



Informatica® Intelligent Cloud Services
October 2025

ランタイム環境

© 著作権 Informatica LLC 2021, 2025

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（電子的複製、写真複製、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 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: 2025-12-02

目次

序文	7
Informatica のリソース.....	7
Informatica マニュアル.....	7
Informatica Intelligent Cloud Services Web サイト.....	7
Informatica Intelligent Cloud Services コミュニティ.....	7
Informatica Intelligent Cloud Services マーケットプレイス.....	8
データ統合のコネクタのドキュメント.....	8
Informatica ナレッジベース.....	8
Informatica Intelligent Cloud Services Trust Center.....	8
Informatica グローバルカスタマサポート.....	8
 第 1 章 : ランタイム環境	9
 第 2 章 : Hosted Agent	11
 第 3 章 : Secure Agent グループ	13
複数のエージェントを含む Secure Agent グループ.....	13
Secure Agent グループに対するサービスとコネクタの割り当て.....	14
サービス割り当てのガイドライン.....	15
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.....	16
サービスとコネクタの割り当ての例.....	16
Secure Agent グループの共有.....	17
共有された Secure Agent グループでのフラットファイル接続.....	18
Secure Agent グループの操作.....	18
グループへの Secure Agent の追加.....	20
既存のグループへの新規 Secure Agent の追加.....	21
グループからの Secure Agent の削除.....	21
Secure Agent グループの依存関係の表示.....	21
 第 4 章 : エラスティックランタイム環境	23
データを保護するためのセキュリティ.....	23
前提条件の確認.....	25
AWS 環境の設定.....	26
手順 1. AWS リソースを作成する.....	27
手順 2. クラスティンストーラポリシーを作成する.....	30
手順 3. クラスティンストーラロールを作成する.....	33
手順 4. ワーカーポリシーを作成する.....	33
手順 5. ワーカーロールの作成.....	35
手順 6. ジャンプホストを作成する (オプション).....	35
手順 7. マスターノードを作成する.....	36

エラスティックランタイム環境の作成.	36
環境設定.	37
エラスティックランタイム環境のデプロイ.	39
手順 1. マスターノードに SSH 接続する.	40
手順 2. リソースのクリーンアップ.	40
手順 3. クラスティンストーラをダウンロードする.	40
手順 4. マスターノードでのクラスティンストーラディレクトリの作成.	40
手順 5. config.txt ファイルを更新する.	41
手順 6. クラスティンストーラを実行する.	43
手順 7. マスターノードに EFS ファイルシステムをマウントする.	43
手順 8. エラスティックランタイム環境が実行されていることを確認する.	43
データストレージへのファイルのアップロード.	44
パラメータファイルのアップロード.	44
フラットファイル接続用のフラットファイルのアップロード.	44
補足ファイルのアップロード.	44
エラスティックランタイム環境での操作.	45
エラスティックランタイム環境でのコネクタ.	47
REST API を使用したイメージのダウンロード.	48
トラブルシューティング.	48
一般的な検証エラーのトラブルシューティング.	49
プロキシエラーのトラブルシューティング.	50
AWS エラーのトラブルシューティング.	51
マスターノードと作業ノードのエラーのトラブルシューティング.	52
ALMS デプロイエラーのトラブルシューティング.	53
EFS エラーのトラブルシューティング.	54
その他のエラーのトラブルシューティング.	54
IAM ポリシーリファレンス.	56
クラスティンストーラポリシー文.	56
ワーカーポリシー文.	59

第 5 章: サーバーレスランタイム環境. 61

AWS でのサーバーレスランタイム環境のセットアップ.	62
環境の設定.	62
VPC 設定タスク.	66
serverlessUserAgentConfig.yml ファイルの設定.	73
サーバーレスランタイム環境でのプロキシサーバー.	73
Administrator のサーバーレスランタイム環境.	75
サーバーレスランタイムの検証.	79
サーバーレスランタイム環境の管理.	80
サーバーレスランタイム環境のセットアップ (Microsoft Azure)	82
手順 1. ユーザーの同意設定の確認.	82
手順 2. サブネットの設定.	83
手順 3. serverlessUserAgentConfig.yml ファイルの設定.	84

手順 4. Informatica 組織の作成.	84
手順 5. サーバーレスランタイム環境を作成.	87
サーバーレスランタイム環境の管理.	90
Azure の外部にあるデータベースまたはエンドポイントの VNet の設定.	92
コマンドタスクの実行.	92
Azure でのサーバーレスランタイム環境のトラブルシューティング.	92
serverlessUserAgentConfig.yml ファイルの設定方法.	93
serverlessUserAgentConfig.yml ファイルへの入力.	93
エラスティックサーバーのファイルのコピー.	95
JDBC V2 コネクタ JAR ファイルのコピー.	96
Java トランスフォーメーション JAR ファイルのコピー.	96
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.	96
環境の実行中におけるファイルの追加.	97
サーバーレスランタイム環境でのコネクタ.	97
第 6 章 : Secure Agent.	100
Secure Agent の操作.	100
Windows での Secure Agent の停止および再起動.	103
Linux での Secure Agent の停止および再起動.	103
Secure Agent でのサービスの停止と開始.	104
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.	105
Secure Agent サービスの停止.	105
Secure Agent サービスの開始.	106
エージェントのブラックアウト期間の設定.	106
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.	107
ブラックアウトファイルの構造.	107
Secure Agent の名前変更.	108
Secure Agent の削除.	109
Secure Agent のアップグレード.	109
Secure Agent の移行.	109
Secure Agent Manager.	110
Secure Agent のログ.	110
Secure AgentJava バージョン.	114
Secure Agent のトラブルシューティング.	115
第 7 章 : Secure Agent のインストール.	117
AWS でのインストール.	117
Google Cloud のインストールの使用.	120
Google Cloud での接続に関する問題のトラブルシューティング.	121
Microsoft Azure でのインストール.	122
Windows でのインストール.	124
Windows での Secure Agent の要件.	125
Windows での Secure Agent のダウンロードおよびインストール.	126

Windows でのプロキシ設定の構成.	128
Windows Secure Agent サービスのログインの設定.	129
Windows での Secure Agent のアンインストール.	130
Linux でのインストール.	130
Linux での Secure Agent の要件.	131
Linux での Secure Agent のダウンロードおよびインストール.	132
Linux でのプロキシ設定の構成.	133
Linux での Secure Agent のアンインストール.	134
Secure Agent インストールのトラブルシューティング.	135
索引.	136

序文

「ランタイム環境」を使用して、Informatica Intelligent Cloud ServicesSMで使用するランタイム環境を作成および設定する方法を確認します。Informatica Intelligent Cloud Services ホステッドエージェントの使用方法、Secure Agent のダウンロードとインストール、Secure Agent グループの作成と設定、および Secure Agent のトラブルシューティングの方法を確認します。

Informatica のリソース

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

Informatica マニュアル

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

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

Informatica Intelligent Cloud Services Web サイト

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

Informatica Intelligent Cloud Services コミュニティ

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

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

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

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

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

Informatica Intelligent Cloud Services マーケットプレイス

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) 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> に掲載されています。

第 1 章

ランタイム環境

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

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

ランタイム環境は、次の方法で設定できます。

Informatica Cloud 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」 \(ページ 11\)](#)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」 \(ページ 13\)](#)を参照してください。

エラスティックランタイム環境の作成

エラスティックランタイム環境は、エラスティックスケーリングを使用して、リソース管理を最適化するランタイム環境オプションを提供します。エラスティックランタイム環境を使用して、変動するワークロードの需要に対応し、ワークロードコストを管理します。

AWS にエラスティックランタイム環境をデプロイすることができます。

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 5 章, 「サーバーレスランタイム環境」 \(ページ 61\)](#)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 Secure Agent がすでに他のジョブを実行している場合は、クラスタを作成してジョブを正常に実行できるように、Secure Agent に十分なリソースがあることを確認してください。Secure Agent に十分なリソースがない場合、Secure Agent 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。Secure Agent には、少なくとも 8 つのコアと 32GB のメモリを搭載したマシンを使用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 SQL Data Warehouse V3 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
- Microsoft Fabric Data Warehouse コネクタ
- Microsoft Fabric Lakehouse コネクタ
- Microsoft Fabric OneLake コネクタ
- Microsoft SQL Server コネクタ
- MySQL コネクタ
- NetSuite 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、ジョブの組織に関連付けられているデータ統合で **【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、そのグループは、タスクまたはバックグラウンドプロセス（メタデータ呼び出しなど）を、実行中またはキューに入れられているタスクの数が最も少ないエージェントに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 104)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。

Runtime Environments Generate Install Token Download Secure Agent...

Integration tasks can run in Secure Agent groups or the Hosted Agent. Install multiple Secure Agents and group them to balance workloads and improve scalability. Be sure to allow specific IP addresses for the Secure Agents. For more information, see this article [here](#).
Note: Be sure you've enabled Services and Connectors in the Secure Agent group. For more information, see this [topic](#) in the user documentation.

Environments (362) Manage Cloud Secure Agents New Runtime Environment

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_sar (1) (...)		Stopped		Agent Group	Sep 22, 2021, 9:26 AM
agent_discale_aws_ila...		No Secure Agents		Agent Group	Jan 11, 2023, 8:30 AM
agent_discale_aws_ila...		No Secure Agents		Agent Group	Mar 21, 2023, 5:47 AM
agent_discale_aws_in...		No Secure Agents		Agent Group	Aug 3, 2021, 7:25 AM

26 - 50 of 362 Items Page 2 of 15 Items Per Page: 25

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、ファイル取り込みとレプリケーション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または取り込みおよびレプリケーション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が、データ統合サーバーサービス（データ統合ジョブ用）、一括取り込みサービス（ファイル取り込みおよびレプリケーションジョブ用）、またはデータベース取り込みエージェントサービス（アプリケーション取り込みおよびレプリケーションジョブとデータベース取り込みおよびレプリケーションジョブ用）のいずれかのサービスのみを実行している場合は、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、接続で使用す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。組織で使用する任意のサービスを有効化または無効化することができます。

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。組織で使用する任意のサービスを有効化または無効化することができます。

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。

注: アプリケーション取り込みとレプリケーションとデータベース取り込みとレプリケーションで、Secure Agent グループから Secure Agent を削除して、別の Secure Agent グループに追加する場合は、少なくとも 60 分待ってから、それらを使用してアプリケーション取り込みおよびレプリケーションジョブやデータベース取り込みおよびレプリケーションジョブを実行してください。Secure Agent ランタイム情報の内部キャッシュは、デフォルトでは 1 時間ごとに更新されます。

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。タスクで使用す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せん。

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。

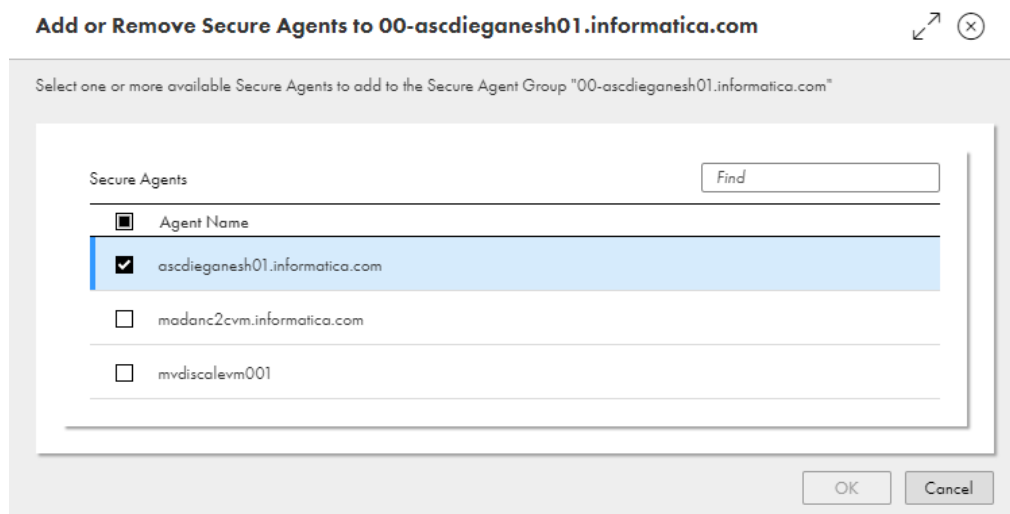
グループへの Secure Agent の追加

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。

注: アプリケーション取り込みとレプリケーションとデータベース取り込みとレプリケーションで、Secure Agent グループから Secure Agent を削除して、別の Secure Agent グループに追加する場合は、少なくとも

60 分待ってから、それらを使用してアプリケーション取り込みおよびレプリケーションジョブやデータベース取り込みおよびレプリケーションジョブを実行してください。Secure Agent ランタイム情報の内部キャッシュは、デフォルトでは 1 時間ごとに更新されます。

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事ができます。

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

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

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







USW1PFOUFLSJ Dependencies

UsesUsed By

Used By (6)

↓↑

🔍

Name	Type	Location	Updated By	Status
 Cloud Integration Hub	Connection		jrandolp05	
 #_USW1PFOUFLSJ	Connection		ltroy05	
 freddy	Connection		jrandolp05	
 /MappingTask1	Mapping Task	Default	jrandolp05	Invalid
 /MappingTask2	Mapping Task	Default	jrandolp05	Valid
 mt_FilterCut	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

エラスティックランタイム環境

エラスティックランタイム環境は、エラスティックスケールリングを使用して、リソース管理を最適化するランタイム環境オプションを提供します。エラスティックランタイム環境を使用して、変動するワークロードの需要に対応し、ワークロードコストを管理します。

エラスティックランタイム環境は、Kubernetes を使用して Secure Agent を実行し、クラスターノードでデータを処理します。データを処理するクラスターノードは、Informatica Intelligent Cloud Services からのワークロードの需要に基づいてスケールアップまたはスケールダウンできます。

エラスティックランタイム環境を作成するには、次のタスクを完了します。

1. 正しい権限を持つ AWS アカウントがあり、組織の管理者が管理者で正しい機能特権を持っていることを確認します。
2. AWS 環境を設定し、必要な AWS リソースを作成して設定します。
3. 管理者でエラスティックランタイム環境を作成します。
4. エラスティックランタイム環境を AWS にデプロイします。
5. 必要に応じて、ファイルをデータストレージにアップロードして、エラスティックランタイム環境でできるようにします。

データを保護するためのセキュリティ

Informatica は、VPC 内にエラスティックランタイム環境をデプロイして管理し、タスクで使用するデータソースにアクセスして、出力ログを保存するためのきめ細かな認証および承認メカニズムを実装します。

エラスティックランタイム環境は、信頼性を高めるためにワークロードレベルで分離されています。ユーザーは、組織を通じて環境の設定を行います。次に、マスターノードが AWS リソースを自動スケールリングして管理します。イメージ、アーティファクト、および設定は、Informatica Intelligent Cloud Services コントロールプレーンに個別に保存されます。

エラスティックランタイム環境とのデータのやり取りには、ユーザーとマスターノードに対する異なる認証方法および承認方法が含まれます。

認証

エラスティックランタイム環境を設定するには、ユーザーはパスワードや SSO などのメカニズムを介してログインし、組織に対する認証を行います。マスターノードは、IAM インスタンスプロファイルを使用して AWS リソースを管理します。

認証

エラスティックランタイム環境では、Informatica Intelligent Cloud Services と IAM ロールを使用して、ユーザーおよびインスタンスが Informatica Intelligent Cloud Services と AWS リソースにアクセスして管理することを許可します。

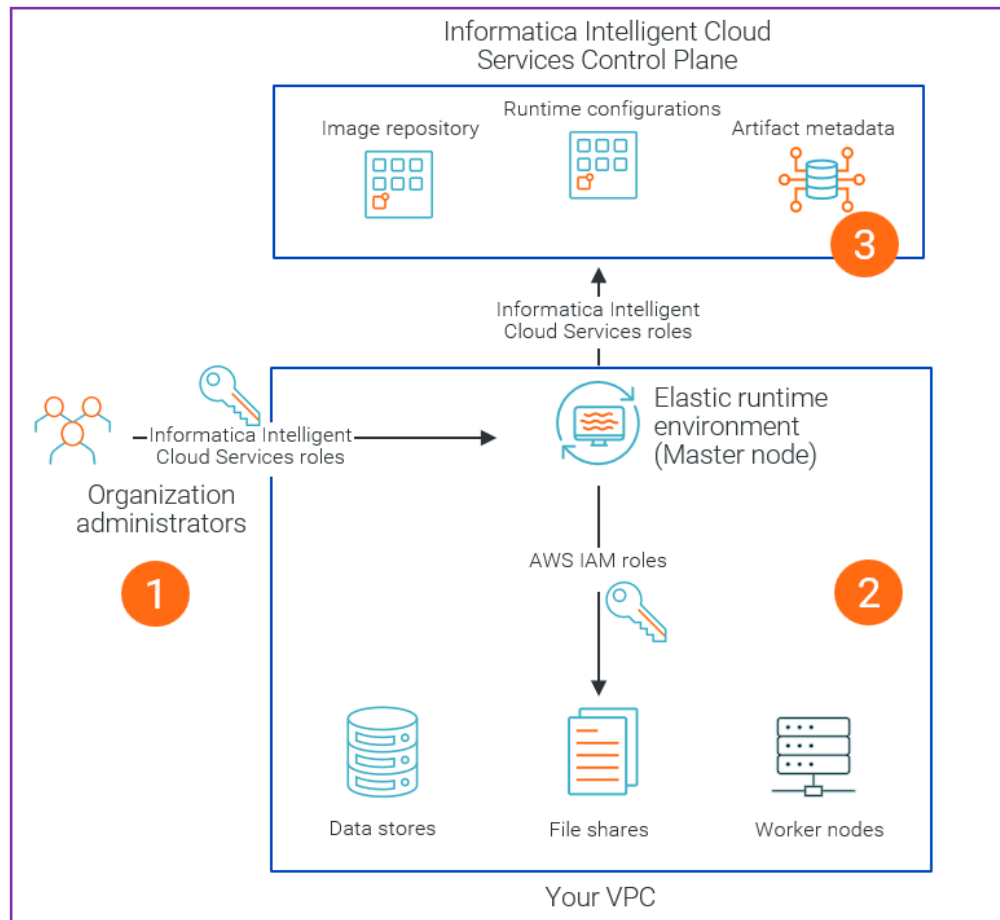
ユーザーベースの承認

ユーザーには、Informatica Intelligent Cloud Services ロールを通じて、Informatica Intelligent Cloud Services およびエラスティックランタイム環境にアクセスして管理する権限が割り当てられます。このロールにより、エラスティックランタイム環境を作成、変更、およびデプロイし、Secure Agent にアクセスするための特権がユーザーに付与されます。また、ロールによって、部門レベルのアクセスのためにエラスティックランタイム環境を分離し、それぞれの部門が独自のエラスティックランタイム環境を管理する権限を持つようにします。

インスタンスベースの承認

マスターノードには、環境内のワーカーノードと VPC 内の AWS リソースにアクセスして管理する権限があります。マスターノードには、1 つ以上の IAM ポリシーとインスタンスプロファイルに関連付けられた IAM ロールを介して承認が付与されます。ポリシーは、ファイル共有や仮想マシンなどのエラスティックランタイム環境が使用する AWS リソースへのきめ細かなアクセスを提供します。例えば、マスターノードには、EC2 インスタンスの作成と自動スケーリング設定の変更が許可されています。

次の画像に、Informatica がロールを使用して、Informatica Intelligent Cloud Services および AWS リソースにアクセスして管理するための承認を管理する方法を示します。



1. Informatica Intelligent Cloud Services ロールは、組織内のエラスティックランタイム環境を設定するためのアクセス権を付与します。
2. IAM ロールは、エラスティックランタイム環境のデータストア、ファイル共有、およびワーカーノードへのアクセス権を付与します。
3. Informatica Intelligent Cloud Services ロールは、Informatica のイメージリポジトリ、アーティファクトリ、およびランタイム設定ストアなど、Informatica Intelligent Cloud Services コントロールプレーン内のリソースへのアクセス権を付与します。

前提条件の確認

エラスティックランタイム環境をセットアップする前に、正しい権限を持つ AWS アカウントがあり、組織の管理者が Administrator で正しい機能特権を持っていることを確認します。

次の前提条件を確認します。

- リソースの作成権限を持つ AWS アカウントがあること。組織に専任の AWS 管理者がいる場合、AWS 管理者は Informatica 管理者と協力してリソースを作成できます。

- Informatica Intelligent Cloud Services 組織管理者に、次の Administrator 機能特権があること。
 - エラスティックランタイム環境 - イメージの取得
 - エラスティックランタイム環境 - トークンの管理
- 機能特権の詳細については、「ユーザー管理」を参照してください。

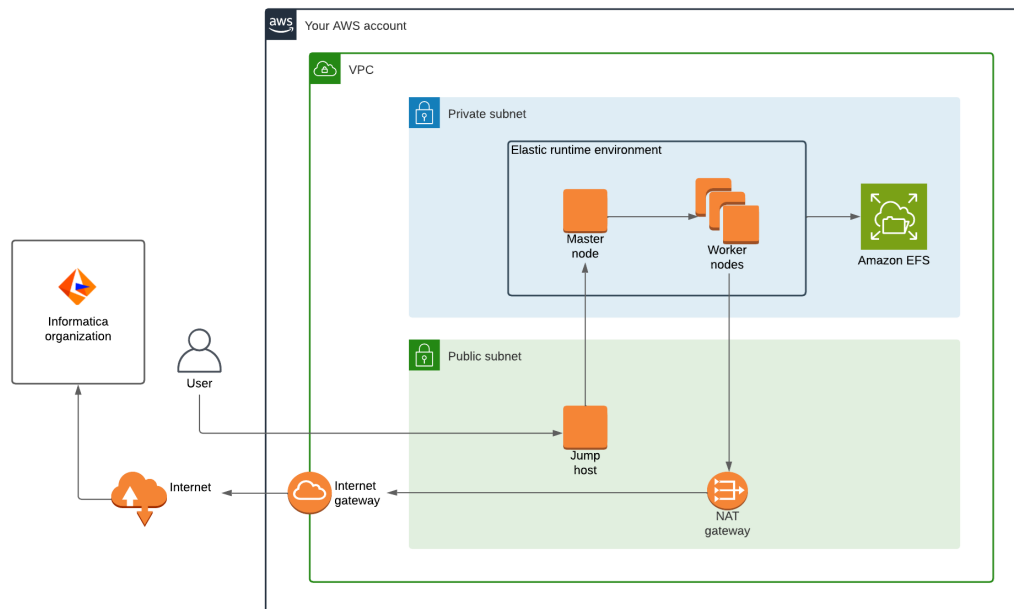
AWS 環境の設定

エラスティックランタイム環境をデプロイする前に、AWS 環境を設定し、必要な AWS リソースを作成して設定します。

AWS 環境を設定するには、次のタスクを完了します。

1. エラスティックランタイム環境が Secure Agent を起動するためや、ジョブを実行するために使用できる AWS リソースを作成および設定します。
2. クラスタがエラスティックランタイム環境とやり取りできる権限が含まれたクラスタインストーラポリシーを作成します。
3. クラスタインストーラがエラスティックランタイム環境をデプロイできるようにする、クラスタインストーラの IAM ロールを作成します。
4. 作業ノードがエラスティックランタイム環境でデータを処理できる権限が含まれたワーカーポリシーを作成します。
5. 作業ノードがエラスティックランタイム環境でデータを処理できるようにする、作業ノードの IAM ロールを作成します。
6. 必要に応じて、ジャンプホストの EC2 インスタンスを起動して、エラスティックランタイム環境にリモートでアクセスします。エンタープライズネットワーク経由でプライベートサブネットにアクセスできる場合、ジャンプホストを作成する必要はありません。
7. マスターノードの EC2 インスタンスを起動します。

次の画像に、デPLOYされたエラスティックランタイム環境で AWS 環境がどのように表示されるかを示します。



手順 1. AWS リソースを作成する

エラスティックランタイム環境が Secure Agent を起動するためや、ジョブを実行するために使用できる AWS リソースを作成および設定します。

次の AWS リソースを作成して設定します。

VPC

VPC には、Secure Agent をホストする Kubernetes クラスタなどすべての AWS リソースが含まれています。

AWS アカウントで VPC を作成します。IPv4 CIDR 手動入力を使用し、VPC が使用する CIDR ブロックを入力します。

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。パブリックサブネットを作成するには、次のガイドラインに従ってください。

- 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ます。
- IPv4 VPC CIDR ブロックを設定するには、VPC の作成時に指定したのと同じ IPv4 CIDR ブロックを使用します。
- IPv4 サブネット CIDR ブロックを設定するには、VPC CIDR 範囲内にある CIDR 範囲を使用します。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。例えば、VPC に 10.1.0.0/16 を使用する場合、パブリックサブネットに 10.1.0.0/20 を使用できます。

プライベートサブネット

プライベートサブネットは、IDMC サーバーとリソースをホストします。プライベートサブネットを作成するには、次のガイドラインに従ってください。

- パブリックサブネットの作成に使用したのと同じ可用性ゾーンを使用します。

- IPv4 VPC CIDR ブロックを設定するには、VPC の作成時に指定したのと同じ IPv4 CIDR ブロックを使用します。
- IPv4 サブネット CIDR ブロックを設定するには、VPC CIDR 範囲内にある CIDR 範囲を使用します。例えば、VPC に 10.1.0.0/16 を使用する場合、プライベートサブネットに 10.1.240.0/20 を使用できます。

エラスティックランタイム環境で作業ノードの最大数に対応するために使用可能な IP アドレスが十分にある範囲を選択します。例えば、環境に作業ノードが少なくとも 1 個、最大で 10 個ある場合、作業ノードに対応するために、プライベートサブネットに少なくとも 10 個の IP アドレスが使用可能な状態である必要があります。

NAT ゲートウェイ

NAT ゲートウェイは、プライベートサブネット内のノード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。NAT ゲートウェイは、プライベートノードがパブリックインターネットから確実に分離されるようにします。

NAT ゲートウェイを作成するには、次のガイドラインに従ってください。

- サブネットとしてパブリックサブネットを使用します。
- 接続タイプを **[パブリック]** に設定します。
- NAT ゲートウェイにエラスティック IP アドレスを割り当てます。

インターネットゲートウェイ

インターネットゲートウェイは、インターネットアクセスに使用します。パブリックサブネットとインターネットゲートウェイによって、ジャンプホストはパブリックインターネットからの SSH 接続を受信できます。

AWS でインターネットゲートウェイを作成し、VPC にアタッチします。

ジャンプホストの詳細については、[「手順 6.ジャンプホストを作成する（オプション）」（ページ 35）](#)を参照してください。

パブリックルートテーブル

パブリックルートテーブルは、パブリックサブネット内のトラフィックをルーティングします。パブリックルートテーブルを作成するには、次のガイドラインに従ってください。

- 作成した VPC を使用します。
- 0.0.0.0/0 を宛先および作成したインターネットゲートウェイとして使用するルートを追加します。
- サブネットの関連付けを編集し、作成したパブリックサブネットを選択します。

プライベートルートテーブル

プライベートルートテーブルは、プライベートサブネット内のトラフィックをルーティングします。プライベートルートテーブルを作成するには、次のガイドラインに従ってください。

- 作成した VPC を使用します。
- 0.0.0.0/0 を宛先および作成した NAT ゲートウェイとして使用するルートを追加します。
- サブネットの関連付けを編集し、作成したプライベートサブネットを選択します。

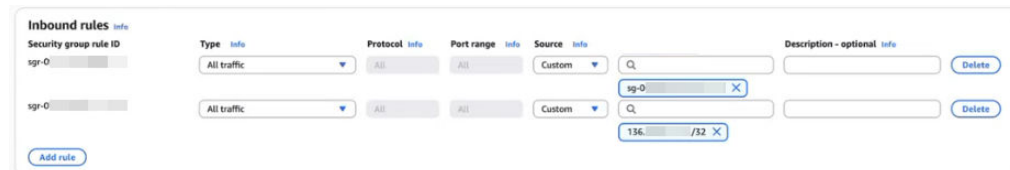
エラスティックランタイム環境のセキュリティグループ

セキュリティグループは、エラスティックランタイム環境への SSH アクセスを許可します。このセキュリティグループは、config.txt ファイルで指定します。config.txt ファイルの詳細については、[「「エラスティックランタイム環境のデプロイ」（ページ 39）」](#)を参照してください。

セキュリティグループを作成するには、次のガイドラインに従ってください。

- 既存のセキュリティグループを使用するか、新しいセキュリティグループを作成します。
- 作成した VPC を使用します。
- 次のタイプのトラフィックを許可する受信ルールを追加します。
 - 同じセキュリティグループからのすべてのトラフィック
 - AWS リソースの作成に使用しているローカルマシンからのすべてのトラフィック

次の画像に、受信ルールの例を示します。



必要な受信ルールが欠落している場合は、クラスティンストーラによって入力されます。

ジャンプホストのセキュリティグループ（オプション）

ジャンプホストはパブリックサブネット内の EC2 インスタンスであり、プライベートサブネット内のエラスティックランタイム環境のノードに SSH 接続するために使用できます。セキュリティグループは、ローカルマシンからジャンプホストへの SSH アクセスを許可します。エンタープライズネットワーク経由でプライベートサブネットにアクセスできる場合、ジャンプホストまたはジャンプホストのセキュリティグループを作成する必要はありません。

ジャンプホストのセキュリティグループを作成する場合は、次のガイドラインを使用してください。

- 作成した VPC を使用します。
- 送信元<local machine IP address>/32 からのポート 22 での SSH トラフィックを許可する受信ルールを追加します。

ジャンプホストの作成の詳細については、[「手順 6.ジャンプホストを作成する（オプション）」（ページ 35）](#)を参照してください。

システムストレージ用（必須）およびデータストレージ用（オプション）の EFS ファイルシステム

エラスティックランタイム環境は、システムストレージ用とデータストレージ用に EFS ファイルシステムを使用します。システムストレージは Secure Agent の操作に必要で、データストレージには、フラットファイル、JAR ファイル、およびライブラリなど、エラスティックランタイム環境がタスクの実行に使用できるファイルが格納されます。

システムストレージ用の EFS ファイルシステムを作成し、そのアクセスポイントを作成します。必要に応じて、データストレージ用の別の EFS ファイルシステムを作成し、そのアクセスポイントを作成することもできます。

各ファイルシステムを作成するには、次のガイドラインに従ってください。

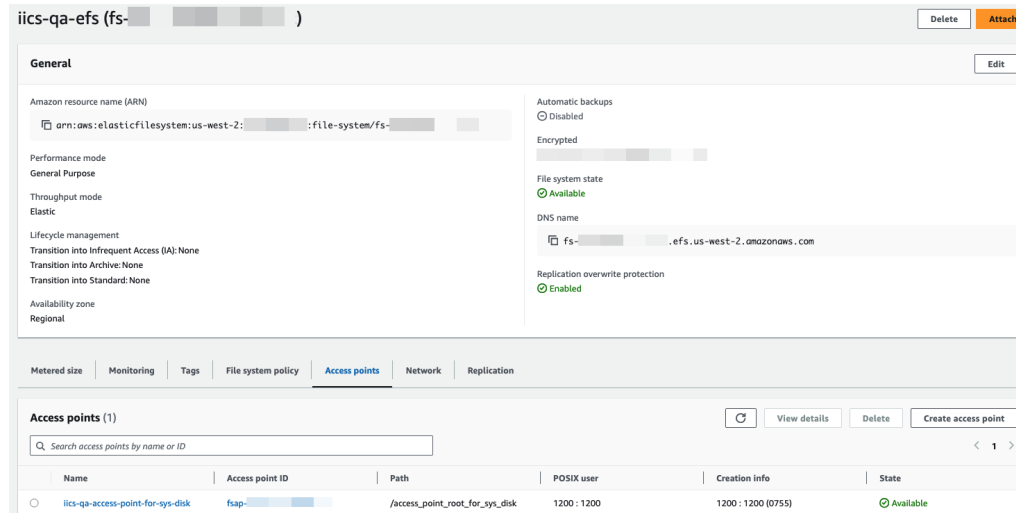
- VPC には、作成した VPC を使用します。
- システムディスクには、マウントターゲットを指定せず、AWS によって追加されたデフォルトのマウントターゲットを削除します。クラスティンストーラは、マウントターゲットを EFS ファイルシステムに自動的に追加します。

データディスクには、マウントターゲットとしてプライベートサブネットを指定します。
- **[ネットワークアクセス]** ページで、ファイルシステムをカスタマイズして、可用性ゾーンは作成した可用性ゾーンの名前に、セキュリティグループは作成したセキュリティグループの名前に設定します。
- ファイルシステムは、必ずカスタマイズした後に作成してください。

各アクセスポイントを作成するには、次のガイドラインに従ってください。

- ファイルシステムには、作成したファイルシステムを使用します。
- /ert_sysdisk または /ert_datadisk などのルートディレクトリを入力します。
- POSIX ユーザーには、ユーザー ID 1200 とグループ ID 1200 を使用します。
- ルートディレクトリ作成権限で、所有者ユーザー ID 1200、所有者グループ ID 1200、およびアクセスポイント権限 0755 を使用します。

次の図は、AWS マネジメントコンソールの EFS ファイルシステムの例を示しています。



手順 2. クラスタインストーラポリシーを作成する

クラスタがエラスティックランタイム環境とやり取りできる権限が含まれたクラスタインストーラポリシーを作成します。

クラスタインストーラポリシーを作成するには、このセクションの JSON ドキュメントを使用して、プレースホルダを置き換えます。

次の表に、各プレースホルダを示します。

プレースホルダ	説明
<AWS アカウント ID>	AWS アカウント ID。
<クラスタインストーラロール>	クラスタインストーラロール名 (cluster_installer_role など)。名前は、ロールの AWS 命名規則に従っている必要があります。 注: このステップでロール名を決定し、ロールの作成時に同じロール名を使用できます。クラスタインストーラロールの作成の詳細については、 「手順 3. クラスタインストーラロールを作成する」 (ページ 33) を参照してください。
<ワーカーロール>	ワーカーロール名 (worker_node_role など)。名前は、ロールの AWS 命名規則に従っている必要があります。 注: このステップでロール名を決定し、ロールの作成時に同じロール名を使用できます。クラスタインストーラロールの作成の詳細については、 「手順 5. ワーカーロールの作成」 (ページ 35) を参照してください。

次の JSON ドキュメントには、ポリシーのコンテンツが含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor2",
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor3",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateKeyPair",
        "ec2:CreateTags",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource": [
        "arn:aws:ec2:*:<AWS account ID>:security-group/*",
        "arn:aws:ec2:*:<AWS account ID>:network-interface/*",
        "arn:aws:ec2:*:<AWS account ID>:launch-template/*",
        "arn:aws:ec2:*:<AWS account ID>:instance/*",
        "arn:aws:ec2:*:<AWS account ID>:subnet/*",
        "arn:aws:ec2:*:<AWS account ID>:volume/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:<AWS account ID>:key-pair/*"
      ]
    }
  ]
}
```

```

{
  "Sid": "VisualEditor5",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": [
    "arn:aws:ec2:*:<AWS account ID>:network-interface/*",
    "arn:aws:ec2:*:<AWS account ID>:key-pair/*",
    "arn:aws:ec2:*:<AWS account ID>:launch-template/*",
    "arn:aws:ec2:*:<AWS account ID>:instance/*",
    "arn:aws:ec2:*:<AWS account ID>:volume/*",
    "arn:aws:ec2:*:<AWS account ID>:subnet/*",
  ],
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": [
        "RunInstances",
        "CreateKeyPair",
        "CreateLaunchTemplate",
        "CreateLaunchTemplateVersion",
        "network-interface",
        "CreateTags",
        "CreateAutoScalingGroup"
      ]
    }
  }
},
{
  "Sid": "VisualEditor13",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": [
    "arn:aws:iam::<AWS account ID>:role/<cluster installer role>",
    "arn:aws:iam::<AWS account ID>:role/<worker role>"
  ]
},
{
  "Sid": "VisualEditor21",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:ListSecrets",
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource",
    "secretsmanager>DeleteSecret",
    "secretsmanager:UpdateSecret"
  ],
  "Resource": "arn:aws:secretsmanager:*:<AWS account ID>:secret:*"
},
{
  "Sid": "VisualEditor10",
  "Effect": "Allow",
  "Action": [
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource": "*"
},
{
  "Sid": "VisualEditor11",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSubnets"
  ],
  "Resource": "*"
},
{
  "Sid": "EC2Management",
  "Effect": "Allow",

```



```

    "Action": [
      "ec2:AssociateIamInstanceProfile",
      "ec2:CreateKeyPair",
      "ec2:CreateLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion",
      "ec2:CreateTags",
      "ec2>DeleteLaunchTemplate",
      "ec2>DeleteTags",
      "ec2:ModifyLaunchTemplate",
      "ec2:RunInstances",
      "ec2:TerminateInstances",
      "iam:PassRole"
    ],
    "Resource": "*"
  }
]
}

```

クラスインストーラポリシーの権限の詳細については、[「クラスインストーラポリシー文」](#)（ページ 56）を参照してください。

手順 3。クラスインストーラロールを作成する

クラスインストーラがエラスティックランタイム環境をデプロイできるようにする、クラスインストーラの IAM ロールを作成します。

クラスインストーラロールを作成するには、次のガイドラインに従ってください。

- 信頼できるエンティティを **[AWS サービス]**、ユースケースを **[Amazon EC2]** に設定します。
- クラスインストーラポリシーで指定したのと同じクラスインストーラロール名を使用します。
- 信頼関係を編集し、次のポリシーを指定します。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

- AWS がロールのインスタンスプロファイルを自動作成しない場合は、インスタンスプロファイルを手動で作成します。

手順 4.ワーカーポリシーを作成する

作業ノードがエラスティックランタイム環境でデータを処理できる権限が含まれたワーカーポリシーを作成します。

ワーカーポリシーを作成するには、次の JSON ドキュメントを使用します。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DescribeActions",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:DescribeMountTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",

```

```

        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeTags",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeScalingActivities",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*"
},
{
    "Sid": "AutoscalingCapacity",
    "Effect": "Allow",
    "Action": [
        "autoscaling:SetDesiredCapacity",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling>DeleteAutoScalingGroup",
        "autoscaling>DeleteTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "EC2Management",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateTags",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteTags",
        "ec2:ModifyLaunchTemplate",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "iam:PassRole"
    ],
    "Resource": "*"
},
{
    "Sid": "EFSManagement",
    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem>DeleteAccessPoint"
    ],
    "Resource": "*"
},
{
    "Sid": "SecretsManagerAccess",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
    ],
    "Resource": "*"
}
]
}

```

ワーカーポリシーの権限の詳細については、[「ワーカーポリシー文」 \(ページ 59\)](#)を参照してください。

手順 5. ワーカーロールの作成

作業ノードがエラスティックランタイム環境でデータを処理できるようにする、作業ノードの IAM ロールを作成します。

ワーカーロールを作成するには、次のガイドラインに従ってください。

- 信頼できるエンティティを **[AWS サービス]**、ユースケースを **[Amazon EC2]** に設定します。
- クラスタインストラポリシーで指定したのと同じワーカーロール名を使用します。
- 信頼関係を編集し、次のポリシーを指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- AWS がロールのインスタンスプロファイルを自動作成しない場合は、インスタンスプロファイルを手動で作成します。

手順 6. ジャンプホストを作成する（オプション）

必要に応じて、ジャンプホストの EC2 インスタンスを起動して、エラスティックランタイム環境にリモートでアクセスします。エンタープライズネットワーク経由でプライベートサブネットにアクセスできる場合、ジャンプホストを作成する必要はありません。

ジャンプホストはパブリックサブネット内の EC2 インスタンスであり、プライベートサブネット内のエラスティックランタイム環境のノードに SSH 接続するために使用できます。エラスティックランタイム環境はプライベートサブネットで実行されるように設計されているため、ジャンプホストは環境にリモートでアクセスできません。

ジャンプホストを使用すると、エラスティックランタイム環境がインターネットに公開されないため、安全でスケーラブルなインフラストラクチャを実現するためのベストプラクティスと言えます。ジャンプホストによって、攻撃対象領域が大幅に縮小し、エラスティックランタイム環境への不正アクセスが防止されます。また、アクセスは SSH 認証とセキュリティグループルールを使用し制御されます。ジャンプホストが侵害された場合、エラスティックランタイム環境内のノードはファイアウォールとセキュリティグループによって保護されます。

AWS のインスタンス起動ウィザードを使用してジャンプホストを作成します。次のガイドラインを使用します。

- OS イメージとして Amazon Linux を使用します。
- t3.small インスタンスタイプを使用します。
- 新しいキーペアを作成します。
- 作成した VPC を使用します。
- サブネットには、作成したパブリックサブネットを選択します。
- **[パブリック IP の自動割り当て]** を有効にします。
- ジャンプホスト用に作成したセキュリティグループを使用します。詳細については、「[手順 1. AWS リソースを作成する](#)」(ページ 27) を参照してください。

次に、インスタンスを起動します。

手順 7. マスターノードを作成する

マスターノードの EC2 インスタンスを起動します。

AWS のインスタンス起動ウィザードを使用してマスターノードを作成します。次のガイドラインを使用します。

- パブリック Informatica AMI を使用してインスタンスを起動し、マスターノードを作成します。infa-elastic-master-node を検索し、現在のリリースの AMI を選択します。
例えば、2025 年 7 月リリースの場合、AMI は infa-elastic-master-node-2025-07-M になります。
- 少なくとも 2 個の CPU と 4 GB のメモリを備えたインスタンスタイプを使用します。
- ジャンプホストの起動時に作成したキーペアを使用します。
- ネットワーク設定で、作成した VPC を使用します。
- 作成したプライベートサブネットをサブネットとして使用します。
- **[パブリック IP の自動割り当て]** を無効にします。
- エラスティックランタイム環境用に作成したセキュリティグループを使用します。詳細については、「[手順 1. AWS リソースを作成する](#)」(ページ 27) を参照してください。
- IAM インスタンスプロファイルを設定するには、クラスティンストーラロールのインスタンスプロファイルを使用します。

次に、インスタンスを起動します。

エラスティックランタイム環境の作成

管理者でエラスティックランタイム環境を作成します。

1. 管理者で、**[ランタイム環境]** ページを開きます。
2. **[新しいランタイム環境]** を選択します。
3. **[全般]** ページで、エラスティックランタイム環境の名前を入力します。
4. 環境タイプとして **[エラスティックランタイム環境]** を選択します。
5. 必要に応じて、説明を入力します。
6. **次へ** をクリックします
7. **[コンポーネントの有効化]** ページで、有効にするサービスを選択します。
8. エラスティックランタイム環境で有効にするコネクタを選択します。

エラスティックランタイム環境で利用できるコネクタのリストについては、[「エラスティックランタイム環境でのコネクタ」](#) (ページ 47) を参照してください。

9. Secret Manager など、有効にする追加のサービスを選択します。

注: エラスティックランタイム環境の作成時にサービスとコネクタを有効にしない場合は、後で有効にすることができます。詳細については、「[「エラスティックランタイム環境での操作」](#)」(ページ 45) を参照してください。Secret Manager の設定手順については、「[組織の管理](#)」を参照してください。

10. **[作成]** をクリックします。
11. **[環境設定]** タブで、エラスティックランタイム環境のプロパティを設定します。

環境設定

エラスティックランタイム環境プロパティを設定し、Informatica Intelligent Cloud Services がエラスティックランタイム環境で Kubernetes クラスタを実行してデータを処理する方法を決定します。

プラットフォーム

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
地域	エラスティックランタイム環境を作成するリージョン。 注: エラスティックランタイム環境をデプロイした後に、リージョンを更新することはできません。
ワーカーインスタンスタイプ	ワーカーノードをホストするインスタンスのタイプ。 インスタンスタイプが AWS セットアップでサポートされているか確認するには、AWS ドキュメントを参照してください。 注: Secure Agent サービスのワーカーノードは、マスターノードと同じインスタンスタイプを使用します。
ワーカーインスタンスプロファイル	作業ノードにアタッチするインスタンスプロファイル。インスタンスプロファイルは、ARN の末尾にある値です。
高可用性の有効化	エラスティックランタイム環境の高可用性を有効にします。 高可用性が有効になっている場合、エラスティックランタイム環境では奇数のマスターノードが維持されます。セットアップの一環として元のマスターノードを 1 つ手動で作成するため、環境では指定したサブネットの数に基づいて、追加の偶数のマスターノードが作成されます。例えば、2 つのサブネットを指定すると、環境には合計 3 つのマスターノードが存在するようになります。 注: ワーカーノードは常に高可用性であり、高可用性が有効になっているかどうかに関係なく、複数の可用性ゾーンとサブネットにまたがって作成されます。 高可用性について詳しくは、Kubernetes のドキュメントを参照してください。
サブネット	高可用性が有効になっている場合の異なるリージョンのサブネット ID。少なくとも 2 つのサブネットのサブネット ID を入力してください。例: subnet-01234567890abcdef マスターノードの総数が奇数である場合、マスターノードはそれぞれのサブネットに作成されます。元のマスターノードを含む環境内の各マスターノードは、異なるリージョンに存在する必要があります。作成されたマスターノードは元のマスターノードと同じ構成を使用しますが、IP アドレスは異なります。
EBS ボリュームサイズ	データ処理中の一時ストレージ用に作業ノードにアタッチする EBS ボリュームのサイズ。

注: エラスティックランタイム環境を高可用性にして、マスターノードがダウンしたときに単一障害点とならないようにすることができます。高可用性を有効にすると、1 つのマスターノードがダウンしても他のマスターノードを使用できるため、ジョブを引き続き実行することができます。エラスティックランタイム環境が高可用性である場合は、次のシナリオでのジョブの失敗に注意してください。

- すべてのマスタノードがダウンすると、ジョブは失敗します。

- 非常に多くのマスタノードがダウンすると、Kubernetes API サーバーが使用できなくなります。失敗の数のしきい値は $(n+1)/2$ です。n はマスタノードの数です。例えば、クラスタに 3 つのマスタノードがあり、2 つのマスタノードがダウンした場合、Kubernetes API サーバーは使用できなくなり、クラスタでのジョブは失敗します。

ジョブ自動スケーリングポリシー

エラスティックランタイム環境では、次のワーカーノードセットが使用されます。

- ジョブを実行するワーカーノード。ジョブ自動スケーリングポリシーにより、組織内でジョブを実行するために作成されるワーカーノードの数が決定されます。
- Secure Agent サービスを実行するワーカーノード。このワーカーノードのセットは、大量のジョブに対応するために自動的にスケーリングされます。

ワーカーノードのアイドルタイムアウトに達するまでにエラスティックランタイム環境にジョブが送信されない場合、ワーカーノードの数は次の式を使用して計算されます。

$(\text{min worker nodes in job auto-scaling policy}) + (\text{worker nodes for Secure Agent services})$

ジョブ自動スケーリングポリシーのワーカーノードの最小数がゼロに設定されている場合でも、環境には Secure Agent サービスを実行するワーカーノードが少なくとも 1 つ存在します。

次の表に、ジョブの自動スケーリングポリシーのプロパティとその説明を示します。

プロパティ	説明
作業ノードの最小数	ワーカーノードの最小数。
作業ノードの最大数	ワーカーノードの最大数。
ワーカーノードのアイドルタイムアウト	作業ノードがタイムアウトするまでのアイドル時間の長さ。

システムストレージ

以下の表に、システムプロパティに関する説明を示します。

プロパティ	説明
タイプ	システムストレージのタイプ。[EFS] を選択します。
ファイルシステム	EFS ファイルシステムのファイルシステム ID。
ソースマウント	エラスティックランタイム環境にマウントするファイルシステムパス。 注: 最初のスラッシュは除外します。例えば、パスが/sysdisk である場合は、sysdisk を使用します。
アクセスポイント	EFS ファイルシステムのアクセスポイント ID。ID は ARN の末尾にある英数字の値です。

データストレージ

以下の表に、データストレージプロパティに関する説明を示します。

プロパティ	説明
タイプ	データストレージのタイプ。[EFS] を選択します。
ファイルシステム	EFS ファイルシステムのファイルシステム ID。
ソースマウント	エラスティックランタイム環境にマウントするファイルシステムパス。 注: 最初のスラッシュは除外します。例えば、パスが/datadisk である場合は、datadisk を使用します。
アクセスポイント	EFS ファイルシステムのアクセスポイント ID。ID は ARN の末尾にある英数字の値です。

詳細設定

以下の表に詳細プロパティを示します。

プロパティ	説明
クラウドエコシステムのタグ	クラウドリソースのタグ。タグを少なくとも 1 つ追加してください。 NAME タグと Name タグは、システム用に予約されています。 注: エラスティックランタイム環境をデプロイした後に、タグを更新することはできません。
ランタイムプロパティ	エラスティックランタイム環境と、その環境で実行するジョブをカスタマイズするためのプロパティ。

エラスティックランタイム環境のデプロイ

AWS にエラスティックランタイム環境をデプロイして、Informatica Intelligent Cloud Services からのデータを処理する際に Kubernetes クラスタを使用できるようにします。

以下のタスクを完了させます。

1. マスターノードに SSH 接続し、クラスタインストーラをダウンロードして実行できるようにします。
2. エラスティックランタイム環境を再デプロイする場合は、リソースをクリーンアップします。
3. クラスタインストーラをダウンロードして、インストール用の config.txt ファイルとインストールスクリプトを取得します。
4. エラスティックランタイム環境のマスターノードにディレクトリを作成します。
5. config.txt ファイルを更新して、AWS 環境と Informatica Intelligent Cloud Services アカウントに関する詳細をクラスタインストーラに提供します。
6. クラスタインストーラを実行して、エラスティックランタイム環境をデプロイします。
7. マスターノードに各 EFS ファイルシステムをマウントします。
8. Administrator でデータ統合サーバーとクラスタノードの状態を確認して、エラスティックランタイム環境が実行されていることを確認します。

手順 1. マスターノードに SSH 接続する

マスターノードに SSH 接続し、クラスタインストーラをダウンロードして実行できるようにします。

1. 必要に応じて、ジャンプホストに SSH 接続します。
 - a. 組織の IT チームに連絡して、ローカルマシンでプライベートキーのパスフレーズを作成し、パブリックキーを使用して認証するようにジャンプホストを設定します。
パスフレーズの作成と認証の設定の例については、ナレッジベース記事 [HOW TO: Create a key-pair \(Public and Private key\) using OpenSSH on UNIX for Support Console](#) を参照してください。
 - b. 次のコマンドを実行して、ローカルマシンからジャンプホストに SSH で接続します。

```
ssh -i <private key name>.pem <user name>@<jump host public IP address>
```
2. 次のコマンドを実行して、マスターノードに SSH 接続します。

```
ssh -i <private key name>.pem cloud-user@<master node private IP address>
```

手順 2. リソースのクリーンアップ

エラスティックランタイム環境を再デプロイする場合は、クラスタアンインストーラを実行して、AWS と Kubernetes のリソースをクリーンアップします。

注: クラスタアンインストーラを実行した後にのみ、クラスタアンインストーラを実行してください。クラスタインストーラを実行していない場合、アンインストーラは失敗します。

1. アンインストーラを実行する前に、エラスティックランタイム環境で実行されているジョブがないことを確認してください。アンインストーラの実行を元に戻すことはできず、アンインストーラの実行によって実行中のジョブはすべて終了します。
2. アンインストーラを実行するには、マスターノードで次のコマンドを実行します。

```
./cluster_uninstall.sh
```

クラスタアンインストーラにより、自動スケーリンググループ、EC2 インスタンス、起動テンプレート、およびシークレットなどのリソースが削除されます。

手順 3. クラスタインストーラをダウンロードする

クラスタインストーラをダウンロードして、インストール用の config.txt ファイルとインストールスクリプトを取得します。

1. Administrator で、**[ランタイム環境]** ページを開きます。
2. **[ランタイムインストーラのダウンロード]** を選択します。
3. **[環境タイプ]** として **[エラスティック]** を選択します。
4. **[ダウンロード]** を選択します。

クラスタインストーラを含む ZIP ファイルがローカルマシンにダウンロードされます。

手順 4. マスターノードでのクラスタインストーラディレクトリの作成

エラスティックランタイム環境のマスターノードにディレクトリを作成します。

1. マスターノードで次のコマンドを実行して、エラスティックランタイム環境のディレクトリを作成します。

```
mkdir ert
```
2. クラスタインストーラを ert ディレクトリにコピーします。

3. 次のコマンドを実行してディレクトリに移動します。
`cd ert`
4. 次のコマンドを実行してファイルを解凍します。
`unzip cluster-installer.<version>.zip`

手順 5.config.txt ファイルを更新する

config.txt ファイルを更新して、AWS 環境と Informatica Intelligent Cloud Services アカウントに関する詳細をクラスタインストーラに提供します。

マスターノードのエラスティックランタイム環境ディレクトリで、次のコマンドを実行して config.txt ファイルを開きます。

```
vi config.txt
```

次の表に、config.txt ファイルで更新する値を示します。

変数	説明
IDS_HOST	組織の POD のドメイン。例えば、dm-us.informaticacloud.com です。ドメインを見つけるには、 POD Availability and Networking で POD を検索して、 [ログイン URL] フィールドのプロパティをコピーします。
USER	Informatica Intelligent Cloud Services のユーザー名。
PASS	Informatica Intelligent Cloud Services のパスワード。
runtimeEnvironmentId	エラスティックランタイム環境 ID。 ID をを見つけるには、Administrator の [ランタイム環境] ページに移動して、URL からエラスティックランタイム環境 ID をコピーします。 例えば、https://usw1.dmr-us.informaticacloud.com/cloudUI/products/administer/main/elastic-agent/KUBERNETES/0141GU25000000000002/overview という URL の場合、エラスティックランタイム環境 ID は 0141GU250000000000002 です。
PROXY_USER	オプション。送信プロキシサーバーに接続するユーザー名。
PROXY_HOST	オプション。Secure Agent が使用する送信プロキシサーバーのホスト名。
PROXY_PORT	オプション。送信プロキシサーバーのポート番号。
majorVersion	リリースバージョン。例えば、2025 年 7 月リリースの場合は 202507 を使用します。
SECURITY_GROUP_NAME	エラスティックランタイム環境へのアクセスを許可するセキュリティグループの名前。 必要な受信ルールが欠落しており、クラスタインストーラロールにセキュリティグループを変更するための権限が割り当てられている場合、クラスタインストーラはそれらのルールを設定し、インストールを続行します。それ以外の場合、クラスタのインストールは停止します。インストールを続行するには、セキュリティグループを手動で編集し、必要な受信ルールを追加します。 必要な受信ルールの詳細については、「 手順 1。AWS リソースを作成する 」(ページ 27) を参照してください。
VPC_NAME	作成した VPC の名前。

注: 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、エラスティックランタイム環境はプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。プロキシサーバーの設定は config.txt ファイルで行うことができます。クラスインストールが実行されると、プロキシサーバーのパスワードの入力を求めるメッセージが表示されます。エラスティックランタイム環境のデプロイ後にプロキシサーバーの設定を変更することはできません。

config.txt ファイルには、次の情報が含まれています。

```
# Distributed Configuration for Cluster Installer
# =====
# Customize the following variables to match your environment.
#
# IDS_HOST
#   The host address or URL for the IDS service.
export IDS_HOST="<POD URL like dm-us.informaticacloud.com>"
# USER
#   Informatica Intelligent Cloud Services user name for the organization that you want to log in to.
export USER="<IICS user name>"
# PASS
#   Informatica Intelligent Cloud Services password.
export PASS="<IICS password>"
# runtimeEnvironmentId
#   A unique identifier for your runtime environment.
export runtimeEnvironmentId="<elastic runtime environment ID from Administrator>"
# PROXY_USER PROXY_HOST PROXY_PORT
# Specify these values if your organization uses HTTP proxy for outbound communication.
# You will be prompted to enter Proxy password by the cluster installation script if PROXY_USER is specified.
export PROXY_USER="<proxy server user name>"
export PROXY_HOST="<proxy server host name>"
export PROXY_PORT="<proxy server port number>"
#
# majorVersion
#   Major version number for your release. Update as needed.
export majorVersion="<version like 202507>"

# Following variables are provided so that you can customize cluster creation as per your organization
# policies.
#
# KEY_PAIR_NAME and KUBE_CONFIG_SECRET_NAME
#   These values identify the key pair and its secret name used to access your cluster.
#   Name of the Key Pair that is used to login to the nodes in the cluster
KEY_PAIR_NAME="idmc-elastic-rte-key-pair"
KUBE_CONFIG_SECRET_NAME="idmc-elastic-rte-kube-config"
#
# ORG_ADMIN_CREDS_SECRET_NAME
#   The name of the secret that stores organization administrator credentials.
ORG_ADMIN_CREDS_SECRET_NAME="idmc-elastic-rte-org-creds"
#
# SECURITY_GROUP_NAME
#   The security group name defined for access within your environment.
SECURITY_GROUP_NAME="<security group name like sg_ert>"
#
# NODE_NAME_PREFIX
#   Prefix for naming the nodes in your cluster.
NODE_NAME_PREFIX="idmc-elastic-rte"
#
# AGENT_APP_LAUNCH_TEMPLATE_NAME and AGENT_APP_ASG_NAME
#   Launch template and auto scaling group names for the agent application.
AGENT_APP_LAUNCH_TEMPLATE_NAME="idmc-elastic-rte-agent-app-launch-tmpl"
AGENT_APP_ASG_NAME="idmc-elastic-rte-agent-app-asg"
#
# JOB_NODE_LAUNCH_TEMPLATE_NAME and JOB_NODE_ASG_NAME
#   Launch template and auto scaling group names for job nodes.
JOB_NODE_LAUNCH_TEMPLATE_NAME="idmc-elastic-rte-job-node-launch-tmpl"
JOB_NODE_ASG_NAME="idmc-elastic-rte-jon-node-asg"
#
# CONTROL_PLANE_ELB_NAME
#   The load balancer name for the control plane in high-availability setups.
#   Used only when High Availability (HA) mode is enabled.
CONTROL_PLANE_ELB_NAME="idmc-elastic-rte-control-plane-elb"
```

```
#
# efsNameTag
# Tag for EFS (Elastic File System) shared storage to added upon creation
export efsNameTag="idmc-elastic-rte-efs-name"
#
# IS_RUNNING_ON_MASTER
# Set to false if this script is not executed on the master node; otherwise, leave as true.
IS_RUNNING_ON_MASTER=true
#
# VPC_NAME
# Provide the VPC name if the script is not running directly on the master node.
VPC_NAME="<VPC name like vpc_ert>"
#
# resourceCreationLogFile
# Log file name where created resources will be recorded.
export resourceCreationLogFile="resource_creation_log.txt"
```

手順 6. クラスティンストローを実行する

プロキシを使用するか使用しないかにかかわらず、クラスティンストローを実行して、エラスティックランタイム環境をデプロイします。

プロキシを使用したクラスティンストローの実行

プロキシを使用してクラスティンストローを実行するには、次のタスクを実行します。

1. 次のコマンドを実行します。
./create_cluster_nodes_ha.sh
2. **【プロキシパスワードの入力】** 行にパスワードを入力します。パスワードを入力すると、セキュリティ上の理由から入力した文字が非表示になります。

注: プロキシモードでインストローを実行しているときに Ctrl+C を使用すると、インストールが終了します。

プロキシを使用しないクラスティンストローの実行

プロキシを使用せずにクラスティンストローを実行するには、次のタスクを実行します。

1. マスターノードで次のコマンドを実行します。
nohup ./create_cluster_nodes_ha.sh &
2. インストールプロセスを監視するには、次のコマンドを実行します。
tail -f nohup.out

手順 7. マスターノードに EFS ファイルシステムをマウントする

マスターノードに各 EFS ファイルシステムをマウントします。EFS ファイルシステムのマウントの詳細については、AWS のドキュメントを参照してください。

手順 8. エラスティックランタイム環境が実行されていることを確認する

Administrator でデータ統合サーバーとクラスタノードの状態を確認して、エラスティックランタイム環境が実行されていることを確認します。

1. Administrator で、**【ランタイム環境】** ページを開きます。
2. エラスティックランタイム環境を展開します。
3. データ統合サーバーが実行されていることと、1 つ以上のインスタンスが実行されていることを確認します。

注: データ統合サーバーがインスタンスを開始するまでに数分かかる場合があります。

データストレージへのファイルのアップロード

データストレージ用の EFS ファイルシステムにファイルをアップロードして、エラスティックランタイム環境でできるようにします。

次のようなタイプのファイルをアップロードできます。

- タスク内のフラットファイル接続用のフラットファイル
- マッピングタスク用のパラメータファイル
- 特定のトランスフォーメーションおよび接続のための JAR ファイルやライブラリなどの補足ファイル

パラメータファイルのアップロード

パラメータファイルをデータストレージにアップロードして、エラスティックランタイム環境でできるようにします。

ファイルシステムのマウントポイントの下にパラメータファイルを格納します。

フラットファイル接続用のフラットファイルのアップロード

フラットファイルをデータストレージにアップロードして、タスクのフラットファイル接続で 사용할 ことができます。

次の場所を使用して、データストレージ用の EFS ファイルシステムにフラットファイルをアップロードします。

`/etc/infra/pod/<elastic runtime environment ID>/`

エラスティックランタイム環境 ID を見つけるには、管理者の **【ランタイム環境】** ページを開いて、URL からエラスティックランタイム環境 ID をコピーします。

例えば、`https://usw1.dmr-us.informaticacloud.com/cloudUI/products/administer/main/elastic-agent/KUBERNETES/0141GU25000000000002/overview` という URL の場合、エラスティックランタイム環境 ID は `0141GU2500000000000002` です。

フラットファイル接続を作成するときは、ディレクトリを `/etc/infra/pod/<elastic runtime environment ID>/` に設定します。フラットファイル接続の詳細については、目的のコネクタのヘルプを参照してください。

補足ファイルのアップロード

補足ファイルには、特定のトランスフォーメーションおよび接続に必要な JAR ファイルおよびライブラリが含まれています。補足ファイルをデータストレージにアップロードして、エラスティックランタイム環境で 使用 できるようにします。

次のような補足ファイルをアップロードできます。

データベースドライバ

Java トランスフォーメーション用の JAR ファイルと Java ライブラリ

ネイティブライブラリと実行可能ファイル

SAP 接続ドライバとライブラリ

SSL/TLS 証明書とキーストア

1. ファイルシステムのマウントポイントの下に、ファイルを格納するためのディレクトリを作成します。
例えば、ファイルシステムのマウントポイントとして使用する `/mnt/efs` ディレクトリを作成した場合は、JDBC ドライバを格納するための `/mnt/efs/jdbc` ディレクトリを作成できます。

2. 補足ファイルを適切なディレクトリにコピーします。
3. REST API を使用して、補足ファイルの仕様を更新します。
詳細については、[Updating the supplementary file specification](#) を参照してください。

エラスティックランタイム環境での操作

エラスティックランタイム環境を作成した後に、編集、監視、および削除を行うことができます。依存関係の表示や権限の変更を行うこともできます。

以下のタスクが実行できます。

環境の名前または説明を変更する。

エラスティックランタイム環境の名前または説明を変更するには、**[アクション]** メニューを展開して、**[環境プロパティの編集]** を選択します。

環境設定を更新します。

環境プロパティを更新するには、エラスティックランタイム環境をドリルダウンし、**[環境設定]** タブでプロパティを編集します。

プロパティ値を更新して設定を保存した後に、デプロイされたエラスティックランタイム環境で変更が有効になるまでにはしばらく時間がかかります。特定の変更を確認するには、管理者でライフサイクルグラフを表示するか、AWS アカウントのログを表示します。

サービスとコネクタを有効または無効にします。

サービスを有効にすると、エラスティックランタイム環境でそのサービスに関連付けられた製品機能を実行できるようになります。特定のコネクタを有効にすると、環境で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なります。

サービスとコネクタを有効にするには、**[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。

Secure Agent サービスを設定します。

パフォーマンスを最適化するために、または Informatica グローバルカスタマサポートから指示があった場合に、Secure Agent サービスの設定、またはサービスのプロパティの変更を行うことができます。

[サービス設定] タブで Secure Agent サービスのプロパティを変更するか、Secure Agent サービスのカスタムプロパティを追加します。Secure Agent サービスのプロパティをシステムのデフォルトにリセットするには、**[リセット]** を選択します。

Secure Agent サービスとその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。

環境を削除する。

実行中のインスタンスがない場合は、エラスティックランタイム環境を削除できます。

インスタンスをクリーンアップするには、クラスタアンインストーラを実行します。詳細については、「[手順 2.リソースのクリーンアップ](#)」(ページ 40)」を参照してください。

エラスティックランタイム環境を削除するには、**[アクション]** メニューを展開して、**[削除]** を選択します。

監査ログ、ノード、およびジョブを監視します。

エラスティックランタイム環境を監視するには、エラスティックランタイム環境をドリルダウンし、**【監視】** タブを開きます。次のような詳細を表示できます。

- エラスティックランタイム環境で実行されている Secure Agent サービスで発生するイベントを表示するための監査ログ。
- エラスティックランタイム環境内のノード数を経時的に示すライフサイクルグラフ。
- エラスティックランタイム環境に送信されたすべてのジョブのリスト。ジョブの停止と再開、およびログファイルのダウンロードを行うことができます。

イメージを表示します。

エラスティックランタイム環境では、イメージを使用して Informatica Intelligent Cloud Services および Secure Agent サービスを起動します。

Informatica は、ユーザーがイメージリポジトリにアクセスし、イメージをダウンロードしてスキャンし、エンタープライズレベルのセキュリティとコンプライアンスのニーズを満たしていることを確認できるようにしています。Informatica は、新しいイメージが利用可能になるとユーザーに通知して、次のリリースのデプロイウィンドウの前にイメージをスキャンできるようにします。

エラスティックランタイム環境が使用するイメージを表示するには、次のいずれかのオプションを使用します。

- エラスティックランタイム環境をドリルダウンし、**【イメージ】** タブを開きます。それぞれのイメージには、Informatica のイメージリポジトリ内のイメージ名、イメージタグ、およびリポジトリパスが含まれます。
- REST API を使用してトークンを取得し、Informatica のイメージリポジトリからイメージをプルします。

依存関係を表示する。

依存関係を表示して、エラスティックランタイム環境を使用しているタスクまたは接続や、エラスティックランタイム環境が使用しているオブジェクトを見つけます。依存関係を表示するには、**【アクション】** メニューを展開して、**【依存関係の表示】** を選択します。

権限を変更する。

エラスティックランタイム環境の権限を変更するには、**【アクション】** メニューを展開して、**【権限】** を選択します。組織のユーザーグループごとにエラスティックランタイム環境に対する権限を定義できます。

次の表に、設定可能な権限を示します。

権限	説明
読み取り	エラスティックランタイム環境の詳細を表示し、タスクでエラスティックランタイム環境を使用します。
更新	エラスティックランタイム環境を編集します。
削除	エラスティックランタイム環境を削除します。
実行	エラスティックランタイム環境を実行します。
変更権限	エラスティックランタイム環境の権限を変更します。

エラスティックランタイム環境でのコネクタ

コネクタは、エラスティックランタイム環境で実行されるタスクで使用できます。

エラスティックランタイム環境では、次のコネクタを使用するタスクを実行できます。

Amazon Athena Amazon Redshift V2 Amazon S3 V2 Ariba V2 BigMachines ボックス Concur V2 Coupa V2 Databricks Eloqua REST File Processor Google Analytics Google BigQuery V2 Google Cloud Storage V2 IBM MQ JDBC V2 JIRA JIRA クラウド Kafka 大規模言語モデル LDAP Marketo V3 Microsoft Azure Blob Storage V3 Microsoft Azure Data Lake Storage Gen2 Microsoft Azure Cosmos DB SQL API Microsoft Azure Synapse SQL Microsoft Dynamics 365 for Operations Microsoft Dynamics 365 for Sales Microsoft Excel Microsoft Fabric データウェアハウス Microsoft Fabric レイクハウス Microsoft Fabric OneLake Microsoft SharePoint Microsoft SharePoint Online Microsoft SQL Server* MongoDB V2 MySQL NetSuite	NetSuite RESTlet V2 OData コンシューマ OData V2 Protocol Reader OData V2 Protocol Writer ODBC Oracle* Oracle Autonomous Database Oracle Business Intelligence Publisher V1 Oracle Cloud Object Storage Oracle CRM Cloud V1 Oracle Financials Cloud V1 Oracle HCM Cloud V1 PostgreSQL* Quickbooks V2 REST V2 Salesforce Salesforce Data Cloud Salesforce Marketing Cloud SalesforcePardot SAP ADSO Writer SAP BAPI SAP BW BEx クエリ SAP HANA SAP OData V2 SAP OData V4 SAP ODP Extractor ServiceNow Snowflake Data Cloud SuccessFactors ODATA SurveyMonkey Tableau V2 TableauV3 Veeva Vault Web Service Consumer Workday V2 Xero Zendesk V2 Zuora AQuA
---	--

*クラウドインスタンスにデプロイされた場合にのみ適用されます。

REST API を使用したイメージのダウンロード

REST API を使用して Informatica のイメージリポジトリからイメージをダウンロードし、コンプライアンスの要件に応じて脆弱性をスキャンできるようにします。

イメージをダウンロードするには、組織に「エラスティックランタイム環境 - トークンの管理」特権が必要です。機能特権の詳細については、「[ユーザー管理](#)」を参照してください。Docker コマンドを実行するには、マシンに Docker をインストールします。

1. プラットフォーム REST API バージョン 3 containerimagetoken リソースを使用して、イメージリポジトリのトークンを取得します。

トークンを作成するか、組織の既存のトークンを使用することができます。詳細については、「[Getting a new token](#)」または「[Getting all tokens for an organization](#)」を参照してください。

2. プラットフォーム REST API バージョン 3 ais リソースを使用して、エラスティックランタイム環境のイメージ情報を取得します。

詳細については、[Getting runtime environment image information](#) を参照してください。

3. イメージのスキャンに使用するマシンで、次の Docker コマンドを実行してイメージリポジトリに接続します。

```
docker login infacloud-k8s-agent-docker-dev.jfrog.io --username <Informatica organization ID> --password <token value>
```

4. Docker コマンドを実行してイメージをダウンロードします。

例えば、バージョン 64.1 をダウンロードするには次のコマンドを使用します。

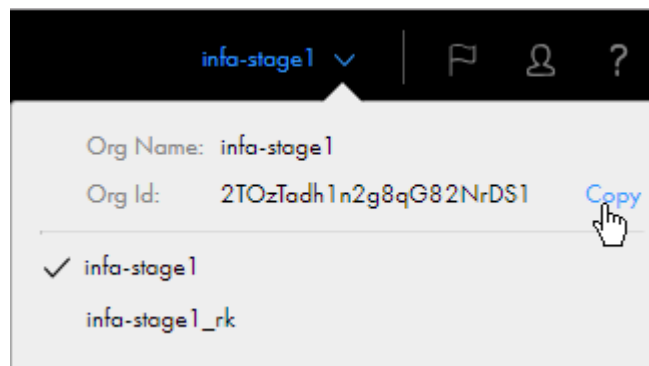
```
docker pull infacloud-k8sagent-docker-dev-jfrog.io/Data Integration:64.1
```

トラブルシューティング

対処方法に従って、エラスティックランタイム環境のエラーをトラブルシューティングします。

エラスティックランタイム環境についてさらにサポートが必要な場合は、Informatica グローバルカスタマサポートにお問い合わせください。サポートを受けるには、組織 ID の提供が必要になる場合があります。組織 ID は【組織】メニューから確認できます。

次の図は、【組織】メニューを示しています。



組織 ID は、管理者の【組織】ページで検索することもできます。

一般的な検証エラーのトラブルシューティング

次の表に、エラスティックランタイム環境の一般的な検証エラーを示します。

メッセージ	対処
変数<<NAME>>が定義されていません	欠落している変数が、config.txt ファイルに適切な値で定義されていることを確認してください。
<<COUNT>>個の変数が config.txt で定義されていません	すべての変数が config.txt ファイルに定義されていることを確認してください。
高可用性（HA）モードがオンのときに、<<COUNT>>個の変数が config.txt に定義されていません	高可用性に関連するすべての変数が config.txt ファイルに定義されていることを確認してください。
<<VPC_NAME>>を取得できませんでした	VPC_NAME が有効であることを確認してください。クラスターインストーラに対する AWS ロールと権限がマスターノードに割り当てられていることを確認してください。
IDMC AMI ID を取得できませんでした	マスターノードに割り当てられている AWS ロールと権限を確認してください。
サブネット<<NAME>>を取得できませんでした	マスターノードに割り当てられている AWS ロールと権限を確認してください。
AMI ID <<AMI_ID>>のルートボリューム名を取得できませんでした	マスターノードに割り当てられている AWS ロールと権限を確認してください。
インスタンス<<NAME>>が存在するかどうか確認できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス記述権限があることを確認してください。
認証に失敗しました。config.txt を確認してください	config.txt ファイル内のユーザー名とパスワードが正しいことを確認してください。
インスタンス<<INSTANCE_ID>>のサブネットを取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス記述権限があることを確認してください。
マスターノードでスクリプトが実行されていない場合は、VPC_NAME を定義する必要があります	config.txt ファイルに VPC_NAME と IS_RUNNING_ON_MASTER の値があることを確認してください。
MASTER_INSTANCE_TYPE が定義されていません	Administrator の 【環境設定】 タブでマスターインスタンスタイプが定義されていることを確認してください。
リージョン<<NAME>>のインスタンスタイプ<<TYPE>>が無効です	Administrator の 【環境設定】 タブでリージョンとインスタンスタイプが定義されていることを確認してください。
HA_MODE の値<<VALUE>>が無効です。true または false にする必要があります	REST API を使用している場合は、heEnabled フィールドに Boolean 値が含まれていることを確認してください。
<<values>>である場合、HA 以外のモードではサブネットを 1 つだけ指定する必要があります	高可用性が有効になっていない場合、指定できるサブネットは 1 つだけです。Administrator の 【環境設定】 タブでサブネット名を確認してください。

メッセージ	対処
<<values>>である場合、HA モードではサブネットを 3 つ指定する必要があります	高可用性が有効になっている場合は、サブネットを 3 つ指定する必要があります。Administrator の【環境設定】タブでサブネット名を確認してください。
サブネット<<NAME>>が存在しません	Administrator の【環境設定】タブに表示されているサブネット名が正しいことを確認してください。
指定されたサブネットは<<COUNT>>個の可用性ゾーンにのみマッピングされます	Administrator の【環境設定】タブに表示されているサブネット名と、マスターノードのサブネットが同じでないことを確認してください。

プロキシエラーのトラブルシューティング

次の表に、エラスティックランタイム環境のプロキシエラーを示します。

メッセージ	対処
プロキシ接続に失敗しました	指定したプロキシ接続の詳細を使用して www.informatica.com に到達できることを確認してください。
プロキシポート[<<PORT>>]が無効です	プロキシポート番号を確認してください。ポート値は、1 から 65535 まで（両端を含む）の数値である必要があります。
<<file>>が存在しません	<<FILE>>が次のいずれかの値であることを確認してください。 <ul style="list-style-type: none"> - agent_token.dat - agent_nwid.dat - agent_key.dat - infaagent.ini - agentcore.cfg - proxy.ini
プロキシ設定が無効です。	このメッセージの前に表示されたエラーを確認して修正してください。
エージェントトークンを生成できませんでした	ProxyUtil バイナリで proxy.ini ファイルを生成できませんでした。Informatica グローバルカスタマサポートにお問い合わせください。
プロキシのパスワードが指定されていません	プロキシのパスワードが入力されていませんでした。 プロキシモードが有効になっている場合は、インストーラがキーボード入力からパスワードを読み取る必要があるため、インストーラをバックグラウンドモードで実行しないでください。
プロキシ設定をセットアップできませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
containerd のプロキシを設定できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
proxy.ini のシークレットを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
containerd をセットアップできませんでした。プロキシパスワードが指定されていません。	このメッセージの前に表示されたエラーを確認して修正してください。

AWS エラーのトラブルシューティング

次の表に、エラスティックランタイム環境の AWS Secrets Manager エラーを示します。

メッセージ	対処
AWS Secrets Manager で<<NAME>>というシークレットを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS シークレット作成特権が割り当てられていることを確認してください。
AWS Secrets Manager で<<NAME>>というシークレットを更新できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS シークレット更新特権が割り当てられていることを確認してください。
シークレット<<NAME>>の値を読み取れませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS シークレット読み取り特権が割り当てられていることを確認してください。

次の表に、エラスティックランタイム環境の AWS セキュリティグループエラーを示します。

メッセージ	対処
ポート<<PORT_NUMBER>>に対するセキュリティグループ \$SECURITY_GROUP_NAME のイングレスルールを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS セキュリティグループルール作成特権が割り当てられていることを確認してください。
セキュリティグループ<<NAME>>を取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS セキュリティグループルール読み取り特権が割り当てられていることを確認してください。
セキュリティグループ<NAME>>を作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS セキュリティグループ作成特権が割り当てられていることを確認してください。
SSH のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
DNS のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
BGP のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
Kube API サービスのセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
NFS/EFS のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
etcd のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
VXLAN のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。

メッセージ	対処
Kubelet API のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
Kube Proxy のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
Kube-scheduler のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
Kube-controller-manager のセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
ノードポートのセキュリティグループルールを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。

マスターノードと作業ノードのエラーのトラブルシューティング

次の表に、エラスティックランタイム環境のマスターノードの作成に関連するエラーメッセージを示します。

メッセージ	対処
<<NAME>> ノードを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS RunInstances 権限があることを確認してください。
<<NAME>> インスタンスを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS RunInstances 権限があることを確認してください。
<<COUNT>> 回再試行してもノードの準備ができていませんでした	AWS マネジメントコンソールでマスターノードのステータスと起動ログを確認してください。
<<NAME>> のインスタンス ID を取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS DescribeInstances 権限があることを確認してください。

次の表に、高可用性が有効になっている場合のマスターノードの Elastic Load Balancing に関連するエラーメッセージを示します。

メッセージ	対処
ロードバランサ<<NAME>>を作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS ELB 作成権限があることを確認してください。
ELB からすべてのインスタンスの登録を解除できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス登録解除権限があることを確認してください。
ELB DNS を取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS ELB 記述権限があることを確認してください。

メッセージ	対処
マスターインスタンス<<INSTANCE_ID>>を<ELB_NAME>>に追加できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス登録権限があることを確認してください。
最初のマスターインスタンス<<INSTANCE_ID>> <<IP>>を<ELB_NAME>>に追加できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス登録権限があることを確認してください。
インスタンス<<INSTANCE_ID>>をロードバランサ<<NAME>>に登録できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS インスタンス登録権限があることを確認してください。
ロードバランサ<<NAME>>のインスタンスのヘルスを取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS ELB 記述権限があることを確認してください。
ロードバランサ<<NAME>>の詳細を取得できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS ELB 記述権限があることを確認してください。

次の表に、エラスティックランタイム環境の作業ノードの起動テンプレートと Auto Scaling グループに関連するエラーメッセージを示します。

メッセージ	対処
起動テンプレート<<NAME>>を作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS 起動テンプレート作成権限があることを確認してください。
ASG <<NAME>>を作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS Auto Scaling グループ作成権限があることを確認してください。
<<COUNT>>回試行しても ASG を作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに AWS Auto Scaling グループ作成権限があることを確認してください。

ALMS デプロイエラーのトラブルシューティング

次の表に、エラスティックランタイム環境の ALMS デプロイエラーを示します。

メッセージ	対処
ALMS マニフェストを生成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
RTE <<ID>>のサービスを取得できませんでした。応答コード: <<CODE>>	エラスティックランタイム環境で Secure Agent サービスが有効になっていることを確認してください。
この RTE <<ID>>には ALMS が設定されていません	エラスティックランタイム環境で Secure Agent サービスが有効になっており、イメージがリポジトリで使用可能であることを確認してください。
この RTE <<ID>>の ALMS イメージバージョンが見つかりません	このメッセージの前に表示されたエラーを確認して修正してください。

メッセージ	対処
実行する ALMS バージョンを取得できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
クラスタオートスケーラのマニフェストを作成できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。

EFS エラーのトラブルシューティング

次の表に、エラスティックランタイム環境の EFS エラーを示します。

メッセージ	対処
EFS のマニフェストを生成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに適切な AWS EFS 権限があることを確認してください。
EFS マウントターゲットを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに適切な AWS EFS 権限があることを確認してください。
クラスタ設定で指定した EFS ID \$systemDiskId が無効です	マスターノードにアタッチされているインスタンスプロファイルに適切な AWS EFS 権限があることを確認してください。
サブネット<<ID>>、セキュリティグループ = <<ID>>で EFS <<ID>>のマウントターゲットを作成できませんでした	マスターノードにアタッチされているインスタンスプロファイルに適切な AWS EFS 権限があることを確認してください。

その他のエラーのトラブルシューティング

次の表に、エラスティックランタイム環境に関連する一般的なエラーメッセージを示します。

メッセージ	対処
内部エラー: 使用方法: <<NAME>> masterIP isRunningOnMaster コマンド	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
内部エラー: 使用方法: <NAME>> masterIP isRunningOnMaster fileName	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 ELB_NAME instance_id_1 ... instance_id_n	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 instance_id AMI_NAME	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 \"asg_info_1 ... asg_info_n\" node_idle_timeout [toleration]	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 ELB_NAME	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。

メッセージ	対処
使用方法: \$0 proxyHost proxyPort proxyUser	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 ec2_instance_type_1 ... ec2_instance_type_n	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
使用方法: \$0 PROXY_HOST PROXY_PORT PROXY_USER	サービスエラー。Informatica グローバルカスタマサポートにお問い合わせください。
ファイル<<NAME>>を<<IP>>にコピーできませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
<<COUNT>>回再試行した後に試行を中止しました	このメッセージの前に表示されたエラーを確認して修正してください。
ワーカー情報を取得できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
クラスタコンポーネントをデプロイできませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
タグを処理できませんでした	Administrator の 【環境設定】 タブの詳細プロパティでタグを確認してください。
RTE <<ID>>のクラスタ設定 dateDeployed フィールドを更新できませんでした。応答コード: <<CODE>>	このメッセージの前に表示されたエラーを確認して修正してください。
clusterConfig dateDeployed フィールドを更新できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
RTE <<ID>>のクラスタ ID を取得できませんでした。応答コード: <<CODE>>	このメッセージの前に表示されたエラーを確認して修正してください。
RTE <<ID>>のクラスタ設定を取得できませんでした。応答コード: <<CODE>>	このメッセージの前に表示されたエラーを確認して修正してください。
クラスタ設定を取得できませんでした	このメッセージの前に表示されたエラーを確認して修正してください。
リージョン<<NAME>>の CspRegionInstanceInfo を取得できませんでした。応答コード: <<NAME>>	このメッセージの前に表示されたエラーを確認して修正してください。
リポジトリ <<NAME>>からトークンを取得できませんでした	リポジトリトークンがクォータである 20 個を超えていないことを確認してください。

メッセージ	対処
Failed to execute `kubectl get namespace grep -q idmc-system` E0715 22:33:37.559917 memcache.go:265] "未処理のエラー" err="現在のサーバー API グループリストを取得できませんでした: Get \"http://localhost:8080/api?timeout=32s\": dial tcp [::1]:8080: connect: connection refused" サーバー localhost:8080 への接続が拒否されました - 適切なホストまたはポートを指定しましたか?	インストール中にエラーが発生しました。このエラーメッセージは無視してください。
EC2 インスタンスを削除した後のインスタンス数が一致しません	EC2 インスタンスが AWS から削除された後も、Informatica Intelligent Cloud Services では引き続きステータスが【稼働中】になっている可能性があるため、報告されたインスタンス数に不一致があります。

IAM ポリシーリファレンス

ポリシーリファレンスでは、クラスティンストーラとワーカーポリシーの文について説明しているため、AWS 環境でクラスティンストーラとワーカーロールが持つアクセスレベルを把握できます。

クラスティンストーラポリシー文

クラスティンストーラポリシーの文の説明を使用して、AWS 環境でクラスティンストーラが持つアクセスレベルを把握します。クラスティンストーラポリシーには、クラスティンストーラがエラスティックランタイム環境をデプロイするために必要とする権限が含まれています。

Auto Scaling

次の文は、ロールが自動スケーリンググループを管理できるようにします。

```
{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:DeleteAutoScalingGroup",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeTags",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:DeleteTags",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLifecycleHooks",
    "autoscaling:ResumeProcesses",
    "autoscaling:SetDesiredCapacity",
    "autoscaling:SuspendProcesses"
  ],
  "Resource": "*"
},
```


EC2 リソースの記述とセキュリティグループの管理

次の文は、ロールが EC2 リソースの属性を記述および更新し、セキュリティグループの Ingress を承認できるようにします。

```
{
  "Sid": "VisualEditor1",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeTags",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DeleteLaunchTemplate",
    "ec2:ModifyInstanceAttribute",
    "ec2:DescribeVpcs"
  ],
  "Resource": "*"
},
```

EC2 インスタンスの実行

次の文は、ロールが EC2 インスタンスを実行できるようにします。

```
{
  "Sid": "VisualEditor2",
  "Effect": "Allow",
  "Action": "ec2:RunInstances",
  "Resource": "*"
},
```

キー、タグ、および起動テンプレートの作成

次の文は、ロールがキー、タグ、および起動テンプレートを作成できるようにします。

```
{
  "Sid": "VisualEditor3",
  "Effect": "Allow",
  "Action": [
    "ec2:CreateKeyPair",
    "ec2:CreateTags",
    "ec2:CreateLaunchTemplate"
  ],
  "Resource": [
    "arn:aws:ec2:*:<AWS account ID>:security-group/*",
    "arn:aws:ec2:*:<AWS account ID>:network-interface/*",
    "arn:aws:ec2:*:<AWS account ID>:launch-template/*",
    "arn:aws:ec2:*:<AWS account ID>:instance/*",
    "arn:aws:ec2:*:<AWS account ID>:subnet/*",
    "arn:aws:ec2:*:<AWS account ID>:volume/*",
    "arn:aws:ec2:*:<AWS account ID>:image/*",
    "arn:aws:ec2:*:<AWS account ID>:key-pair/*"
  ]
},
```

EC2 リソースのタグ付け

次の文は、EC2 リソースにタグを作成するための条件付き権限を提供します。

```
{
  "Sid": "VisualEditor5",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": [
    "arn:aws:ec2:*:<AWS account ID>:network-interface/*",

```

```

        "arn:aws:ec2:*:<AWS account ID>:key-pair/*",
        "arn:aws:ec2:*:<AWS account ID>:launch-template/*",
        "arn:aws:ec2:*:<AWS account ID>:instance/*",
        "arn:aws:ec2:*:<AWS account ID>:volume/*",
        "arn:aws:ec2:*:<AWS account ID>:subnet/*",
    ],
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": [
                "RunInstances",
                "CreateKeyPair",
                "CreateLaunchTemplate",
                "CreateLaunchTemplateVersion",
                "network-interface",
                "CreateTags",
                "CreateAutoScalingGroup"
            ]
        }
    }
},

```

AWS サービスへのロール情報の受け渡し

次の文は、クラスティンストーラが AWS サービスにロールの詳細を渡して、権限を引き受けることができるようにします。

```

{
    "Sid": "VisualEditor13",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::<AWS account ID>:role/<cluster installer role>",
        "arn:aws:iam::<AWS account ID>:role/<worker role>"
    ]
},

```

AWS Secrets Manager

次の文は、ロールが AWS Secrets Manager でシークレットを管理できるようにします。

```

{
    "Sid": "VisualEditor21",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource",
        "secretsmanager>DeleteSecret",
        "secretsmanager:UpdateSecret"
    ],
    "Resource": "arn:aws:secretsmanager:*:<AWS account ID>:secret:*"
},

```

EFS ファイルシステムの管理

次の文は、ロールが EFS ファイルシステムを管理できるようにします。

```

{
    "Sid": "VisualEditor10",
    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource": "*"
},

```

サブネットの記述

次の文は、サブネットを記述するための読み取り専用アクセスを提供します。

```
{
  "Sid": "VisualEditor11",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSubnets"
  ],
  "Resource": "*"
},
```

EC2 管理

次の文は、EC2 管理権限を提供します。

```
{
  "Sid": "EC2Management",
  "Effect": "Allow",
  "Action": [
    "ec2:AssociateIamInstanceProfile",
    "ec2:CreateKeyPair",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
    "ec2:CreateTags",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteTags",
    "ec2:ModifyLaunchTemplate",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "iam:PassRole"
  ],
  "Resource": "*"
}
```

ワーカーポリシー文

ワーカーポリシーの文の説明を使用して、AWS 環境で作業ノードが持つアクセスレベルを把握します。ワーカーポリシーには、作業ノードがエラスティックランタイム環境でデータを処理するために必要とする権限が含まれています。

リソースの説明

次の文は、読み取り専用のリソースの説明を提供します。

```
{
  "Sid": "DescribeActions",
  "Effect": "Allow",
  "Action": [
    "elasticfilesystem:DescribeMountTargets",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeTags",
    "autoscaling:DescribeLifecycleHooks",
    "autoscaling:DescribeScalingActivities",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeVpcs",
    "secretsmanager:DescribeSecret",
    "secretsmanager:ListSecrets"
  ],
  "Resource": "*"
},
```

Auto Scaling

次の文は、ロールが自動スケーリンググループを管理できるようにします。

```
{
  "Sid": "AutoscalingCapacity",
  "Effect": "Allow",
  "Action": [
    "autoscaling:SetDesiredCapacity",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:DeleteAutoScalingGroup",
    "autoscaling:DeleteTags",
    "autoscaling:SuspendProcesses",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource": "*"
},
```

Amazon EC2

次の文は、ロールが EC2 のリソースを管理できるようにします。

```
{
  "Sid": "EC2Management",
  "Effect": "Allow",
  "Action": [
    "ec2:AssociateIamInstanceProfile",
    "ec2:CreateKeyPair",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
    "ec2:CreateTags",
    "ec2:DeleteLaunchTemplate",
    "ec2:DeleteTags",
    "ec2:ModifyLaunchTemplate",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "iam:PassRole"
  ],
  "Resource": "*"
},
```

Amazon EFS

次の文は、ロールが EFS ファイルシステム上のアクセスポイントを作成および削除できるようにします。

```
{
  "Sid": "EFSManagement",
  "Effect": "Allow",
  "Action": [
    "elasticfilesystem:CreateAccessPoint",
    "elasticfilesystem:DeleteAccessPoint"
  ],
  "Resource": "*"
},
```

AWS Secrets Manager

次の文は、ロールが AWS Secrets Manager でシークレットにアクセスして更新できるようにします。

```
{
  "Sid": "SecretsManagerAccess",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
    "secretsmanager:UpdateSecret"
  ],
  "Resource": "*"
}
```

第 5 章

サーバーレスランタイム環境

サーバーレスランタイム環境は、Secure Agent 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す。

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。

- 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フェース (ENI) を作成してクラウド環境に接続します。
- Azure Virtual Network (VNet)

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。

[サーバーレス環境設定] ページにアクセスする必要があるユーザーには、少なくとも Secure Agent グループに対する読み取り権限が必要です。権限の設定の詳細については、[「Secure Agent グループの操作」 \(ページ 18\)](#)を参照してください。

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。

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、Amazon Virtual Private Cloud (VPC) でホストできます。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フェース (ENI) を作成してクラウド環境に接続します。

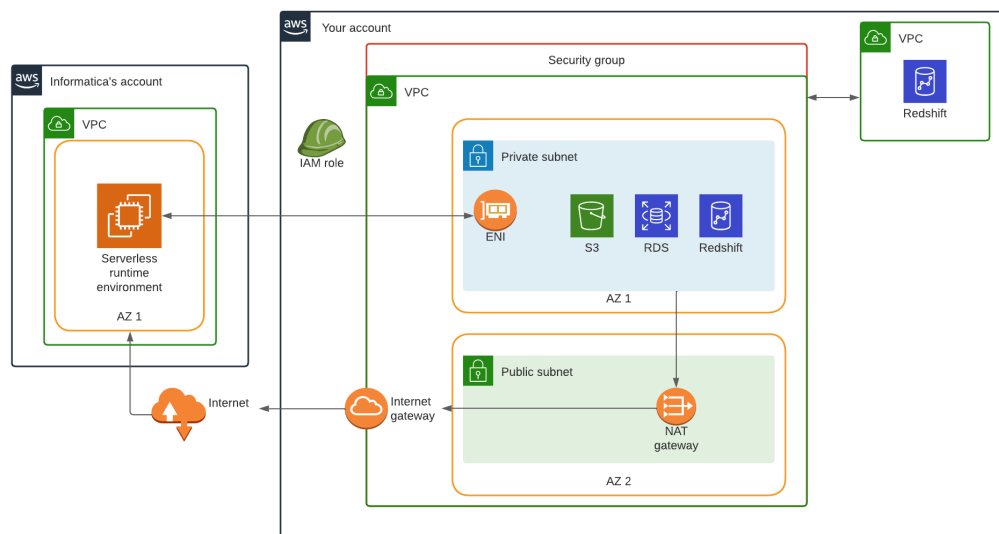
サーバーレスランタイム環境を作成する前に、Informatica の VPC のサーバーレスランタイム環境に接続するために、VPC で AWS リソースを作成および設定する必要があります。

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。

環境の設定

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が 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。

DMZ NAT ゲートウェイ（信頼できる IP アドレスのみ許可されている場合）

組織が、信頼できる IP アドレスのみを許可するように設定されている場合は、DMZ NAT ゲートウェイの IP アドレスを信頼できる IP アドレスのリストに追加する必要があります。詳細については、「[組織管理](#)」を参照してください。

次の表に、各 POD の DMZ NAT ゲートウェイ IP アドレスを示します。

POD	追加する NAT IP アドレス
NA West 1、NA East 2、US West 3、US East 4、 US West 5、US East 6	44.242.20.143 44.239.8.148 54.221.247.69 54.160.9.90 3.131.176.232 18.142.14.24 3.1.147.184 18.220.76.98 13.56.74.27 52.52.220.198
Canada Central 1	3.97.103.68 3.96.182.201
EM West 1 (アイルランド)	3.64.66.226 3.125.185.124 54.76.54.130 54.78.183.88 35.176.60.118 18.135.50.152 35.152.49.63 35.152.45.151 15.237.157.126 15.237.97.211 13.49.61.89 13.53.141.231
UK	34.250.251.16 18.170.170.192 13.37.37.71 18.157.124.91 13.53.147.238 15.161.184.93 15.160.41.209
AP Southeast 1 (オーストラリア)	54.253.179.190 3.24.111.61 35.72.149.44 13.112.143.134 3.34.56.248 52.79.244.47 52.76.184.230 18.140.193.120 65.1.80.5 13.234.141.216 18.163.244.73 18.167.71.151
AP Northeast 2 (日本)	18.181.99.0 13.208.101.21

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",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions"
      ],
      "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>"
    }
  }
}
]
}

```

VPC 設定タスク

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 アドレスを追加し、システムディスクを設定し、JAR ファイルと外部ライブラリの場所を設定し、REST API を認証するように TLS を設定できます。

必要に応じて、次の VPC 設定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プロパティの詳細については、[「システムディスクのプロパティの設定」 \(ページ 78\)](#)を参照してください。
- 既存の EFS または NFS ディレクトリをサーバーレスランタイム環境でデータディスクとして使用する場合は追加の設定。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。
- 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、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。詳細については、[「データディスクの設定」 \(ページ 71\)](#)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、AWS のマニュアル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、[「データディスクのプロパティの設定」 \(ページ 79\)](#)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。

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

2. serverlessUserAgentConfig.yml ファイルを作成します。テンプレートについては、[「serverlessUserAgentConfig.yml ファイルへの入力」 \(ページ 93\)](#)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"> - serverlessUserAgentConfig.yml - JDBC V2 コネクタ JAR ファイル - REST V3 コネクタのトラストストア証明書とキーストア証明書 - Java トランスフォーメーション用の JAR ファイル - Python トランスフォーメーション用のインストールファイルとリソースファイル <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。

1. Amazon S3 の補足ファイルの場所に移動します。
2. serverless_agent_config フォルダに、SSL というサブフォルダを作成します。
3. SSL フォルダにトラストストア証明書とキーストア証明書を追加します。
一方向の安全な通信を行うには、トラストストア証明書を追加します。双方向の安全な通信を行うには、トラストストア証明書とキーストア証明書の両方を追加します。
4. 次のコードスニペットをテキストエディタにコピーし、補足ファイルの場所にある各証明書への相対パスを追加します。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<REST V3 truststore certificate name>.jks
        - fileCopy:
            sourcePath: SSL/<REST V3 keystore certificate name>.jks
```
5. serverless_agent_config フォルダで、serverlessUserAgentConfig.yml ファイルを開きます。
6. コードスニペットを serverlessUserAgentConfig.yml ファイルに追加し、ファイルを保存します。
サーバーレスランタイム環境は、実行時に証明書を使用できるように、証明書を補足ファイルの場所から固有の参照ディレクトリにコピーします。
7. REST V3 接続プロパティで、/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<証明書名>.jks という形式を使用して、サーバーレスランタイム環境の各トラストストアファイルパスおよびキーストアファイルパスを指定します。

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

serverlessUserAgentConfig.yml ファイルの設定

serverlessUserAgentConfig.yml ファイルは、設定プロセスの後半で補足ファイルの場所を作成するときに必要です。

詳細な手順については、[「serverlessUserAgentConfig.yml ファイルの設定方法」](#) (ページ 93)を参照してください。

サーバーレスランタイム環境でのプロキシサーバー

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できます。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。

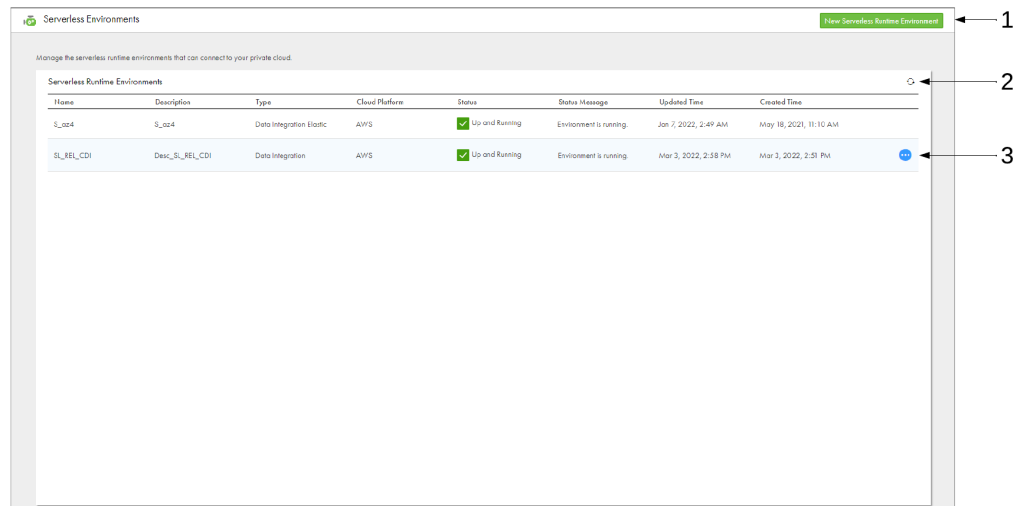
```
s3.<region>.amazonaws.com
s3.amazonaws.com
ec2.<region>.amazonaws.com
sts.<region>.amazonaws.com
efs.<region>.amazonaws.com
elasticfilesystem.<region>.amazonaws.com
```

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。

Administrator のサーバーレスランタイム環境

AWS で環境を作成した後に、Administrator の【サーバーレス環境】 ページで対応する環境を作成します。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します。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。

基本設定のプロパティの設定

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。 <ul style="list-style-type: none">- 詳細モード外のマッピングを実行するには、【データ統合】を選択します。- 詳細モードでマッピングを実行するには、【詳細データ統合】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。

プロパティ	説明
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のプロパティの設定

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。
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。

プロパティ	説明
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の設定

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。このセクションを使用して、デフォルトディレクトリの変数を設定し、同時に実行できるタスクの数を減らします。

注: システム管理者または Informatica グローバルカスタマサポートの指示がない限り、他の変数やプロパティは変更しないでください。

デフォルトディレクトリの変数の設定

サーバーレスランタイム環境によって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されるシステム変数を設定できます。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、システム変数をより簡単に見つけることができます。

以下の表に、システム変数を示します。

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

システム変数名	説明
\$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用します。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

同時タスクの数の削減

デフォルトでは、サーバーレスランタイム環境は 150 個のタスクを同時に実行できます。タスクの数を減らすには、「Service = Data_Integration_Server」と「Type = Tomcat」の maxDTMProcesses プロパティを使用します。1～150 文字の値を使用することができます。

システムディスクのプロパティの設定

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。
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。

データディスクのプロパティの設定

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、「[環境の設定](#)」 (ページ 62) 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

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

サーバーレスランタイム環境の編集

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。
- **失敗しました。** 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】** アクション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。

サーバーレスランタイム環境の再デプロイ

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。
- サーバーレスランタイム環境が失敗状態です。

サーバーレスランタイム環境を再デプロイする前に、Monitor を使用して、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。

環境を再デプロイするには、次の手順を実行します。

- Administrator で、サーバーレスランタイム環境の **【アクション】** メニューから **【再デプロイ】** を選択します。

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。

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。

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の使用

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の設定

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のセットアップ (Microsoft Azure)

サーバーレスランタイム環境は、Azure Virtual Network (VNet) でホストできます。サーバーレスランタイム環境は、Azure Native ISV Service で設定します。

サーバーレスランタイム環境を作成するには、Intelligent Data Management Cloud サブスクリプションライセンスが必要です。

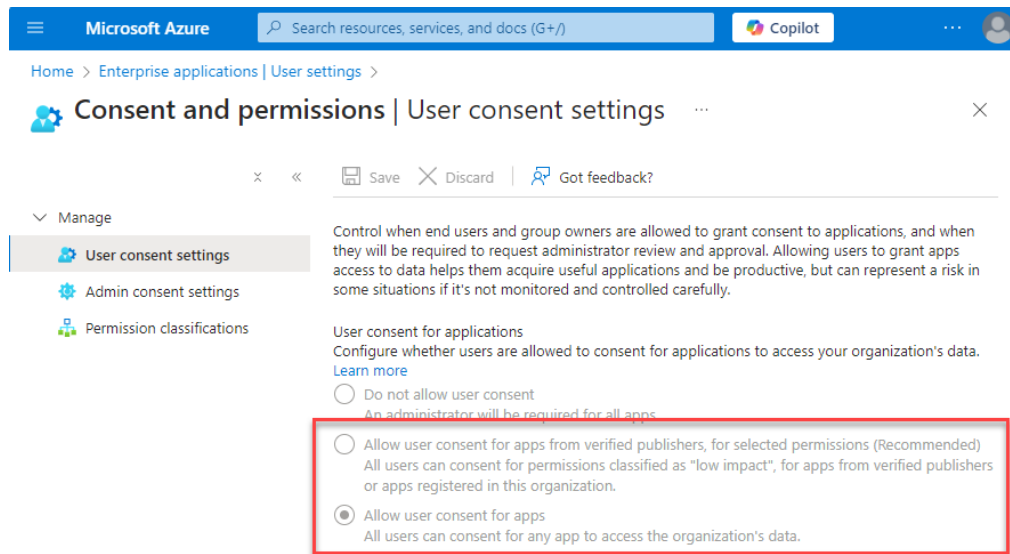
Azure でサーバーレスランタイム環境を設定するには、次の手順を実行します。

1. ユーザーの同意設定を確認します。
2. サブネットを設定します。
3. Azure Native ISV Service で組織を作成します。
4. サーバーレスランタイム環境を作成します。

手順 1.ユーザーの同意設定の確認

ユーザーの同意設定によっては、Azure 管理者が Informatica アプリケーションを承認することが必要になる場合があります。

1. Azure portal のホームページで、**[エンタープライズアプリケーション]** を選択します。
2. **[セキュリティ]** を展開して、**[同意とアクセス許可]** をクリックします。
[ユーザーの同意設定] ページが表示されます。



3. 自分に割り当てられたユーザーの同意設定を確認します。

- [ユーザーの同意設定] ページが **【確認済みの発行元からのアプリに対して選択されたアクセス許可を与えることへのユーザーの同意を許可する】** に設定されている場合、サーバーレスランタイム環境を作成する前に、Azure 管理者に Informatica アプリケーションの承認を依頼する必要があります。アプリケーションの承認の詳細については、Microsoft のドキュメントの [Review admin consent requests](#) を参照してください。
- 同意設定で **【アプリに対するユーザーの同意を許可する】** が表示されている場合、Azure 管理者からの承認は必要ありません。サーバーレスランタイム環境の作成に進むことができます。

手順 2. サブネットの設定

Azure サーバーレスランタイム環境で使用する特定のサブネットを割り当てます。

サブネットがインターネットに接続されていることを確認します。この接続を構築する場合は、パブリック IP アドレスを使用して NAT ゲートウェイを設定するなど、複数の方法があります。

委任サブネットでサービスエンドポイント Microsoft.AzureActiveDirectory が有効になっていることを確認します。パブリック IP アドレスを使用して NAT ゲートウェイを設定した場合、この操作は必須ではありません。

使用可能な IP アドレスが十分にある場合、同じサブネット上のサーバーレスランタイム環境の数の制限はありません。

次の表に、サブネットの委任を介してリンクされた VNET/サブネットのリージョンを示します。

POD	サブネットの委任を介してリンクされた VNET/サブネットのリージョン
US West 1 Azure (USW1-1)	米国(西部) 米国(東部) 米国 (東部) 2 米国 (中央南部) 米国(中部)

POD	サブネットの委任を介してリンクされた VNET/サブネットのリージョン
US West 3 Azure (USW3-1)	米国(西部) 米国 (東部) 2 米国 (中央南部) 米国(中部)
Canada Central 1 Azure (CAC2)	カナダ(中部) カナダ(東部)
EM Central 1 Azure (EMC1)	ヨーロッパ(西部) ドイツ(中西部) ヨーロッパ(北部)
EM SouthEast 1 Azure (EMSE1)	(中東) UAE North
AP East 2 Azure (APSE2)	(アジア太平洋) 東南アジア
オーストラリア Azure (APAUC1)	オーストラリア(中部) オーストラリア(南東部) オーストラリア(東部)

1. Azure Cloud Shell を使用して、次のコマンドを実行します。

```
az provider register --namespace 'Informatica.DataManagement'
```

このコマンドにより、サブネットが配置されているサブスクリプションに「Informatica.DataManagement」リソースプロバイダが登録されます。
2. 新しいサブネットを作成し、このサブネットを次のサービスに委任します: Informatica.DataManagement/organizations。
注: サブネットのサービス Informatica.DataManagement/organizations への委任は、サブネット関連の設定がすべて完了した後に行う必要があります。そうしないと、サブネットの設定中に問題が発生する可能性があります。

手順 3。serverlessUserAgentConfig.yml ファイルの設定

serverlessUserAgentConfig.yml ファイルは、設定プロセスの後半で補足ファイルの場所を作成するときに必要です。

詳細な手順については、[「serverlessUserAgentConfig.yml ファイルの設定方法」 \(ページ 93\)](#)を参照してください。

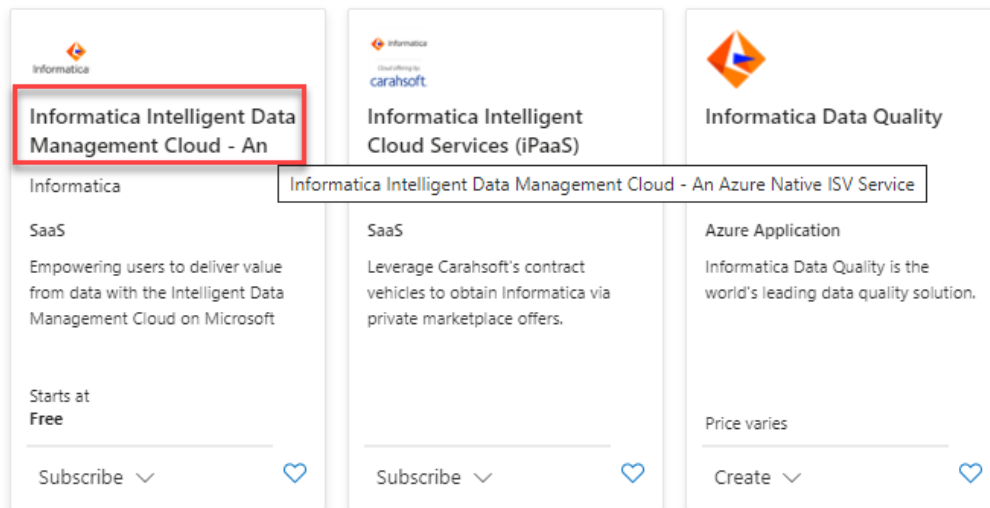
手順 4。Informatica 組織の作成

Informatica シングルサインオンアプリに登録し、サブネットを設定した後に、新しい組織を作成するか、既存の組織にリンクさせます。

1. Azure ポータルのホームページで、**[Marketplace]** を選択します。
2. **[Informatica]** を検索します。
名前に「Informatica」が含まれる複数のプランが表示される場合があります。

3. **[Informatica Intelligent Data Management Cloud - Azure Native ISV Service]** という名前のプランを選択します。

タイトルビューまたはリストビューの場合、名前は切り詰められます。正しいプランを選択したことを確認するには、名前にカーソルを合わせます。次の図は、正しいプランを示しています。



4. 契約書に指定されているプランを選択し、**[サブスクリプション] > [はい、続行します]** をクリックします。
[Informatica 組織の作成] ページが表示されます。
5. **[基本]** タブに次の情報を入力します。

フィールド	値
サブスクリプション	Informatica 組織の作成に使用する Azure サブスクリプションを選択します。 このサブスクリプションの所有者またはコントリビュータのロールが割り当てられている必要があります。
リソースグループ	リソースグループを選択するか、新しいリソースグループを作成します。このリソースグループに対するコントリビュータロールが割り当てられている必要があります。 リソースグループは Azure ソリューションの関連リソースを保持するコンテナです。
リソース名	Azure リソースの名前を入力します。
リージョン	「Informatica 組織」タイプのリソースがプロビジョニングされる地域を選択します。
Informatica 地域	最も近い地域を選択します。これにより、接続先の POD が決定されます。

フィールド	値
組織	新しい組織を作成するか、既存の組織にリンクするかを選択します。 既存の組織にリンクする場合は、既存の Informatica の請求を続行するか、Azure Marketplace の請求を使用するかを選択することができます。 注: リンクできるのは、プロダクションまたはサンドボックスライセンスタイプを持つ親組織のみです。サブ組織に対して、またはライセンスタイプが試用版の場合にリンクさせることはできません。詳細については、「 組織管理 」を参照してください。
組織名	既存の組織にリンクしている場合は、 【既存の Informatica 組織にリンク】 をクリックし、ログイン資格情報を入力します。Azure ポータルで作成された Informatica 組織が、既存の組織に自動的にリンクされます。
プラン	前の手順で選択したプランが表示されます。変更する場合は、 【プランの変更】 をクリックします。

6. 必要に応じて、**【次へ: タグ】** をクリックして、Azure リソースを分類する場合に役立つタグを作成します。



次にタグの例を示します。

- 名前: <管理者の名前>、値: <電子メールアドレス>
- 名前: <ビジネスユニット>、値: <ユーザーのビジネスユニット>

Basics **Tags** Review + create

Tags are name/value pairs that enable you to categorize Azure resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn More](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ①	Value ①	Resource
admin	: mfox@informatica.com	Informatica 
business unit	: Analytics	Informatica 
<input type="text"/>	: <input type="text"/>	Informatica

Review + create < Previous Next: Review + create >

7. **【次へ: レビュー+作成】** をクリックします。

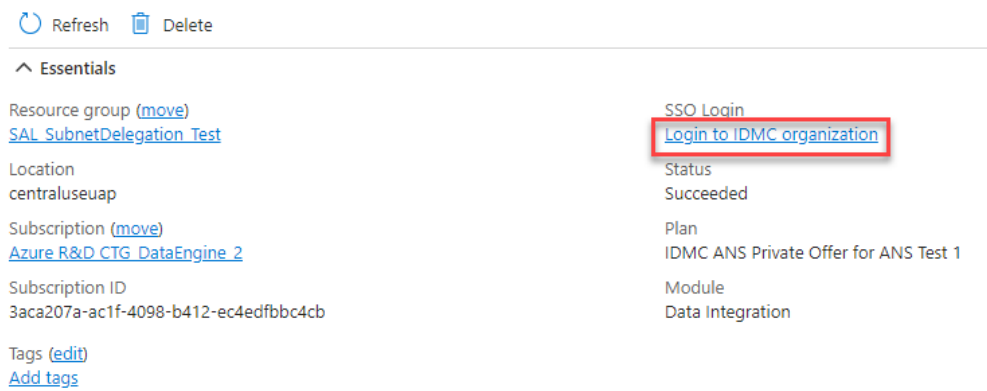
情報が正しいことを確認し、ページの上部に **【検証に合格しました】** と表示されていることを確認します。サービスの作成時に、このプロセスが次の表の情報に従って Active Directory のプロパティを検証します。

フィールド	検証
名	名には、文字、ハイフン、および単一引用符 (') のみを含めることができます。

フィールド	検証
姓	姓には、文字、ハイフン、および単一引用符 (') のみを含めることができます。
会社名	会社名は 255 文字以下である必要があります。
国	会社名は 255 文字以下である必要があります。
電子メール	電子メールは有効な電子メール形式である必要があります。
電話番号	電話番号は 10 - 25 文字にする必要があります。電話番号は、プラス記号で始まり、使用できるのは数字、スペース、丸括弧、ハイフン、ピリオドのみです。

いずれかのフィールドが検証に失敗した場合、サービスの作成は失敗します。

8. デプロイメントプロセスを開始するには、**【作成】** をクリックします。
デプロイメントが完了すると、**【デプロイメントが成功しました】** と表示されます。
9. 組織のリソースダッシュボードを表示するには、**【リソースに移動】** をクリックします。
10. リソースダッシュボードで **【IDMC 組織にログイン】** をクリックします。



注: サーバーレスランタイム環境を作成する前に、Informatica Intelligent Cloud Services にログインすることが重要です。

11. 個人情報が正しいことを確認し、サブスクリプション契約に同意することを確認します。
12. **【確認】** をクリックして、Informatica Intelligent Cloud Services にログインします。
この手順は、ユーザーをシステムに追加するために必要です。

手順 5。サーバーレスランタイム環境を作成

Azure Native ISV Service を使用する場合は、Informatica Intelligent Cloud Services ではなく、Azure ポータルでサーバーレスランタイム環境を作成および管理します。

注: システムディスクとプロキシサーバーの機能は、現在 Azure サーバーレスランタイム環境ではサポートされていません。

1. Azure ポータルの組織のリソースページで、**【サーバーレスランタイム環境】** をクリックします。
この時点では、サーバーレスのランタイム環境がないため、リストは空です。
2. **【新しいサーバーレス環境の作成】** をクリックします。
この設定は、**【基本】**、**【プラットフォームの詳細】**、**【ランタイム設定】**、および **【タグ】** という 4 つのタブに分かれています。

3. **【基本】** タブで、次の情報を入力します。

フィールド	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。 <ul style="list-style-type: none"> - 詳細モード以外のマッピングを実行するには、【データ統合およびデータ取り込み/レプリケーション】 を選択します。 - 詳細モードでマッピングを実行するには、【詳細データ統合】 を選択します。
タスクあたりの最大コンピュータユニット数	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。 このプロパティは、データ取り込みおよびレプリケーションには適用されません。
タスクのタイムアウト（分）	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。 このプロパティは、データ取り込みおよびレプリケーションには適用されません。

4. **【プラットフォームの詳細】** タブで、次の情報を入力します。

フィールド	説明
リージョン	サーバーレスランタイム環境がホストされているリージョンを選択します。
仮想ネットワーク	使用する仮想ネットワークを選択します。
サブネット	使用する仮想ネットワーク内のサブネットを選択します。 注: 「手順 2. サブネットの設定」 （ページ 83）が完了したことを確認します。

フィールド	説明
補足ファイルの場所	<p>ADLS Gen2 の補足ファイルの場所。次の形式を使用します。</p> <pre>abfs://<file_system>@<account_name>.dfs.core.windows.net/<path></pre> <p>例えば、JDBC 接続を使用するには、JDBC JAR ファイルを補足ファイルの場所に配置してから、次の場所を入力します。</p> <pre>abfs://discaleqa@serverlessadlsngen2acct.dfs.core.windows.net/serverless</pre> <p>Azure サーバーレスランタイム環境内でコマンドタスクを実行する場合は、補足ファイルの場所内に <code>command_scripts</code> という名前のフォルダを作成します。</p> <p>例えば、次の場所にフォルダを作成します。</p> <pre>abfs://discaleqa@serverlessadlsngen2acct.dfs.core.windows.net/serverless/command_scripts</pre> <p>コマンドタスクの詳細については、「タスクフロー」の「コマンドタスクステップ」を参照してください。</p> <p>注: 補足ファイルの場所に余分なスペースや特殊文字がないことを確認してください。これらの文字がある場合はデプロイメントが失敗する可能性があります。</p> <p>補足ファイルの場所を指定する場合は、マネージド ID を選択するか、カスタムプロパティでサービスプリンシパルの資格情報を指定して、サーバーレスランタイム環境にファイルの場所へのアクセス権を付与します。</p>
データディスク	<p>NFS ファイルシステム内のファイルにアクセスします。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、NFS ディレクトリ内のファイルにアクセスできます。データディスクの設定の詳細については、「データディスクの操作」(ページ 90)を参照してください。</p> <p>データディスクを設定するには、次のプロパティを設定します。</p> <ul style="list-style-type: none"> - タイプ。現在サポートされているのは NFS ディレクトリのみです。 - サーバーホスト/IP。NFS サーバーのホスト名または IP アドレス。 - 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。 - マウントオプション。マウントオプションが必要な場合は、次の形式のカンマ区切りリストで入力します: <key1>=<value1>, <key2>=<value2>
マネージド ID	<p>サーバーレスランタイム環境に補足ファイルの場所へのアクセス権を付与するユーザー割り当てマネージド ID。カスタムプロパティでサービスプリンシパルの資格情報を使用してアクセス権を付与しない場合は必須です。</p>
カスタムプロパティ	<p>サーバーレスランタイム環境の追加プロパティ。</p> <p>サービスプリンシパルの資格情報を使用して欲しくファイルの場所へのアクセス権を付与するには、次のカスタムプロパティとそれらの適切な値を追加します。</p> <ul style="list-style-type: none"> - <code>ServicePrincipalId</code> - <code>ServicePrincipalSecret</code>。設定が保存されるとシークレットはマスクされるため、正確に入力されていることを確認してください。 <p>マネージド ID を設定しない場合は、サービスプリンシパルの資格情報が必要です。マネージド ID およびサービスプリンシパルの資格情報を設定すると、サーバーレスランタイム環境はマネージド ID を使用してファイルの場所にアクセスします。</p> <p>Informatica グローバルカスタマサポートは、他のカスタムプロパティを追加するように指示する場合があります。</p> <p>Azure サーバーレスランタイム環境のクローンを作成する場合は、元の値がマスクされた文字列に置き換えられるため、<code>ServicePrincipalSecret</code> を再入力する必要があります。</p>

注: 設定を保存した後に、補足ファイルの場所、マネージド ID、またはカスタムプロパティを変更することはできません。修正が必要な場合は、設定のクローンを作成します。クローンの作成の詳細については、「[サーバーレスランタイム環境の管理](#)」(ページ 90)を参照してください。

5. **[ランタイム設定]** タブで、サーバーレスランタイム環境の動作を指定するためのプロパティを入力します。

このタブは、Informatica グローバルカスタマサポートの指示がない限り変更を加えないようにしてください

6. **【タグ】** ページで、Azure リソースを分類し、一括請求を表示する場合に役立つタグを作成します。
名前と値のペアとして必要な数のタグを入力します。
7. **【レビュー+作成】** ページで、すべてのエントリが正しいことを確認してから、**【作成】** をクリックします。
修正するために戻る必要がある場合は、**【前へ】** をクリックして、適切なタブに戻ります。
サーバーレスランタイム環境の使用と管理の詳細については、Informatica ドキュメントポータル
の「[Serverless Runtime Environments](#)」を参照してください。

データディスクの操作

サーバーレスランタイム環境で使用するファイルが NFS ディレクトリにあり、すべてのマッピングを更新する必要がない場合は、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。この機能は、NFS バージョン 4.x プロトコルでのみ機能します。

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 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 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。

Azure サーバーレスランタイム環境で既存の NFS ディレクトリをデータディスクとして使用する場合は、ID=501 のユーザーに、NFS ストレージのマウントディレクトリからの読み取りと書き込みの権限が付与されていることを確認します。ユーザー ID 501 は、Azure サーバーレスランタイム環境がマウントされた NFS ディレクトリにアクセスするために使用する cldagnt ユーザーです。

ユーザー 501 が存在しない場合は、そのユーザーを作成し、適切な権限を割り当てます。

注: NFS サーバーへのアクセスを妨げるネットワークファイアウォールがある場合は、Azure サーバーレスランタイム環境の作成に使用された、委任されたサブネットから NFS サーバーへのアクセスを許可する必要があります。

サーバーレスランタイム環境の管理

Azure でサーバーレスランタイム環境を作成した後に、サーバーレスランタイム環境の編集、削除、クローン作成などの管理タスクを実行できます。これらのタスクは、Azure ポータルを使用して実行します。

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。
- **失敗しました。**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、Azure ポータルで **【環境の開始】** アクションを使用するか、Administrator の **【ランタイム環境】** ページで **【再デプロイ】** アクション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は、Azure ポータルまたは Administrator の **［ランタイム環境］** ページから編集することができます。ただし、マネージド ID プロパティを編集できるのは Azure ポータルからのみです。

サーバーレスランタイム環境の再デプロイ

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。
- サーバーレスランタイム環境が失敗状態です。

サーバーレスランタイム環境を再デプロイする前に、Monitor を使用して、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。

環境を再デプロイするには、次の手順を実行します。

- Administrator で、サーバーレスランタイム環境の **［アクション］** メニューから **［再デプロイ］** を選択します。

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。

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、Azure ポータルを使用します。

サーバーレスランタイム環境の起動

失敗したために実行されていなかったサーバーレスランタイム環境を起動します。

サーバーレスランタイム環境を [「サーバーレスランタイム環境の編集」 \(ページ 90\)](#) した後に、Azure ポータルから環境を起動します。

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すばやく作成できます。例えば、クラウド環境内の別のサブネットに接続する同様のサーバーレスランタイム環境を作成することができます。

サーバーレスランタイム環境のクローンを作成するには、Azure ポータルを使用します。

ヒント: 作成されたクローンの環境がすぐに表示されない場合は、Azure ポータルの **［サーバーレスランタイム環境］** ページで **［更新］** をクリックします。

Azure の外部にあるデータベースまたはエンドポイントの VNet の設定

Oracle を使用しているか、オンプレミスまたは Azure エコシステムの外部でホストされているデータベースまたはエンドポイントを使用している場合は、VNet で追加の設定を行う必要があります。

以下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。
- 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、Gen2 または BLOB を使用して Azure ストレージアカウント上の場所を設定します。次の形式を使用します。
`abfs://<file_system>@<account_name>.dfs.core.windows.net/<path>`
例えば、JDBC 接続を使用するには、JDBC JAR ファイルを補足ファイルの場所に配置してから、次の場所を入力します。
`abfs://discaleqa@serverlessadlsgen2acct.dfs.core.windows.net/serverless`
- 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。

コマンドタスクの実行

Azure サーバーレスランタイム環境でコマンドタスクを実行するには、シェルスクリプトを特定のフォルダに配置する必要があります。

Azure サーバーレスランタイム環境の「[手順 5。サーバーレスランタイム環境を作成](#)」(ページ 87)に/`command_scripts` という名前のフォルダがあることを確認します。

1. コマンドタスクで実行するスクリプトファイルを/`command_scripts` フォルダに配置します。/`command_scripts` フォルダには独自のサブフォルダを含めることができます。
/`command_scripts` フォルダに配置されたファイルは、Secure Agent マシンの Secure Agent インストールディレクトリ内の次のフォルダに同期されます。
`apps/Common_Integration_Components/data/command/serverless/command_scripts`
2. タスクフローにコマンドタスクステップを追加します。コマンドタスクで指定されたスクリプトは、Secure Agent Docker コンテナで実行されます。
`apps/Common_Integration_Components/data/command/serverless/command_scripts` の下のファイルは、docker コンテナ内の/`command_scripts` フォルダの下にマウントされます。相対パスを使用して、他のファイルを参照することもできます。スクリプトの作業ディレクトリは/`command_scripts` に設定されています。
コマンドタスクの詳細については、「タスクフロー」の「コマンドタスクステップ」を参照してください。

Azure でのサーバーレスランタイム環境のトラブルシューティング

Azure でリージョンを変更した後、サーバーレスランタイム環境の起動に失敗するのはなぜですか？

入力したリージョンが正しくないため、サーバーレスランタイム環境の起動に失敗した可能性があります。リージョンを選択すると、変更することはできません。サーバーレスランタイム環境を削除し、正しいリージョンを使用して再作成する必要があります。

ネットワークセキュリティグループが自動作成され、リージョンにアタッチされます。リージョンを変更すると、ネットワークセキュリティグループが新しいリージョンと一致なくなり、環境の起動に失敗します。これを修正する唯一の方法は、環境を削除して新しい環境を作成することです。

serverlessUserAgentConfig.yml ファイルの設定方法

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。これは、AWS と Azure 両方のサーバーレスランタイム環境に適用されます。

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」 \(ページ 93\)](#) 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」 \(ページ 95\)](#) 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」 \(ページ 96\)](#) 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」 \(ページ 96\)](#) 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」 \(ページ 96\)](#) 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」 \(ページ 97\)](#) 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
```

```

    swagger: # List of Swagger files to copy to the instance machine.
    - fileCopy:
        sourcePath: restv2/<swagger_file_name>.json
    keystore: # List of keystore files to copy to the instance machine.
    - fileCopy:
        sourcePath: restv2/key
    truststore: # List of truststore files to copy to the instance machine.
    - fileCopy:
        sourcePath: restv2/key.ext
    wsconsumer:
    wsdls:
    - fileCopy:
        sourcePath: s3/
    jdbc:
    drivers:
    - fileCopy:
        sourcePath: s3/file
    autoDeploy:
    # A change in this event will trigger a minor version upgrade with the new configurations.
    # In this case, the Data Integration Server app will get a minor version upgrade.
    general: # General section for Data Integration Server app autoDeploy event.
    ssls:
    - fileCopy:
        sourcePath: SSL/RESTV2_JWTpyn.jks
    importCerts:
    certName: cname
    alias: IICS
    sap:
    jcos: # List of jco related files to copy.
    - fileCopy:
        sourcePath: sap/jco/libsapjco3.so
    - fileCopy:
        sourcePath: sap/jco/sapjco3.jar
    nwrfs: # List of nwrfs related files to copy.
    - fileCopy:
        sourcePath: sap/nwrfs/libicudata.so.50
    - fileCopy:
        sourcePath: sap/nwrfs/libicudcnumber.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

```

```
# Database Ingestion and Replication app
databaseIngestion:
  autoDeploy:
    jdbc:
      drivers:
        - fileCopy:
            sourcePath: google/<file_name>.jar
        - fileCopy:
            sourcePath: oracle/jdbc/<file_name>.jar
    hanami:
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: hanami/<file_name>.jar
    mysql:
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: mysql/jdbc/<file_name>.jar
    netsuiteami:
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: netsuite/<file_name>.jar
    odp:
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: sap-odp/<file_name>.jar
    sapami:
      jdbc:
        drivers:
          - fileCopy:
              sourcePath: sap-ami/<file_name>.jar
    oracle:
      oci:
        drivers:
          - fileCopy:
              sourcePath: oci/<file_name>.zip
```

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。

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	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	Salesforce 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
MongoDB 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 Fabric Lakehouse コネクタ
Amazon Redshift V2 コネクタ	Microsoft Fabric OneLake コネクタ
Amazon S3 V2 コネクタ	Microsoft SQL Server コネクタ
Azure AI Search コネクタ*	MongoDB V2 コネクタ*
BigMachines コネクタ	MySQL コネクタ
Concur V2 コネクタ	NetSuite Mass Ingestion コネクタ
Coupa V2 コネクタ	OData コネクタ
Cvent コネクタ	OData Consumer コネクタ
Databricks Delta コネクタ	OData V2 Protocol Reader コネクタ
Db2 for i Database Ingestion コネクタ	ODBC コネクタ
Db2 for zOS Database Ingestion コネクタ	Oracle コネクタ
DB2 Warehouse on Cloud コネクタ	Oracle Database Ingestion コネクタ
Dropbox コネクタ	Oracle Fusion Cloud Mass Ingestion コネクタ
Eloqua Bulk API コネクタ	PostgreSQL コネクタ
Google Analytics コネクタ	REST V2 コネクタ
Google BigQuery V2 コネクタ	REST V3 コネクタ
Google Cloud Storage V2 コネクタ	Salesforce コネクタ
JDBC (JDBC_IC) コネクタ	Salesforce Marketing Cloud コネクタ
JDBC V2 コネクタ	Salesforce Mass Ingestion コネクタ
JIRA コネクタ	SAP ADSO Writer コネクタ
Kafka コネクタ*	SAP BAPI コネクタ
Marketo V3 コネクタ	SAP ODP Extractor コネクタ
Microsoft Azure Blob Storage V3 コネクタ	SAP HANA コネクタ
Microsoft Azure Cosmos DB SQL API コネクタ	SAP HANA Database Ingestion コネクタ
Microsoft Azure Data Lake Storage Gen1 V3 コネクタ	SAP OData V2 コネクタ
Microsoft Azure Data Lake Storage Gen2 コネクタ	ServiceNow コネクタ
Microsoft Azure Synapse SQL コネクタ	ServiceNow Mass Ingestion コネクタ
Microsoft Azure Synapse Analytics データベース取り込みコネクタ	Snowflake Data Cloud Connector
Microsoft CDM Folders V2 コネクタ	SuccessFactors ODATA コネクタ
Microsoft Dynamics 365 for Operations コネクタ	Web サービスコンシューマコネクタ
Microsoft Dynamics 365 for Sales コネクタ	Workday V2 コネクタ
Microsoft Dynamics 365 Mass Ingestion コネクタ	Workday Mass Ingestion コネクタ
Microsoft Fabric Data Warehouse コネクタ	Xero コネクタ
	Xactly コネクタ
	Zendesk V2 コネクタ
	Zendesk Mass Ingestion 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。

第 6 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ブルサービスを使用します。例えば、データ統合サーバーはすべてのデータ統合ジョブを実行し、プロセスサーバーはアプリケーション統合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 設定などの一意の設定プロパティセットがあります。Secure Agent サービスの詳細については、「*Secure Agent サービス*」を参照してください。

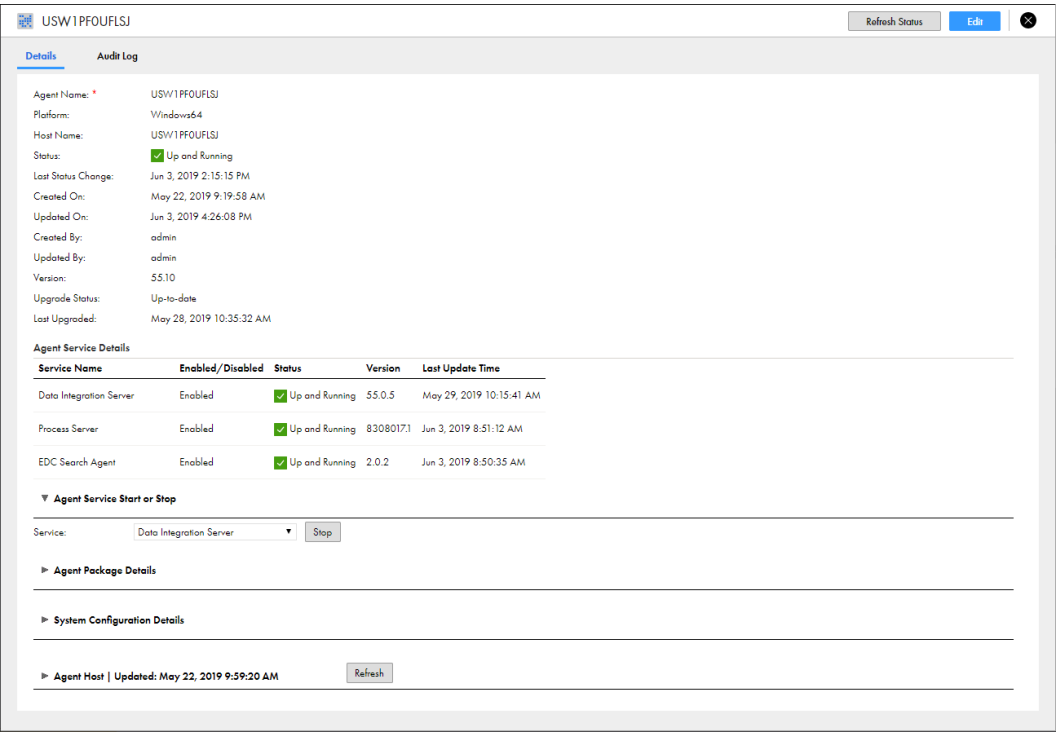
1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールして実行できます。Secure Agent をインストールすると、組織内のすべてのユーザーがその Secure Agent を共有します。Secure Agent のプロパティを設定し、別の Secure Agent グループに移動することができます。また、拡張性を向上させるために、Secure Agent グループに複数のエージェントを追加することもできます。

Secure Agent の操作

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

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

次の図に、エージェントの詳細ページを示します。



次のタスクを実行できます。

Secure Agent の詳細を表示する。

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

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

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

Secure Agent サービスの詳細を表示する。

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

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

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

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

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

7 日後、<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。コネクタで使用す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

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 の停止および再起動

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: 2024 年 7 月リリース以降、従来の `infaagent startup` および `infaagent shutdown` コマンドは機能しなくなります。

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 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」 \(ページ 14\)](#)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>
```

```
</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 注: Secure Agent ではバックスラッシュ (\) をエスケープ文字と解釈するため、Windows マシンでも UNIX マシンでもファイルパスにはスラッシュ (/) を使用してください。 Secure Agent からアクセスできるファイルパスにする必要があります。

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

ブラックアウトファイルの構造

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

ブラックアウトファイルの構造は次のとおりです。

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

ファイルには、以下の要素が含まれます。

要素	必須/ オプション	説明
BlackoutWindows	必須	ブラックアウト期間ごとに BlackoutWindow 要素が含まれています。 BlackoutWindow 要素は 1 つ以上含まれている必要があります。
BlackoutWindow	必須	ブラックアウト期間を 1 つ定義します。 RepeatFrequency 要素、Start 要素、End 要素を 1 つずつ含める必要があります。
RepeatFrequency	必須	ブラックアウト期間の繰り返し頻度。 次のいずれかの値を含める必要があります。 <ul style="list-style-type: none">- 1 回- 日次- 平日- 日曜日- 月曜日- 火曜日- 水曜日- 木曜日- 金曜日- 土曜日
Start	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の開始時刻。例: 2019-07-25 10:26:55。 タイムゾーンは Secure Agent ゾーンです。
End	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の終了時刻。例: 2019/07/26 11:45:00。 タイムゾーンは Secure Agent ゾーンです。

要素値は引用符で囲まないでください。

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 の移行

例えば、Secure Agent が仮想マシン上で実行されていて、マシンのクローンを作成する場合などに、Secure Agent をあるマシンから別のマシンに移行することができます。Secure Agent を移行するには、Secure Agent を新しいマシンにダウンロードしてインストールし、新しいエージェントを元の Secure Agent グループに追加します。

警告: 作成されたクローンのマシンで既存の Secure Agent を起動して実行しないようにしてください。この操作を行うと、製品のアップグレード後にエージェントが起動しなくなる可能性があります。

1. 元の Secure Agent が稼働中であることを確認してください。
2. Secure Agent を新しいマシンにダウンロードしてインストールします。
3. 新しい Secure Agent を Secure Agent グループから削除します。

この操作を行うと、エージェントは「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。Secure Agent グループには、未割り当ての任意のエージェントを追加できます。

4. 新しい Secure Agent を元の Secure Agent グループに追加します。
これにより、元の Secure Agent グループをランタイム環境として使用する接続とジョブは、移行後も実行を継続します。
Secure Agent グループに対するエージェントの追加および削除の詳細については、「[「Secure Agent グループの操作」 \(ページ 18\)](#)」を参照してください。
5. 元の Secure Agent に接続プロパティを保存する場合は、**【組織】** ページで接続資格情報を更新し、新しい Secure Agent を選択します。
6. 必要に応じて、元の Secure Agent を Secure Agent グループから削除し、元のマシン上のエージェントを停止してアンインストールします。

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 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。 <ul style="list-style-type: none">- 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 統合ハブアプ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。

Data Access Management Proxy サービス

ファイル	説明
<install>\apps \Data_Access_Management_Proxy\<version> \log\casapp_lcm_<version>.log	Secure Agent フレームワークによって呼び出されたライフサイクルコマンドのログが含まれています。

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。
<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	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。 <ul style="list-style-type: none">- AS2、HTTP、SFTP、MLLP などのファイルサーバーに関連するログ- 暗号化、復号化、圧縮、解凍などのタスクを転送します。- 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）。- ファイラサーバーのユーザー- fis-proxy への接続

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（「OI 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。

ファイル	説明
<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 AgentJava バージョン

Secure Agent は組み込み Java インスタンスを使用するため、Secure Agent インストールディレクトリの外部にある外部 Java インストールに依存しません。

Secure Agent を最初にインストールすると、組み込み Java インスタンスは次のフォルダに配置されます。

<Secure Agent installation directory>/jdk

アップグレード中に新しい Java バージョンをインストールすると、そのパッケージは次のフォルダに保存されます。

<Secure Agent installation directory>/apps/jdk

次の画像に、複数の Java バージョンの例を示します。

Name	Date modified	Type
conf	7/13/2025 5:36 PM	File folder
zulu8.82.0.22-sa-fx-jdk8.0.432	7/13/2025 5:36 PM	File folder
zulu8.86.0.26-sa-fx-jdk8.0.452	10/5/2025 5:35 PM	File folder
zulu17.54.22-sa-fx-jdk17.0.13	7/13/2025 5:36 PM	File folder
zulu17.58.22-sa-fx-jdk17.0.15	10/5/2025 5:35 PM	File folder

現在使用されている Java のバージョンは、次のフォルダ内のファイルを調べることで確認できます。

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

conf フォルダには次のようなファイルがあります。

- jdk17_version には、使用中の JDK 17.x のバージョンが一覧表示されます。
- バージョン には、使用中の JDK 8.x のバージョンが一覧表示されます。

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 プロセスに関連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。
<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す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。

2. 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、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 であるとしてします。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:	✓ 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 7 章

Secure Agent のインストール

Secure Agent は、クラウド環境やローカル環境など、さまざまな方法でインストールできます。

Secure Agent は次の方法でインストールできます。

AWS、Google Cloud、または Microsoft Azure クラウド環境

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。

Google Cloud では、最初に Google Cloud の資格情報を使用してログインし、次に Secure Agent と仮想ネットワークの詳細を入力します。オンラインウィザードによってインストールが完了します。

Azure では、最初に Azure の資格情報を使用してログインし、次に Secure Agent と仮想ネットワークの詳細を入力します。オンラインウィザードによってインストールが完了します。

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、Google Cloud、または Azure を使用していない場合は、最初にクラウド環境で VM をセットアップしてから、適切な手順に従って Secure Agent を Windows または Linux にインストールします。

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。

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。

- 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、マシンイメージの読み取りと起動の権限が必要です。

注: 次のディレクトリをセキュリティスキャンから除外します: <Secure Agent インストールディレクトリ>/apps。このディレクトリ内のファイルをスキャンすると、Secure Agent の動作が妨げられる可能性があります。

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 アドレッシングの有効化	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。 警告: 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。

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。

Google Cloud のインストールの使用

Secure Agent インストーラは、設定ページで入力したいいくつかのプロパティに基づいて、Google Cloud 上にランタイム環境を作成します。Google Cloud のサブスクリプションに、リソースをデプロイする権限が含まれている必要があります。

注: 次のディレクトリをセキュリティスキャンから除外します: <Secure Agent インストールディレクトリ>/apps。このディレクトリ内のファイルをスキャンすると、Secure Agent の動作が妨げられる可能性があります。

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. **【Google Cloud プラットフォーム】** を選択します。
4. **【次へ】** をクリックします。
5. 使用する Google アカウントを選択します。
6. 以下のプロパティを入力します。

プロパティ	説明
プロジェクト	プロジェクトにより、Informatica Intelligent Cloud Services が Google サービスと対話する方法と、使用するリソースを定義します。ドロップダウンリストから Google Cloud プロジェクトを選択します。 注: プロジェクトがない場合は、インストールウィザードを終了し、Google Cloud でプロジェクトを作成します。Informatica Intelligent Cloud Services 内からプロジェクトを作成することはできません。
Secure Agent 名	Secure Agent の名前を入力します。名前は、次のルールに準拠している必要があります。 <ul style="list-style-type: none">- 名前は最大 43 文字で、文字、数字、ハイフンの組み合わせを使用できます。- 最初の文字は小文字にする必要があります。- 最後の文字をハイフンにすることはできません。- すべての文字は小文字にする必要があります。 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。
リージョン	Secure Agent をデプロイするリージョンを選択します。組織と顧客に対する適切なリージョンを選択してください。

プロパティ	説明
マシンタイプ	仮想マシンのマシンタイプを選択します。Google のマシンタイプに慣れていない場合は、少なくとも 4 コア、16GB のメモリを搭載したマシンをサイズを使用してください。
仮想ネットワーク	Google サブスクリプション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するかを指定します。 仮想ネットワークは、ハードウェアとソフトウェアを使用して物理ネットワークをエミュレートします。
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。
サブネット	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。

- Google アカウントでコストが発生することを承認するには、**【この操作により Google Cloud Platform でコストが発生することに同意します】** チェックボックスをオンにします。
- 【作成】** をクリックします。
Informatica Intelligent Cloud Services 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。

Google Cloud での接続に関する問題のトラブルシューティング

Google Cloud のファイアウォールにより、VM へのアクセスがブロックされる可能性があります。この問題が発生した場合は、VM インスタンスへの RDP および SSH アクセスを許可するファイアウォールルールを追加します。

Google Cloud によってアクセスがブロックされると、次のエラーが発生してランタイム環境は起動に失敗します。

Connection Failed. We are unable to connect to the VM on port 22.

- Google Cloud コンソールで、「**ファイアウォールルール**」ページに移動します。
- 【ファイアウォールルールの作成】** をクリックします。
- 次の設定でファイアウォールルールを作成します。

設定項目	値
名前	ファイアウォールルールの名前を入力します。例: allow-ingress-from-iap(<name>)
トラフィックの方向	受信
一致時のアクション	許可

設定項目	値
ターゲット	ネットワーク内のすべてのインスタンス
ソースフィルタ	IP 範囲
ソース IP 範囲	35.235.240.0/20
プロトコルとポート	TCP を選択し、22,3389 と入力して、RDP および SSH を許可します。

4. **【作成】** をクリックします。

Microsoft 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: 次のディレクトリをセキュリティスキャンから除外します: <Secure Agent インストールディレクトリ>/apps。このディレクトリ内のファイルをスキャンすると、Secure Agent の動作が妨げられる可能性があります。

続行する前に、リソースのデプロイを許可するアクセス許可を持つ Microsoft Azure サブスクリプションがあることを確認してください。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"> - ネットワークセキュリティグループ - 仮想ネットワーク（サブネットを含む） - ネットワークインタフェース - パブリック IP アドレス - OS ディスク - 仮想マシン <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>注: 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>ヒント: 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>ヒント: 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。

Windows でのインストール

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。

- 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 マシンには、少なくとも次のような属性があります。
 - x86 64 ビットアーキテクチャ
 - 4 つの CPU コア
 - 16 GB RAM
 - 5 GB の空きディスク容量
- 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。

詳細については、ナレッジベースの記事

「[Minimum requirements and best practices when installing Informatica Cloud Secure Agent](#)」を参照してください。

ファイアウォールの設定

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

Secure Agent はインターネットに接続するためにポート 443 (HTTPS) を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。また、次のディレクトリをセキュリティスキャンから除外します: <Secure Agent インストールディレクトリ>/apps。このディレクトリ内のファイルをスキャンすると、Secure Agent の動作が妨げられる可能性があります。

許可されるドメインと IP アドレスのリストは、POD (デプロイメントポイント) によって異なる場合があります。POD は、サービスを開いたときに表示される URL で特定することができます。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。

さまざまな POD に対して許可する必要があるすべてのドメインと IP アドレスのリストについては、「[Pod Availability and Networking](#)」を参照してください。

Windows での Secure Agent の権限の設定

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 設定の構成

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。
注: ファイルパスにマルチバイト文字が含まれていないことを確認します。パスにマルチバイト文字が含まれていると、Secure Agent が起動しないことがあります。
 - 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 でのプロキシ設定の構成

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、ブラウザで構成されている設定項目に基づいて Secure Agent のデフォルトのプロキシサーバー設定が構成されます。プロキシ設定は、次のディレクトリにあるプロキシ設定ファイル proxy.ini に保存されます。

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

次のコードに、プロキシ設定ファイルのデフォルトの内容を示します。

```
InfAgent.ProxyPassword=ZU8KjIzgtVrVmFRMUPzPMw\=\=
InfAgent.ProxyNtDomain=
InfAgent.ProxyHost=foo.bar.com
InfAgent.ProxyPasswordEncrypted=true
InfAgent.NonProxyHost=localhost|127.*|[\:\:1]
InfAgent.ProxyUser=
InfAgent.ProxyPort=12345
InfAgent.AuthenticationOrder=
```

プロキシホストとポート、およびプロキシサーバーへの接続に使用するユーザー名とパスワードを更新するには、Secure Agent Manager を使用します。Secure Agent Manager では、入力した値が検証されます。詳細については、「[「Secure Agent Manager によるプロキシ設定の更新」 \(ページ 128\)](#)」を参照してください。

他のプロパティを更新するには、プロキシ設定ファイルを直接編集します。プロキシ設定ファイルを編集するときは、エラーを避けるために正しい形式を使用していることを確認してください。詳細については、「[「プロキシ設定ファイルのプロキシ設定の更新」 \(ページ 129\)](#)」を参照してください。

Secure Agent がデータソースとターゲットに接続できるようにするには、プロキシ設定ファイルの構成とともに、JVM オプションでもプロキシ設定を構成します。詳細については、該当するコネクタのヘルプを参照してください。

一部のユースケースでは、Secure Agent がプロキシサーバーをバイパスし、一時的なセキュリティ認証情報を保存するインスタンスメタデータサービス (IMDS) と直接通信する必要があります。例えば、Azure マネージド ID を使用して詳細モードでマッピングのソースとターゲットにアクセスする場合や、Amazon S3 V2 接続で **[ロールの引き受けに EC2 ロールを使用]** プロパティを有効にしている場合は、プロキシサーバーをバイパスする必要があります。エージェントが IMDS と直接通信できるようにするには、プロキシ設定ファイルを編集し、IMDS の IP アドレス 169.254.169.254 をプロパティ *InfAgent.NonProxyHost* の値に設定します。

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。

Secure Agent Manager によるプロキシ設定の更新

プロキシホスト、プロキシポート、およびプロキシサーバーへの接続に使用するユーザー名とパスワードを更新するには、Secure Agent Manager を使用してプロキシ設定を編集します。

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。

フィールド	説明
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。

プロキシ設定ファイルのプロキシ設定の更新

Secure Agent Manager で更新できないプロキシ設定を更新するには、プロキシ設定ファイルを直接編集します。

1. proxy.ini ファイルを開きます。
2. 必要に応じてプロパティ値を更新します。ホスト名と IP アドレスのリストを結合するには、パイプ文字 (|) を区切り文字として使用します。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できます。
例えば、次の値を設定すると、2 つの形式を使用して CIDR ブロック 172.16.0.0/16 のクラス A IP アドレスが除外されます。
`InfAgent.NonProxyHost=localhost|127.0.0.1|123.432.172.16.*|172.16.0.0/16`
3. 変更を有効にするには、Secure Agent を再起動します。

プロキシの詳細が、プロキシサーバーの Secure Agent Manager 設定ページに表示されます。

Windows Secure Agent サービスのログインの設定

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。

Linux での Secure Agent の要件

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

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

- Secure Agent 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。
- Secure Agent マシンが x86 64 ビットアーキテクチャを実行しており、少なくとも 11 GB 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、次のコマンドを実行します。

1. Secure Agent マシンの適切なディレクトリに変更します。

- 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`

2. 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 を RHEL 9 にインストールする場合は、次のコマンドを使用して追加のシンボリックリンクを作成します。

```
sudo ln -s libidn2.so.0 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。

詳細については、ナレッジベースの記事

「[Minimum requirements and best practices when installing Informatica Cloud Secure Agent](#)」を参照してください。

ファイアウォールの設定

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

Secure Agent はインターネットに接続するためにポート 443 (HTTPS) を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。また、次のディレクトリをセキュリティスキャンから除外します: `<Secure Agent インストールディレクトリ>/apps`。このディレクトリ内のファイルをスキャンすると、Secure Agent の動作が妨げられる可能性があります。

許可されるドメインと IP アドレスのリストは、POD（デプロイメントポイント）によって異なる場合があります。POD は、サービスを開いたときに表示される URL で特定することができます。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。

さまざまな POD に対して許可する必要があるすべてのドメインと IP アドレスのリストについては、「[Pod Availability and Networking](#)」を参照してください。

Linux での Secure Agent の権限の設定

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やマルチバイト文字が含まれていないことを確認します。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。パスにマルチバイト文字が含まれていると、Secure Agent が起動しないことがあります。

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があります。

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 でのプロキシ設定の構成

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、ブラウザで構成されている設定項目に基づいて Secure Agent のデフォルトのプロキシサーバー設定が構成されます。プロキシ設定は、次のディレクトリにあるプロキシ設定ファイル proxy.ini に保存されます。

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

次のコードに、プロキシ設定ファイルのデフォルトの内容を示します。

```
InfAgent.ProxyPassword=ZU8KjIzgtVrVmFRMUPzPMw\=\=  
InfAgent.ProxyNtDomain=  
InfAgent.ProxyHost=foo.bar.com  
InfAgent.ProxyPasswordEncrypted=true  
InfAgent.NonProxyHost=localhost|127.*|[\:\:1]  
InfAgent.ProxyUser=  
InfAgent.ProxyPort=12345  
InfAgent.AuthenticationOrder=
```

プロキシホストとポート、およびプロキシサーバーに接続するためのユーザー名とパスワードを更新するには、コマンドラインを使用します。コマンドラインでは、入力した値が検証されます。詳細については、「[「コマンドラインによるプロキシ設定の更新」 \(ページ 134\)](#)」を参照してください。

他のプロパティを更新するには、プロキシ設定ファイルを直接編集します。プロキシ設定ファイルを編集するときは、エラーを避けるために正しい形式を使用していることを確認してください。詳細については、「[「プロキシ設定ファイルのプロキシ設定の更新」 \(ページ 134\)](#)」を参照してください。

Secure Agent がデータソースとターゲットに接続できるようにするには、プロキシ設定ファイルの構成とともに、JVM オプションでもプロキシ設定を構成します。詳細については、該当するコネクタのヘルプを参照してください。

一部のユースケースでは、Secure Agent がプロキシサーバーをバイパスし、一時的なセキュリティ認証情報を保存するインスタンスメタデータサービス (IMDS) と直接通信する必要があります。例えば、Azure マネージド ID を使用して詳細モードでマッピングのソースとターゲットにアクセスする場合や、Amazon S3 V2 接続で **[ロールの引き受けに EC2 ロールを使用]** プロパティを有効にしている場合は、プロキシサーバーをバイパスする必要があります。エージェントが IMDS と直接通信できるようにするには、プロキシ設定ファイルを編集し、IMDS の IP アドレス 169.254.169.254 をプロパティ *InfraAgent.NonProxyHost* の値に設定します。

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。

コマンドラインによるプロキシ設定の更新

プロキシホスト、プロキシポート、およびプロキシサーバーに接続するためのユーザー名とパスワードを更新するには、コマンドラインを使用してプロキシ設定ファイルを更新します。

1. 次のディレクトリに移動します。
`<Secure Agent installation directory>/apps/agentcore/conf`
2. プロキシ設定ファイル `proxy.ini` を更新するには、次のコマンドを実行します。
`./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name> <proxy password>`
3. Secure Agent を再起動します。

プロキシ設定ファイルのプロキシ設定の更新

コマンドラインで更新できないプロキシ設定を更新するには、プロキシ設定ファイルを直接編集します。

1. `proxy.ini` ファイルを開きます。
2. 必要に応じてプロパティ値を更新します。ホスト名と IP アドレスのリストを結合するには、パイプ文字 (`|`) を区切り文字として使用します。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できます。

例えば、次の値を設定すると、2 つの形式を使用して CIDR ブロック 172.16.0.0/16 のクラス A IP アドレスが除外されます。
`InfraAgent.NonProxyHost=localhost|127.|[\\:\\.1]|123.432.|172.16.*|172.16.0.0/16`
3. 変更を有効にするには、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。

索引

C

Cloud アプリケーション統合コミュニティ
URL [7](#)
Cloud 開発者コミュニティ
URL [7](#)

H

Hosted Agent
説明 [11](#)

I

Informatica Intelligent Cloud Services
Web サイト [7](#)
Informatica グローバルカスタマサポート
連絡先情報 [8](#)

L

Linux
Secure Agent のアンインストール [134](#)
Secure Agent の起動および停止 [103](#)
プロキシの設定 [133](#)

P

POD
特定方法 [125](#), [131](#)

S

Secure Agent
IP アドレス許可リスト [125](#), [131](#)
Linux でのアンインストール [134](#)
Linux での起動および停止 [103](#)
Linux での権限 [132](#)
Linux での登録 [132](#)
Linux での要件 [131](#)
Linux へのインストール [132](#)
Secure Agent Manager [110](#)
Secure Agent グループ [13](#)
Secure Agent グループからの削除 [21](#)
Secure Agent グループへの追加 [20](#)
VM のクローン作成 [109](#)
Windows サービスログインの設定 [129](#)
Windows でのアンインストール [130](#)
Windows での起動 [124](#)
Windows での権限 [125](#)
Windows での停止および再起動 [103](#)

Secure Agent (続く)
Windows での登録 [126](#)
Windows での要件 [125](#)
Windows へのインストール [126](#)
アップグレード [109](#)
インストール [117](#)
サービスの開始 [106](#)
サービスの開始および停止 [104](#)
サービスの停止 [105](#)
サービスを開始および停止する際のガイドライン [105](#)
ドメイン許可リスト [125](#), [131](#)
トラブルシューティング [115](#)
ブラックアウトファイルの構造 [107](#)
ブラックアウトファイルの上書き [107](#)
ブラックアウト期間の設定 [106](#)
移行 [109](#)
概要 [100](#)
拡張性 [13](#)
削除 [109](#)
詳細の表示、更新ステータス [100](#)
通信ポート [125](#), [131](#)
負荷分散 [13](#)
名前の変更 [108](#)
Secure Agent Manager
Secure Agent の停止および再起動 [103](#)
起動 [124](#)
使用 [110](#)
Secure Agent グループ
Secure Agent の削除 [21](#)
Secure Agent の追加 [20](#)
Secure Agent の追加および削除 [18](#)
グループの共有 [17](#)
サービスとコネクタの有効化および無効化 [16](#)
サービスの有効化および無効化 [14](#), [18](#)
サービス割り当てのガイドライン [15](#)
依存性の表示 [21](#)
概要 [13](#)
既存のグループへの新規エージェントの追加 [21](#)
共有グループでのファイル接続 [18](#)
権限の変更 [18](#)
作成 [18](#)
削除 [18](#)
名前の変更 [18](#)
Secure Agent コネクタ
有効化および無効化 [16](#)
Secure Agent サービス
有効化および無効化 [14](#), [16](#)
Secure Agent のインストール
トラブルシューティング [135](#)

W

Web サイト [7](#)
Windows
プロキシの設定 [128](#)

Windows サービス
Secure Agent ログインの設定 [129](#)

あ

アップグレード通知 [8](#)

え

エラスティックランタイム環境
コネクタ [47](#)
概要 [23](#)

お

オブジェクトの依存関係
Secure Agent グループの表示 [21](#)

さ

サーバーレスランタイム環境
クローン作成 [81](#), [91](#)
コネクタ [97](#)
サーバーレスコンピューティングユニット [81](#)
ディザスタリカバリ [81](#)
トラブルシューティング [92](#)
開始 [91](#)
概要 [61](#)
再デプロイ [80](#), [91](#)
作成 [75](#)
削除 [81](#), [91](#)
編集 [90](#)
編集権 [80](#)
要件 [62](#)

し

システムステータス [8](#)

す

ステータス
Informatica Intelligent Cloud Services [8](#)

て

ディレクトリ
アクセスする Secure Agent ログインの設定 [129](#)

と

トラブルシューティング
Secure Agent [115](#)
Secure Agent のインストール [135](#)
サーバーレスランタイム環境 [92](#)

ふ

ファイアウォール
設定 [125](#), [131](#)
ブラックアウト期間
Secure Agent に対する設定 [106](#)
Secure Agent のブラックアウトファイル構造 [107](#)
Secure Agent ブラックアウトファイルの上書き [107](#)
プロキシ設定
Linux での設定 [133](#)
Windows 上での設定 [128](#)

め

メンテナンスの停止 [8](#)

ら

ランタイム環境
Hosted Agent [11](#)
Secure Agent グループ [13](#)
Secure Agent グループの共有 [17](#)
Secure Agent のインストール [117](#)
サービスとコネクタの有効化および無効化 [16](#)
サービスの有効化および無効化 [14](#)
サービス割り当てのガイドライン [15](#)
概要 [9](#)
共有グループでのファイル接続 [18](#)
設定 [117](#), [120](#), [122](#)