



Informatica® Intelligent Cloud Services  
April 2024

**ランタイム環境**

Informatica Intelligent Cloud Services ランタイム環境  
April 2024

© 著作権 Informatica LLC 2021, 2024

本ソフトウェアおよびマニュアルは、使用および開示の制限を定めた個別の使用許諾契約のもとでのみ提供されています。本マニュアルのいかなる部分も、いかなる手段（電子的複写、写真複写、録音など）によっても、Informatica LLC の事前の承諾なしに複製または転載することは禁じられています。

米政府の権利プログラム、ソフトウェア、データベース、および関連文書や技術データは、米国政府の顧客に配信され、「商用コンピュータソフトウェア」または「商業技術データ」は、該当する連邦政府の取得規制と代理店固有の補足規定に基づきます。このように、使用、複製、開示、変更、および適応は、適用される政府の契約に規定されている制限およびライセンス条項に従うものとし、政府契約の条項によって適当な範囲において、FAR 52.227-19、商用コンピュータソフトウェアライセンスの追加権利を規定します。

Informatica、Informatica Cloud、Informatica Intelligent Cloud Services、PowerCenter、PowerExchange、および Informatica ロゴは、米国およびその他の国における Informatica LLC の商標または登録商標です。Informatica の商標の最新リストは、Web (<https://www.informatica.com/trademarks.html>) にあります。その他の企業名および製品名は、それぞれの企業の商標または登録商標です。

本ソフトウェアまたはドキュメンテーション（あるいはその両方）の一部は、第三者が保有する著作権の対象となります。必要な第三者の通知は、製品に含まれています。

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、[infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com) までご報告ください。

Informatica 製品は、それらが提供される契約の条件に従って保証されます。Informatica は、商品性、特定目的への適合性、非侵害性の保証等を含めて、明示的または黙示的ないかなる種類の保証をせず、本マニュアルの情報を「現状のまま」提供するものとします。

発行日: 2024-06-17

# 目次

<b>序文</b> .....	6
Informatica のリソース.....	6
Informatica マニュアル.....	6
Informatica Intelligent Cloud Services Web サイト.....	6
Informatica Intelligent Cloud Services コミュニティ.....	6
Informatica Intelligent Cloud Services マーケットプレイス.....	7
データ統合のコネクタのドキュメント.....	7
Informatica ナレッジベース.....	7
Informatica Intelligent Cloud Services Trust Center.....	7
Informatica グローバルカスタマサポート.....	7
<b>第 1 章 : ランタイム環境</b> .....	8
<b>第 2 章 : Hosted Agent</b> .....	9
<b>第 3 章 : Secure Agent グループ</b> .....	11
複数のエージェントを含む Secure Agent グループ.....	11
Secure Agent グループに対するサービスとコネクタの割り当て.....	12
サービス割り当てのガイドライン.....	13
Secure Agent グループのサービスとコネクタの有効化または無効化.....	14
サービスとコネクタの割り当ての例.....	14
Secure Agent グループの共有.....	15
共有された Secure Agent グループでのフラットファイル接続.....	15
Secure Agent グループの操作.....	16
グループへの Secure Agent の追加.....	17
既存のグループへの新規 Secure Agent の追加.....	18
グループからの Secure Agent の削除.....	19
Secure Agent グループの依存関係の表示.....	19
<b>第 4 章 : Secure Agent</b> .....	21
Secure Agent の操作.....	21
Secure Agent でのサービスの停止と開始.....	24
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.....	25
Secure Agent サービスの停止.....	26
Secure Agent サービスの開始.....	26
エージェントのブラックアウト期間の設定.....	26
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.....	27
ブラックアウトファイルの構造.....	28
Secure Agent の名前変更.....	29
Secure Agent の削除.....	29

Secure Agent のアップグレード. . . . .	29
Secure Agent のデータ暗号化. . . . .	30
Windows でのデータ暗号化キーの変更. . . . .	30
Linux でのデータ暗号化キーの変更. . . . .	31
Secure Agent Manager. . . . .	32
Secure Agent でのプロキシサーバーの使用. . . . .	32
非プロキシホストを除外するためのプロキシの設定. . . . .	33
Windows での Secure Agent の停止および再起動. . . . .	33
Linux での Secure Agent の起動および停止. . . . .	34
Secure Agent のログ. . . . .	34
Secure Agent のトラブルシューティング. . . . .	37
<b>第 5 章 : クラウド環境での Secure Agent のインストール. . . . .</b>	<b>40</b>
AWS でのインストール. . . . .	40
Azure でのインストール. . . . .	43
<b>第 6 章 : ローカル環境での Secure Agent のインストール. . . . .</b>	<b>46</b>
Windows での Secure Agent のインストール. . . . .	46
Windows での Secure Agent の要件. . . . .	47
Windows での Secure Agent のダウンロードおよびインストール. . . . .	48
Windows でのプロキシ設定. . . . .	50
Windows Secure Agent サービスへのログインの設定. . . . .	50
Windows での Secure Agent のアンインストール. . . . .	51
Linux での Secure Agent のインストール. . . . .	51
Linux での Secure Agent の要件. . . . .	52
Linux での Secure Agent のダウンロードおよびインストール. . . . .	53
Linux でのプロキシ設定. . . . .	54
Linux での Secure Agent のアンインストール. . . . .	55
Secure Agent インストールのトラブルシューティング. . . . .	55
<b>第 7 章 : AWS でのサーバーレスランタイム環境のセットアップ. . . . .</b>	<b>56</b>
手動での環境の作成および設定. . . . .	57
テンプレートを使用した VPC の作成. . . . .	59
AWS CloudFormation テンプレートを使用した新しい VPC の作成. . . . .	60
AWS CloudFormation テンプレートを使用した既存の VPC への接続. . . . .	63
スタックのトラブルシューティング. . . . .	65
VPC 設定の一般的なタスク. . . . .	66
信頼済みの Informatica IP アドレスの追加. . . . .	67
システムディスクの設定. . . . .	69
データディスクとしての EFS または NFS ディレクトリの使用. . . . .	70
データディスクの設定. . . . .	71
補足ファイルの場所の作成. . . . .	71
REST API を認証するための TLS の設定. . . . .	72

serverlessUserAgentConfig.yml ファイルの設定. . . . .	73
serverlessUserAgentConfig.yml ファイルへの入力. . . . .	73
エラスティックサーバーのファイルのコピー. . . . .	75
JDBC V2 コネクタ JAR ファイルのコピー. . . . .	75
Java トランスフォーメーション JAR ファイルのコピー. . . . .	75
Python トランスフォーメーションリソースファイルのコピー. . . . .	76
環境の実行中におけるファイルの追加. . . . .	76
プロキシサーバーの使用. . . . .	77
serverlessUserAgentConfig.yml ファイルでのプロキシの設定. . . . .	77
JVM オプションでのプロキシの設定. . . . .	77
プロキシサーバーでのドメインの許可. . . . .	78
<b>第 8 章 : サーバーレスランタイム環境. . . . .</b>	<b>79</b>
Azure でのサーバーレスランタイム環境の作成. . . . .	79
AWS でのサーバーレスランタイム環境の作成. . . . .	80
サーバーレスランタイム環境のプロパティ. . . . .	80
サーバーレス設定ファイルの使用. . . . .	84
サーバーレスランタイムの検証. . . . .	85
サーバーレスランタイム環境の管理. . . . .	86
サーバーレスランタイム環境の編集. . . . .	86
サーバーレスランタイム環境の再デプロイ(AWS). . . . .	86
サーバーレスランタイム環境のクローン作成. . . . .	87
サーバーレスランタイム環境の削除. . . . .	87
サーバーレスコンピューティングユニットのメータリング. . . . .	87
ディザスタリカバリ (AWS) . . . . .	88
サーバーレスランタイム環境でのコネクタ. . . . .	88
<b>索引. . . . .</b>	<b>91</b>

# 序文

ランタイム環境の説明を使用して、Informatica Intelligent Cloud Services<sup>SM</sup>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](mailto: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 マーケットプレイス

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/>

## データ統合のコネクタのドキュメント

データ統合の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](mailto: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。

サブスクライブするには、[Informatica Intelligent Cloud Services Status](#) ページで **【サブスクライブして更新】** をクリックします。電子メール、SMS テキストメッセージ、Webhook、RSS フィード、またはこの 4 つの任意に組み合わせとして送信される通知を受信するという選択ができます。

## Informatica グローバルカスタマサポート

グローバルサポートセンターには、Informatica Network または電話でお問い合わせください。

Informatica Network でオンラインサポートリソースを検索するには、Informatica Intelligent Cloud Services のヘルプメニューで **【サポートにお問い合わせください】** をクリックして、**Cloud Support** ページに移動します。**Cloud Support** ページには、システムステータス情報とコミュニティディスカッションが記載されています。追加のリソースを検索する場合や電子メールで Informatica グローバルカスタマサポートに問い合わせる場合は、Informatica Network にログインし、**【サポートが必要な場合】** をクリックしてください。

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> に掲載されていません。

# 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 ホステッドエージェントを使用します。**

ホステッドエージェントを使用する場合は、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 をインストールし、ネットワーク内または AWS や Google Cloud、Microsoft Azure、Oracle Cloud Infrastructure 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。複数のエージェントを 1 つの Secure Agent グループに追加できます。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 8 章, 「サーバーレスランタイム環境」 \(ページ 79\)](#)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

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

Informatica Intelligent Cloud Services では 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、または設定することはできません。

Hosted Agent は、次のコネクタを使用する同期、マッピング、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 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 Storage 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。

Secure Agent グループに対して次のアクションを実行できます。

- グループから Secure Agent を追加および削除できます。
- 複数のエージェントを Secure Agent グループに追加できます。  
**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。
- サブ組織と Secure Agent グループを共有できます。

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を実行する場所を指定します。

## 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。複数のエージェントを 1 つの Secure Agent グループに追加できます。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

組織は、Secure Agent グループに対して、組織が使用ライセンスを取得している特定の Informatica Intelligent Cloud Services およびコネクタを有効化または無効化することができます。

次のアクションを実行できます。

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

アプリケーションの統合やデータ統合などのサービスは、グループ内のエージェントが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できるようにする場合に有効化することができます。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。

サービスを有効にすると、必要な Secure Agent サービスも有効になります。それぞれのサービスに必要な 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。

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

グループ内のエージェントが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には、特定のコネクタを有効にします。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。

セルフホステッド Git リポジトリや EDC 統合などの追加のサービスを有効化または無効化することができます。

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 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。

**[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化または無効化します。

Name	Version	Status	Description	Type	Update Time
ABC		Running		Agent Group	Jul 27, 2022, 1:05 PM
> AGENT_CRRT (1)		Stopped		Agent Group	May 22, 2022, 12:08 AM
AGENT_CRRT_bck		No Secure Agents		Agent Group	Jun 24, 2021, 12:58 AM
AGENT_CRRT_ec2		No Secure Agents		Agent Group	Apr 13, 2022, 6:26 PM
AGENT_CRRT_ilabam...		No Secure Agents		Agent Group	Aug 4, 2021, 6:10 AM
> AGENT_CRRT_inv76 (...)		Stopped		Agent Group	Sep 13, 2021, 7:16 AM
AGENT_CRRT_linux1		No Secure Agents		Agent Group	May 13, 2021, 1:32 AM
> AGENT_CRRT_ssr (1) (...)		Stopped		Agent Group	Sep 22, 2021, 9:26 AM
agent_discale_aws_jla...		No Secure Agents		Agent Group	Jan 11, 2023, 8:30 AM
agent_discale_aws_jla...		No Secure Agents		Agent Group	Mar 21, 2023, 5:47 AM
agent_discale_aws_jn...		No Secure Agents		Agent Group	Aug 3, 2021, 7:25 AM

## 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サービスを有効化または無効化する場合は、次のガイドラインを使用してください。

- 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。
- 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。
- 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 グループのサービスとコネクタの有効化または無効化

Secure Agent グループに対する Informatica Intelligent Cloud Services およびコネクタを有効化または無効化できます。デフォルトでは、新しく作成された Secure Agent グループでは、すべてのサービスとコネクタが無効になっています。グループで実行するサービスと接続を有効にします。

1. [Administrator] 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、[サービスとコネクタの有効化または無効化] を選択します。  
Secure Agent グループのすべてのサービスとコネクタが一覧表示されたダイアログボックスが表示されます。
3. [サービス] タブで、有効化または無効化する Informatica Intelligent Cloud Services を選択します。  
特定のサービスが [追加サービス] タブに表示される場合もあります。
4. [コネクタ] タブで、有効化または無効化するコネクタを選択します。
5. [追加サービス] タブで、有効化または無効化する Secure Agent サービスを選択します。  
例えば、組織でソース管理を使用していて、Secure Agent グループでその管理を無効にする場合は、GitRepoConnectApp サービスを無効にします。  
このリストに表示されるサービスは、ライセンスによって異なります。ここにリストされているサービスが表示されない場合もあります。
6. [OK] をクリックします。  
変更内容は、グループ内のすべての Secure Agent に反映されます。

## サービスとコネクタの割り当ての例

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。

## 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できるようになります。

**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および一括取り込みファイルのみを実行する場合は、Secure Agent グループを共有します。その他のエージェントサービスの場合、共有 Secure Agent グループでジョブを実行することはできません。

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できます。

## 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、接続で使わ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。また、グループのサービスとコネクタを有効にすることもできます。

**ヒント:** Secure Agent グループに対してアクションを実行する前に、**[新しいランタイム環境]** の横にある更新アイコンをクリックしてページを更新します。

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、グループの名前と、必要に応じて説明を入力します。グループを作成した後、グループに Secure Agent を追加できます。

**注:** Secure Agent グループ名にマルチバイト文字を使用していて、クラウドホスト環境でグループを作成する場合は、その環境でもこれらの文字がサポートされていることを確認してください。

## Secure Agent グループのプロパティを編集します。

Secure Agent グループの名前を変更する場合、または説明を追加あるいは更新する場合は、**[アクション]** メニューを展開し、**[環境のプロパティの編集]** を選択して、ダイアログボックスのフィールドに値を入力します。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。

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、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、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、**[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、この設定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]** 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。

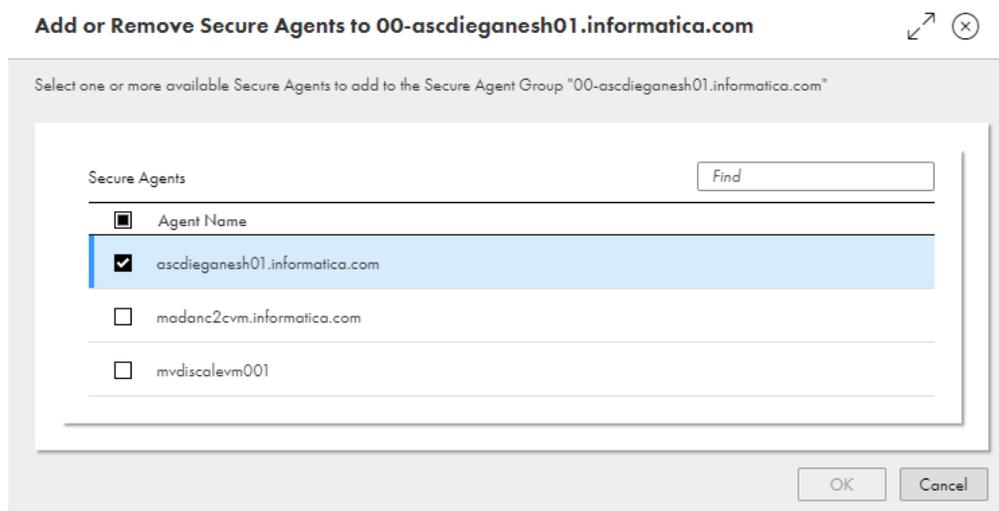
権限	説明
読み取り	Secure Agent グループに関する詳細を表示し、タスクで Secure Agent グループを使用します。
更新	Secure Agent グループを編集します。
削除	Secure Agent グループを削除します。
変更	Secure Agent グループの権限を変更します。

## 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。Secure

Agent をグループに追加すると、Secure Agent はそのグループに対して有効になっているすべてのサービスとコネクタを継承します。

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. **[Secure Agent]** 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。  
必要なエージェントがリストにない場合は、現在別のグループに割り当てられていることを意味します。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。  
リストに多数のエージェントが表示されている場合は、**[検索]** ボックスを使用してエージェントをすばやく探すことができます。



4. **[OK]** 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。Secure Agent をグループに追加すると、Secure Agent はそのグループに対して有効になっているすべてのサービスとコネクタを継承します。

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. **[Secure Agent]** のリストで、グループから削除するエージェントの横にあるチェックマークをオフにします。
4. **[OK]** をクリックします。

削除された Secure Agent 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。

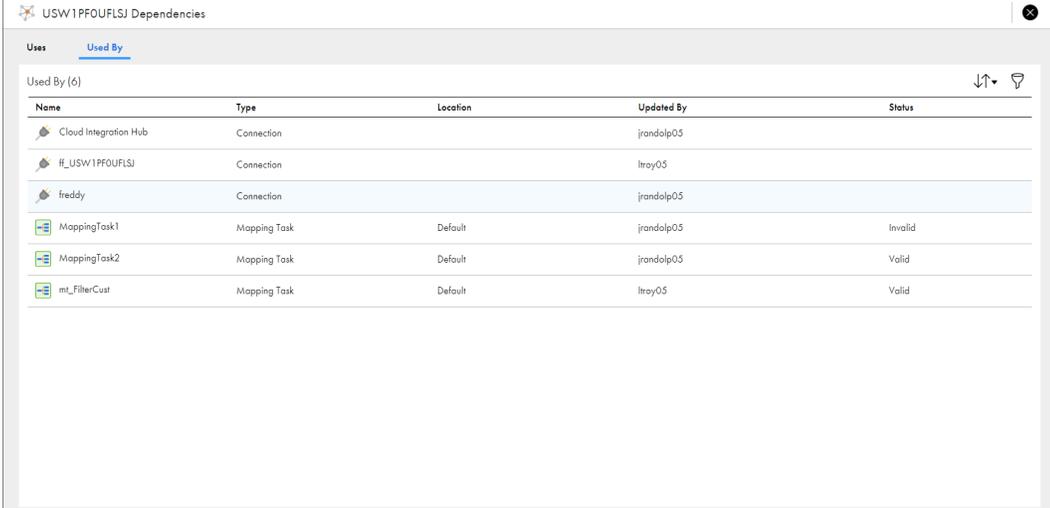
## Secure Agent グループの依存関係の表示

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

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。



Name	Type	Location	Updated By	Status
Cloud Integration Hub	Connection		jrandolp05	
#_USW1PF0UFLSJ	Connection		ltroy05	
freddy	Connection		jrandolp05	
/MappingTask1	Mapping Task	Default	jrandolp05	Invalid
/MappingTask2	Mapping Task	Default	jrandolp05	Valid
mt_FilterCust	Mapping Task	Default	ltroy05	Valid

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列名を選択します。

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、データ処理にプラグイン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およびプロセスオーケストレーションジョブを実行します。。それぞれの Secure Agent サービスには、Tomcat 設定や Tomcat JRE 設定などの一意的な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。

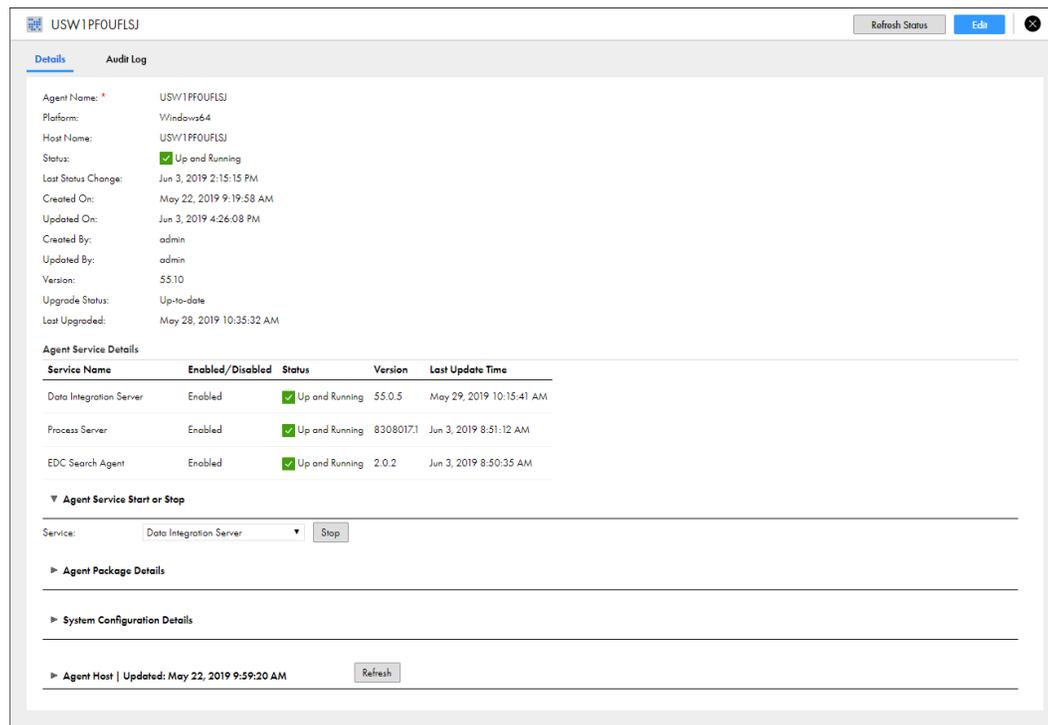
1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールして実行できます。Secure Agent をインストールすると、組織内のすべてのユーザーがその Secure Agent を共有します。Secure Agent のプロパティを設定し、別の Secure Agent グループに移動することができます。また、拡張性を向上させるために、Secure Agent グループに複数のエージェントを追加することもできます。

## 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行うように、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 64.0.38 のデータ統合サーバーを使用している場合、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 のインストールディレクトリ>/apps/Data\_Integration\_Server/64.0.38.1

データ統合サーバーを停止および再起動すると、Secure Agent によって次のディレクトリが作成されます。

<Secure Agent のインストールディレクトリ>/apps/Data\_Integration\_Server/64.0.38.2

Secure Agent によってディレクトリ.../64.0.38.1 が削除されることはありません。

## 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 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

データ統合サーバーの BlackoutWindowsFile Tomcat カスタムプロパティを設定することで、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。

エージェントの詳細ページでデータ統合サーバーに次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 <b>注:</b> 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。 <ul style="list-style-type: none"><li>- 1 回</li><li>- 日次</li><li>- 平日</li><li>- 日曜日</li><li>- 月曜日</li><li>- 火曜日</li><li>- 水曜日</li><li>- 木曜日</li><li>- 金曜日</li><li>- 土曜日</li></ul>
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ください。

# 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。  
**注:** Secure Agent 名にマルチバイト文字を使用していて、そのエージェントがクラウドホスト環境にある場合は、その環境でもこれらの文字がサポートされていることを確認してください。
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。

**注:** Secure Agent は、エージェントのバージョンが現在のメジャーリリースであり、エージェントが実行されている場合にのみアップグレードできます。例えば、新しいメジャーリリースによって Secure Agent がバージョン 65.x にアップグレードされる場合、このアップグレードにはエージェントがバージョン 64.x であること、およびエージェントが実行中であることが必要です。

# 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、攻撃者が Secure Agent を別のマシンにコピーして実行することを防止します。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。

Secure Agent 内に保存されているすべての情報を暗号化するために、Informatica は暗号化方式として AES 256 を使用します。この方法では、Secure Agent に固有のキーを使用します。暗号化キーは、マシン固有の情報を使用して生成され、<Secure Agent のインストールディレクトリ>/apps/agentcore/conf に格納されます。

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
<code>INFA_AGENT_EXCLUDE_SEC_PROPS</code>	除外するプロパティを指定します。 <code>rotateDeviceKey</code> コマンドで除外した同じ値を設定します。
<code>INFA_AGENT_ADDITIONAL_SEC_PROPS</code>	追加するプロパティを指定します。 <code>rotateDeviceKey</code> 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、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\=\n
InfaAgent.ProxyNtDomain=\n
InfaAgent.ProxyHost=foo.bar.com
InfaAgent.ProxyPasswordEncrypted=true
InfaAgent.NonProxyHost=localhost|127.*|[\:\  
InfaAgent.ProxyUser=\n
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.|[\:\  
|123.432.
```

- ホスト名:

```
InfaAgent.NonProxyHost=localhost|127.|[\:\  
|.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、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 のインストールディレクトリ>/apps/agentcore
2. Secure Agent を起動するには、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 のログ

さまざまな Secure Agent サービスは独自のログを生成します。これらのログは、問題のトラブルシューティングに役立ちます。

**ヒント:** 次のファイルパス内の「<install>」は、Secure Agent がインストールされているディレクトリを表します。

### 全般

次の表に、一般的な Secure Agent ログファイルに関する説明と、ファイルが存在する\apps サブディレクトリを示します。

ファイル	説明
<install>\apps\agentcore \agentcore.log	エージェントアプリケーションのアップグレードや通信用のトンネルを開く処理など、Secure Agent によって管理されるすべての操作を追跡します。
<install>\apps\agentcore \infaagent.log	エージェントのブートストラップに関連するログが含まれています。
<install>\apps\agentcore \agentUpgrLog.txt	エージェントコアのアップグレードのタイムスタンプを保持します。
<install>\apps\agentcore \consoleAgentManager.log	エージェントの登録に関連するログが含まれています。
<install>\apps\Administrator\logs \tomcat\tomcat.log	パッケージの事前ダウンロードに関連するログが含まれています。

## B2B プロセッサ

ファイル	説明
<install>\apps\B2BProcessor \<version>\logs\b2b-aaap.log	主要な実行エントリポイント、失敗メッセージ、B2B プロセッササービスステータスに関する情報が含まれています。

## CIH プロセッサ

CIHProcessor ログは、Cloud 統合ハブでプライベートリポジトリを使用したときに生成されます。

ファイル	説明
<install>\apps \CIHProcessor \<version>\logs\cih- aaap.log	次の項目に関する情報が含まれています。 - Cloud 統合ハブのエージェントアプリケーションの開始と停止に関するログ。 - プライベートステージングデータベースでの CRUD ランタイム操作に関するログ。例えば、CIH トピックの作成、読み取り、更新、削除アクションのログや、Cloud 統合ハブパブリケーションおよびサブスクリプションの読み取りまたは書き込み操作のログが含まれます。
<install>\apps \CIHProcessor \<version>\log\prs- audit.log	CIHProcessor によって公開された API の entry と exit のアクセスログが含まれます。

## 共通統合コンポーネント

ファイル	説明
<install>\apps \Common_Integration_Components\logs \<version>\app.log	共通統合コンポーネントサービスに関する情報が含まれています。
<install>\apps \Common_Integration_Components\logs \<version>\tomcat.out	共通統合コンポーネントサービスの標準出力に関するログ情報が含まれています。

## データ統合サーバー

ファイル	説明
<install>\apps\agentcore	「全般」セクションに記載されているログファイルを参照してください。
<install>\apps \Data_Integration_Server\logs \tomcat	Tomcat サーバーに関する情報が含まれています。
<install>\apps \Data_Integration_Server\logs \tomcat\tomcat<version>.log	データ統合サーバーサービスに関する情報が含まれています。

ファイル	説明
<install>\apps \Data_Integration_Server\<version> \tomcat.out	データ統合サーバーの標準出力ログに関する情報が含まれています。
<install>\apps \Data_Integration_Server\<version> \scripts.log	データ統合サーバーのライフサイクルスクリプトに関する情報が含まれています（例: デプロイ、起動、ステータス、および停止のスクリプト）。
<install>\apps \Data_Integration_Server\logs \session logs	データ統合サーバーのタスクセッションに関する情報が含まれています。

## ファイル統合サービス

ファイル	説明
<install>\apps \FileIntegrationService\logs \FileIntegrationService.log	<p>ファイル統合サービスに関連するログが含まれています。これには次のような情報が含まれます。</p> <ul style="list-style-type: none"> <li>- AS2、HTTP、SFTP、MLLP などのファイルサーバーに関連するログ</li> <li>- 暗号化、復号化、圧縮、解凍などのタスクを転送します。</li> <li>- API によってトリガされるジョブ（SFTP/AS2/FTP へのファイルの送信など）。</li> <li>- ファイラサーバーのユーザー</li> <li>- fis-proxy への接続</li> </ul>

## 一括取り込みランタイム

ファイル	説明
<install>\apps \MassIngestionRuntime\logs \informaticamft.log	ファイル一括取り込みおよび MassIngestionRuntime サービスを実行するファイルリスナログに関連するログ情報が含まれています。また、このサービスの起動とステータスに関連するログが含まれています。

## オペレーションインサイトデータコレクタ

ファイル	説明
<install>\apps \OpsInsightsDataCollector\logs \App.log	オペレーションインサイトデータコレクタ（「FOI データコレクタ」とも呼ばれます）の起動情報が含まれています。
<install>\apps \OpsInsightsDataCollector\logs \datacollector.log	オンプレミスとクラウドのデータコレクションに関する情報が含まれています。また、オペレーションインサイトデータコレクタサービスによって実行されるパブリッシュに関する情報が含まれています。

## プロセスサーバー

ファイル	説明
<install>\apps\process-engine\logs\catalina.log	プロセスサーバーからのログ情報が含まれています。これは、ランタイムエラーを診断するために役立ちます。
<install>\apps\process-engine\logs\scripts.log	データベースやサーバー自体を含むプロセスサーバーのコンポーネントを開始または停止するために、agentcore によって実行されるスクリプトからのログが含まれています。
<install>\apps\process-engine\logs\localhost-access.log	例えば、IP アドレス、時刻、GET や POST などの要求メソッド、要求の送信元のリソースなどの、要求に関連付けられた情報が含まれています。
<install>\apps\process-engine\logs\PostGreSql\upgrade.log	データベースのバージョンがアップグレードされたかどうか、またはいつアップグレードされたかに関する情報を取得するログが含まれています。
<install>\apps\process-engine\logs\PostGreSql\postgresql.log	データベース関連の問題の診断に役立つ、PostgreSQL データベースのログが含まれています。

# Secure Agent のトラブルシューティング

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. 次のログを確認します。

ファイル	説明
<Secure Agent インストールディレクトリ>\apps\agentcore\infaagent.log	Secure Agent の起動およびシャットダウンに関する情報が含まれます。
<Secure Agent インストールディレクトリ>\apps\agentcore\agentcore.log	Secure Agent 関連のアクティビティに関する情報（エージェントに対して有効になっているすべてのサービスの詳細など）が含まれます。
<Secure Agent インストールディレクトリ>\apps\Data_Integration_Server\logs\tomcat\tomcat<バージョン>.log	データ統合サーバーの Tomcat プロセスに関する詳細が含まれます。タスクの開始時刻、終了時刻、統計情報など、タスク実行の詳細が記録されます。また、データ統合アセットの設計時およびメタデータ関連のアクティビティが含まれます。

ファイル	説明
<Secure Agent インストールディレクトリ>\apps \Data_Integration_Server\<<バージョン> \tomcat.out	Tomcat プロセスの開始時刻と停止時刻など、データ統合サーバーの Tomcat プロセスに関する基本情報が含まれます。また、証明書や SSL 関連情報など、Secure Agent 接続の詳細が含まれます。
<Secure Agent インストールディレクトリ>\apps \Data_Integration_Server\<<バージョン> \scripts.log	データ統合サーバーで使用されるスクリプトの実行方法の詳細など、データ統合サーバーに関する情報が含まれます。 データ統合サーバーに問題がある場合は、このログを使用してください。

- Windows 上で実行される Secure Agent の場合は、Windows 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。

### 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 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、ログインを使用して Informatica Intelligent Cloud Services 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。

### 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。

### Secure Agent の Administrator に常に「Agent Core のアップグレード中」と表示されるのはなぜですか？

Administrator の [ランタイム環境] ページでは、エージェントのステータスが常に「Agent Core のアップグレード中」と表示されます。agentcore.log ファイルに次のメッセージが表示されます。

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

この問題は、エージェントで以前の 1 つ以上のメジャーアップグレードが実行されていない場合に発生します。例えば、バージョン 62.x のエージェントを停止し、再起動したときに現在のバージョンが 65.x であるとし、自動アップグレードは以前のメジャーバージョン 64.x からのアップグレードのみをサポートしますが、お使いのバージョンはバージョン 64.x よりも古いいため、自動アップグレードは失敗します。

この問題を解決するには、Secure Agent を再登録または再インストールします。  
エージェントのバージョンは、Secure Agent の [詳細] タブで確認できます。

Details	Audit Log
Agent Name: *	asCDIEHQILABS01
Platform:	Linux64
Host Name:	asCDIEHQILABS01
Status:	<input checked="" type="checkbox"/> Up and Running
Last Status Change:	Mar 1, 2023 10:14:27 AM
Created On:	Feb 6, 2023 10:23:46 AM
Updated On:	Mar 1, 2023 1:24:07 PM
Created By:	admin
Updated By:	agent
Version:	65.04
Upgrade Status:	Up-to-date
Last Upgraded:	Feb 15, 2023 7:29:53 AM

## 第 5 章

# クラウド環境での Secure Agent のインストール

Secure Agent をインストールする方法は複数ありますが、クラウド環境にインストールするのが一般的です。[ランタイム環境] ページには、AWS または Microsoft Azure のインストールを合理化するためのインストールウィザードが用意されています。

Secure Agent は次の方法でインストールできます。

### AWS または Microsoft Azure クラウド環境の場合

AWS では、インストールを続行するために AWS Marketplace にリダイレクトされます。

Azure では、最初に Azure 資格情報を使用してログインし、次に Secure Agent の重要な設定の詳細を入力します。

これらの環境にインストールする場合、Secure Agent インストーラを個別にダウンロードする必要はありません。

### 異なるクラウド環境の場合

AWS または Azure を使用していない場合は、最初にクラウド環境に VM をセットアップしてから、[「第 6 章, 「ローカル環境での Secure Agent のインストール」 \(ページ 46\)」](#)に記載されている手順を実行します。

### ローカル環境の場合

Windows または Linux を実行しているローカルマシンにインストールするには、最初にシステムが前提条件を満たしていることを確認してから、Secure Agent インストーラをダウンロードします。詳細については、[第 6 章, 「ローカル環境での Secure Agent のインストール」 \(ページ 46\)](#)を参照してください。

## AWS でのインストール

の Secure Agent インストーラを使用して、Amazon Web Services (AWS) にランタイム環境を作成できます。作成するランタイム環境は、1 つの Secure Agent を含む Secure Agent グループです。

AWS にランタイム環境を作成する場合は、Secure Agent がデプロイされる新しいスタックを作成します。スタックは、新規または既存の Virtual Private Cloud (VPC) に作成できます。インストーラにより、VPC 内に Amazon Elastic Compute Cloud (EC2) インスタンスが作成されます。

ランタイム環境を作成するには、次のリソースタイプの作成、変更、削除特権を含む AWS のサブスクリプションが必要です。

- AWS CloudFormation テンプレート。AWS CloudFormation テンプレートは、ap-southeast-2、eu-west-2、eu-central-1、us-west-2 の各リージョンをサポートしています。
- EC2 インスタンス
- エラスティック IP アドレス
- エラスティックネットワークインタフェース
- インターネットゲートウェイ
- ルートテーブル
- セキュリティグループ
- サブネット
- VPC

また、マシンイメージと AWS CloudFormation テンプレートの読み取り権限と起動権限が必要です。

1. [Administrator] 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、[Cloud Secure Agent の管理] をクリックします。
3. [新しい Cloud Secure Agent] をクリックします。
4. [Amazon Web Services] を選択します。
5. [次へ] をクリックします。
6. [環境設定] ページで、インストールトークンをコピーします。  
インストールトークンの有効期限は 24 時間で、再利用することはできません。
7. ランタイム環境を既存の VPC に作成するか、新しい VPC に作成するかを選択します。
8. [AWS での設定を続行] をクリックします。  
AWS の [サインイン] 画面が新しいブラウザタブで開きます。
9. AWS アカウントにサインインします。  
[スタックのクイック作成] ページが開きます。
10. [スタック名] 領域で、スタック名を入力します。
11. [パラメータ] 領域の [ネットワーク設定] で、既存の VPC を使用しているか新しい VPC を使用しているかに基づいて次のプロパティを設定します。
  - 既存の VPC の場合は、次のプロパティを設定します。

プロパティ	値
VPC ID	Secure Agent をデプロイする VPC の ID を選択します。
サブネット ID	VPC 内のサブネットを入力または選択します。
許可されたりリモートアクセス CIDR	Secure Agent をインストールできる IP アドレスを指定する CIDR ブロックを入力します。 CIDR (Classless Inter-Domain Routing)は、IP アドレスを割り当てるための方法です。ネットワークルールで Secure Agent へのリモートアクセスを許可するように設定します。アドレスの"/x"の部分により、サブネットで使用可能な IP アドレスの数が決定されます (例:108.124.81.10/32)。

- 新しい VPC の場合は、次のプロパティを設定します。

プロパティ	値
可用性ゾーン	現在のリージョンの可用性ゾーンを選択します。
VPC CIDR	VPC を作成する IP アドレスを指定する CIDR ブロックを入力します。
サブネット CIDR	選択した可用性ゾーン内のサブネットの IP アドレスを指定する CIDR ブロックを入力します。
許可されたリモートアクセス CIDR	Secure Agent をインストールできる IP アドレスを指定する CIDR ブロックを入力します。

12. **[Amazon EC2 の設定]** で、次のプロパティを設定します。

プロパティ	値
キーペア名	既存の EC2 キーペアの名前を入力して、EC2 インスタンスへの外部アクセスを有効にします。サーバーへの SSH アクセスには、対応するキーペアファイルが必要です。
インスタンスタイプ	EC2 インスタンスのインスタンスタイプを選択するか、デフォルトのインスタンスタイプを受け入れます。 デフォルトは m5.xlarge です。
エラスティック IP アドレスリングの有効化	エラスティック IP アドレスを EC2 インスタンスに割り当てるか、デフォルトのアドレスを受け入れるかを選択します。 デフォルトは [いいえ] です。

13. **[Informatica Intelligent Data Management Cloud (IDMC) アカウントの詳細]** で、次のプロパティを設定します。

プロパティ	値
IDMC POD マスタ URL	IDMC POD マスタ URL のデフォルト値を受け入れます。これは、Informatica Intelligent Cloud Services へのアクセスに使用する URL です。 <b>警告:</b> この URL を変更すると、スタックのデプロイメントが失敗する可能性があります。
IDMC ユーザー名	Informatica Intelligent Cloud Services ユーザー名を入力します。
IDMC ユーザートークン	コピーしたインストールトークンを貼り付けます。 インストールトークンをコピーし忘れた場合は、Informatica Intelligent Cloud Services に切り替えて新しいトークンを生成できます。
Secure Agent グループ名	Secure Agent グループ名のデフォルト値を受け入れます。これは、作成しているランタイム環境の名前です。

14. **[スタックの作成]** をクリックします。

スタックの作成には数分かかります。スタックの作成を必ず監視し、発生する可能性のある問題に対処してください。CloudFormation スタックのトラブルシューティングの詳細については、AWS のマニュアルを参照してください。

スタックが正常に作成されると、EC2 インスタンスのステータスが CREATE\_IN\_PROGRESS から CREATE\_COMPLETE に変わります。

15. Informatica Intelligent Cloud Services の **[環境設定]** ページで、**[完了]** をクリックします。

IICS でランタイム環境が作成され、**[ランタイム環境]** ページに表示されます。

**ヒント:** 保留中の Secure Agent の進行状況を確認するには、**[ランタイム環境]** ページで **[Cloud Secure Agent の管理]** をクリックします。統計がページの上部に表示されます。

Secure Agent サービスが起動するまでに数分かかります。Secure Agent を使用する準備が整うと、ステータスが **[環境設定を保留中]** から **[稼働中]** に変わります。更新されたステータスを表示するには、ページの更新が必要になる場合があります。

## Azure でのインストール

の Secure Agent インストーラを使用して、Microsoft Azure にランタイム環境を設定できます。Azure でデータ統合タスクを実行すると、ワークロードと VM サイズに基づいてコストが発生することに注意してください。

**注:** リソースをデプロイできる権限が割り当てられた Microsoft Azure サブスクリプションが必要です。組織で管理者の同意が有効になっている場合は、アプリの同意の承認について Azure 管理者に問い合わせてください。管理者の同意要求の詳細については、[Microsoft documentation](#) を参照してください。

1. **[Administrator]** 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、**[Cloud Secure Agent の管理]** をクリックします。
3. **[新しい Cloud Secure Agent]** をクリックします。
4. **[Microsoft Azure]** を選択します。
5. **[次へ]** をクリックします。
6. 使用する Microsoft アカウントを選択します。

7. 以下のプロパティを入力します。

プロパティ	説明
サブスクリプション	<p>Microsoft Azure サブスクリプションを選択します。サブスクリプションには、次のリソースをデプロイするための権限が含まれている必要があります。</p> <ul style="list-style-type: none"> <li>- ネットワークセキュリティグループ</li> <li>- 仮想ネットワーク (サブネットを含む)</li> <li>- ネットワークインタフェース</li> <li>- パブリック IP アドレス</li> <li>- OS ディスク</li> <li>- 仮想マシン</li> </ul> <p>プロンプトが表示されるので、必ず Hyperscalar Azure 統合アプリに権限を付与してください。</p> <p><b>注:</b> Azure サブスクリプションがない場合は、インストーラを終了し、Microsoft にサインアップします。Informatica Intelligent Cloud Services 内からサインアップすることはできません。</p>
リソースグループ	<p>リソースグループは、ランタイム環境の関連リソースを保持するコンテナです。Informatica Intelligent Cloud Services は、Secure Agent ごとに 1 つのリソースグループを使用して、そのエージェントの VM リソースの管理を簡素化します。</p> <p>通常は新しいリソースグループを作成しますが、空の既存のグループを使用することもできます。</p> <p><b>ヒント:</b> 各エージェントに属するリソースグループをより簡単に識別するには、Secure Agent と同じ名前または類似した名前を使用します。</p>
リソースグループ名	<p>リソースグループの名前。新しいグループの名前を入力するか、既存のグループを選択します。</p> <p>既存のリソースグループが空であることを確認してください。空ではない場合は、「API 入力検証に失敗しました」というメッセージが表示されます。</p>
ロケーション	<p>Secure Agent をデプロイするリージョンを選択します。組織と顧客に適した Azure リージョンを選択してください。一部のリソースは特定のリージョンでは使用できない場合もあります。</p>
VM 名	<p>作成する仮想マシン (VM) の名前を入力します。</p>
VM ユーザー名	<p>仮想マシンユーザーとして自身の名前を入力します。</p>
VM パスワード	<p>仮想マシンにアクセスするためのパスワードを入力します。</p>
Secure Agent 名	<p>Secure Agent の名前を入力します。デフォルトでは、ランタイム環境はエージェントと同じ名前になります。</p> <p><b>ヒント:</b> 各エージェントに属するリソースグループをより簡単に識別できるように、リソースグループと同じ名前または類似した名前を使用します。</p>
VM サイズ	<p>仮想マシンのサイズを選択します。Azure イメージのサイズ設定に慣れていない場合は、4 コアおよび 16 GB 以上のメモリを備えたサイズを設定してみてください。</p> <p>Azure の時間料金は VM サイズの影響を受けることに注意してください。</p>
仮想ネットワーク	<p>Microsoft Azure サブスクリプションと場所に基づいて既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。</p>

プロパティ	説明
仮想ネットワーク名	既存の仮想ネットワークを選択するか、新しい仮想ネットワークの名前を入力します。既存の仮想ネットワークを選択すると、新しく作成した VM が既存の VNet に関連付けられます。
仮想ネットワークアドレス	既存の仮想ネットワークアドレスを選択するか、新しいアドレスを入力します。
サブネット名	使用するサブネットを選択するか、新しいサブネットの名前を入力します。サブネットには、仮想ネットワークにデプロイされているすべての Azure リソースが保持されます。
サブネットアドレス	すべてのリソースを含むサブネットアドレスを選択するか、新しいサブネットアドレスを入力します。サブネットのアドレッシングにより、複数のネットワークで構成されているシステムで同じインターネットアドレスを共有できます。
CIDR IP アドレス範囲	CIDR IP アドレス範囲を入力します。 CIDR (Classless Inter-Domain Routing) は、IP アドレスを割り当てるための方法です。ネットワークルールで Secure Agent へのリモートアクセスを許可するように設定します。アドレスの“/x”の部分により、サブネットで使用可能な IP アドレスの数が決定されます (例:108.124.81.10/32)。

**ヒント:** 詳細については、Microsoft のドキュメントの「[Explore Azure Virtual Networks](#)」を参照してください。

8. **【作成】** をクリックします。の管理者でランタイム環境が作成され、**【ランタイム環境】** ページに表示されます。

**ヒント:** 保留中の Secure Agent の進行状況を確認するには、**【ランタイム環境】** ページで **【Cloud Secure Agent の管理】** をクリックします。統計がページの上部に表示されます。

## 第 6 章

# ローカル環境での Secure Agent のインストール

ホステッドエージェントを使用できない場合、または AWS あるいは Microsoft Azure にエージェントをインストールしない場合は、ローカル環境に Secure Agent をインストールします。

Secure Agent は次の方法でローカル環境にインストールできます。

### Windows を実行しているローカルマシンまたは VM の場合

Windows では、Secure Agent は Windows サービスとして実行されます。Secure Agent インストーラをダウンロードする前に、Windows 環境が Secure Agent の要件を満たしていることを確認してください。

### Linux を実行しているローカルマシンまたは VM の場合

Linux では、Secure Agent はプロセスとして実行されます。Secure Agent インストーラをダウンロードする前に、Linux 環境が Secure Agent の要件を満たしていることを確認してください。

## 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。

デフォルトでは、Windows を起動すると Secure Agent も起動されます。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 は、BASIC、DIGEST、および NTLMv2 プロキシ認証で動作します。

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. 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 マシンが、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。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 マシンに、Microsoft Visual C++ 2015 Redistributable があること。
- Secure Agent マシンに、少なくとも 4 つの CPU コア、16GB の RAM、および 5GB 以上の空きディスク容量があること。
- Secure Agent マシンが、250GB 以上のディスク容量と 5GB 以上の空き容量を持つボリューム、または Secure Agent インストールの 3 倍のサイズのボリュームのうち、大きい方のボリューム上にあること。
- 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。
- マシンに他の Secure Agent がインストールされていないこと。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してください。

Secure Agent の要件の詳細については、次の記事を参照してください:

<https://knowledge.informatica.com/s/article/526096>

### 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。

ドメインと IP アドレスの許可リストは、POD (Point of Deployment) によって異なる場合があります。POD 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。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Intelligent Cloud Services ドメインの許可リストとさまざまな POD の IP アドレスについては、ドキュメントポータル「[Pod Availability and Networking](#)」を参照するか、管理者の [ランタイム環境] ページの上部にあるリンクをクリックしてください。

### 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 Secure Agent が存在する場合は、その Secure Agent をアンインストールする必要があります。

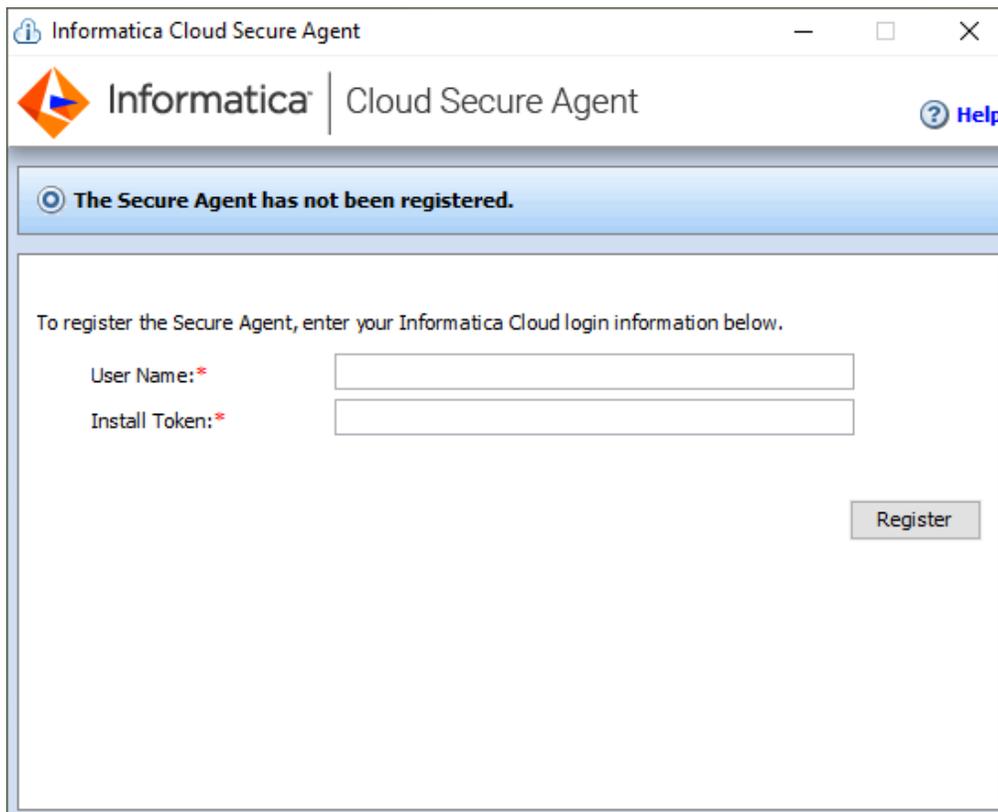
**ヒント:** Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

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. 管理者としてインストールプログラムを実行します。
  - 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。

**[Cloud Secure Agent]** ダイアログボックスが開き、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 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. 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。

次のガイドラインを考慮します。

- 特定のユーザープロファイルを作成して、Secure Agent インストールディレクトリから、すべてのフォルダへのフルアクセス権を持つ Secure Agent をインストールします。root ユーザーとして Secure Agent をインストールしないでください。
- 同じユーザーアカウントで同じマシンに複数の Secure Agent をインストールすることはできません。異なるユーザーアカウントで複数のエージェントが存在する場合があります。
- Informatica ドメイン内のどのノードにも Secure Agent をインストールしないでください。

Secure Agent の要件の詳細については、次の KB の記事を参照してください:

[IICS Minimum requirements and best practices when installing Informatica Cloud Secure Agent.](#)

## 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。

- マシンが、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。
- マシンに 11GB 以上の空きディスク容量があることを確認します。
- libidn.x86\_64 パッケージがインストールされていることを確認します。  
パッケージがない場合は、次のコマンドを使用してインストールします: `sudo yum install libidn.x86_64`  
**注:** パッケージをインストールするコマンドは、Linux ディストリビューションによって異なる場合があります。
- libidn.so.\*ライブラリがインストールされていることを確認します。  
ライブラリが存在しない場合は、次のコマンドを使用してインストールします。
  - 64 ビットシステムの場合: `cd /usr/lib/x86_64-linux-gnu`
  - 32 ビットシステムの場合: `cd /usr/lib/i386-linux-gnu`ライブラリをインストールした後、次のコマンドを使用してシンボリックリンクを作成します。  
`sudo ln -s libidn.so.12 libidn.so.11`
- 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、次の記事を参照してください:

<https://knowledge.informatica.com/s/article/526096>

## 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。

ドメインと IP アドレスの許可リストは、POD (Point of Deployment) によって異なる場合があります。POD 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。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Intelligent Cloud Services ドメインの許可リストとさまざまな POD の IP アドレスについては、ドキュメントポータル内の「[Pod Availability and Networking](#)」を参照するか、管理者の [ランタイム環境] ページの上部にあるリンクをクリックしてください。

## 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。Secure Agent は、BASIC、DIGEST、および NTLMv2 プロキシ認証を使用して動作します。

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、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。

## Secure Agent インストールのトラブルシューティング

Secure Agent のダウンロードに失敗した。

**[Secure Agent のダウンロード]** をクリックした後にダウンロードが失敗した場合は、ドメイン `https://global-package.dm.informaticacloud.com` を許可リストに追加してから、ダウンロードを再試行してください。

詳細については、ナレッジベースの記事

「[Change in Package Dependency Manager IP Addresses and Domain for IDMC](#)」を参照してください。

## 第 7 章

# AWS でのサーバーレスランタイム環境のセットアップ

サーバーレスランタイム環境は、Secure Agent または 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せん。

**注:** Azure Native ISV Services でのサーバーレスランタイム環境の作成については、「[Configure serverless runtime environment on Azure Native ISV](#)」を参照してください。Google Cloud でサーバーレスランタイム環境を作成することはできません。

サーバーレスランタイム環境を作成する前に、既存の VPC を作成するか、AWS アカウントに接続する必要があります。これは、手動で行うか、Informatica が提供する AWS CloudFormation テンプレートを使用して行うことができます。

**注:** クラウド環境は AWS クラウドプラットフォーム上にある必要があり、VPC にはデフォルトのテナントが必要です。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。

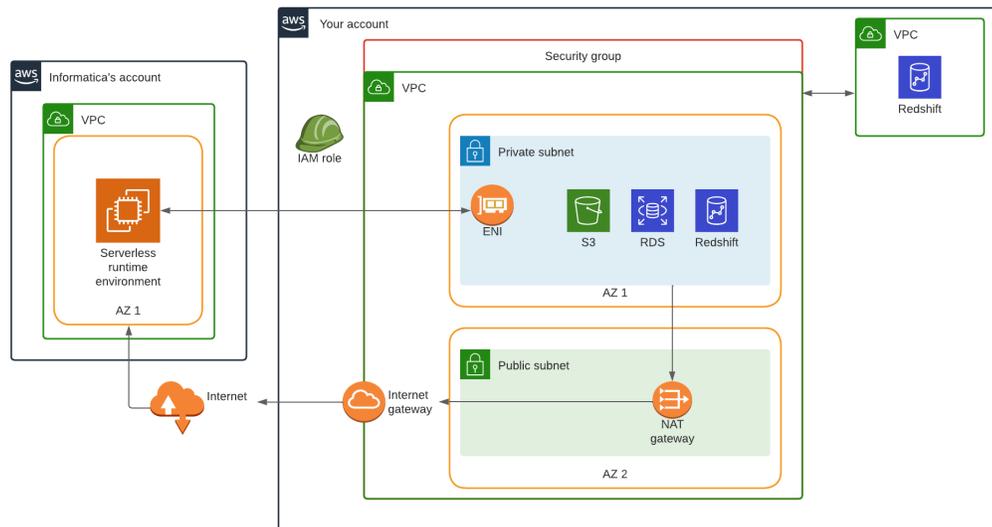
クラウド環境は、次のいずれかの方法を使用して設定できます。

- 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。この方法の詳細については、「[手動での環境の作成および設定](#)」(ページ 57)を参照してください。
- 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、その VPC をサーバーレスランタイム環境に接続できます。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 59)を参照してください。

# 手動での環境の作成および設定

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。

また、次のシナリオのうちのいずれか 1 つ以上に当てはまることを確認してください。

- VPC の DHCP オプションが AmazonProvidedDNS で設定されている。
- DHCP オプションセットにカスタム DNS サーバーがある場合は、AmazonProvidedDNS がオプションセットに含まれている、または DNS サーバーが EC2 内部ホスト名を解決できる。DNS サーバーが EC2 内部ホスト名を解決できるようにするには、DNS クエリを AmazonProvidedDNS に内部的にリダイレクトします。

## 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すると、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 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。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 ロールにより、VPC のプライベートサブネットに関連付けられている ENI を作成、アタッチ、デタッチ、および削除するために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によって使用され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 84)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新しい VPC の作成](#)」 (ページ 60) 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 63) 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. JSON ファイルを S3 の場所から iics-sre-config フォルダに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 71) を参照してください。

## AWS CloudFormation テンプレートを使用した新しい VPC の作成

AWS CloudFormation テンプレートを使用して新たな VPC を作成するときに、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。

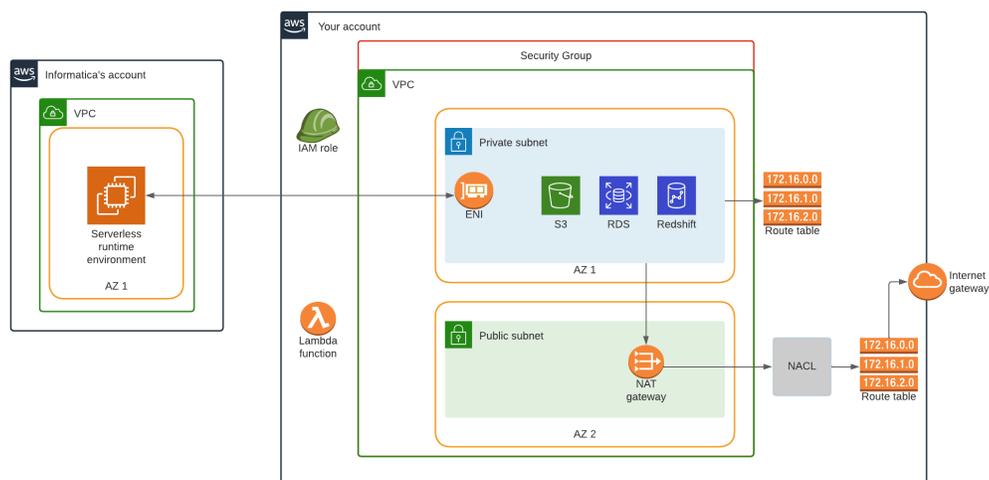
パラメータ	説明
補足ファイルの場所	開発者がデータにアクセスして処理するために使用できる JAR ファイルや外部ライブラリなど補足ファイルを格納するための Amazon S3 の場所。
JSON ファイルの S3 の場所	サーバーレス設定ファイルを生成するための Amazon S3 の場所。

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。

## スタックによって作成された AWS リソース

AWS CloudFormation テンプレートを使用して VPC を作成すると、スタックによってさまざまな AWS リソースが作成されます。

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

## スタックによって実行される設定

AWS CloudFormation テンプレートを使用して VPC を作成すると、スタックによってさまざまな設定が実行されます。

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。

パラメータ	説明
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。

## VPC 設定の一般的なタスク

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 アドレスの追加、システムディスクの設定、JAR ファイルと外部ライブラリの場所の設定、および REST API を認証するための TLS の設定ができます。これらは、VPC を手動で設定するか、テンプレートを使用して設定するかに関係なく適用されます。

必要に応じて、次のタスクを実行します。

- 信頼済みの IP アドレスを追加します。組織が IP アドレスに基づいてフィルタリングを行う場合は、安全な Informatica アドレスを追加して、ファイアウォールによってブロックされないようにします。詳細については、[「信頼済みの Informatica IP アドレスの追加」 \(ページ 67\)](#)を参照してください。
- システムディスクを設定します。システムディスクは、マッピングパフォーマンスの向上に役立ちます。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」 \(ページ 69\)](#)を参照してください。システムディスクの設定方法については、[「システムディスク」 \(ページ 83\)](#)を参照してください。
- 補足ファイルの場所を作成します。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」 \(ページ 71\)](#)を参照してください。
- REST API を認証するための TLS を設定します。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」 \(ページ 72\)](#)を参照してください。

## 信頼済みの Informatica IP アドレスの追加

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。

### US

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
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。

## データディスクとしての EFS または NFS ディレクトリの使用

サーバーレスランタイム環境で既存の EFS または NFS ディレクトリをデータディスクとして使用するには、いくつかの設定手順を実行して、サーバーレスランタイム環境がこれらのディレクトリにアクセスする権限を持つようにします。設定が完了すると、サーバーレスランタイム環境は既存のファイルを読み取り、これらのディレクトリに新しいファイルを書き込みます。

1. 所有している EC2 インスタンスに EFS または NFS ディレクトリをマウントします。
2. EC2 インスタンスにログインします。
3. ID=501 のユーザーを見つけます。存在しない場合は、この ID で新しいユーザーを作成します。  
ユーザー ID 501 は、サーバーレスランタイム環境がマウントされた EFS または NFS ディレクトリにアクセスするために使用するユーザー cldagnt です。
4. ユーザー 501 のマウントされたディレクトリに読み取りおよび書き込み権限を割り当てます。  
詳細については、AWS のマニュアルの [Working with users, groups, and permissions at the Network File System Level](#) のトピックを参照してください。

## データディスクの設定

サーバーレスランタイム環境で使用するファイルが EFS または NFS ディレクトリにある場合は、すべてのマッピングを更新せずに、サーバーレスランタイム環境にデータディスクを作成します。

EFS または NFS の場所をデータディスクにマウントすると、次の機能にアクセスできるようになります。

- フラットファイルのサポート。マッピングでは、マウントされた EFS または NFS の場所からフラットファイルを使用できます。
- パラメータファイルのサポート。マウントされた EFS または NFS の場所に格納されているパラメータファイルを使用できます。これにより、マッピングを変更する必要がなくなるため、Secure Agent グループからサーバーレスランタイム環境へのジョブの移行が簡素化されます。

**ヒント:** データディスクを作成する場合は、マウントされたディレクトリをデータディスクとして使用するための適切なユーザーとアクセス許可が設定されていることを確認してください。詳細については、[「データディスクとしての EFS または NFS ディレクトリの使用」 \(ページ 70\)](#)を参照してください。

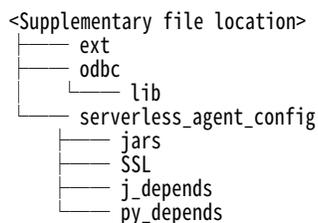
データディスクの設定については、[「データディスク」 \(ページ 84\)](#)を参照してください。

## 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、次の手順を実行します。

1. Amazon S3 に次のファイル構造を作成します。



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」 \(ページ 73\)](#)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

場所	ファイル
<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	<p>次のファイル</p> <ul style="list-style-type: none"> <li>- serverlessUserAgentConfig.yml</li> <li>- JDBC V2 コネクタ JAR ファイル</li> <li>- 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</li> <li>- Java トランスフォーメーション用の JAR ファイル</li> <li>- 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</li> </ul> <p>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。</p>

## 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。

- Amazon S3 の補足ファイルの場所に移動します。
- serverless\_agent\_config フォルダに、SSL というサブフォルダを作成します。
- 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。
- 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
```
- serverless\_agent\_config フォルダで、serverlessUserAgentConfig.yml ファイルを開きます。
- 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。
- 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 ファイルの設定

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。

実行するタスクを選択します。

- serverlessUserAgentConfig.yml ファイルを作成するには、[「serverlessUserAgentConfig.yml ファイルへの入力」 \(ページ 73\)](#)にリストされているテンプレートを使用し、必要に応じて調整を行います。  
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、[「エラスティックサーバーのファイルのコピー」 \(ページ 75\)](#)で提供されるコードスニペットを使用します。
- JDBC V2 コネクタの JAR ファイルをコピーするには、[「JDBC V2 コネクタ JAR ファイルのコピー」 \(ページ 75\)](#)で提供されるコードスニペットを使用します。
- 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、[「Java トランスフォーメーション JAR ファイルのコピー」 \(ページ 75\)](#)で提供されるコードスニペットを使用します。
- 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、[「Python トランスフォーメーションリソースファイルのコピー」 \(ページ 76\)](#)で提供されるコードスニペットを使用します。
- サーバーレスランタイム環境の実行中に補足ファイルの場所にファイルを追加する方法については、[「環境の実行中におけるファイルの追加」 \(ページ 76\)](#)を参照してください。

**注:** serverlessUserAgentConfig.yml ファイルに入力されたパスに含まれるスペースまたは特殊文字をエスケープします。

## 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 ファイルを作成します。

```
# 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_file_name>.json
keystores: # List of keystore files to copy to the instance machine.
- fileCopy:
  sourcePath: restv2/key
truststores: # List of truststore files to copy to the instance machine.
- fileCopy:
  sourcePath: restv2/key.ext
wsconsumer:
  wsdl:
  - 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.
  ssl:
  - 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
  nwrfs: # List of nwrfs related files to copy.
  - fileCopy:
    sourcePath: sap/nwrfs/libicudata.so.50
  - fileCopy:
    sourcePath: sap/nwrfs/libicudecnumber.so
  hana: # 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 ファイルにコネクタ情報を入力する方法の詳細については、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、ネイティブライブラリ、ネイティブバイナリをコピーするには、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/sapjco3.jar
    - fileCopy:
        sourcePath: j_depends/chilkat.jar
    - fileCopy:
        sourcePath: j_depends/chilkatLoader.jar
    - fileCopy:
        sourcePath: j_depends/NativeBinExecutor.jar
nativeLib:
  resources:
    - fileCopy:
        sourcePath: native-lib/libchilkat.so
    - fileCopy:
        sourcePath: native-lib/libsapjco3.so
nativeBin:
  resources:
    - fileCopy:
        sourcePath: native-bin/printEnvVariables.sh
    - fileCopy:
        sourcePath: native-bin/printProcess.sh

```

## Python トランスフォーメーション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

```

## 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。serverlessUserAgentConfig.yml ファイルの詳細については、[「補足ファイルの場所の作成」 \(ページ 71\)](#)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と同期するまでに最大で 10 分かかることがあります。

次のいずれか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。

# プロキシサーバーの使用

組織が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、プロキシサーバーを介して Informatica Intelligent Cloud Services に接続するようにサーバーレスランタイム環境を設定できます。

サーバーレスランタイム環境用にプロキシサーバーを設定するときは、必要なプロキシサーバー設定を `serverlessUserAgentConfig.yml` ファイルで定義してから、メタデータのインポートやマッピングの実行を行います。データ統合は、ファイル内のプロキシエントリをサーバーレスランタイム環境にコピーします。

マッピングを実行するときにプロキシを適用するには、Administrator の **【サーバーレス環境】** ページでプロキシの設定を行います。

特定のコネクタでサーバーレスランタイム環境のプロキシを設定できます。プロキシがコネクタに適用されるかどうかを確認するには、該当するコネクタのヘルプを参照してください。

## serverlessUserAgentConfig.yml ファイルでのプロキシの設定

マッピングを設計してメタデータをインポートするときにプロキシサーバー設定を適用するには、プロキシサーバーの詳細を `serverlessUserAgentConfig.yml` ファイルに追加します。

次のコードスニペットをテンプレートとして使用して、プロキシサーバーの値を `serverlessUserAgentConfig.yml` ファイルに指定します。

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

## JVM オプションでのプロキシの設定

マッピングまたはタスクを実行するときにプロキシサーバー設定を適用するには、Administrator で JVM オプションを設定します。

1. **【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の名前をクリックします。
2. **【編集】** をクリックします。
3. **【ランタイム設定のプロパティ】** セクションで、**【サービス】** として **【データ統合サーバー】** を選択し、**【タイプ】** として **【DTM】** を選択します。
4. JVMOption フィールドのいずれかを編集し、HTTPS または HTTP プロキシサーバーのどちらかを使用して、各パラメータに適切な値を指定します。

次の表に、これらのパラメータについて説明します。

パラメータ	説明
-Dhttp.proxySet=	送信プロキシサーバーが HTTP の場合に、サーバーレスランタイム環境でプロキシ設定を使用する必要があるかどうかを指定します。プロキシを使用するには、-Dhttp.proxySet=True を選択します。
-Dhttps.proxySet=	送信プロキシサーバーが HTTPS の場合に、サーバーレスランタイム環境でプロキシ設定を使用する必要があるかどうかを指定します。プロキシを使用するには、-Dhttps.proxySet=True を選択します。
-Dhttp.proxyHost=	送信 HTTP プロキシサーバーのホスト名。
-Dhttp.proxyPort=	送信 HTTP プロキシサーバーのポート番号。
-Dhttp.proxyUser=	HTTP プロキシサーバーの認証ユーザー名。
-Dhttp.proxyPassword=	認証されたユーザーのパスワード。
-Dhttps.proxyHost=	送信 HTTPS プロキシサーバーのホスト名。
-Dhttps.proxyPort=	送信 HTTPS プロキシサーバーのポート番号。
-Dhttps.proxyUser=	HTTPS プロキシサーバーの認証ユーザー名。
-Dhttps.proxyPassword=	認証されたユーザーのパスワード。

5. **[Save] (保存)** をクリックします。

## プロキシサーバーでのドメインの許可

マッピングを正常に実行するには、プロキシサーバーで、マッピング内のデータを処理するために必要な AWS エンドポイントからのトラフィックが許可されている必要があります。

次のドメインからのトラフィックを許可します。

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

サーバーレスランタイム環境に接続する VPC を含んだリージョンを指定します。

## 第 8 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、Hosted Agent のマルチテナントモデルとは異なり、分離されたシングルテナントモデルを使用する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。

シングルテナントモデルには、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、次のクラウドプラットフォームでホストされます。

- Azure Virtual Network (VNet)
- Amazon Virtual Private Cloud (VPC)。サーバーレスランタイム環境は、エラスティックネットワークインターフェイス (ENI) を作成してクラウド環境に接続します。

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。

## Azure でのサーバーレスランタイム環境の作成

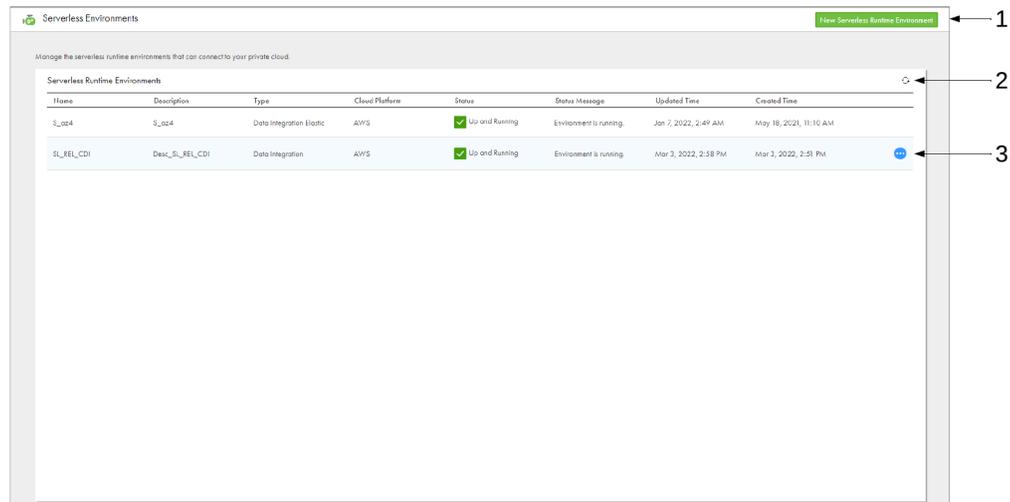
サーバーレスランタイム環境を作成し、Azure ポータルでプロパティを設定します。サーバーレスランタイム環境のプロパティを表示するには、Azure ポータルで環境の **【アクション】** メニューを展開し、**【プロパティの表示】** を選択します。

Azure Native ISV Services でサーバーレスランタイム環境を作成および管理する手順については、[「Configure serverless runtime environment on Azure Native ISV」](#) を参照してください。

# AWS での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。サ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

サーバーレスランタイム環境の「基本設定」セクションには、Informatica アカウント番号や現在のステータスなど、環境に関する一般的な情報が表示されます。

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。
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、 <b>[データ統合]</b> を選択します。 - 詳細モードでマッピングを実行するには、 <b>[詳細データ統合]</b> 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

サーバーレスランタイム環境の「プラットフォーム設定」セクションには、リージョン、サブネット、セキュリティグループなど、プラットフォームに関する技術情報が表示されます。

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。 説明の長さは最大 256 文字で、英数字および次の特殊文字を含めることができます： ._-:/()#,@[]+=&;{}!\$"*
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。

プロパティ	説明
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。
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。 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。

## ランタイム設定のプロパティ

サーバーレスランタイム環境の [ランタイム設定のプロパティ] セクションでは、環境の動作を指定します。

**注:** デフォルトディレクトリの変数を設定しますが、システム管理者または Informatica グローバルカスタムサポートから指示されない限り、他の変数やプロパティを変更しないでください。

次の表に、サーバーレスランタイム環境がソースディレクトリ、ターゲットディレクトリ、一時ファイルなどの場所に使用するシステム変数を示します。システムのデフォルトを確認し、必要に応じて更新します。

ディレクトリ名に次の特殊文字を含めることはできません: \* ? < > " | ,

**ヒント:** リストをフィルタリングして「Service = Data\_Integration\_Server」および「Type = PMRDTM\_CFG」を表示することで、デフォルトのディレクトリ変数をより簡単に探すことができます。

システム変数名	説明
\$PMLookupFileDir	ルックアップファイルのディレクトリ。 デフォルトは、\$PMRootDir です
\$PMBadFileDir	拒否ファイル用のディレクトリ。 デフォルトは\$PMRootDir/error です
\$PMCacheDir	インデックスファイルとデータキャッシュファイルのディレクトリ。 デフォルトは、\$PMRootDir/cache です
\$PMStorageDir	操作の状態ファイルのディレクトリ。高可用性オプションがある場合、またはリカバリ用のワークフローが有効である場合、データ統合サービスはこれらのファイルをリカバリ用に使います。これらのファイルには、各ワークフローおよびセッションの操作の状態が格納されます。 デフォルトは、\$PMRootDir です
\$PMTargetFileDir	ターゲットファイルのディレクトリ。 デフォルトは、\$PMRootDir です
\$PMSourceFileDir	ソースファイルのディレクトリ。 デフォルトは、\$PMRootDir です
\$PMExtProcDir	外部プロシージャのディレクトリ。 デフォルトは、\$PMRootDir です
\$PMTempDir	一時ファイルのディレクトリ。 デフォルトは、\$PMRootDir/Temp です

## システムディスク

サーバーレスランタイム環境でシステムディスクを設定すると、データ統合でのマッピングパフォーマンスを向上させることができます。

システムディスクの設定に関するルールと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 69) を参照してください。

以下の表に、システムディスクのプロパティを示します。

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。

プロパティ	説明
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。

## データディスク

サーバーレスランタイム環境でデータディスクを設定すると、EFS または NFS ディレクトリ内のファイルにアクセスできます。

詳細については、「[データディスクとしての EFS または NFS ディレクトリの使用](#)」 (ページ 70) および「[データディスクの設定](#)」 (ページ 71) を参照してください。

以下の表に、データディスクのプロパティを示します。

プロパティ	説明
タイプ	データディスクタイプ。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。
ターゲットマウント	Secure Agent にマウントするファイルシステム。
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」 \(ページ 59\)](#) 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、[「手動での環境の作成および設定」 \(ページ 57\)](#) 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。

特に明記されていない限り、このセクションで説明する管理アクションは、AWS および Azure のサーバーレスランタイム環境に適用されます。

### サーバーレスランタイム環境の編集

サーバーレスランタイム環境で編集できるプロパティは、環境のステータスに応じて異なります。

サーバーレスランタイム環境のステータスに基づいて、次のようなプロパティを編集することができます。

- 稼働中。更新できるのは、**【タスクあたりの最大コンピューティングユニット】** フィールドと **【タスクのタイムアウト】** フィールドのみです。更新された値は、後続のタスクの実行で有効になります。
- 失敗。すべてのプロパティを更新することができます。更新されたプロパティは、**【再デプロイ】** (AWS) または **【環境の開始】** アクション (Azure) を使用すると有効になります。

サーバーレスランタイム環境に他のステータスが表示されている場合は、サーバーレスランタイム環境を削除して、新しいサーバーレスランタイム環境を作成する必要があります。

サーバーレスランタイム環境を編集するには、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、**【編集】** を選択します。この操作は、Azure および AWS のサーバーレスランタイム環境で実行することができます。

Azure Native ISV Services で作成されたサーバーレスランタイム環境の場合は、Azure ポータルを使用してプロパティを編集することもできます。

### サーバーレスランタイム環境の再デプロイ(AWS)

再デプロイアクションにより、環境の変更後、または環境が特定の理由でシャットダウンした場合に、サーバーレスランタイム環境が再起動します。

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。

- 組織の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、同じ設定でクラウド環境内の別のサブネットに接続するサーバーレスランタイム環境や別のセキュリティグループを使用する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。

**注:** Azure Native ISV Services で作成された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、Azure portal を使用します。

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】を選択します。

## サーバーレスランタイム環境の削除

不要になったサーバーレスランタイム環境を削除します。

**注:** Azure Native ISV Services で作成されたサーバーレスランタイム環境を削除するには、Azure portal を使用します。

サーバーレスランタイム環境を削除する前に、次のタスクを実行します。

- 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。
- 【依存関係の表示】 アクションを使用して、環境がタスク、マッピング、または接続によって使用されているかどうかを確認します。依存関係が存在する場合は、環境を削除する前に削除します。

サーバーレスランタイム環境を削除するには、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、【削除】を選択します。

# サーバーレスコンピューティングユニットのメータリング

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 (AWS)

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

接続の作成時に、AWS または Azure で設定されたサーバーレスランタイム環境を指定できます。

設定されたサーバーレスランタイム環境に適用できるコネクタのリストは、Azure と AWS で異なる場合があります。

## AWS サーバーレスランタイム環境

AWS で設定されたサーバーレスランタイム環境は、次のようなコネクタに使用することができます。

Amazon Athena コネクタ	MongoDB コネクタ
Amazon Aurora コネクタ	Microsoft SQL Server コネクタ
Amazon Redshift V2 コネクタ	MongoDB V2 コネクタ*
Amazon DynamoDB V2 コネクタ*	MySQL コネクタ
Amazon S3 V2 コネクタ	NetSuite RESTlet V2
BigMachines コネクタ	OData コネクタ
Box コネクタ	OData Consumer コネクタ
Concur V2 コネクタ	OData V2 Protocol Reader コネクタ
Coupa V2 コネクタ	ODBC コネクタ
Cvent コネクタ	Oracle コネクタ
Databricks Delta コネクタ	PostgreSQL コネクタ
Dropbox コネクタ	REST V2 コネクタ
Eloqua Bulk API コネクタ	REST V3 コネクタ
Google Analytics コネクタ	Salesfore OAuth コネクタ
Google BigQuery V2 コネクタ	Salesforce コネクタ
Google Cloud Storage V2 コネクタ	Salesforce Marketing Cloud コネクタ
JDBC (JDBC_IC) コネクタ	SAP ADSO Writer コネクタ
JDBC V2 コネクタ	SAP BAPI コネクタ
JIRA コネクタ	SAP BW Bex クエリコネクタ
Kafka コネクタ*	SAP テーブルコネクタ
Marketo REST コネクタ	SAP ODP Extractor コネクタ
Marketo V3 コネクタ	SAP HANA コネクタ
Microsoft Azure Blob Storage V3 コネクタ	ServiceNow コネクタ
Microsoft Azure Cosmos DB SQL API コネクタ	Snowflake Data Cloud Connector
Microsoft Azure Data Lake Storage Gen1 V3 コネクタ	SuccessFactors ODATA コネクタ
Microsoft Azure Data Lake Storage Gen2 コネクタ	Web サービスコンシューマコネクタ
Microsoft Azure Synapse SQL コネクタ	Workday V2 コネクタ
Microsoft CDM Folders V2 コネクタ	Xero コネクタ
Microsoft Dynamics 365 for Operations コネクタ	Xactly コネクタ
Microsoft Dynamics 365 for Sales コネクタ	Zendesk V2 コネクタ

\*AWS のサーバーレスランタイム環境は、詳細モードのマッピングのコネクタにのみ適用されます。

## Azure サーバーレスランタイム環境

Azure で設定されたサーバーレスランタイム環境は、次のようなコネクタに使用することができます。

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

\*Azure のサーバーレスランタイム環境は、詳細モードのマッピングのコネクタにのみ適用されます。

# 索引

## C

Cloud アプリケーション統合コミュニティ  
URL [6](#)  
Cloud 開発者コミュニティ  
URL [6](#)

## H

Hosted Agent  
説明 [9](#)

## I

Informatica Intelligent Cloud Services  
Web サイト [6](#)  
Informatica グローバルカスタマサポート  
連絡先情報 [7](#)

## L

Linux  
Secure Agent のアンインストール [55](#)  
Secure Agent の起動および停止 [34](#)  
プロキシの設定 [54](#)

## P

POD  
特定方法 [47, 52](#)

## S

Secure Agent  
IP アドレス許可リスト [47, 52](#)  
Linux でのアンインストール [55](#)  
Linux でのデータ暗号化キーの変更 [31](#)  
Linux での起動および停止 [34](#)  
Linux での権限 [53](#)  
Linux での登録 [53](#)  
Linux での要件 [52](#)  
Linux へのインストール [53](#)  
rotateDeviceKey コマンド [30](#)  
Secure Agent Manager [32](#)  
Secure Agent グループ [11](#)  
Secure Agent グループからの削除 [19](#)  
Secure Agent グループへの追加 [18](#)  
Windows サービスログインの設定 [50](#)  
Windows でのアンインストール [51](#)  
Windows でのデータ暗号化キーの変更 [30](#)  
Windows での起動 [46](#)

Secure Agent (続く)  
Windows での権限 [47](#)  
Windows での停止および再起動 [33](#)  
Windows での登録 [48](#)  
Windows での要件 [47](#)  
Windows へのインストール [48](#)  
アップグレード [29](#)  
インストール [40, 46](#)  
サービスの開始 [26](#)  
サービスの開始および停止 [24](#)  
サービスの停止 [26](#)  
サービスを開始および停止する際のガイドライン [25](#)  
データ暗号化 [30](#)  
ドメイン許可リスト [47, 52](#)  
トラブルシューティング [37](#)  
ブラックアウトファイルの構造 [28](#)  
ブラックアウトファイルの上書き [27](#)  
ブラックアウト期間の設定 [26](#)  
概要 [21](#)  
拡張性 [11](#)  
削除 [29](#)  
詳細の表示、更新ステータス [21](#)  
通信ポート [47, 52](#)  
負荷分散 [11](#)  
名前の変更 [29](#)  
Secure Agent Manager  
Secure Agent の停止および再起動 [33](#)  
起動 [46](#)  
使用 [32](#)  
Secure Agent グループ  
Secure Agent の削除 [19](#)  
Secure Agent の追加 [18](#)  
Secure Agent の追加および削除 [16](#)  
グループの共有 [15](#)  
サービスとコネクタの有効化および無効化 [14](#)  
サービスの有効化および無効化 [12, 16](#)  
サービス割り当てのガイドライン [13](#)  
依存性の表示 [19](#)  
概要 [11](#)  
既存のグループへの新規エージェントの追加 [18](#)  
共有グループでのファイル接続 [15](#)  
権限の変更 [16](#)  
作成 [16](#)  
削除 [16](#)  
名前の変更 [16](#)  
Secure Agent コネクタ  
有効化および無効化 [14](#)  
Secure Agent サービス  
有効化および無効化 [12, 14](#)  
Secure Agent のインストール  
トラブルシューティング [55](#)

## W

Web サイト [6](#)

## Windows

プロキシの設定 [33, 50](#)

## Windows サービス

Secure Agent ログインの設定 [50](#)

## あ

アップグレード通知 [7](#)

## お

オブジェクトの依存関係

Secure Agent グループの表示 [19](#)

## さ

サーバーレスランタイム環境

クローン作成 [87](#)

コネクタ [88](#)

サーバーレスコンピューティングユニット [87](#)

ディザスタリカバリ [88](#)

プロパティ [80](#)

概要 [79](#)

再デプロイ [86](#)

作成 [80](#)

編集中 [86](#)

要件 [56](#)

## し

システムステータス [7](#)

## す

ステータス

Informatica Intelligent Cloud Services [7](#)

## て

ディレクトリ

アクセスする Secure Agent ログインの設定 [50](#)

## と

トラブルシューティング

Secure Agent [37](#)

Secure Agent のインストール [55](#)

## ふ

ファイアウォール

設定 [47, 52](#)

ブラックアウト期間

Secure Agent に対する設定 [26](#)

Secure Agent のブラックアウトファイル構造 [28](#)

Secure Agent ブラックアウトファイルの上書き [27](#)

プロキシ設定

Linux での設定 [54](#)

Windows 上での設定 [33, 50](#)

## め

メンテナンスの停止 [7](#)

## ら

ランタイム環境

Hosted Agent [9](#)

Secure Agent グループ [11](#)

Secure Agent グループの共有 [15](#)

Secure Agent のインストール [40, 46](#)

サービスとコネクタの有効化および無効化 [14](#)

サービスの有効化および無効化 [12](#)

サービス割り当てのガイドライン [13](#)

概要 [8](#)

共有グループでのファイル接続 [15](#)

設定 [40, 43](#)