ID、ロール名などのリソースプロパティを検証して一覧表示します。IAM ロールによって、AWS アカウントと Informatica AWS アカウント間の信頼を確立し、サーバーレスランタイム環境が ENI を作成して、クラウド環境のデータソースに安全に接続できるようにします。IAM ロールには、リソースを表示するための権限が必要です。IAM ロールの設定の詳細については、「手動による VPC の作成および設定」 (ページ 46)を参照してください。

検証には、次のロール権限が必要です。

- ec2:DescribeRegions
- ec2:DescribeAvailabilityZones

- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups

リソースの検証に失敗すると、サーバーレスランタイム環境の起動が失敗します。**[サーバーレス環境]** ページまたは特定の［サーバーレスランタイム環境構成］ページのダウンロードオプションを使用して、詳細な検証メッセージをダウンロードできます。検証結果とメッセージは、失敗した環境にのみ表示されます。

サーバーレスランタイム環境のプロパティに加えて、検証プロセスでは、サブネットで使用可能な IP アドレスの数がチェックされます。サブネットで使用可能な IP アドレスが不十分な場合、サーバーレスランタイム環境の作成は失敗します。

注: サブネット ID が Amazon アカウントに存在しない場合、検証プロセスは Amazon Virtual Private Cloud（VPC）ID を検証しません。

サーバーレスランタイム環境のプロパティとネットワーク設定は、サーバーレスランタイム環境で次のタスクを実行した場合に検証されます。

- 新しいサーバーレスランタイム環境を作成する。
- 失敗したサーバーレスランタイム環境を編集し、更新を保存する。
- サーバーレスランタイム環境のクローンを作成し、構成を保存する。
- 失敗したサーバーレスランタイム環境を再デプロイする。

サーバーレスランタイム環境の管理

サーバーレスランタイム環境を作成した後、サーバーレスランタイム環境の編集、再デプロイ、クローン作成などの管理タスクを実行できます。

サーバーレスランタイム環境の編集

環境のステータスに基づいて、サーバーレスランタイム環境のプロパティを編集できます。

- 稼働中。サーバーレスコンピューティングユニットの最大数またはタスクタイムアウトを更新できます。

  サーバーレスコンピューティングユニットの最大数またはタスクタイムアウトを編集すると、更新された値が後続のタスク実行で有効になります。
- 失敗。任意のプロパティを更新できます。プロパティを有効にするには、サーバーレスランタイム環境を再デプロイします。

サーバーレスランタイム環境が異なるステータスを持つ場合は、サーバーレスランタイム環境を削除し、新しい環境を作成してプロパティを編集する必要があります。

サーバーレスランタイム環境を削除する前に、次のタスクを完了します。

- Monitor を使用して、環境でジョブが実行されていないことを確認します。
- サーバーレスランタイム環境を使用している接続およびタスクから、そのサーバーレスランタイム環境を削除します。

サーバーレスランタイム環境の再デプロイ

次の状況では、サーバーレスランタイム環境を再デプロイできます。

- ライセンスを変更する。
- 組織ですべてのサーバーレスコンピューティングユニットを使い切ったため、サーバーレスランタイム環境がシャットダウンする。組織にコンピューティングユニットをさらに追加して、サーバーレスランタイム環境を再デプロイできます。
- クラウド環境で設定を更新する。例えば、補足ファイルの場所にあるファイルを更新する場合や、IAM ロールにアタッチされたポリシーを更新する場合です。

サーバーレスランタイム環境を再デプロイする前に、Monitor で、ジョブがランタイム環境で実行されていないことを確認してください。次に、Administrator で、サーバーレスランタイム環境の **[アクション]** メニューを展開し、**[再デプロイ]** をクリックします。

注: マッピングを実行する前に、再デプロイが完了するまで待ちます。再デプロイ中に実行されているジョブはすべて失敗します。

サーバーレスランタイム環境のクローン作成

サーバーレスランタイム環境のクローンを作成して、同様の設定を持つ別の環境を作成できます。例えば、クラウド環境内の別のサブネットに接続したり、別のセキュリティグループを使用したりする、同様のサーバーレスランタイム環境を作成することができます。

サーバーレスランタイム環境のクローンを作成するには、サーバーレスランタイム環境の **[アクション]** メニューを展開して、**[クローン]** をクリックします。

サーバーレスコンピューティングユニット

サーバーレスコンピューティングユニットとは、サーバーレスランタイム環境でタスクを実行するために使用できる CPU とメモリを表します。

サーバーレスランタイム環境を作成するときは、各タスクがサーバーレスランタイム環境から要求できるサーバーレスコンピューティングユニットの最大数を設定します。マッピングタスクを作成するときは、タスクが要求できるコンピューティングユニットの最大数を上書きできます。Monitor では、タスクが要求および使用したコンピューティングユニットの数を表示できます。

タスクが指定されたタスクタイムアウトよりも長く実行している場合、サーバーレスランタイム環境によってタスクが強制終了されます。

メーターに関する詳細については、「*組織の管理*」を参照してください。

ディザスタリカバリ

障害がサーバーレスランタイム環境をホストするリージョンまたは可用性ゾーンに影響を与える場合は、組織のディザスタリカバリ計画の一環として、安定したリージョンまたは可用性ゾーンの一時的なサーバーレスランタイム環境にジョブをリダイレクトします。

ディザスタリカバリの手順

障害の発生中は、サーバーレスランタイム環境のすべての仮想マシンがシャットダウンし、その環境でジョブを実行できなくなります。

データの損失とダウンタイムを最小限に抑えるには、次のタスクを実行します。

1. 安定したリージョンまたは可用性ゾーンに一時的なサーバーレスランタイム環境を作成します。
2. ジョブで使用される接続が、安定したリージョンまたは可用性ゾーンで使用できることを確認します。
3. 不完全なジョブ実行に関連するデータをクリーンアップします。データがターゲットに部分的にロードされている場合は、新しい行を書き込む前にデータを手動で削除するか、マッピングを更新してターゲットを切り詰めます。
4. ジョブを一時的な環境にリダイレクトします。

プライマリ環境の復元

プライマリサーバーレスランタイム環境をホストするリージョンまたは可用性ゾーンが回復したら、プライマリ環境をリストアできます。

プライマリ環境をリストアするには、以下の操作を実行します。

1. プライマリ環境の AWS アカウントで作成された ENI をクリーンアップします。
2. プライマリ環境を再デプロイします。
3. ジョブをプライマリ環境にリダイレクトします。
4. 一時的な環境を削除します。

サーバーレスランタイム環境でのコネクタ

サーバーレスランタイム環境で使用できるコネクタは、環境で実行されるマッピングのタイプによって決まります。

次のいずれかのマッピングタイプに基づいてコネクタを使用します。

詳細モードのマッピング

サーバーレスランタイム環境は、次のコネクタを使用してソースおよびターゲットに接続できます。

- Amazon DynamoDB V2
- Amazon Redshift V2
- Amazon S3 V2
- Databricks Delta
- Google Cloud Spanner
- JDBC V2
- Kafka

- MongoDB V2
- REST V3
- Snowflake Data Cloud

詳細モード外のマッピング

サーバーレスランタイム環境は、次のコネクタを使用してソースおよびターゲットに接続できます。

- Amazon Aurora コネクタ
- Amazon Redshift V2 コネクタ
- Amazon S3 V2 コネクタ
- Box コネクタ
- Box Oauth コネクタ
- Concur V2 コネクタ
- Coupa V2 コネクタ
- Databricks Delta コネクタ
- DB2 Warehouse on Cloud コネクタ
- Eloqua Bulk API コネクタ
- Google Analytics コネクタ
- Google BigQuery V2 コネクタ
- Google Cloud Spanner コネクタ
- Google Cloud Storage V2 コネクタ
- JDBC（JDBC_IC）コネクタ
- JDBC V2 コネクタ
- Marketo V3 コネクタ
- Microsoft Azure Blob Storage V3 コネクタ
- Microsoft Azure Cosmos DB SQL API コネクタ
- Microsoft Azure Data Lake Storage Gen1 V3 コネクタ
- Microsoft Azure Data Lake Storage Gen2 コネクタ
- Microsoft Azure Synapse SQL コネクタ
- Microsoft Dynamics 365 for Sales コネクタ
- Microsoft SQL Server コネクタ
- MySQL コネクタ
- NetSuite RESTlet V2（NetSuite V2）コネクタ
- ODBC コネクタ
- Oracle コネクタ
- PostgreSQL コネクタ
- REST V2 コネクタ
- Salesforce コネクタ
- Salesforce Marketing Cloud コネクタ

- Salesforce Oauth コネクタ
- SAP コネクタ - SAP ADSO Writer、SAP BAPI、SAP テーブル、SAP ODP Extractor、および SAP HANA
- ServiceNow コネクタ
- Snowflake Data Cloud コネクタ
- SuccessFactors ODATA コネクタ
- SuccessFactors SOAP コネクタ
- Web サービスコンシューマ(WS コンシューマ)コネクタ
- Workday V2 コネクタ
- Zendesk V2 コネクタ

注: サーバーレスランタイム環境の使用方法は、コネクタ固有です。詳細については、該当するコネクタのヘルプを参照してください。

索引