



Informatica® Intelligent Cloud Services
July 2022

Data Integration Elastic の管理

© 著作権 Informatica LLC 2020, 2022

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

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

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

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

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、infa_documentation@informatica.com 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: 2022-09-16

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 : 概要	9
管理プロセス	9
クラスタデプロイメントタイプ	10
エラスティッククラスタ	11
エラスティッククラスタのライフサイクル	11
セルフサービスクラスタ	13
ローカルクラスタ	13
第 2 章 : AWS の設定	14
始める前に	14
組織の権限の確認	14
AWS サブスクリプションの確認	15
AWS 環境でのロールとポリシーの確認	15
リソースへのアクセスの詳細	17
クラスタファイルの格納場所の作成	22
VPC とサブネットの作成 (オプション)	22
十分な数の IP アドレスを含むサブネットの作成	22
ルーティング設定の確認	23
受信トラフィックの承認	23
Amazon EC2 のユーザー定義のセキュリティグループの作成	23
ELB セキュリティグループの作成	23
マスタセキュリティグループの作成	24
ワーカーセキュリティグループの作成	25
デフォルトのセキュリティグループの使用 (代替)	25
Secure Agent のダウンロードとインストール	26
AWS のドメインのホワイトリスト登録	26
IAM ロールの作成	27
手順 1. クラスタオペレータのロールを作成する	28
手順 2. クラスタオペレータポリシーの作成	28

手順 3. クラスタオペレータポリシーのアタッチ.	31
手順 4. クラスタオペレータロールの最大 CLI/API セッション期間の設定.	32
手順 5. Secure Agent ロールの作成または再利用.	32
手順 6. AssumeRole 権限を Secure Agent ロールに追加.	32
手順 7. Secure Agent ロールを含めるようにクラスタオペレータロールの信頼関係を設定.	33
手順 8. ユーザー定義のマスタロールおよびワーカーロールの作成.	33
手順 9. 保存ステージングデータとログファイルの暗号化（オプション）.	43
手順 10. Amazon データソースのロールベースのセキュリティポリシーの作成（オプション）.	44
手順 11. Secure Agent ロールのログアクセスポリシーの作成または再利用.	46
環境変数の設定（オプション）.	48
エラスティックサーバーの設定.	48
AWS ポリシーの詳細参照.	49
クラスタオペレータロールの詳細.	50
マスタロールの詳細.	58
ワーカーロールの詳細.	62
マスタとワーカーのロールタイプのリファレンス.	64
マスタおよびワーカーポリシーの制限に関するリファレンス.	65
第 3 章 : Google Cloud の設定.	67
始める前に.	67
組織の権限の確認.	67
Google Cloud サービスの確認.	67
リソースへのアクセスの詳細.	68
クラスタファイルの格納場所の作成.	71
Secure Agent のダウンロードとインストール.	71
Google Cloud のドメインのホワイトリスト登録.	71
クラスタのプロキシの設定.	72
ロールとサービスアカウントの作成.	72
Secure Agent ロールとサービスアカウントの作成.	73
マスタロールとサービスアカウントの作成.	76
ワーカーノードロールとサービスアカウントの作成.	77
VPC およびサブネットの準備.	78
手順 1. 十分な数の IP アドレスを含むサブネットの作成.	78
手順 2. Google Cloud NAT ゲートウェイの作成.	78
手順 3. VPC ネットワークでのファイアウォールルールの作成.	79
JAVA_HOME 環境変数の設定.	80
第 4 章 : Microsoft Azure の設定.	81
始める前に.	81
組織の権限の確認.	81
Microsoft Azure 製品を確認する.	82
リソースへのアクセスの詳細.	82
Secure Agent のダウンロードとインストール.	85

Azure のドメインのホワイトリスト登録	85
クラスタのプロキシの設定	86
クラスタファイルのストレージアカウントの作成	86
クラスタリソースグループの作成	87
Secure Agent 向けのマネージド ID の作成	87
手順 1。マネージド ID を作成する	87
手順 2。エージェントロールの作成	87
手順 3。ロールの割り当ての追加	90
クラスタ用のサービスプリンシパルの作成	90
手順 1。サービスプリンシパルを作成する	91
手順 2。クラスタロールの作成	91
手順 3。ロールの割り当ての追加	92
手順 4。資格情報の Key Vault への保存	92
手順 5。アクセスポリシーを Key Vault に追加します	92
JAVA_HOME 環境変数の設定	93
第 5 章 : セルフサービスクラスタの設定	94
始める前に	94
組織の権限の確認	94
リソースへのアクセスの詳細	94
Secure Agent のダウンロードとインストール	97
ユーザー管理のサービスアカウントの作成	97
最適化されたクラスタロールの作成	97
クラスタロールの作成バイインディング	98
エラスティック構成でのサービスアカウントの設定	98
Informatica が管理するサービスアカウントの作成（代替）	99
注釈と許容	100
Amazon EKS クラスタ認証	101
シーケンスジェネレータートランスフォーメーション	102
セルフサービスクラスタのドメインのホワイトリスト登録	102
第 6 章 : ローカルクラスタの設定	103
組織の権限の確認	103
ステージングとログの場所の作成	103
Secure Agent のダウンロードとインストール	104
ローカルクラスタのドメインのホワイトリスト登録	104
クラウド権限の設定	105
第 7 章 : エラスティック構成	108
AWS のプロパティ	109
構成の検証	113
GPU ワーカーインスタンスタイプ	114
Graviton ワーカーインスタンスタイプ	114

スポットインスタンス.	115
高可用性.	116
新しいステージングの場所へのアクセス.	116
クラウドリソースへのタグのプロパゲート.	116
クラウドリソースのデフォルトタグ.	117
データ暗号化.	117
Google Cloud のプロパティ.	118
クラウドリソースへのラベルのプロパゲート.	121
データ暗号化.	121
Microsoft Azure プロパティ.	122
構成の検証.	125
スポットインスタンス.	125
高可用性.	126
新しいステージングの場所へのアクセス.	126
クラウドリソースへのタグのプロパゲート.	126
クラウドリソースのデフォルトタグ.	127
データ暗号化.	127
セルフサービスクラスタのプロパティ.	128
ランタイムプロパティ.	132
ローカルクラスタのプロパティ.	132
データ暗号化.	134
クラスタノードのリソース要件.	134
リソース要件の再設定.	135
リソース要件の例.	136
初期化スクリプト.	136
初期化スクリプトのエラー.	137
ランタイム環境またはステージングの場所の更新.	137
第 8 章: トラブルシューティング.	139
エラスティッククラスタのトラブルシューティング.	139
AWS 上のエラスティッククラスタのトラブルシューティング.	141
Microsoft Azure 上のエラスティッククラスタのトラブルシューティング.	144
エラスティックジョブのトラブルシューティング.	145
セルフサービスクラスタのトラブルシューティング.	147
Secure Agent マシンとクラウドリソースのシャットダウン.	147
付録 A: コマンドリファレンス.	148
generate-policies-for-userdefined-roles.sh.	148
list-clusters.sh.	149
delete-clusters.sh.	150
cluster-operations.sh.	152
索引.	155

序文

[データ統合エラスティックの管理] を使用して、お使いのクラウド環境内でエラスティッククラスタを作成またはデプロイするためのリソースを Secure Agent がプロビジョニングする方法について学習します。Informatica Cloud(R)Data Integration Elastic とお使いのクラウドプラットフォームを統合し、組織でエラスティック構成を作成します。

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/>

データ統合コネクタのドキュメント

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

Informatica ナレッジベース

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

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

Informatica Intelligent Cloud Services Trust Center

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

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

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

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

Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

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

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

第 1 章

概要

Data Integration Elastic を使用すると、組織は Kubernetes クラスタでデータ統合ジョブ（エラスティックジョブ）を実行できます。

Data Integration Elastic がユーザーに代わってクラスタを作成して完全に管理することも、ユーザーが独自の Kubernetes クラスタを作成して Data Integration Elastic に接続することもできます。

管理者、開発者、および Secure Agent は、次のように連携して環境をセットアップします。

ユーザー（管理者）

Data Integration Elastic とお使いのクラウドプラットフォームを統合し、Secure Agent をクラウドプラットフォームが提供するサービスまたは製品に接続します。

開発者

開発者は、エラスティックマッピングを作成し、ソースからターゲットへのデータフローロジックを設計します。開発者は、エラスティックジョブを実行してクラウド上のデータを処理します。

Secure Agent

Secure Agent は、Data Integration Elastic とお使いのクラウドプラットフォームの間のファイアウォール経由での安全な通信を実現する軽量プログラムです。エージェントは、開発者がクラスタ上で実行するエラスティックジョブを送信および管理します。

Data Integration Elastic を使用するには、組織に適切なライセンスが必要です。

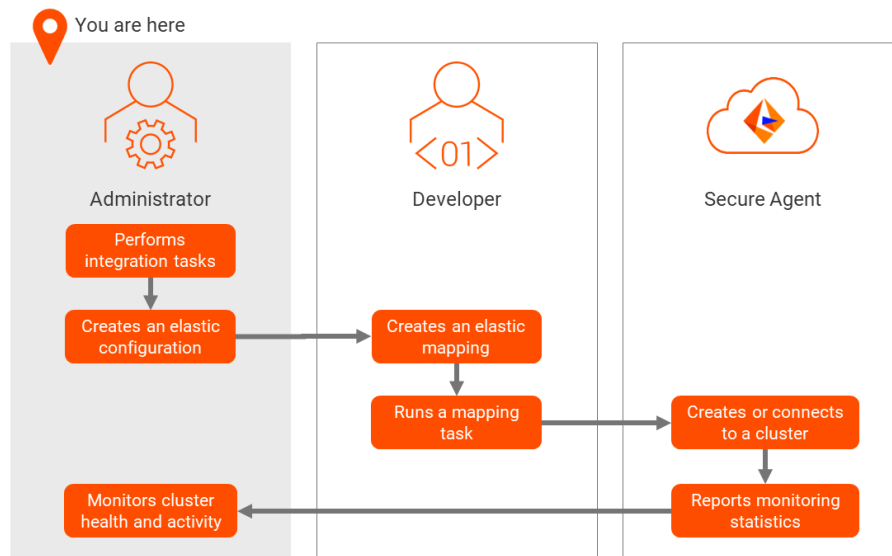
管理プロセス

管理プロセスには、Data Integration Elastic とお使いのクラウドプラットフォームを統合してエラスティック構成を作成する手順が含まれています。

管理者は、次の手順を実行します。

1. Data Integration Elastic とお使いのクラウドプラットフォームを統合します。
2. エラスティック構成を作成し、Data Integration Elastic に接続する Kubernetes クラスタとクラウドリソースを定義します。
3. 開発者がクラスタ上でエラスティックジョブを作成し実行している間、クラスタの健全性とアクティビティを監視します。

次の図では、管理タスクを強調表示しています。



注: AWS クラウドプラットフォームを使用する場合は、統合タスクを実行してエラスティック構成を作成する代わりに、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。詳細については、「ランタイム環境」を参照してください。

クラスタデプロイメントタイプ

組織が実行するプロジェクトとプロジェクトフェーズに最適なインフラストラクチャに応じて、クラスタデプロイメントを選択できます。

次のクラスタデプロイメントタイプを使用できます。

エラスティッククラスタ

エラスティッククラスタは、ワークロードに基づいてインテリジェントにスケーリングされ、組織の総所有コストを最小限に抑える、フルマネージドのサーバーレスインフラストラクチャを提供します。

Data Integration Elastic は、起動、シャットダウン、自動スケーリング、アップグレードなど、クラスタのライフサイクル全体を管理します。Data Integration Elastic は、コンピューティングインフラストラクチャをインテリジェントに管理するもので、スポットインスタンスを使用してエラスティッククラスタを作成することで、組織のコストをさらに削減できます。

詳細については、「[エラスティッククラスタ](#)」(ページ 11)を参照してください。

セルフサービスクラスタ

セルフサービスクラスタは、組織が実行し、Data Integration Elastic に再利用する Kubernetes クラスタです。Kubernetes クラスタは、Amazon EKS や AKS などのプロバイダ管理の Kubernetes サービス、または自己管理サービスのいずれかで実行できます。

セルフサービスクラスタを使用すると、名前空間、コンテキスト、注釈、および許容によって分離を行うことで、コンピューティング環境をより細かく制御できます。クラスタを管理するため、Data Integration Elastic に必要な権限は環境内の最小限の権限で済みます。

詳細については、「[セルフサービスクラスタ](#)」(ページ 13)を参照してください。

ローカルクラスタ

ローカルクラスタは、Secure Agent マシンで起動できる単純な単一ノードクラスタです。ローカルクラスタを使用すると、プロジェクトを Data Integration Elastic に瞬時にオンボードできます。

詳細については、[「ローカルクラスタ」 \(ページ 13\)](#)を参照してください。

エラスティッククラスタ

エラスティッククラスタは、サーバーレス Spark エンジンでエラスティックジョブを処理するために使用する一時クラスタです。

エラスティッククラスタでデータを処理すると、次のような利点があります。

- エラスティッククラスタは完全管理されます。Secure Agent をセットアップした後、最初のジョブをサブミットすると、このエージェントによってエラスティッククラスタが稼働されます。環境への Secure Agent のアクセス制限を設定するための権限を設定できます。
- 自動スケーリングテクノロジーによって、ワークロードのサイズおよび指定したリソース境界に基づいて、クラスタがスケールアップまたはスケールダウンされます。ワークロードが小さければ小さいほど、その期間中にジョブによって使用されるリソースも少なくなり、エラスティッククラスタは処理の負荷の増大に対応します。
- エラスティッククラスタは、ジョブを実行している間のみリソースを使用します。Secure Agent は、エラスティック構成で選択したクラスタシャットダウン方法に基づいて、クラスタを停止するタイミングを決定します。
- Informatica の AI エンジンである CLAIRE(R)は、最適なジョブのパフォーマンスを引き出すために、機械学習を使用してクラスタで実行されるジョブを自動的に調整します。
- Spark パフォーマンスのチューニングプロセスによって、エラスティックマッピングおよびクラスタキャパシティのデータサイズを分析し、Spark エンジンでデータの処理を自動調整します。
- 高可用性、リカバリ、およびレジリエンスによって、中断時でもジョブを継続して円滑に実行できます。
- データはクラウド環境に残ったままとなります。

エラスティッククラスタのライフサイクル

クラスタのライフサイクルとは、エラスティッククラスタで発生する一連のイベントです。

クラスタのライフサイクルには、次のイベントが含まれます。

1. エラスティッククラスタを作成するエージェント
2. クラスタで実行されるジョブ
3. クラスタを停止するエージェント

エージェントがクラスタを作成する

エラスティッククラスタを作成するには、Secure Agent でジョブのランタイム環境に関連付けたエラスティック構成を使用します。

このエージェントでは、以下のタスクを実行します。

1. エラスティッククラスタについての構成情報を含むクラスタ構成を作成する。この構成は、Secure Agent で入力する YAML ファイルを使用して格納されます。

2. エラスティッククラスタを作成するのに必要なリソースをプロビジョニングする。クラスタが停止すると、エージェントはリソースを削除します。

注: Informatica は、安全なパスウェイを使用して、Informatica 固有の JFrog リポジトリからクラスタノードのジョブ関連のコンテナイメージを取得します。Google Cloud 上のクラスタの場合は、パブリックインターネットにアクセスして、クラスタノードで論理クラスタレイヤを作成するために必要となるファイルを取得します。

クラスタで実行されるジョブ

エラスティッククラスタが作成された後、エージェントは、エラスティックジョブをクラスタにプッシュし、サーバーレス Spark エンジンを利用してジョブのデータロジックを処理します。

エラスティックジョブを実行すると、エージェントで Spark エンジンの一連の手順となる実行計画が生成されます。実行計画によってデータロジックは複数の Spark タスクに分割され、Spark ドライバおよび実行プログラムが起動して Spark タスクが同時に処理されます。

開発者はクラスタのライフサイクルにわたって追加のエラスティックジョブを実行し、クラスタノードやクラスタストレージのように、リソースがプロビジョニング/プロビジョニング解除されるたびにジョブのサイズや数にクラスタを適応させます。

ジョブごとに、エージェントによってセッションログ、Spark ドライバログ、および Spark 実行プログラムログが生成されます。また、エージェントによって、ジョブ内の Spark タスクごとにエージェントジョブログが生成されます。

エージェントがクラスタを停止する

すべてのジョブが完了すると、Secure Agent は、エラスティック構成で選択したクラスタシャットダウン方法に基づいて、クラスタを停止するタイミングを決定します。

エージェントは、履歴データに基づいてスマートシャットダウンを実行したり、指定したアイドルタイムアウトに基づいてクラスタを停止したりします。

Secure Agent は、次の状況でもクラスタを停止します。

- クラスタの開始または停止に失敗した。
- エージェントが一定の時間内に Kubernetes API サーバー内に到達できない。

Secure Agent がクラスタを停止した後、エージェントは、infa_rpm.tar ファイルのステージング位置に残った一部の Informatica バイナリを除くすべてのクラスタリソースが削除されていることを確認します。これらのバイナリはクラスタ上でジョブを実行するために必要で、エージェントによる次回クラスタの起動時にファイルが再利用されます。

エージェントは、次の状況の場合に infa_rpm.tar ファイルを削除します。

- エラスティック構成でランタイム環境をクリアする場合。
- エラスティック構成を別のランタイム環境に関連付ける場合。
- Secure Agent マシン上のエージェントプロセスがシャットダウンされた。

別のエラスティックジョブを実行すると、エージェントでクラスタが再起動されます。

セルフサービスクラスタ

セルフサービスクラスタは、ユーザーが管理する Kubernetes クラスタです。セルフサービスクラスタを使用すると、Kubernetes クラスタの権限と認証の構成を管理できます。セルフサービスの Kubernetes クラスタは、Azure 仮想マシンを使用して Azure にデプロイすることも、EC2 マシンを使用して AWS にデプロイすることもできます。

データ統合エラスティックをクラウドプラットフォームで維持するカスタマイズされた Kubernetes クラスタと統合して、エラスティック構成を作成できます。Secure Agent は、エラスティック構成を使用してエラスティックジョブをクラスタにプッシュし、Spark エンジンを利用してジョブ内のデータロジックを処理します。

セルフサービスクラスタを使用する主な利点は次のとおりです。

- クラスタコントロールプレーンをより細かく制御できます。
- クラスタにフルアクセスでき、すべてのコンポーネントを管理できます。
- クラスタのデプロイメントと管理をより細かく制御できます。例えば、複数のノードグループを実装したり、ノードごとに異なるインスタンスタイプを選択したりできます。

他のクラスタとは異なり、Secure Agent はセルフサービスクラスタを作成しません。セルフサービスの Kubernetes クラスタはユーザーが Virtual Private Cloud (VPC) 上に作成します。セルフサービスクラスタを作成すると、クラスタの kubeconfig ファイルが生成されます。kubeconfig ファイルは、クラスタ設定を含む YAML ファイルです。

Administrator でセルフサービスクラスタのエラスティック構成を作成するときに、kubeconfig ファイルへのパスと、Kubernetes クラスタに接続してそのクラスタでエラスティックジョブを実行するための関連する設定情報を入力します。エージェントはエラスティックジョブをクラスタにプッシュし、Spark エンジンを利用してジョブ内のデータロジックを処理します。

セルフサービスクラスタをシャットダウンすると、Secure Agent はデータ統合エラスティックのすべてのリソースをクラスタから削除します。

クラスタはユーザーによって管理されているため、Informatica はセルフサービスクラスタのクラスタノードを自動スケーリングしません。

ローカルクラスタ

ローカルクラスタでは、セットアッププロセスが簡素化されているため、エラスティックマッピングの作成と実行をすばやく開始できます。

最小限のクラウド権限とリソース要件で、ローカルマシンにローカルクラスタをセットアップできます。ローカルクラスタには単一のノードがあり、その処理容量はローカルマシンに依存します。クラスタで実行中のジョブがない場合、ローカルクラスタは5分後にタイムアウトします。

第 2 章

AWS の設定

エラスティック構成の作成を組織内で開始する前に、AWS をセットアップして Data Integration Elastic と連携します。

以下のタスクを完了させます。

1. 環境の要件を確認する。
2. クラスタファイルの格納場所を作成します。
3. 必要に応じて、VPC とサブネットを作成します。
4. Amazon EC2 用のユーザー定義のセキュリティグループを作成します。
5. Amazon EC2 上の Linux 仮想マシンに Secure Agent をダウンロードしてインストールします。
6. IAM ロールを作成します。
7. 必要に応じて、Secure Agent マシンで環境変数を設定します。
8. エラスティックサーバーを設定します。

注: AWS 環境で、これらのタスクを実行してエラスティック構成を作成する代わりに、サーバーレスランタイム環境を使用することができます。詳細については、「ランタイム環境」を参照してください。

始める前に

環境をセットアップする前に、環境とクラウドプラットフォームの要件を確認してください。

以下のタスクを完了させます。

- 組織で正しい特権を持っていることを確認してください。
- 必要な AWS サブスクリプションがあることを確認します。
- ご使用の環境のロールとポリシーの詳細を確認します。
- Data Integration Elastic がクラウドプラットフォーム上のリソースにアクセスする方法を学びます。

組織の権限の確認

組織のエラスティック構成に対する適切な特権が割り当てられていることを確認します。

エラスティック構成に対する特権によって、Administrator および Monitor の [エラスティッククラスタ] ページへのアクセスレベルは異なります。

エラスティック構成の表示とエラスティッククラスタの監視を行うには、少なくとも読み取り権限が必要です。

AWS サブスクリプションの確認

AWS 環境でエラスティッククラスタを作成するために必要な AWS サブスクリプションがあることを確認します。

Data Integration Elastic では、次のサービスを使用します。

Amazon Elastic Block Service (Amazon EBS)

Amazon EBS ボリュームは、Amazon EC2 インスタンスにローカルストレージとしてアタッチされます。このローカルストレージを使用して、サーバーレス Spark エンジンがエラスティックジョブを実行するために必要とする情報を格納します。例えば、ローカルストレージを使用して、Spark 画像の内容を保存します。また、Spark エンジンでは、データロジックの処理や処理中のデータ保持にもローカルストレージが必要となります。

Amazon Elastic Compute Cloud (Amazon EC2)

エラスティッククラスタをホストする Amazon EC2 インスタンスを開始します。1 つ目の Amazon EC2 インスタンスでマスタノードをホストし、追加のインスタンスでワーカーノードをホストします。

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling は、ジョブ処理の要件に基づいて、エラスティッククラスタ内のクラスタノードを自動的に追加または削除します。

Amazon Elastic Load Balancing (Amazon ELB)

ロードバランサは、Secure Agent からの受信エラスティックジョブを受け入れ、エラスティッククラスタへのジョブのエントリポイントを提供します。

Amazon Identity and Access Management (IAM)

AWS IAM は、Data Integration Elastic が AWS 環境でどのサービスとリソースを使用できるかを指定するためのアクセス制御を提供します。

Amazon Route 53

エラスティッククラスタのノードが Route 53 を使用した同じクラスタ内の他のノードに情報を伝達します。

Amazon Simple Storage Service (Amazon S3)

エラスティッククラスタは、Amazon S3 バケット内にステージングされます。また、Amazon S3 を使用して、エラスティックジョブに生成されるログを格納します。

AWS 環境でのロールとポリシーの確認

Secure Agent とエラスティッククラスタでは、IAM ロールとそれらのロールにアタッチする IAM ポリシーを使用して、AWS 環境のデータにアクセスして処理します。例えば、エージェントとクラスタはロールを使用して、EC2 インスタンスなどのクラウドリソースを管理し、ステージング、ログ、初期化スクリプトファイルなどの S3 上のデータにアクセスします。

ロール

AWS 環境では、次の IAM ロールを使用します。

クラスタオペレータロール

クラスタオペレータロールは、エラスティッククラスタをホストするクラウドリソースを管理するための昇格された権限を持つ IAM ロールです。

Secure Agent ロール

Secure Agent ロールは、Secure Agent の IAM ロールです。この IAM ロールは、Secure Agent が実行される Amazon EC2 インスタンスである Secure Agent マシンにアタッチされます。

Secure Agent は、Secure Agent ロールを使用して、エラスティッククラスタを管理するクラスタオペレータロールを引き受けます。また、Secure Agent は、Secure Agent ロールを使用して、ジョブを処理し、クラウド上の一部のリソースにアクセスします。

マスタロール

マスタロールは、エラスティッククラスタのマスタノードの権限を定義する IAM ロールです。

ワーカーロール

ワーカーロールは、エラスティッククラスタのワーカーノードの権限を定義する IAM ロールです。

ロールの詳細については、[「IAM ロールの作成」 \(ページ 27\)](#)を参照してください。

ポリシー

各 IAM ロールは、1 つ以上の IAM ポリシーを使用します。

次の表に、各ポリシーについてと、それぞれのポリシーで使用されるロールについて説明します。

ポリシー	ロールでの使用	説明
cluster_operator_policy	クラスタオペレータロール	必須。エラスティッククラスタのクラウドリソースを作成および管理するための最小限の権限を提供します。
assume_role_agent_policy	Secure Agent ロール	必須。Secure Agent が Secure Agent ロールを使用して、クラスタオペレータロールを引き受けることを許可します。
data_source_access_policy	Secure Agent ロール ワーカーロール	Amazon データソースにロールベースのセキュリティを使用していて、一意のポリシーを作成する場合に必要です。エラスティックジョブの Amazon データソースへのアクセスを提供します。
log_access_agent_policy	Secure Agent ロール	Secure Agent ロールとワーカーロールの間に信頼関係を構成しない場合に必要です。エラスティックジョブの最後にエージェントのジョブログをアップロードするために、ログの場所へのアクセスを提供します。
minimal_master_policy	マスタロール	必須。マスタロールに最小限の権限を提供します。
staging_log_access_master_policy	マスタロール	必須。ステージングとログの場所へのアクセスを提供します。
init_script_master_policy	マスタロール	初期化スクリプトを使用する場合にのみ必要です。初期化スクリプトパスと、初期化スクリプトおよびクラウド初期化ログを保存する場所へのアクセスを提供します。
minimal_worker_policy	ワーカーロール	必須。ワーカーロールに最小限の権限を提供します。
ebs_autoscaling_worker_policy	ワーカーロール	EBS ボリュームが自動スケールの場合にのみ必要。EBS ボリュームの自動スケールを実行するための権限を提供します。

ポリシー	ロールでの使用	説明
staging_log_access_worker_policy	ワーカーロール	必須。ステージングとログの場所へのアクセスを提供します。
init_script_worker_policy	ワーカーロール	初期化スクリプトを使用する場合にのみ必要です。初期化スクリプトパスと、初期化スクリプトおよびクラウド初期化ログを保存する場所へのアクセスを提供します。

リソースへのアクセスの詳細

データを処理するために、Secure Agent およびエラスティッククラスタは、クラウドプラットフォーム上のリソース、ソースおよびターゲットデータ、ステージングおよびログの場所などの、エラスティックジョブの一部であるリソースにアクセスします。

リソースへのアクセスは実行されるタスクによって異なります。

- エラスティックマッピングの設計
- エラスティッククラスタの作成
- エラスティックジョブの実行
- ログのポーリング

エラスティックマッピングの設計

エラスティックマッピングの設計は、データ統合でのエラスティックマッピング以外のマッピングの設計に似ています。マッピングを設計すると、Secure Agent はソースとターゲットにアクセスするため、ユーザーはデータの読み取りと書き込みができます。

例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで使用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

Secure Agent は、ジョブで使用されるコネクタのタイプに基づいて、ソースおよびターゲットにアクセスします。

Amazon データソースへの直接アクセスを持つコネクタ

マッピングが Amazon データソースへの直接アクセスがあるコネクタを使用する場合、Secure Agent はロールベースのセキュリティまたは資格情報ベースのセキュリティを使用してソースまたはターゲットにアクセスします。ロールベースのセキュリティの場合、Secure Agent は Secure Agent ロールを使用してデータソースにアクセスします。接続レベルで IAM ロールを指定すると、エージェントはランタイムにデータソースにアクセスするために接続レベルのロールを引き受けます。資格情報ベースのセキュリティの場合、Secure Agent は接続レベルの AWS 資格情報を介してソースまたはターゲットにアクセスします。

Amazon データソースへの直接アクセスがないコネクタ

マッピングが Amazon データソースへの直接アクセスがあるコネクタを使用しない場合、Secure Agent は接続プロパティを使用してソースまたはターゲットにアクセスします。例えば、Secure Agent は接続プロパティ内に指定するユーザー名およびパスワードを使用してデータベースにアクセスすることがあります。

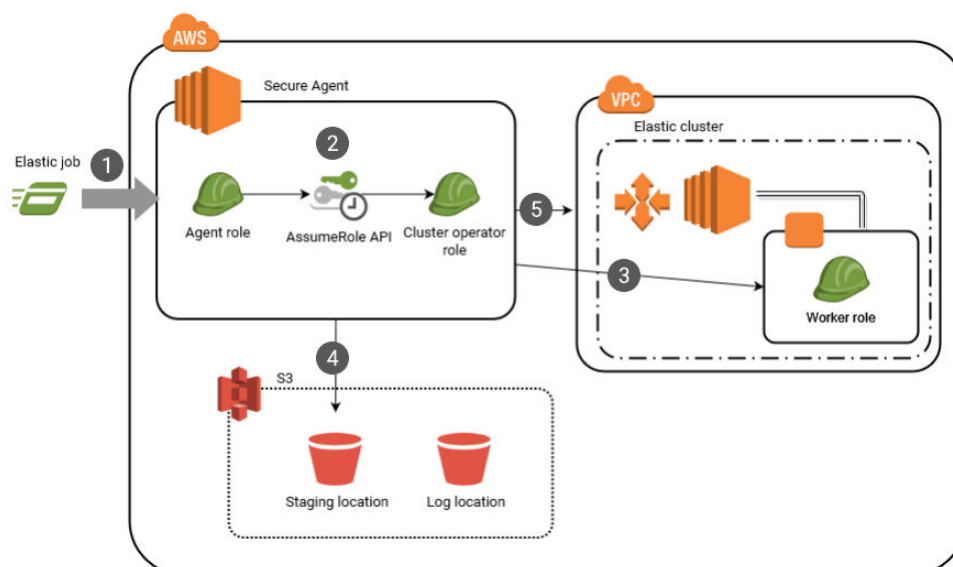
エラスティッククラスタの作成

エラスティッククラスタを作成するために、Secure Agent は、クラスタリソースを作成するための要求を AWS に送信する前に、ステージングの場所とログの場所にアクセスします。

Secure Agent は、クラスタオペレータロールの権限を使用して、次のタスクを実行します。

- ユーザー定義のマスタロールおよびワーカーロールを設定する場合は、ステージングの場所およびログの場所へのワーカーロールのアクセス権を検証する。
- ステージングの場所にクラスタ情報を保存する。
- AWS でクラスタリソースを作成する。

次の図は、Secure Agent がクラスタを作成するときの一連のイベントを示しています。



1. エラスティックジョブを実行します。
2. Secure Agent は、Secure Agent ロールを使用して AWS に対する昇格した権限を取得し、クラスタオペレータロールを引き受けます。
3. ユーザー定義のマスタロールおよびワーカーロールを設定する場合、Secure Agent ではクラスタオペレータロールを使用してワーカーロールを引き受けます。Secure Agent は、ワーカーロールの権限を使用して、クラスタがステージングの場所およびログの場所へのアクセス権を持っているか確認します。
4. Secure Agent が、ステージングの場所にクラスタ情報を保存します。
5. Secure Agent がエラスティッククラスタを作成します。

Amazon データソースへの直接アクセスを持つジョブの実行

エラスティックジョブが Amazon データソースへ直接アクセスできるコネクタを使用している場合、ジョブは資格情報ベースのセキュリティまたはロールベースのセキュリティを使用して Amazon リソースにアクセスします。

Amazon リソースは、セキュリティタイプに基づいて次の方法でアクセスされます。

資格情報ベースのセキュリティ

資格情報ベースのセキュリティを実装する場合、接続レベルの AWS 資格情報が、Amazon データソースおよびステージングの場所などの Amazon リソースへのアクセスに使用されます。ログの場所にアクセスするために、ワーカーロールが使用されます。

資格情報ベースのセキュリティは、ロールベースのセキュリティよりも優先されます。ジョブのソースまたはターゲットによって AWS 資格情報が提供される場合、ステージングの場所にアクセスするためにこの資格情報が再利用されます。例えば、ジョブで JDBC V2 ソースと Amazon S3 V2 ターゲットが使用される場合、S3 ターゲットにアクセスするために使用される AWS 資格情報が、このジョブのステージングの場所にアクセスするために再利用されます。

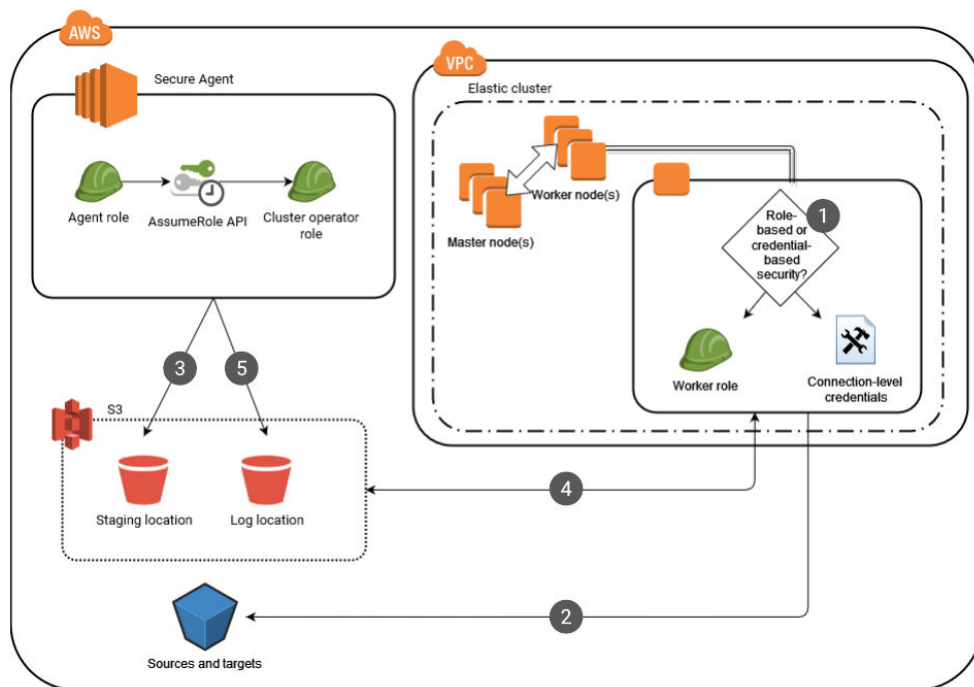
ロールベースのセキュリティ

ロールベースのセキュリティを実装する場合、ユーザー定義またはデフォルトのワーカーロールアクセスが、Amazon データソース、ステージングの場所およびログの場所などの Amazon リソースへのアクセスに使用されます。

注: デフォルトのマスタロールおよびワーカーロールを使用する場合は、Secure Agent ロールにアタッチされるポリシーがワーカーロールに渡されます。ワーカーロールに渡されるポリシーによって、Amazon リソースにワーカーロールに対するアクセス権が付与されます。

ジョブが完了すると、Secure Agent ではログの場所にアクセスしてエージェントジョブのログをアップロードします。Secure Agent は、Secure Agent ロールを使用してログの場所にアクセスします。

次の画像に、ジョブをエラスティッククラスタで実行するときのリソースへのアクセス方法について示します。



1. ジョブを実行するために、ワーカーノードはロールベースのセキュリティまたは資格情報ベースのセキュリティのいずれかを介して Amazon リソースにアクセスします。資格情報ベースのセキュリティを使

- 用する場合、ワーカーノードは接続レベルの AWS 資格情報を使用します。ロールベースのセキュリティを使用する場合、ワーカーノードはワーカーロールを使用します。
2. ワーカーノードは接続レベルの AWS 資格情報またはワーカーロールを使用して、ソースおよびターゲットデータにアクセスします。
 3. Secure Agent によって、クラスタオペレータロールを使用してステージングの場所にジョブの依存関係が保存されます。
 4. ワーカーノードは接続レベルの AWS 資格情報またはワーカーロールを使用して、ジョブの依存関係を取得し、ステージングの場所でデータをステージングします。ワーカーノードはワーカーロールを使用してログの場所にログを保存します。
 5. Secure Agent によって、Secure Agent ロールを使用して、エージェントジョブのログがログの場所にアップロードされます。

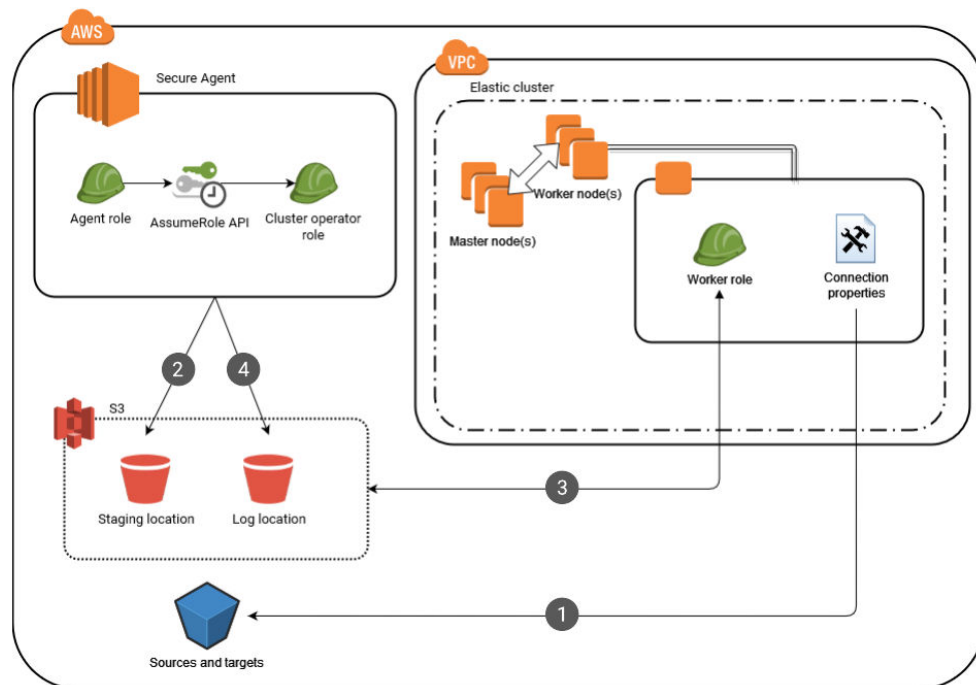
Amazon データソースへの直接アクセスを持たないジョブの実行

エラスティックジョブが Amazon データソースへの直接アクセスがあるコネクタを使用しない場合、そのジョブは、接続プロパティおよびワーカーロール内の権限を使用して、ジョブリソースにアクセスします。

次の表に、各リソースへのアクセス方法を示します。

リソース	アクセスに使用される手段
ソースおよびターゲット	接続プロパティ。 例えば、接続プロパティ内に提供するユーザー名およびパスワードが Amazon Aurora のデータベースへのログインに使用される場合があります。
ステージングの場所	ユーザー定義またはデフォルトのワーカーロール。
ログの場所	ジョブの実行時のユーザー定義またはデフォルトのワーカーロール。 ジョブの完了時の Secure Agent ロール。 Secure Agent は、ログの場所にアクセスしてエージェントジョブのログをアップロードする必要があります。ログの場所にアクセスするには、エージェントで Secure Agent ロールを使用します。

次の画像に、ジョブをエラスティッククラスタで実行するときのリソースへのアクセス方法について示します。



1. ワーカーノードは接続プロパティを使用してソースおよびターゲットデータにアクセスします。
2. Secure Agent によって、クラスタオペレーターロールを使用してステージングの場所にジョブの依存関係が保存されます。
3. ワーカーノードはワーカーロールを使用して、ステージングの場所からジョブの依存関係を取得し、ステージングの場所のデータをステージングし、ログの場所にログを保存します。
4. Secure Agent によって、Secure Agent ロールを使用して、エージェントジョブのログがログの場所にアップロードされます。

注: ジョブ内のいずれかのコネクタがソースまたはターゲットへの直接アクセスに AWS 資格情報を使用する場合、接続レベルの AWS 資格情報が、ステージングの場所へのアクセス権を取得するためにワーカーロールよりも優先されます。

ログのポーリング

Monitor を使用すると、Secure Agent はログの場所にアクセスしてログをポーリングします。

Secure Agent は、ジョブで使用されるコネクタのタイプに基づいて、ログをポーリングします。

Amazon データソースへの直接アクセスを持つコネクタ

ジョブで Amazon データソースに直接アクセスできるコネクタを使用する場合、Secure Agent は資格情報ベースのセキュリティまたはロールベースのセキュリティのいずれかを使用してログの場所にアクセスします。資格情報ベースのセキュリティの場合、Secure Agent は接続レベルの AWS 資格情報を介してログをポーリングします。ロールベースのセキュリティの場合、Secure Agent では Secure Agent ロールの権限を使用してログをポーリングします。

Amazon データソースへの直接アクセスがないコネクタ

ジョブが Amazon データソースへの直接アクセスがあるコネクタを使用しない場合、Secure Agent は Secure Agent ロールの権限を介してログをポーリングします。

クラスタファイルの格納場所の作成

Amazon S3 で、ステージング、ログ、および初期化スクリプトファイルを保存する場所を作成します。

次の格納場所を作成します。

- クラスタがランタイムにステージングファイルを保存するために使用する場所
- クラスタ上で実行されるエラスティックジョブ用のログファイルを保存するためにクラスタが使用する場所
- オプションで、クラスタに追加のソフトウェアをインストールするためにクラスタノードが実行する初期化スクリプトを格納できる場所

ステージングの場所には、クラスタがクラスタノード全体に配布するアーティファクトやマッピングでプレビューするデータなどの一時データが格納されます。エラーにより、マッピングでステージングの場所のプレビューデータをクリアできない可能性があるため、ステージングの場所にアクセスできるユーザーがソースデータの表示を許可されていることを確認してください。

初期化スクリプトを作成する場合は、スクリプトを適切な場所に追加します。

VPC とサブネットの作成（オプション）

エラスティッククラスタをホストする固有の VPC およびサブネットを作成する場合、クラスタの要件に基づいて VPC およびサブネットを準備します。

以下のタスクを完了させます。

- エラスティッククラスタ内のエラスティックロードバランサおよびノードを支援するために、十分な数の IP アドレスをサポートするサブネットを作成します。
- VPC およびサブネットがクラスタで要求を転送できるように、ルーティング設定を確認します。
- Spark ドライバが Secure Agent と通信できるように、Secure Agent マシンで受信トラフィックを承認します。

十分な数の IP アドレスを含むサブネットの作成

エラスティッククラスタ内のエラスティックロードバランサおよびノードを支援するために、十分な数の IP アドレスをサポートするサブネットを作成します。

次のガイドラインに従い、サブネットごとに必要な IP アドレスの数を計算します。

1. エラスティックロードバランサが適切にスケーリングできるようにするために、IP アドレスを 8 つ追加します。
2. マスターノード用に IP アドレスを 1 つ追加します。可用性の高いクラスタを使用する場合、代わりに IP アドレスを 3 つ追加します。
3. ワーカーノードの最大数と同数の IP アドレスを追加します。

例えば、エラスティッククラスタで最大 10 のワーカーノードを使用できる場合、各サブネットで少なくとも 19 の IP アドレスをサポートする必要があります。

ルーティング設定の確認

VPC およびサブネットがエラスティッククラスタの要求をルーティングできることを確認します。

VPC およびサブネットが要求をルーティングできるようにするには、AWS で次の項目を確認します。

- VPC には、ルートテーブル、インターネットゲートウェイ、ネットワーク ACL など、必要なすべてのネットワークコンポーネントが含まれます。
- DNS ホスト名および DNS 解決は有効です。
- ルートテーブルでは、EC2 インスタンスが VPC に接続されたインターネットゲートウェイを使用できます。

詳細については、AWS のマニュアルを参照してください。

受信トラフィックの承認

Spark ドライバが Secure Agent と通信できるように、Secure Agent マシンで受信トラフィックを承認します。

以下のタスクを完了させます。

1. Secure Agent マシンに接続された AWS セキュリティグループにインバウンドルールを追加します。
2. インバウンドトラフィックを承認するようにポート 0-65535 を指定します。
3. CIDR 注釈で VPC を指定します。

Amazon EC2 のユーザー定義のセキュリティグループの作成

ELB、マスタ、ワーカーのセキュリティグループを作成して、AWS 環境のセキュリティ設定を微調整します。セキュリティグループごとに適切な受信ルールと送信ルールを構成します。これらのタスクを完了した後、エラスティック構成のセキュリティグループを指定できます。

すばやく設定したい場合は、Secure Agent が作成するデフォルトのセキュリティグループを使用できます。詳細については、[「デフォルトのセキュリティグループの使用 \(代替\)」 \(ページ 25\)](#) を参照してください。デフォルトのセキュリティグループとユーザー定義のセキュリティグループを組み合わせることはできません。例えば、ユーザー定義の ELB セキュリティグループを作成する場合は、ユーザー定義のマスタセキュリティグループとワーカーセキュリティグループも作成する必要があります。

Amazon EC2 向けのセキュリティグループを作成する方法の詳細については、AWS のマニュアルを参照してください。

ELB セキュリティグループの作成

ELB セキュリティグループでは、Kubernetes API サーバーとエラスティッククラスタの外部にあるクライアント間の受信ルールを定義します。また、Kubernetes API サーバーとクラスタノード間の送信ルールも定義します。このセキュリティグループは、エージェントがエラスティッククラスタにプロビジョニングするロードバランサにアタッチされます。

受信ルール

受信ルールは、HTTPS を使用して Kubernetes API サーバーにアクセスできるエラスティッククラスタの外部のノードを識別します。

受信ルールでは、次のトラフィックを許可する必要があります。

- エラスティッククラスタを作成する Secure Agent からの受信トラフィック。
- 同じクラスタ内のマスタノードからの受信トラフィック。
- 同じクラスタ内のワーカーノードからの受信トラフィック。

次の図に、必要な受信ルールを示します。

Inbound rules (3)							
Filter security group rules							
	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	sgr-072b989330211b389	-	HTTPS	TCP	443	sg-06a5d3ae5439a983a / nodes-5aj...	From worker security group protocol [443] and port [443].
<input type="checkbox"/>	sgr-0184592fb5c66751b	IPv4	HTTPS	TCP	443		Agent API access
<input type="checkbox"/>	sgr-07c4d8d97ccd81e5d	-	HTTPS	TCP	443	sg-0b4f93297a739d4b3 / masters-5...	From master security group protocol [tcp] and port [443].

送信ルール

デフォルトの送信ルールを使用して、すべての送信トラフィックを許可します。

このルールの宛先を制限することはできますが、宛先にはクラスタ内のすべてのマスタノードへの HTTPS トラフィックが含まれている必要があります。

マスタセキュリティグループの作成

マスタセキュリティグループは、エラスティッククラスタ、ELB セキュリティグループ、および Secure Agent のマスタノードとワーカーノード間の受信ルールを定義します。また、他のノードへの送信ルールも定義します。このセキュリティグループは、クラスタのすべてのマスタノードにアタッチされます。

受信ルール

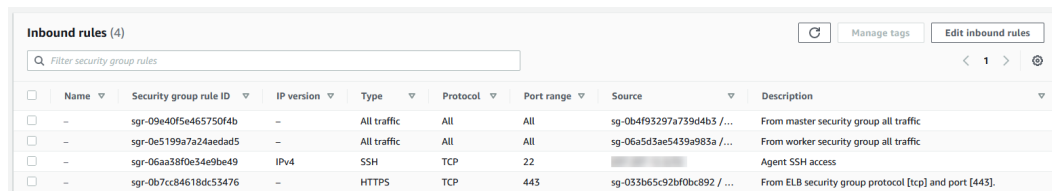
受信ルールでは、次のトラフィックを許可する必要があります。

- 同じクラスタ内のワーカーノードからの受信トラフィック。例えば、クラスタの内外にネットワークトラフィックを転送する「kubernetes」という名前のサービスまたは kube-proxy を介して API サーバーにアクセスするワーカーノードなどです。ポート範囲が 1024 から 65535 のカスタム TCP と UDP、およびポート 443 の TCP を使用する HTTPS のルールを設定することで、ワーカーノードの受信ルールを簡略化できます。
- 同じクラスタ内の他のマスタノードからの受信トラフィック。
- 同じクラスタ内の ELB セキュリティグループから、ポート 443 で HTTPS over TCP を使用する受信トラフィック。
- ポート 22 を介した SSH を使用した受信トラフィック。

ユーザー定義のマスタセキュリティグループを作成して使用する場合、Secure Agent は、クラスタの外部からの SSH アクセスに関する次のデフォルトルールを無視します。

- SSH プロトコルを使用してポート 22 を介してワーカーノードに接続できる、クラスタの作成元である Secure Agent の IP アドレス。
- カスタムプロパティを使用してソースクラスレスドメイン間ルーティング（CIDR）アドレスを設定する機能。
- カスタムプロパティを使用した SSH ポートの設定。
- カスタムプロパティを使用して、パブリックキーのエージェントノードにローカルファイルパスを設定する機能。

次の図に、必要な受信ルールを示します。



<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-09e40f5e465750f4b	-	All traffic	All	All	sg-0b4f93297a739d4b3 / ...	From master security group all traffic
<input type="checkbox"/>	-	sgr-0e5199a7a24aedad5	-	All traffic	All	All	sg-06a5d3ae5439a983a / ...	From worker security group all traffic
<input type="checkbox"/>	-	sgr-06aa38f0e34e9be49	IPv4	SSH	TCP	22	[REDACTED]	Agent SSH access
<input type="checkbox"/>	-	sgr-0b7cc84618dc53476	-	HTTPS	TCP	443	sg-035b65c92bf0bc892 / ...	From ELB security group protocol [tcp] and port [443].

送信ルール

デフォルトの送信ルールを使用して、すべての送信トラフィックを許可します。

マスタノードからの送信トラフィックには、他のマスタノード、ELB セキュリティグループ、ワーカーノード、Secure Agent、Amazon S3、EC2、IAM などの AWS 上のその他のマネージドサービス、その他のストレージサービス、およびその他のパブリックサービスを含めることができます。

ワーカーセキュリティグループの作成

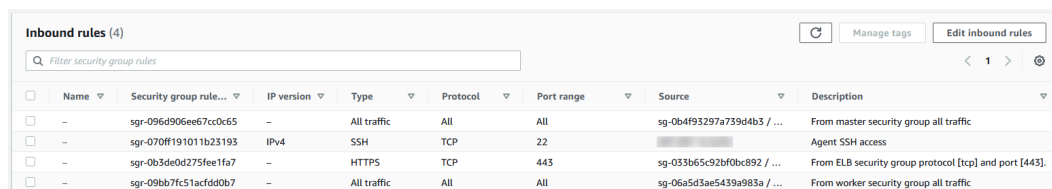
ワーカーセキュリティグループは、エラスティッククラスタおよびその他のノードで、ワーカーノード間の受信ルールと送信ルールを定義します。このセキュリティグループは、クラスタのすべてのワーカーノードにアタッチされます。

受信ルール

受信ルールでは、次のトラフィックを許可する必要があります。

- クラスタ内の他のワーカーノードからの受信トラフィック。例えば、関連するポッド間の通信などです。
- クラスタ内の任意のマスタノードからの受信トラフィック。例えば、マスタノードはワーカーノードの kubelet に接続して、ログを取得したり、ポート転送をサポートしたりします。
- 同じクラスタ内の ELB セキュリティグループからの、ポート 443 の TCP による HTTPS を使用した受信トラフィック。
- クラスタの外部からの受信 SSH アクセス。このルールは、マスタセキュリティグループに対して定義された SSH 受信ルールと同一であり、SSH を使用してワーカーノードにアクセスする場合にのみ必要です。

次の図に、必要な受信ルールを示します。



<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-09e40f5e465750f4b	-	All traffic	All	All	sg-0b4f93297a739d4b3 / ...	From master security group all traffic
<input type="checkbox"/>	-	sgr-070f191011b23193	IPv4	SSH	TCP	22	[REDACTED]	Agent SSH access
<input type="checkbox"/>	-	sgr-0b3de0d275fee1fa7	-	HTTPS	TCP	443	sg-035b65c92bf0bc892 / ...	From ELB security group protocol [tcp] and port [443].
<input type="checkbox"/>	-	sgr-09bb7fc51acfd0b7	-	All traffic	All	All	sg-06a5d3ae5439a983a / ...	From worker security group all traffic

送信ルール

デフォルトの送信ルールを使用して、すべての送信トラフィックを許可します。

ワーカーノードからの送信トラフィックには、ELB セキュリティグループ、マスタノード、他のワーカーノード、Secure Agent、Amazon S3、EC2、および IAM などの AWS 上のその他のマネージドサービス、その他のストレージサービス、およびその他のパブリックサービスを含めることができます。さらに、送信ルールでは、エラスティックジョブが Redshift や Snowflake データベースなどのデータソース、および Secure Agent が公開する REST エンドポイントなどの外部サービスと通信できるようにする必要があります。

デフォルトのセキュリティグループの使用（代替）

Secure Agent は、エラスティッククラスタを作成するときに、デフォルトの ELB セキュリティグループ、マスタセキュリティグループ、およびワーカーセキュリティグループを生成できます。これらのデフォルトのセ

セキュリティグループは、Kubernetes クライアント、API サーバー、マスタノード、ワーカーノード、およびその他のサービス間の通信ガイドラインを定義します。

Secure Agent がデフォルトのセキュリティグループを生成できるようにするには、クラスタオペレータロールのクラスタオペレータポリシーに次の権限が必要です。

```
ec2:DescribeSecurityGroups
ec2:CreateSecurityGroup
ec2:DeleteSecurityGroup
ec2:AuthorizeSecurityGroupEgress
ec2:AuthorizeSecurityGroupIngress
ec2:RevokeSecurityGroupEgress
ec2:RevokeSecurityGroupIngress
```

クラスタオペレータロールとクラスタオペレータポリシーの詳細については、[「IAM ロールの作成」](#) (ページ 27) を参照してください。

Secure Agent のダウンロードとインストール

Amazon EC2 インスタンスの Linux 仮想マシンに Secure Agent をダウンロードおよびインストールします。この EC2 インスタンスは、Secure Agent マシンと呼ばれます。

次の表に、Secure Agent マシンの最小リソース要件を一覧表示します。

コンポーネント	最小要件
CPU あたりのコア数	4 以上
メモリ	16GB
ディスク空き容量	100GB

Secure Agent をインストールした後、Secure Agent マシンに OpenSSL をインストールします。

Secure Agent のインストールに関する詳細については、「ランタイム環境」を参照してください。

AWS のドメインのホワイトリスト登録

Secure Agent が AWS 環境でエラスティッククラスタを作成する場合、クラスタノードは、マシンイメージなどのアーティファクトを取得し、ソースとターゲットにアクセスするために、特定のドメインにアクセスする必要があります。

次のドメインをホワイトリストに登録します。

```
infacloud.jfrog.io
infacloud-ct-cdie-docker.jfrog.io
infacloud-discale-docker-stable.jfrog.io
discale-docker-stable.artifacts.cloudtrust.rocks
informatica.snowflakecomputing.com
```

```
.s3.amazonaws.com  
.s3.<staging bucket region>.amazonaws.com
```

Amazon S3 または Amazon Redshift オブジェクトをソースまたはターゲットとして使用する場合は、エージェントがアクセスする各ソースおよびターゲットバケットへの受信トラフィックを許可します。

さらに、GPU 対応のワーカーインスタンスを使用する場合は、次のドメインをホワイトリストに登録します。

```
.docker.com  
.docker.io  
.nvidia.com  
.nvidia.github.io
```

また、AWS の適切なリージョンをホワイトリストに登録します。

```
sts.us-east-2.amazonaws.com  
sts.us-west-2.amazonaws.com
```

注: 組織で送信プロキシサーバーを使用していない場合は、Informatica グローバルカスタマサポートに連絡して、S3 アクセスに使用されるプロキシ設定を無効にしてください。

IAM ロールの作成

クラスタオペレータ、Secure Agent、マスタロール、およびワーカーロールを作成し、AWS 環境でクラスタ操作を実行するために各ロールに適切なポリシーを作成します。

IAM ロールを作成するには、次のタスクを完了します。

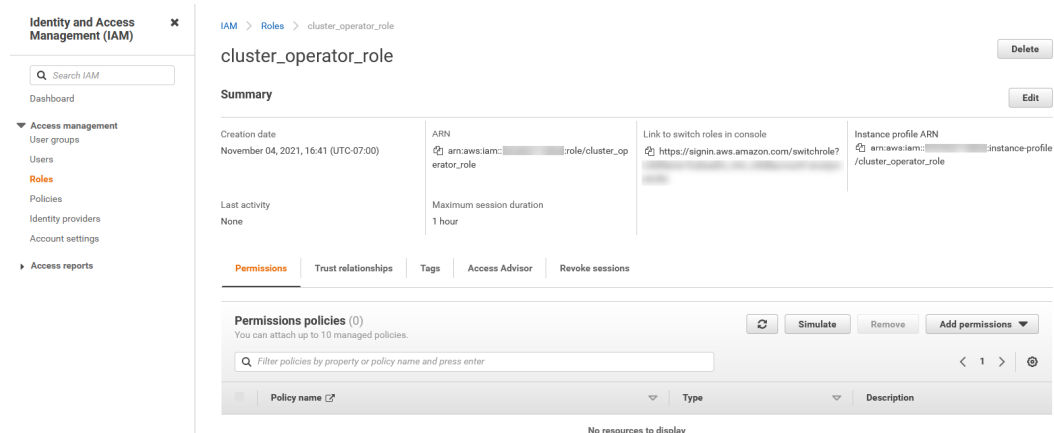
1. クラスタオペレータロールを作成する。
2. クラスタオペレータポリシーを作成する。
3. クラスタオペレータポリシーをクラスタオペレータロールにアタッチする。
4. クラスタオペレータロールの最大 CLI/API セッション期間を設定する。
5. Secure Agent ロールを作成または再利用する。
6. AssumeRole 権限を Secure Agent ロールに追加する。
7. Secure Agent ロールを含めるようにクラスタオペレータロールの信頼関係を設定する。
8. ユーザー定義のマスタおよびワーカーロールを作成する。
9. 必要に応じて、保存時のステージングデータとログファイルを暗号化する。
10. 必要に応じて、Amazon データソースのロールベースのセキュリティポリシーを作成する。
11. Secure Agent ロールのログアクセスポリシーを作成または再利用する。

注: お使いの環境内で Secure Agent の権限を最小限に抑えるには、クラスタオペレータロールを Secure Agent マシンにアタッチしないようにします。

手順 1. クラスタオペレータのロールを作成する

AWS で、クラスタオペレータの IAM ロールを作成します。ロールに `cluster_operator_role` という名前を付けます。

次の図は、AWS マネジメントコンソールでクラスタオペレータロールがどのように表示されるかを示しています。

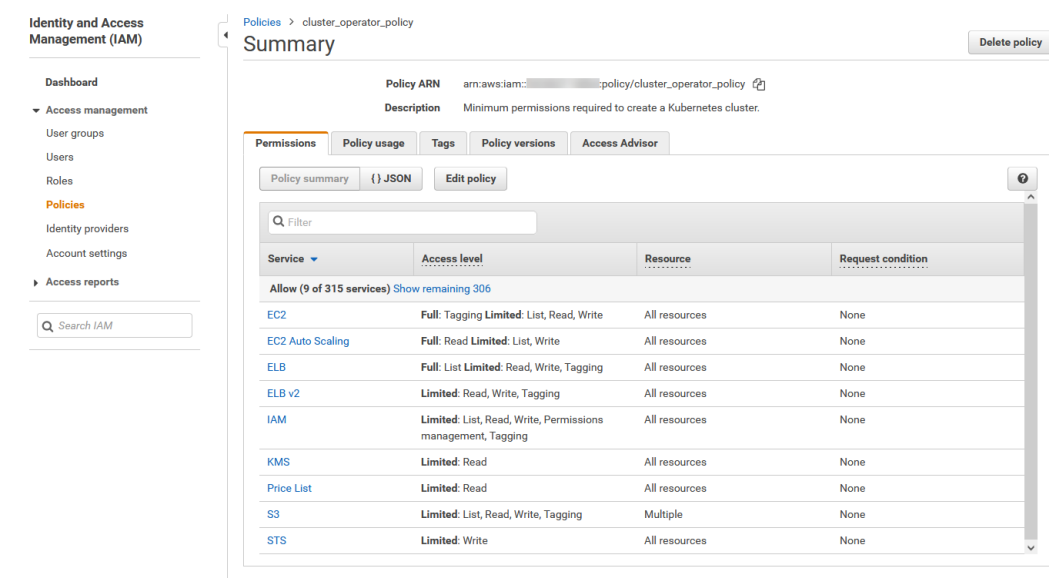


IAM ロールの作成手順については、AWS のドキュメントを参照してください。AWS は、AWS マネジメントコンソールや AWS CLI を使用するなど、IAM ロールを作成する方法をいくつか提供しています。

手順 2. クラスタオペレータポリシーの作成

クラスタオペレータロールの IAM ポリシーを作成します。ポリシーに `cluster_operator_policy` という名前を付けます。クラスタオペレータポリシーには、クラスタオペレータロールがエラスティッククラスタ向けにクラウドリソースを作成および管理するために必要な権限が含まれています。

次の図は、AWS マネジメントコンソールでクラスタオペレータポリシーがどのように表示されるかを示しています。



次の JSON ドキュメントをポリシーのテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetBucketLogging",
        "s3:ListBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketVersioning",
        "s3:GetReplicationConfiguration",
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketCORS",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "s3:GetObjectVersion",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::staging_bucket",
        "arn:aws:s3:::staging_bucket/folder/",
        "arn:aws:s3:::staging_bucket/folder/*",
        "arn:aws:s3:::logging_bucket",
        "arn:aws:s3:::logging_bucket/folder/",
        "arn:aws:s3:::logging_bucket/folder/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInternetGateways",
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:ImportKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:DeleteKeyPair",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DescribeRouteTables",
        "ec2:CreateRouteTable",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteRouteTable",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateVpc",
        "ec2:DeleteVpc",
        "ec2:ModifyVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:CreateSubnet",
        "ec2:DeleteSubnet",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",

```

```

"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:RevokeSecurityGroupEgress",
"ec2:DeleteSecurityGroup",
"ec2:CreateTags",
"ec2:DescribeTags",
"ec2:DeleteTags",
"ec2:CreateVolume",
"ec2:DescribeVolumes",
"ec2:DeleteVolume",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:RunInstances",
"ec2:DescribeInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:DescribeInstanceTypes",
"ec2:TerminateInstances",
"ec2:DescribeRegions",
"ec2:DescribeAvailabilityZones",
"ec2:CreateLaunchTemplate",
"ec2:DescribeLaunchTemplateVersions",
"ec2:DescribeLaunchTemplates",
"ec2:DeleteLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:DeleteLaunchTemplateVersions",
"autoscaling:AttachLoadBalancers",
"autoscaling:DescribeTags",
"autoscaling:CreateAutoScalingGroup",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeScalingActivities",
"autoscaling:UpdateAutoScalingGroup",
"autoscaling:DeleteAutoScalingGroup",
"autoscaling:TerminateInstanceInAutoScalingGroup",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:AttachLoadBalancerToSubnets",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:CreateLoadBalancerListeners",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"pricing:GetProducts",
"iam:GetInstanceProfile",
"iam:GetContextKeysForPrincipalPolicy",
"iam:ListInstanceProfiles",
"iam:SimulatePrincipalPolicy",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:CreateRole",
"iam:GetRole",
"iam:ListRoles",
"iam:PassRole",
"iam:ListRolePolicies",
"iam:CreateServiceLinkedRole",
"iam:DeleteRole",
"iam:GetRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfilesForRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:PutRolePolicy",
"iam:AttachRolePolicy",
"iam:DetachRolePolicy",

```

```

        "iam:DeleteRolePolicy",
        "iam:GetUser",
        "kms:DescribeKey",
        "kms:Get*",
        "sts:AssumeRole",
        "sts:DecodeAuthorizationMessage"
    ],
    "Resource": "*"
}
]
}

```

組織の要件に基づいて、テンプレートに権限を追加します。各権限については、[「AWS ポリシーの詳細参照」\(ページ 49\)](#)を参照してください。

Amazon S3 でのアクションは、エラスティック構成で指定したすべてのステージング、ログ、および初期化スクリプトの場所に対して指定する必要があります。

例えば、ステージングの場所 dev/Stageing/、ログの場所 dev/Logging/、および初期化スクリプトの場所 dev/InitScript/を使用する場合、ポリシーでは、Amazon S3 でのアクションに関する次のリソースを一覧表示する必要があります。

```

"Resource": [
    "arn:aws:s3:::dev",
    "arn:aws:s3:::dev/Staging/",
    "arn:aws:s3:::dev/Staging/*",
    "arn:aws:s3:::dev/Logging/",
    "arn:aws:s3:::dev/Logging/*",
    "arn:aws:s3:::dev/InitScript/",
    "arn:aws:s3:::dev/InitScript/*"
]

```

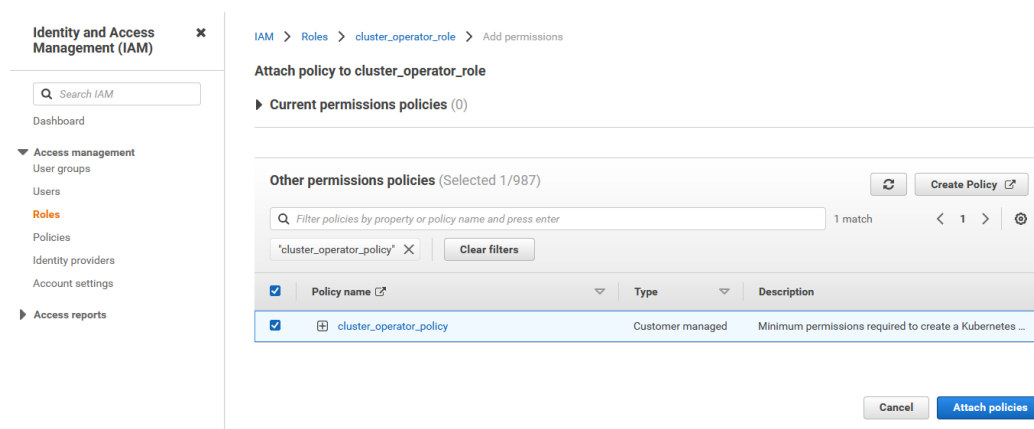
別のエラスティック構成でステージング、ログ、および初期化スクリプトの場所の異なるセットを使用する場合、これらの場所をリソースとして同じポリシーに追加する必要があります。

頻繁に変更される S3 の場所に対応するために、ワイルドカードを使用できます。詳細については、AWS のマニュアルを参照してください。

手順 3。クラスタオペレータポリシーのアタッチ

AWS で、IAM ポリシー `cluster_operator_policy` を IAM ロール `cluster_operator_role` にアタッチします。

次の図は、クラスタオペレータポリシーをクラスタオペレータロールにアタッチしたときに AWS マネジメントコンソールがどのように表示されるかを示しています。



手順 4. クラスタオペレータロールの最大 CLI/API セッション期間の設定

IAM ロール `cluster_operator_role` で CLI/API セッションの最長時間を 30 分以上に設定します。

時間を長くすると、Secure Agent は単一のセッション内でクラウドリソースにアクセスできる時間が長くなり、エラスティッククラスタでより長いジョブを実行できます。

詳細については、AWS のマニュアルを参照してください。

手順 5. Secure Agent ロールの作成または再利用

Secure Agent では、ジョブの実行中に特定のクラウドリソースにアクセスするために IAM ロールを必要とします。この IAM ロールは、Secure Agent がインストールされている Amazon EC2 インスタンスにアタッチされます。

Secure Agent ロールを作成または再利用できます。この IAM ロールに `agent_role` と名前を付けます。

Secure Agent ロールの作成

Secure Agent ロールを作成するには、AWS で次のタスクを実行します。

1. `agent_role` の名前で IAM ロールを作成します。
2. IAM ロール `agent_role` を Secure Agent がインストールされている Amazon EC2 インスタンスにアタッチします。

Secure Agent ロールの再利用

Secure Agent がインストールされている Amazon EC2 インスタンスにアタッチされた IAM ロールをすでに作成している場合は、IAM ロールを Secure Agent ロールとして指定できます。

手順 6. AssumeRole 権限を Secure Agent ロールに追加

Secure Agent は、エラスティッククラスタを管理するための昇格された権限を取得するために、クラスタオペレータロールを引き受ける必要があります。Secure Agent がクラスタオペレータロールを引き受けるには、Secure Agent ロールに AssumeRole 権限が必要です。

AssumeRole 権限を設定するには、AWS で次のタスクを実行します。

1. `assume_role_agent_policy` という名前で次の IAM ポリシーを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::{{account-id}}:role/cluster_operator_role"
  }
}
```

注: Resource 要素の値はクラスタオペレータロールの ARN です。

2. IAM ポリシー `assume_role_agent_policy` を IAM ロール `agent_role` にアタッチします。

手順 7. Secure Agent ロールを含めるようにクラスタオペレータロールの信頼関係を設定

Secure Agent はクラスタオペレータロールを引き受ける必要があるため、クラスタオペレータロールは Secure Agent を信頼する必要があります。

IAM ロール `cluster_operator_role` の信頼関係を編集し、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"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{{account-id}}:role/agent_role"
      },
      "Action": "sts:AssumeRole",
    }
  ]
}
```

注: Principal 要素の値は Secure Agent ロールの ARN です。

必要に応じて、外部 ID を設定し、クラスタオペレータロールを引き受けることができるエンティティを制限できます。Secure Agent はクラスタオペレータロールを引き受けるよう試行するたびに、毎回外部 ID を指定する必要があります。

例えば、次のポリシーを使用して外部 ID 「123」を設定できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{{account-id}}:role/agent_role"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "123"
        }
      }
    }
  ]
}
```

手順 8. ユーザー定義のマスタロールおよびワーカーロールの作成

ユーザー定義のマスタロールおよびワーカーロールを作成して、エラスティッククラスタ内のマスタノードとワーカーノードの権限を調整します。ノードは、権限を使用して、エラスティックジョブで Spark アプリケー

ションを実行します。上記のタスクが完了した後、エラスティック構成でマスタインスタンスプロファイルおよびワーカーインスタンスプロファイルを指定できます。

すばやく設定したい場合は、デフォルトのマスタロールとワーカーロールを使用できます。詳細については、[「デフォルトのマスタロールと作業ロールの使用（代替）」（ページ 43）](#)および [「マスタとワーカーのロールタイプのリファレンス」（ページ 64）](#)を参照してください。

ユーザー定義のロールを作成するには、以下のタスクを完了します。

1. マスタロールとワーカーロールを作成する。
2. マスタポリシーを作成する。
3. ワーカーポリシーを作成する。
4. マスタロールとワーカーロールにポリシーをアタッチする。
5. クラスタオペレータロールがワーカーロールを引き受けることを許可する。
6. クラスタオペレータロールがマスタロールを引き受けることを許可する。

マスタロールとワーカーロール、インスタンスプロファイル、およびクラスタオペレータロールは、同じ AWS アカウントで定義される必要があります。

Secure Agent は、エラスティッククラスタを開始するときに、クラスタオペレータロールを使用して、インスタンスプロファイルが存在するかどうか、マスタロールとワーカーロールに必要なクラスタディレクトリ（ステージング、ログ、および初期化スクリプトの場所など）へのアクセス権があるかどうかを検証します。検証に失敗すると、クラスタは作成出来ません。

手順 8.1. マスタロールとワーカーロールの作成

AWS で、マスタノードとワーカーノードの IAM ロールを作成します。ロールにそれぞれ `master_role` および `worker_role` と名前を付けます。

マスタロールおよびワーカーロールを作成する場合、AWS は各ロールのインスタンスプロファイルを自動的に生成します。

ポリシーコンテンツで複数のエラスティッククラスタのステージング、ログ、および初期化スクリプトの場所にアクセスする場合、さまざまなエラスティック構成間で同じインスタンスプロファイルを再使用できます。

手順 8.2. マスタポリシーの作成

マスタロールの IAM ポリシーを作成します。インラインポリシーまたは管理対象ポリシーとして各ポリシーを定義できます。

次の表で、各 IAM ポリシーについて説明します。

ポリシー	説明
<code>minimal_master_policy</code>	必須。マスタロールに最小限の権限を提供します。
<code>staging_log_access_master_policy</code>	必須。ステージングとログの場所へのアクセスを提供します。
<code>init_script_master_policy</code>	初期化スクリプトを使用する場合にのみ必要です。初期化スクリプトパスと、初期化スクリプトおよびクラウド初期化ログを保存する場所へのアクセスを提供します。

各権限とそれが必要な理由については、[「AWS ポリシーの詳細参照」（ページ 49）](#)を参照してください。ポリシーの編集の詳細については、[「マスタおよびワーカーポリシーの制限に関するリファレンス」（ページ 65）](#)を参照してください。

注: generate-policies-for-userdefined-roles.sh コマンドを実行してポリシーコンテンツを生成することもできます。コマンドの詳細については、[「generate-policies-for-userdefined-roles.sh」](#) (ページ 148)を参照してください。このコマンドは出力ファイル my-userdefined-master-worker-role-policies.json を作成します。

minimal_master_policy

IAM ポリシー minimum_master_policy は、ユーザー定義のマスタロールの最小要件を示しています。

次の JSON ドキュメントを minimal_master_policy のテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumesModifications",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/KubernetesCluster": "*.k8s.local"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeScalingActivities"
      ],
      "Resource": [
        "*"
      ]
    }
  ],
}
```

```

{
  "Effect": "Allow",
  "Action": [
    "autoscaling:SetDesiredCapacity",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringLike": {
      "autoscaling:ResourceTag/KubernetesCluster": "*.k8s.local"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:AttachLoadBalancerToSubnets",
    "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
    "elasticloadbalancing:ConfigureHealthCheck",
    "elasticloadbalancing>DeleteLoadBalancer",
    "elasticloadbalancing>DeleteLoadBalancerListeners",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DetachLoadBalancerFromSubnets",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:ModifyLoadBalancerAttributes",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringLike": {
      "elasticloadbalancing:ResourceTag/KubernetesCluster": "*.k8s.local"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup",
    "elasticloadbalancing:DeregisterTargets",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:ModifyTargetGroup",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringLike": {
      "elasticloadbalancing:ResourceTag/KubernetesCluster": "*.k8s.local"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [

```

```

        "iam:ListServerCertificates",
        "iam:GetServerCertificate"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:Get*"
    ],
    "Resource": [
        "arn:aws:s3:::<cluster-staging-dir1>/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

staging_log_access_master_policy

IAM ポリシー `staging_log_access_master_policy` は、ステージングの場所とログの場所へのアクセスを提供します。

次の JSON ドキュメントを `staging_log_access_master_policy` のテンプレートとして使用できます。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetEncryptionConfiguration",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<cluster-staging-bucket-name1>",
                "arn:aws:s3:::<cluster-logging-bucket-name1>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::<cluster-staging-dir1>/*",
                "arn:aws:s3:::<cluster-logging-dir1>/*"
            ]
        }
    ]
}

```

init_script_master_policy

IAM ポリシー `init_script_master_policy` は、クラスタコンピューティングシステムがマスタノードにクラスタの初期化スクリプトディレクトリおよび初期化スクリプトログディレクトリへのアクセスを許可するために必要になります。

次の JSON ドキュメントを `init_script_master_policy` のテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-init-script-bucket-name>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-init-script-dir>/*"
      ]
    }
  ]
}
```

手順 8.3. ワーカーポリシーの作成

ワーカーロールの IAM ポリシーを作成します。インラインポリシーまたは管理対象ポリシーとして各ポリシーを定義できます。

次の表で、各 IAM ポリシーについて説明します。

ポリシー	説明
<code>minimal_worker_policy</code>	必須。ワーカーロールに最小限の権限を提供します。
<code>ebs_autoscaling_worker_policy</code>	EBS ボリュームが自動スケールの場合にのみ必要。
<code>staging_log_access_worker_policy</code>	必須。ステージングとログの場所へのアクセスを提供します。
<code>init_script_worker_policy</code>	初期化スクリプトを使用する場合にのみ必要です。初期化スクリプトパスと、初期化スクリプトおよびクラウド初期化ログを保存する場所へのアクセスを提供します。

各権限とそれが必要な理由については、[「AWS ポリシーの詳細参照」](#) (ページ 49)を参照してください。ポリシーの編集の詳細については、[「マスタおよびワーカーポリシーの制限に関するリファレンス」](#) (ページ 65)を参照してください。

注: `generate-policies-for-userdefined-roles.sh` コマンドを実行してポリシーコンテンツを生成することもできます。コマンドの詳細については、[「generate-policies-for-userdefined-roles.sh」](#) (ページ 148)を参照してください。このコマンドは出力ファイル `my-userdefined-master-worker-role-policies.json` を作成します。

minimal_worker_policy

IAM ポリシー `minimal_worker_policy` は、ユーザー定義のワーカーロールの最小要件を一覧表示します。

次の JSON ドキュメントを `minimal_worker_policy` のテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-staging-dir1>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

ebs_autoscaling_worker_policy

IAM ポリシー `ebs_autoscaling_worker_policy` は、EBS ボリュームを自動スケーリングするために、ワーカーノードで必要になります。

次の JSON ドキュメントを `ebs_autoscaling_worker_policy` のテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeVolumes",
        "ec2:CreateVolume",
        "ec2:ModifyInstanceAttribute"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
    {
      "Action": [
        "ec2:CreateTags"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/KubernetesCluster": "*.k8s.local"
        }
      },
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/CREATED_BY": "infa-storage-scalerd-*"
        }
      },
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  ]
}
```

staging_log_access_worker_policy

IAM ポリシー `taging_log_access_worker_policy` は、クラスタコンピューティングシステムがワーカーノードにステージングディレクトリおよびログディレクトリへのアクセスを許可するために必要になります。

次の JSON ドキュメントを `staging_log_access_worker_policy` のテンプレートとして使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```



```

        "Action": [
            "s3:GetBucketLocation",
            "s3:GetEncryptionConfiguration",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::<cluster-staging-bucket-name1>",
            "arn:aws:s3:::<cluster-logging-bucket-name1>"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObjectAcl",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::<cluster-staging-dir1>/*",
            "arn:aws:s3:::<cluster-logging-dir1>/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:DescribeKey"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

init_script_worker_policy

IAM ポリシー `staging_log_access_worker_policy` は、クラスタコンピューティングシステムがワーカーノードにクラスタの初期化スクリプトディレクトリおよび初期化スクリプトログディレクトリへのアクセスを許可するために必要になります。

次の JSON ドキュメントを `init_script_worker_policy` のテンプレートとして使用できます。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-init-script-bucket-name1>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-init-script-dir1>/*"
      ]
    }
  ]
}

```

```
} ]
```

手順 8.4. マスタロールとワーカーロールへのポリシーのアタッチ

各 IAM ポリシーを適切な IAM ロールにアタッチします: master_role または worker_role。

次の表に、各ロールにアタッチするポリシーを示します。

ロール	ポリシー
master_role	<ul style="list-style-type: none">- minimal_master_policy- staging_log_access_master_policy- init_script_master_policy
worker_role	<ul style="list-style-type: none">- minimal_worker_policy- ebs_autoscaling_worker_policy- staging_log_access_worker_policy- init_script_worker_policy

手順 8.5. クラスタオペレータロールによるワーカーロールの引き受けの許可

クラスタオペレータロールは、エラスティック構成を検証するために、ワーカーロールを引き受けることができる必要があります。

IAM ロール worker_role の信頼関係を編集し、次のポリシーを指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<AWS account>:role/<cluster_operator_role>"
        ]
      },
      "Service": "ec2.amazonaws.com"
    },
    {
      "Action": "sts:AssumeRole"
    }
  ]
}
```

手順 8.6. クラスタオペレータロールによるマスタロールの引き受けの許可

クラスタオペレータロールは、エラスティック構成を検証するために、マスタロールを引き受けることができる必要があります。

IAM ロール master_role の信頼関係を編集し、次のポリシーを指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<AWS account>:role/<cluster_operator_role>"
        ]
      },
      "Service": "ec2.amazonaws.com"
    },
    {
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
}
]
```

デフォルトのマスタロールと作業ロールの使用（代替）

すばやく設定したい場合は、デフォルトのマスタロールとワーカーロールを使用できます。この場合、Secure Agent は、エージェントがエラスティッククラスタを開始したときにロールを自動的に作成します。

エージェントは、Kubernetes サービスに必要な権限に基づいてポリシーをロールにアタッチします。ロールベースのセキュリティを使用していて、ジョブが Amazon データソースに直接アクセスできる場合、エージェントは Secure Agent ロールにアタッチされているポリシーを特定し、ワーカーロールにこのポリシーを渡します。

デフォルトのロールを使用するには、IAM ロール `cluster_operator_role` に次のポリシーを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole",
        "iam>DeleteInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

手順 9.保存ステージングデータとログファイルの暗号化（オプション）

オプションとして、S3 バケットの Amazon S3 デフォルト暗号化を設定し、Amazon S3 に保存されたステージングデータとログファイルが自動的に暗号化されるようにできます。

S3 バケットの Amazon S3 デフォルト暗号化は、次の暗号化オプションのいずれかを使用して設定できます。

Amazon S3 で管理された暗号化キーによるサーバー側の暗号化（SSE-S3）

個々のステージングファイルおよびログファイルを暗号化するには、またはステージングの場所とログの場所を含む S3 バケットを暗号化するには、SSE-S3 を使用します。

AWS KMS で管理されたキーによるサーバー側の暗号化 (SSE-KMS)

SSE-KMS を使用して、個別のステージングファイルおよびログファイルを暗号化します。ユーザー定義のマスタロールおよびワーカーロールを作成する場合、ステージングの場所とログの場所を含む S3 パケットも暗号化できます。

暗号化オプションの詳細については、AWS のマニュアルを参照してください。

SSE-KMS を使用してユーザー定義のマスタロールおよびワーカーロールを作成する場合、マスタロールおよびワーカーロールがデータの暗号化および復号化のためにアクセスできる customer master key (カスタママスターキー) (CMK) ID を制限できます。

マスタロールおよびワーカーロールにアタッチされるポリシー内にキー ID を指定します。各ポリシーで、AWS Key Management Service (キー管理サービス) (KMS) でのアクションを決定する次のステートメント内のリソース要素を編集します。

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": [
    "*"
  ]
}
```

注: SSE-KMS を使用する場合は、Amazon アカウントのデフォルトの AWS マネージド CMK を使用する必要があります。カスタム CMK を作成することはできません。

手順 10. Amazon データソースのロールベースのセキュリティポリシーの作成 (オプション)

ロールベースのセキュリティは、IAM ロールを使用してデータソースにアクセスします。Amazon S3 V2 コネクタや Amazon Redshift V2 コネクタなどのコネクタが AWS に直接アクセスする場合は、Secure Agent ロールとワーカーロールがデータソースにアクセスすることを許可するポリシーを作成し、AWS 環境での権限を微調整します。

AWS に直接アクセスできないコネクタを使用している場合は、この手順をスキップできます。例えば、JDBC V2 コネクタはドライバを使用して Amazon Aurora 上のデータをクエリし、その基盤データに直接アクセスしません。

迅速にセットアップしたい場合は、資格情報ベースのセキュリティを使用できます。詳細については、[「資格情報ベースのセキュリティの使用 \(代替\)」 \(ページ 46\)](#)を参照してください。

以下のタスクを完了させます。

1. Secure Agent ロールとワーカーロールのポリシーを作成します。
2. 必要に応じて、クロスアカウントアクセスを設定します。

デフォルトでは、エージェントロールとワーカーロールはデータソースにアクセスしますが、エージェントロールとワーカーロールを使用する代わりに、接続レベルで IAM ロールを指定してデータソースにアクセスできます。

デフォルトのマスタロールとワーカーロールを使用する場合は、以下のガイドラインを考慮してください。

- Secure Agent ロールを編集する場合は、エージェントを再起動してマスタロールとワーカーロールを更新する必要があります。
- デフォルトのワーカーロールは、Secure Agent ロールの権限境界を尊重しません。

- ステージングの場所、ログの場所、およびクラスタオペレータのロールは、同じ AWS アカウントに存在する必要があります。

手順 10.1. Secure Agent ロールとワーカーロールのポリシーの作成

Secure Agent ロールとワーカーロールがエラスティックジョブの Amazon データソースにアクセスすることを許可するポリシーを作成します。ワーカーロールタイプに基づいてポリシーを作成して配布します。

ユーザー定義のワーカーロール

ユーザー定義のワーカーロールを作成する場合は、次のいずれかの方法でデータソースへのアクセスを提供できます。

新しい管理ポリシーを作成する

新しい管理ポリシーを作成するには、次のタスクを実行します。

1. コネクタに必要なポリシーを作成します。ポリシーに `data_source_access_policy` という名前を付けます。コネクタ要件の詳細については、目的のコネクタのヘルプを参照してください。
2. Secure Agent ロールとワーカーロールの両方にポリシー `data_source_access_policy` をアタッチします。

IAM ポリシー `staging_log_access_worker_policy` を再利用する

ワーカーロールにアタッチされている IAM ポリシー `staging_log_access_worker_policy` を再利用するには、次のタスクを実行します。

1. リソース要素でデータソースを指定します。

例えば、以下のステートメントのリソース要素でステージングおよびログの場所を指定します。

```
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObjectAcl",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObjectAcl"
  ],
  "Resource": [
    "arn:aws:s3:::<cluster-staging-dir>/*",
    "arn:aws:s3:::<cluster-logging-dir>/*"
  ]
}
```

"arn:aws:s3:::<cluster-logging-dir>/*"以下にデータソースを追加します。

2. ワーカーロールの信頼関係に Secure Agent ロールを追加します。
3. Secure Agent ロールの信頼関係にワーカーロールを追加します。

デフォルトのワーカーロール

デフォルトのワーカーロールを使用する場合は、次のタスクを実行します。

1. コネクタに必要なポリシーを作成します。ポリシーに `data_source_access_policy` という名前を付けます。コネクタ要件の詳細については、目的のコネクタのヘルプを参照してください。
2. `data_source_access_policy` ポリシーを Secure Agent ロールにアタッチします。Secure Agent は、ポリシーをワーカーロールに自動的に渡します。

ステップ 10.2. クロスアカウントアクセスの設定（オプション）

複数の Amazon アカウントの S3 バケットへのアカウント間アクセスが必要で、ユーザー定義のマスタロールおよびワーカーロールを使用する場合、AWS のアカウント間 IAM ロールを設定します。

AWS のアカウント間 IAM ロールを設定する場合、以下のタスクを実行します。

- ユーザー定義のワーカーロールのポリシーを編集し、各アカウントの S3 リソースにアクセスします。
- ユーザー定義のワーカーロールがバケットにアクセスするのを許可するバケットポリシーを各アカウントの S3 バケットに追加します。

注: デフォルトのマスタロールおよびワーカーロールとロールベースのセキュリティと、クロスアカウントアクセスを組み合わせることはできません。組織でアカウント間アクセスが必要な場合、次のいずれかのオプションを検討してください。

- ユーザー定義のマスタおよびワーカーロールを作成する。詳細については、「[手順 8.ユーザー定義のマスタロールおよびワーカーロールの作成](#)」(ページ 33)を参照してください。
- 資格情報ベースのセキュリティの使用。詳細については、「[資格情報ベースのセキュリティの使用（代替）](#)」(ページ 46)を参照してください。

アカウント間 IAM ロールの設定方法の詳細については、AWS のドキュメントを参照してください。

資格情報ベースのセキュリティの使用（代替）

すばやく設定したい場合は、IAM ロールを設定する代わりに、データソースの接続プロパティで設定した AWS 資格情報を再利用できます。クラスタノードは、データソース、ステージングファイル、およびログファイルが同じ S3 バケットに保存されている場合にのみ、接続レベルの資格情報を使用してステージングとログの場所にアクセスします。

例えば、ジョブが JDBC V2 ソースと Amazon S3 V2 ターゲットを使用する場合、クラスタノードは Amazon S3 V2 資格情報を使用してジョブのステージングの場所にアクセスします。

注: 接続内の AWS の資格情報は、ジョブが使用する Amazon S3 ステージングの場所にアクセスできる必要があります。資格情報は IAM ロールをオーバーライドします。コネクタの AWS 資格情報を設定していて、その資格情報でエラスティックジョブのデータソースおよびステージングの場所のどちらにもアクセスできない場合、そのジョブは失敗します。

複数の Amazon アカウントで S3 バケットにクロスアカウントアクセスする必要がある場合、接続レベルで各 Amazon アカウントの資格情報を指定します。

手順 11. Secure Agent ロールのログアクセスポリシーの作成または再利用

Secure Agent には、エラスティックジョブの最後にエージェントのジョブログをアップロードするために、ログの場所にアクセスできる権限が必要です。

ログアクセス用の IAM ポリシーを作成または再利用できます。

ログアクセスポリシーの作成

ログアクセス用の IAM ポリシーを作成するには、AWS で次のタスクを実行します。

1. `log_access_agent_policy` と名付けられた次の IAM ポリシーを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Effect": "Allow",
        "Action": [
            "s3:GetBucketLocation",
            "s3:GetEncryptionConfiguration",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::<cluster-logging-bucket-name1>"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObjectAcl",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::<cluster-logging-dir1>/*"
        ]
    }
]
}

```

リソース要素でログの場所を指定します。

2. IAM ポリシー `log_access_agent_policy` を IAM ロール `agent_role` にアタッチします。

ログアクセスポリシーの再利用

ユーザー定義のマスタロールおよびワーカーロールを作成する場合、CCS 用に生成され、ワーカーロールで必要とされるポリシーコンテンツを再利用できます。

ポリシーコンテンツには、Secure Agent が必要とするログの場所へのアクセスが含まれます。ユーザー定義のマスタロールおよびワーカーロールに関する詳細については、[「手順 8.ユーザー定義のマスタロールおよびワーカーロールの作成」 \(ページ 33\)](#)を参照してください。

ポリシーを再利用するには、次のタスクを実行します。

1. ワーカーロールの信頼関係を編集し、IAM ロール `agent_role` を信頼するために次のポリシーを指定します。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:role/<agent_role>"
        ]
      },
      "Service": "ec2.amazonaws.com"
    },
    {
      "Action": "sts:AssumeRole"
    }
  ]
}

```

2. IAM ロール `agent_role` の信頼関係を編集し、ワーカーロールを信頼するために次のポリシーを指定します。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:role/<worker_role>"
        ]
      },
    },
  ]
}

```

```

        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    ]
  }
}

```

環境変数の設定（オプション）

list-clusters.sh や delete-clusters.sh などのコマンドを実行するには、Secure Agent マシンで環境変数を設定します。

次の表で、各環境変数について説明します。

環境変数	説明
JAVA_HOME	コマンドの実行に使用される Secure Agent マシン上の Java バージョン。 Secure Agent マシンの Java バージョンは、JDK 8 と互換性がある必要があります。
PRIVILEGED_ROLE_ARN	IAM ロール cluster_operator_role の ARN。 list-clusters.sh と delete-clusters.sh コマンドによって使用されます。
AGENT_ROLE_EXTERNAL_ID	Secure Agent が IAM ロール cluster_operator_role を引き受けるために使用する外部 ID。 list-clusters.sh と delete-clusters.sh コマンドによって使用されます。

エラスティックサーバーの設定

Administrator で、エラスティックサーバー用のサービスプロパティを設定します。

次の図は、エラスティックサーバーのプロパティを示しています。

System Configuration Details [Reset All]

Service: Elastic Server

Type: All Types

Type	Name	Value
LOG4J_CFG	log4j_app_log_level	'INFO'
AWS_CFG	agent_role_external_id_key	
AWS_CFG	privileged_role_arn_key	arn:aws:iam:<account-id>:role/cluster_operator_role
AWS_CFG	role_session_duration_secs_key	

設定できるエラスティックサーバーのプロパティを次に示します。

タイプ	名前	説明
LOG4J_CFG	log4j_app_log_level	<p>エラスティックサーバーがログファイルに書き込む詳細のレベル。「INFO」などの文字列としてログレベルを入力します。</p> <p>ログレベルを大きくすると、エラスティックサーバーがログファイルに書き込むメッセージに、より優先度の高いログレベルのメッセージが含まれます。例えば、ログレベルが INFO の場合、ログには FATAL、ERROR、WARNING、および INFO コードのメッセージが記録されます。</p> <p>有効な値は次のとおりです。</p> <ol style="list-style-type: none">1. FATAL。サービスがシャットダウンする、または利用不可能になる修復不能なシステム障害が含まれます。2. ERROR。接続の失敗、メタデータの保存または取得の失敗、サービスのエラーが含まれます。3. WARNING。修復可能なシステム障害または警告が含まれます。4. INFO。システムおよびサービスの変更に関するメッセージが含まれます。5. TRACE。ユーザー要求の失敗がログとして記録されます。6. DEBUG。ユーザー要求がログとして記録されます。
AWS_CFG	agent_role_external_id_key	<p>Secure Agent がクラスタオペレータロールを使用する場合に Secure Agent で指定する外部 ID。クラスタオペレータロールの信頼関係で外部 ID を設定する場合に必要です。</p> <p>このプロパティは、AWS 環境でのみ有効です。</p>
AWS_CFG	privileged_role_arn_key	<p>クラスタオペレータロールの ARN。</p> <p>AWS 環境で個別のクラスタオペレータロールと Secure Agent ロールを設定する場合に必要です。</p> <p>このプロパティは、AWS 環境でのみ有効です。</p>
AWS_CFG	role_session_duration_secs_key	<p>AWS AssumeRole API のセッション時間（秒単位）。デフォルトのセッション時間は 1,800 秒（30 分）です。</p> <p>クラスタオペレータロールに設定されている最大 CLI/API セッション期間をオーバーライドします。エラスティックサーバーに設定されているセッション期間がクラスタオペレータロールのセッション期間よりも長い場合、Secure Agent がクラスタオペレータロールを使用できない場合があります。</p> <p>このプロパティは、AWS 環境でのみ有効です。</p>

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。

AWS ポリシーの詳細参照

このセクションには、クラスタオペレータロール、マスタロール、ワーカーロールの AWS ポリシーが含まれています。

クラスタオペレータロールの詳細

次のカテゴリ内で、クラスタオペレータロールの詳細な AWS ポリシー情報を確認できます。

- EC2
- 自動スケーリング
- Elastic Load Balancing
- IAM
- 価格設定
- KMS
- STS
- S3

EC2 ポリシー

Data Integration Elastic では、Amazon Elastic Compute Cloud (EC2) を使用して、クラウドにコンピューティングリソースを提供します。このページのサブカテゴリ内で、Amazon EC2 ポリシーに関する詳細情報を確認できます。

クラスタオペレータロールに Amazon EC2 ポリシーを使用する場合、Data Integration Elastic ではすべての AWS リソースでそれらのポリシーが必要になります。

インターネットゲートウェイ

AWS ポリシー	説明
ec2:CreateInternetGateway	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2:AttachInternetGateway	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2:DescribeInternetGateway	必須。インターネットゲートウェイを記述します。
ec2:DetachInternetGateway	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2>DeleteInternetGateway	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。

キーペア

クラスタオペレータは AWS EC2 キーペアを作成します。これにより、エンドユーザーは EC2 インスタンスに接続できます。Data Integration Elastic では、キーペアを管理するために次のポリシーが必要です。

- ec2:CreateKeyPair
- ec2:ImportKeyPair
- ec2:DescribeKeyPair
- ec2>DeleteKeyPair

ネットワーク

Data Integration Elastic では、ネットワークインタフェースを説明する ec2:DescribeNetworkInterfaces ポリシーが必要です。

ルート

Data Integration Elastic では、エラスティック構成で Virtual Private Cloud (VPC) オプションとサブネットオプションが提供されていない場合にのみ、次のポリシーが必要です。

- ec2:CreateRoute
- ec2>DeleteRoute

Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。

ルートテーブル

AWS ポリシー	説明
ec2:CreateRouteTable	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2:DescribeRouteTables	必須。ルートテーブルの詳細を返します。
ec2:ReplaceRouteTableAssociation	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2:AssociateRouteTable	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。

AWS ポリシー	説明
ec2:DisassociateRouteTable	<p>オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。</p> <p>Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。</p>
ec2:DeleteRouteTable	<p>オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。</p> <p>Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。</p>

VPC

AWS ポリシー	説明
ec2:CreateVpc	<p>オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。</p> <p>Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。</p>
ec2:DescribeVpcs	必須。VPC の詳細を記述します。
ec2:ModifyVpcAttribute	<p>オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。</p> <p>Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。</p>
ec2>DeleteVpc	<p>オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。</p> <p>Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。</p>

サブネット

AWS ポリシー	説明
ec2:CreateSubnet	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。
ec2:DescribeSubnet	必須。サブネットの詳細を記述します。
ec2>DeleteSubnet	オプション。Data Integration Elastic がエラスティック構成で Virtual Private Cloud (VPC) オプションおよびサブネットオプションを提供しない場合にのみ必要です。 Data Integration Elastic は、デフォルトで、エラスティック構成で VPC オプションおよびサブネットオプションを提供します。

セキュリティグループ

AWS ポリシー	説明
ec2:CreateSecurityGroup	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。
ec2:DescribeSecurityGroups	必須。セキュリティグループの詳細を記述します。
ec2:AuthorizeSecurityGroupEgress	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。
ec2:AuthorizeSecurityGroupIngress	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。
ec2:RevokeSecurityGroupEgress	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。
ec2:RevokeSecurityGroupIngress	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。
ec2>DeleteSecurityGroup	オプション。ユーザー定義の Amazon EC2 セキュリティグループを作成して使用する場合にのみ必要です。ユーザー定義のセキュリティグループの詳細については、「 Amazon EC2 のユーザー定義のセキュリティグループの作成 」(ページ 23)を参照してください。

タグ

AWS ポリシー	説明
ec2:CreateTags	必須。Amazon EC2 などの Kubernetes インフラストラクチャのタグを追加します。Kubernetes はタグによってリソースを識別します。タグを使用すると、リソースを管理し、条件文を追加できます。
ec2:DescribeTags	必須。Amazon EC2 などの Kubernetes インフラストラクチャのタグを記述します。
ec2:DeleteTags	必須。Amazon EC2 などの Kubernetes インフラストラクチャのタグを削除します。

ボリューム

クラスタオペレータロールは、etcd ボリュームを直接管理します。エラスティッククラスタでは、etcd ボリュームを使用してメタデータを格納します。Data Integration Elastic では、etcd ボリュームを管理するために次のポリシーが必要です。

- ec2:CreateVolumes
- ec2:DescribeVolumes
- ec2:DeleteVolumes

イメージ

Data Integration Elastic では、Amazon EC2 インスタンスから Amazon Machine Image (AMI) の詳細を取得するために ec2:DescribeImages ポリシーが必要です。

インスタンス

AWS ポリシー	説明
ec2:DescribeInstanceAttribute	必須。作成された Amazon EC2 インスタンスの詳細を取得します。
ec2:ModifyInstanceAttribute	必須。クラスタオペレータが Amazon EC2 インスタンスを管理および作成できるようにします。
ec2:RunInstances	必須。クラスタオペレータが Amazon EC2 インスタンスを管理および作成できるようにします。
ec2:DescribeInstances ec2:DescribeInstanceType	必須。作成された Amazon EC2 インスタンスの詳細を取得します。
ec2:TerminateInstances	必須。クラスタオペレータロールによって作成された EC2 インスタンスを終了します。

リージョン

AWS ポリシー	説明
ec2:DescribeRegions	必須。エラスティック構成で選択したリージョンを記述します。
ec2:DescribeAvailabilityZones	必須。アベイラビリティゾーンの詳細を記述します。

起動テンプレート

クラスタオペレータは、起動テンプレートを使用して EC2 インスタンスを起動します。Data Integration Elastic では、起動テンプレートを管理するために次のポリシーが必要です。

- ec2:CreateLaunchTemplate
- ec2:DescribeLaunchTemplates
- ec2:DeleteLaunchTemplate
- ec2:CreateLaunchTemplateVersion
- ec2:DescribeLaunchTemplateVersions
- ec2:DeleteLaunchTemplateVersions

自動スケーリングポリシー

Data Integration Elastic では、エラスティッククラスタを管理するために自動スケーリンググループが必要です。

Data Integration Elastic では、拡張可能なクラスタノードとノードリカバリのために、すべての AWS リソースに次のポリシーが必要です。

- autoscaling:AttachLoadBalancers
- autoscaling:CreateAutoScalingGroup
- autoscaling:DescribeAutoScalingGroups
- autoscaling:UpdateAutoScalingGroup
- autoscaling:DeleteAutoScalingGroup
- autoscaling:DescribeScalingActivities
- autoscaling:DescribeTags
- autoscaling:TerminateInstanceInAutoScalingGroup

Elastic Load Balancing ポリシー

Data Integration Elastic では、高可用性クラスタ、マスタノードのアクセス制御、およびその他の機能には、Elastic Load Balancer が必要です。

Data Integration Elastic では、すべての AWS リソースに Elastic Load Balancer ポリシーが必要です。

- elasticloadbalancing:AddTags
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer
- elasticloadbalancing:AttachLoadBalancerToSubnets
- elasticloadbalancing:ConfigureHealthCheck
- elasticloadbalancing:CreateLoadBalancer
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing>DeleteLoadBalancer
- elasticloadbalancing:CreateLoadBalancerListeners
- elasticloadbalancing:DescribeInstanceHealth

- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes
- elasticloadbalancing:RegisterInstancesWithLoadBalancer

IAM ポリシー

IAM ポリシーは、すべての AWS リソースに適用されます。このページのサブカテゴリ内で、Amazon EC2 ポリシーに関する詳細情報を確認できます。

インスタンスプロファイル

AWS ポリシー	説明
iam:AddRoleToInstanceProfile	マスタおよびワーカーインスタンスプロファイルを指定しない場合はオプションです。
iam:CreateInstanceProfile	マスタロールとワーカーロールを提供する場合はオプションです。
iam:DeleteInstanceProfile	マスタロールとワーカーロールを提供する場合はオプションです。
iam:GetContextKeysForPrincipalPolicy iam:SimulatePrincipalPolicy	必須。エラスティック構成検証とアップグレードの検証を含む権限の検証を許可します。
iam:GetInstanceProfile	必須。インスタンスプロファイルパス、GUID、ARN、ロールなど、指定されたインスタンスプロファイルに関する情報を取得します。
iam:ListInstanceProfiles	必須。指定されたパスプレフィックスを持つインスタンスプロファイルを一覧表示します。

ロール

AWS ポリシー	説明
iam:CreateRole	マスタロールとワーカーロールを提供する場合はオプションです。
iam:CreateServiceLinkedRole	必須。特定の AWS サービスにリンクされている IAM ロールを作成します。
iam>DeleteRole	マスタロールとワーカーロールを提供する場合はオプションです。
iam:GetRole	必須。ロールパスなど、指定されたロールに関する情報を取得します。
iam:ListRolePolicies	必須。ロールパスなど、指定されたロールに関する情報を取得します。
iam:ListRoles	必須。ロールパスなど、指定されたロールに関する情報を取得します。

ロールポリシー

AWS ポリシー	説明
iam:AttachRolePolicy iam>DeleteRolePolicy iam:DetachRolePolicy iam:PutRolePolicy	マスタロールとワーカーロールを提供する場合はオプションです。
iam:GetRolePolicy	必須。AWS が指定された IAM ロールに組み込む、指定されたインラインポリシードキュメントを取得します。
iam:ListAttachedRolePolicies	必須。指定された IAM ロールに関連付けられているすべての管理ポリシーを一覧表示します。
iam:ListInstanceProfilesForRole	必須。IAM ロールが関連付けられているインスタンスプロファイルを一覧表示します。
iam:RemoveRoleFromInstanceProfile	必須。指定された EC2 インスタンスプロファイルから指定された IAM ロールを削除します。

ユーザー

Data Integration Elastic では、パス、一意の ID、ARN など、指定された IAM ユーザーに関する情報を取得するために、iam:GetUser ポリシーが必要です。

価格設定ポリシー

Data Integration Elastic では、スポットインスタンスを使用するために pricing:GetProducts ポリシーが必要です。

KMS ポリシー

Data Integration Elastic では、ルートボリュームの暗号化が有効で、クラスタオペレータロールにカスタマネージドキー（CMK）が提供されている場合は、kms:DescribeKey ポリシーが必要です。使用する場合、このポリシーはすべての AWS リソースに適用されます。

STS ポリシー

Data Integration Elastic は、特定の状況で次のポリシーを使用します。

AWS ポリシー	説明
sts:AssumeRole	ユーザー定義のマスタロールとワーカーロールを使用する場合に必要です。
sts:DecodeAuthorizationMessage	オプション。AWS の応答から受信した、暗号化されたメッセージをデコードするために使用されます。

S3 ポリシー

Data Integration Elastic では、クラスタステー징ファイルとログファイルには、次のポリシーが必要です。

AWS ポリシー	リソース
s3:GetBucketLocation	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"
s3:GetEncryptionConfiguration	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"
s3:ListBucket	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"
s3:PutObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"
s3:GetObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"
s3:GetObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"
s3>DeleteObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"
s3:PutObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"

マスタロールの詳細

次のカテゴリ内で、マスタロールの詳細な AWS ポリシー情報を確認できます。

- EC2
- 自動スケーリング
- Elastic Load Balancing
- IAM
- KMS
- S3

EC2 ポリシー

Data Integration Elastic では、Amazon Elastic Compute Cloud (EC2) を使用して、クラウドにコンピューティングリソースを提供します。

マスターロールに Amazon EC2 ポリシーを使用する場合、Data Integration Elastic ではすべての AWS リソースでそれらのポリシーが必要になります。

AWS ポリシー	説明
ec2:DescribeInstances	必須。Kubernetes がインスタンスを記述できるようにします。
ec2:DescribeRegions	必須。Kubernetes がリージョンを記述できるようにします。
ec2:CreateRoute	オプション。エラスティック構成で VPC とサブネットを指定しない場合にのみ必要です。
ec2:DescribeRouteTables	必須。Kubernetes インフラストラクチャをセットアップします。
ec2>DeleteRoute	オプション。エラスティック構成で VPC とサブネットを指定しない場合にのみ必要です。
ec2:CreateSecurityGroup	オプション。クラスタオペレータロールが作成するデフォルトのセキュリティグループを使用する場合にのみ必要です。
ec2:CreateSecurityGroup ec2:AuthorizeSecurityGroupIngress ec2:RevokeSecurityGroupIngress ec2>DeleteSecurityGroup	オプション。クラスタオペレータロールが作成するデフォルトのセキュリティグループを使用する場合にのみ必要です。
ec2:DescribeSubnets	必須。サブネットの詳細などを記述するマスタノードを作成します。
ec2:DescribeVpc	必須。VPC の詳細などを記述するマスタノードを作成します。
ec2:CreateTags	必須。EC2 などの Kubernetes インフラストラクチャのタグを追加します。
ec2:ModifyInstanceAttribute	必須。
ec2:CreateVolume	必須。EBS ボリュームなどのストレージを作成します。
ec2:DescribeVolumes	必須。ED2 ノード用に作成されたボリュームの詳細を取得します。
ec2:DescribeVolumesModifications	必須。指定された EBS ボリュームに対する最新のボリューム変更要求を記述します。
ec2:ModifyVolume	必須。ボリュームを変更します。
ec2:AttachVolume	必須。ボリュームをアタッチします。
ec2:DetachVolume	必須。作成したボリュームをデタッチします。
ec2>DeleteVolume	必須。作成したボリュームを削除します。

自動スケーリングポリシー

Data Integration Elastic では、エラスティッククラスタを管理するために自動スケーリンググループが必要です。

自動スケーリンググループにより、拡張可能なクラスタノードとノードのリカバリが可能になります。Data Integration Elastic では、すべての AWS リソースに自動スケーリングポリシーが必要です。マスタノードは、次のポリシーを使用して自動スケーリンググループを管理します。

- autoscaling:DescribeAutoScalingInstances
- autoscaling:DescribeTags
- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeLaunchConfigurations
- autoscaling:DescribeScalingActivities
- autoscaling:SetDesiredCapacity
- autoscaling:TerminateInstanceInAutoScalingGroup
- autoscaling:UpdateAutoScalingGroup

Elastic Load Balancing ポリシー

Data Integration Elastic では、エラスティッククラスタを管理するためにロードバランシングが必要です。

Data Integration Elastic では、すべての AWS リソースに Elastic Load Balancing ポリシーが必要です。マスタノードは、次のポリシーを使用してロードバランシングルールを管理します。

- elasticloadbalancing:AddTags
- elasticloadbalancing:AttachLoadBalancerToSubnets
- elasticloadbalancing:DetachLoadBalancerFromSubnets
- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer
- elasticloadbalancing:ConfigureHealthCheck
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing>DeleteLoadBalancer
- elasticloadbalancing:DescribeListeners
- elasticloadbalancing:ModifyListener
- elasticloadbalancing>DeleteLoadBalancerListeners
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes
- elasticloadbalancing:RegisterInstancesWithLoadBalancer
- elasticloadbalancing:DeregisterInstancesFromLoadBalancer
- elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer
- elasticloadbalancing:DescribeListener
- elasticloadbalancing>DeleteListener
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:ModifyTargetGroup
- elasticloadbalancing:RegisterTargets

- elasticloadbalancing:DescribeTargetHealth
- elasticloadbalancing>DeleteTargetGroup
- elasticloadbalancing:DeregisterTargets
- elasticloadbalancing:SetLoadBalancerPoliciesOfListener
- elasticloadbalancing:DescribeLoadBalancerPolicies

IAM ポリシー

IAM ポリシーは、すべての AWS リソースによって使用されます。

AWS ポリシー	説明
iam:ListServerCertificates	必須。サーバー証明書を一覧表示します。
iam:GetServerCertificate	必須。サーバー証明書を取得します。

KMS ポリシー

Data Integration Elastic では、AWS Key Management Service (KMS) のマスタキーへのアクセスを管理するには、すべての AWS リソースに次のポリシーが必要です。

- kms:Encrypt
- kms:Decrypt
- kms:ReEncrypt
- kms:GenerateDataKey
- kms:DescribeKey

S3 ポリシー

Data Integration Elastic では、クラスタステージングファイルとログファイルには、次のポリシーが必要です。

AWS ポリシー	リソース	
s3:GetBucketLocation	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>" "arn:aws:s3:::<cluster-init-script-bucket-name>"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3:GetEncryptionConfiguration	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"	必須

AWS ポリシー	リソース	
s3:ListBucket	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>" "arn:aws:s3:::<cluster-init-script-bucket-name>"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3:PutObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:GetObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:GetObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*" "arn:aws:s3:::<cluster-init-script-dir>/*"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3>DeleteObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:PutObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須

ワーカーロールの詳細

次のカテゴリ内で、ワーカーロールの詳細な AWS ポリシー情報を確認できます。

- EC2
- 自動スケーリング
- KMS
- S3

EC2 ポリシー

Data Integration Elastic では、Amazon Elastic Compute Cloud (EC2) を使用して、クラウドにコンピューティングリソースを提供します。

AWS ポリシー	リソース	説明
ec2:DescribeInstances	すべて -- "*"	必須。Kubernetes がインスタンスを記述できるようにします。
ec2:DescribeRegions	すべて -- "*"	必須。Kubernetes がリージョンを記述できるようにします。
ec2:CreateTags	すべて -- "*"	必須。EC2 などの Kubernetes インフラストラクチャのタグを追加します。
ec2:DescribeVolumes	すべて -- "*"	ストレージのスケーリングに必要です。

AWS ポリシー	リソース	説明
ec2:CreateVolume	すべて -- "*"	ストレージのスケールアップに必要です。
ec2:ModifyInstanceAttribute	すべて -- "*"	ストレージのスケールアップに必要です。
ec2:AttachVolume	"arn:aws:ec2:*:*:volume/*" "arn:aws:ec2:*:*:instance/*"	ストレージのスケールアップに必要です。

自動スケーリングポリシー

Data Integration Elastic では、すべての AWS リソースに自動スケーリングポリシーが必要です。

AWS ポリシー	説明
autoscaling:DescribeAutoScalingInstances	必須。Kubernetes が自動スケーリングインスタンスを記述できるようにします。
autoscaling:DescribeTags	必須。Kubernetes がタグを記述できるようにします。

KMS ポリシー

Data Integration Elastic では、AWS Key Management Service (KMS) のマスタキーへのアクセスを管理するには、すべての AWS リソースに次のポリシーが必要です。

- kms:Encrypt
- kms:Decrypt
- kms:ReEncrypt
- kms:GenerateDataKey
- kms:DescribeKey

S3 ポリシー

Data Integration Elastic では、クラスタステーシングファイルとログファイルには、次のポリシーが必要です。

AWS ポリシー	リソース	
s3:GetBucketLocation	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>" "arn:aws:s3:::<cluster-init-script-bucket-name>"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3:GetEncryptionConfiguration	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"	必須

AWS ポリシー	リソース	
s3:ListBucket	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>" "arn:aws:s3:::<cluster-init-script-bucket-name>"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3:PutObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:GetObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:GetObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*" "arn:aws:s3:::<cluster-init-script-dir>/*"	必須。ユーザー起動スクリプトが設定されている場合、init スクリプトリソースにはこのポリシーが必要です。
s3>DeleteObject	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須
s3:PutObjectAcl	"arn:aws:s3:::<cluster-staging-dir>/*" "arn:aws:s3:::<cluster-logging-dir>/*"	必須

マスタとワーカーのロールタイプのリファレンス

ユーザー定義とデフォルトのマスタロールとワーカーロールを比較して、組織の要件をより十分に満たすロールタイプを決定します。

次の表では、主要な領域に基づいて各ロールタイプを比較しています。

領域	ユーザー定義のロール	デフォルトのロール
マスタロールとワーカーロールの作成	マスタロールとワーカーロール、および各ロールにアタッチするポリシーについての認識が高まる。	ロールは自動的に作成されるため、各ロールにアタッチされるポリシーを監視する事は難しい。
ポリシーの編集機能	ポリシー内で一部のリソースを制限できる。	ポリシーは編集出来ない。
クラスタオペレーターロールが必要とする IAM 権限の数	必要な IAM 権限の数は少ない。	必要な IAM 権限の数は多い。
Amazon データソースへの直接アクセスのための資格情報ベースのセキュリティ	マスタロールとワーカーロールに影響はない。	マスタロールとワーカーロールに影響はない。

領域	ユーザー定義のロール	デフォルトのロール
Amazon データソースへの直接アクセスのためのロールベースのセキュリティ	ワーカーロールと Secure Agent ロールが両方ともエラスティックジョブで使用するデータソースにアクセスできることを手動で確認する必要がある。 複数の Amazon アカウントでの S3 バケットへのアカウント間アクセスも設定できます。	Secure Agent ロールがエラスティックジョブで使用するデータソースにアクセスできることのみ確認する必要がある。Secure Agent ロールにアタッチされるポリシーはワーカーロールにも自動的にアタッチされるため、ワーカーロールでは常に Secure Agent ロールと同じデータソースにアクセスできます。 複数の Amazon アカウントでの S3 バケットへのアカウント間アクセスは設定できません。
ロールの共有	複数のエラスティック構成で同じマスターロールとワーカーロールを使用できる。	エラスティック構成ごとに別のマスターロールとワーカーロールが作成される。ロールを再使用する事は出来ません。
ステージングとログの場所の変更	ポリシーのステージングとログの場所は手動で更新する必要がある。	ポリシーは自動的に更新される。
製品アップグレード	製品アップグレードによって、マスターロールとワーカーロールに必要なポリシーも変わる場合がある。ポリシーが変わる場合は、ポリシーコンテンツを再生成してリソースに対するアクセスを再度制限する必要があります。	ポリシーは自動的に更新される。

マスターロールとワーカーロールの使用方法的詳細については、[「リソースへのアクセスの詳細」 \(ページ 17\)](#)を参照してください。

マスタおよびワーカーポリシーの制限に関するリファレンス

マスタポリシーとワーカーポリシーのリソースを制限して、マスタノードとワーカーノードがアクセスできるリソースを制限できます。

値に応じて次の要素を制限できます。

値*が含まれるリソース要素

リソース要素の値がワイルドカード*の場合、リソースを制限する事は出来ません。

例えば、マスタノードの生成済みポリシーに次のステートメントを含める事ができます。

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes"
  ]
}
```

```

    ],
    "Resource": [
      "*"
    ]
  },

```

リソース要素の値がワイルドカード*の場合、リソース要素を編集する事は出来ません。

ワイルドカード*の値を含むリソース要素を編集する場合、Secure Agent はエラスティッククラスタの開始に必要なリソースの特定に失敗し、クラスタが正しく開始されない可能性があります。

ステージングデータとログファイルを SSE-KMS を使用して暗号化する場合、AWS Key Management Service (キー管理サービス) (KMS) でのアクションを含むステートメント内のリソースを、リソース要素がワイルドカード (*) であっても編集できます。詳細については、[「手順 9.保存ステージングデータとログファイルの暗号化 \(オプション\)」 \(ページ 43\)](#)を参照してください。

値*が含まれないリソース要素

リソース要素の値がワイルドカード*以外の場合、ステートメントに含まれるリソースを指定するようにリソース要素を制限できます。

例えば、作業ノードの生成済みポリシーに次のステートメントを含める事ができます。

```

{
  "Effect": "Allow",
  "Action": [
    "s3:Get*"
  ],
  "Resource": [
    "arn:aws:s3:::<cluster-staging-dir1>/*",
    "arn:aws:s3:::<cluster-staging-dir2>/*"
  ]
},

```

リソース要素の値がワイルドカード*以外の場合、ステートメント内のリソースを編集する事ができます。この例では、1 つ以上のステージングの場所を定義する S3 リソースにリソース要素を制限できます。

複数のエラスティッククラスタのステージング、ログ、および初期化の場所を指定し、異なるエラスティック構成を使用するクラスタ間で同じポリシーコンテンツを共有できます。

領域間のデータ転送コストを節約するには、同じ領域内の S3 バケットを使用します。各バケットを管理するために、ステージングの場所、ログの場所、初期化スクリプト、およびデータソースに異なるバケットを使用します。

第 3 章

Google Cloud の設定

エラスティック構成の作成を組織内で開始する前に、Google Cloud をセットアップして Data Integration Elastic と連携します。

以下のタスクを完了させます。

1. 使用している環境の要件を確認する。
2. クラスタファイルの格納場所を作成します。
3. Secure Agent をダウンロードして、Google Cloud にある Linux 仮想マシンにインストールします。
4. Google Cloud のドメインをホワイトリストに登録します。
5. オプションで、クラスタのプロキシを設定します。
6. ロールとサービスアカウントを作成します。
7. 必要に応じて、VPC およびサブネットを準備します。
8. オプションで、JAVA_HOME 環境変数を設定する。

始める前に

環境をセットアップする前に、環境とクラウドプラットフォームの要件を確認してください。

以下のタスクを完了させます。

- 組織で正しい特権を持っていることを確認してください。
- 必要な Google Cloud サービスがあることを確認してください。
- Data Integration Elastic がクラウドプラットフォーム上のリソースにアクセスする方法を学びます。

組織の権限の確認

組織のエラスティック構成に対する適切な特権が割り当てられていることを確認します。

エラスティック構成に対する特権によって、Administrator および Monitor の **【エラスティッククラスタ】** ページへのアクセスレベルは異なります。

エラスティック構成の表示とエラスティッククラスタの監視を行うには、少なくとも読み取り権限が必要です。

Google Cloud サービスの確認

Google Cloud でエラスティッククラスタを作成するために必要なサービスが利用できることを確認します。

Google アカウントに次のサービスが必要です。

Google Cloud Storage

エラスティッククラスタおよびエラスティックジョブのステージングデータとログファイルは、Google Cloud Storage に保存されます。

Google Compute Engine

仮想マシンは Secure Agent をホストします。

VPC ネットワーク

エラスティッククラスタをホストするための VPC ネットワークとサブネット。

ネットワークサービス

負荷分散とクラウド NAT を提供するネットワークサービス。

リソースへのアクセスの詳細

データを処理するために、Secure Agent およびエラスティッククラスタは、クラウドプラットフォーム上のリソース、ソースおよびターゲットデータ、ステージングおよびログの場所などの、エラスティックジョブの一部であるリソースにアクセスします。

リソースへのアクセスは実行されるタスクによって異なります。

- エラスティックマッピングの設計
- エラスティッククラスタの作成
- エラスティックジョブの実行
- ログのポーリング

エラスティックマッピングの設計

エラスティックマッピングの設計は、データ統合でのエラスティックマッピング以外のマッピングの設計に似ています。マッピングを設計すると、Secure Agent はソースとターゲットにアクセスするため、ユーザーはデータの読み取りと書き込みができます。

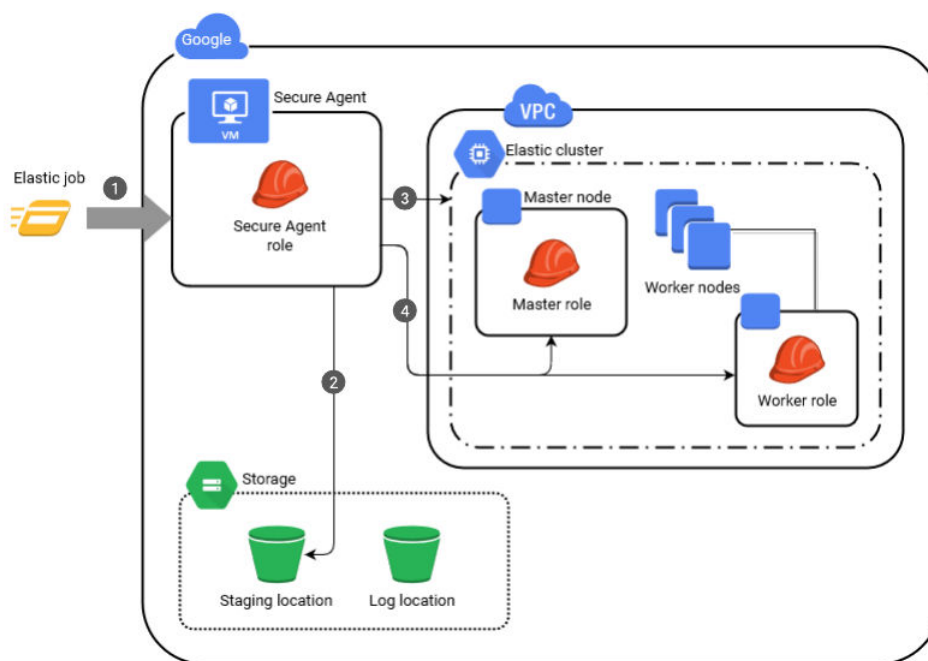
例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで使用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

ソースまたはターゲットにアクセスするために、Secure Agent は Secure Agent サービスアカウントの権限を使用します。

エラスティッククラスタの作成

エラスティックジョブを実行すると、Secure Agent によってエラスティッククラスタが作成されます。エージェントは、クラスタ情報をステージングの場所に保管し、同じリソースにアクセスしてエラスティッククラスタを開始します。

次の図に、Secure Agent がクラスタを作成するときの一連のイベントを示します。

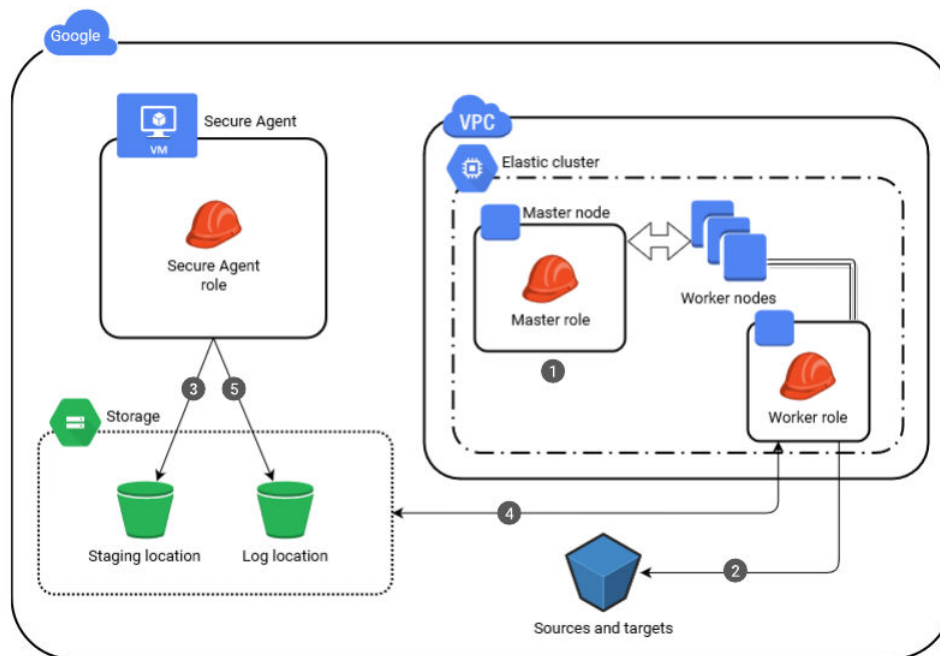


1. エラスティックジョブを実行します。
2. Secure Agent は、Secure Agent ロールの権限を使用して、クラスタ情報をステージングの場所に保存します。
3. Secure Agent は、クラスタリソースを作成し、Secure Agent ロールの権限を使用してエラスティッククラスタを開始します。
4. マスタロールとワーカーロールとサービスアカウントを構成した場合、Secure Agent はサービスアカウントをクラスタノードにアタッチして、ノードに構成された権限を付与します。マスタロールとワーカーロールとサービスアカウントを構成しない場合、クラスタノードは Secure Agent ロールとサービスアカウントを使用します。

ジョブの実行

エラスティックジョブを実行するために、Secure Agent、マスタノード、およびワーカーノードはソースおよびターゲット、ステー징の場所およびログの場所にアクセスします。

次の図に、エラスティッククラスタでジョブを実行する場合のリソースへのアクセス方法を示します。



1. マスタノードは、設定されている場合はマスタロールを使用して、エラスティッククラスタ上のプロセスを調整し、ジョブの必要に応じてワーカーノードの数をスケーリングします。
2. ワーカーノードは、設定されている場合はワーカーロールを使用して、ソースデータとターゲットデータにアクセスします。
3. Secure Agent は、Secure Agent ロールを使用して、ジョブの依存関係をステー징の場所に保存します。
4. ワーカーノードは、設定されている場合はワーカーロールを使用してステー징とログの場所にアクセスして、ステー징の場所からジョブの依存関係を取得し、ステー징の場所にデータをステーディングし、ログの場所にログを保存します。
5. Secure Agent は、Secure Agent ロールを使用して、エージェントジョブログをログの場所にアップロードします。

ログのポーリング

Monitor を使用すると、Secure Agent はログの場所にアクセスしてログをポーリングします。

ログの場所からログをポーリングするために、Secure Agent は Secure Agent サービスアカウントの権限を使用します。

クラスタファイルの格納場所の作成

Google Cloud Storage で、ステージング、ログ、および初期化スクリプトファイルを保存する場所を作成します。

次の格納場所を作成します。

- クラスタがランタイムにステージングファイルを保存するために使用する場所
- クラスタ上で実行されるエラスティックジョブ用のログファイルを保存するためにクラスタが使用する場所
- オプションで、クラスタに追加のソフトウェアをインストールするためにクラスタノードが実行する初期化スクリプトを格納できる場所

ステージングの場所には、クラスタがクラスタノード全体に配布するアーティファクトやマッピングでプレビューするデータなどの一時データが格納されます。エラーにより、マッピングでステージングの場所のプレビューデータをクリアできない可能性があるため、ステージングの場所にアクセスできるユーザーがソースデータの表示を許可されていることを確認してください。

初期化スクリプトを作成する場合は、スクリプトを適切な場所に追加します。

Secure Agent のダウンロードとインストール

Secure Agent をダウンロードして、Google Cloud にある Linux 仮想マシンにインストールします。

次の表に、Secure Agent マシンの最小リソース要件を一覧表示します。

コンポーネント	最小要件
CPU あたりのコア数	4 以上
メモリ	16GB
ディスク空き容量	100GB

Secure Agent をインストールした後、Secure Agent マシンに OpenSSL をインストールします。

Secure Agent のインストールに関する詳細については、「ランタイム環境」を参照してください。

Google Cloud のドメインのホワイトリスト登録

Secure Agent が Google Cloud でエラスティッククラスタを作成する場合、クラスタノードは、マシンイメージなどのアーティファクトを取得し、ソースとターゲットにアクセスするために、特定のドメインにアクセスする必要があります。

次のドメインをホワイトリストに登録します。

```
infacloud.jfrog.io
infacloud-ct-cdie-docker.jfrog.io
infacloud-discale-docker-stable.jfrog.io
discale-docker-stable.artifacts.cloudtrust.rocks
.storage.cloud.google.com
.google.com
```

クラスタのプロキシの設定

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

クラスタにプロキシサーバーを使用するには、Secure Agent のプロキシサーバーを編集します。Google Cloud 上のメタデータサーバーと、クラスタに割り当てる予定の IP アドレスを除外します。

次のファイルでプロキシサーバーの詳細を編集できます。

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

InfAgent.NonProxyHost プロパティを設定して、IP アドレスまたはホスト名を除外します。

Google Cloud 上のメタデータサーバーとクラスタ IP アドレスをプロキシから除外するには、次の手順を実行します。

1. proxy.ini ファイルを開きます。
2. InfAgent.NonProxyHost の値を更新して、メタデータサーバーとクラスタ IP アドレスを除外します。

例えば、次の値を設定するとメタデータサーバーが除外され、2 つの形式を使用して CIDR ブロック 172.16.0.0/16 のクラスタ IP アドレスが除外されます。

InfAgent.NonProxyHost=metadata|metadata.google.internal|172.16.*|172.16.0.0/16

注: パイプ文字 (|) は、ホスト名と IP アドレスのリストを結合する区切り文字です。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。

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。

変更が有効になると、Secure Agent はプロキシを通過せずにメタデータサーバーおよびクラスタと通信しますが、クラスタと通信するコマンドはプロキシを通過する必要があります。

非プロキシホストを除外するようにプロキシを設定する方法の詳細については、「ランタイム環境」を参照してください。

ロールとサービスアカウントの作成

Secure Agent ロールとサービスアカウントを作成して、Google Cloud でエラスティッククラスタを作成および管理する権限をエージェントに付与します。マスタノードとワーカーノードの権限を Secure Agent ロールに含めることも、クラスタノードに対して個別のロールとサービスアカウントを作成することもできます。

次のロールと Google サービスアカウントを作成します。

- Secure Agent ロールとサービスアカウント
- 必要に応じて、マスタノードのロールとサービスアカウント
- 必要に応じて、ワーカーノードのロールとサービスアカウント

Google Cloud サービスアカウントは常に Google Cloud プロジェクトにリンクされています。エラスティックジョブを実行する場合は、ソースとターゲットに 1 セットの資格情報のみを使用するようにしてください。

Secure Agent ロールとサービスアカウントの作成

Secure Agent ロールとサービスアカウントを作成して、Secure Agent に権限を付与します。

Secure Agent ロールの作成

Secure Agent ロールを作成して、Secure Agent の一連の権限を定義します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[ロール]** に移動します。
2. ロールを作成します。
3. ロールのタイトル、説明、および ID を入力します。
ID の形式には<username-agent-role>を使用できます。
4. ロールに権限を追加します。
権限の詳細については、[「Secure Agent ロールの権限」 \(ページ 73\)](#)を参照してください。

Secure Agent サービスアカウントの作成

Secure Agent ロールを使用する Secure Agent サービスアカウントを作成します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[サービスアカウント]** に移動します。
2. サービスアカウントを作成します。
3. 名前、ID、説明などのサービスアカウントの詳細を入力します。
4. プロジェクトへのサービスアカウントアクセスの詳細を入力します。
5. Secure Agent ロール<username-agent-role>を選択します。
6. Secure Agent サービスアカウントを Secure Agent マシンのデフォルトのサービスアカウントとして設定します。

Secure Agent ロールの権限

次の表に、Secure Agent ロールの最小必要権限を示します。

操作	権限
<ul style="list-style-type: none">- 外部静的 IP アドレスを作成する- IP アドレスを削除または解放する	<code>compute.addresses.create</code> <code>compute.addresses.delete</code> <code>compute.addresses.get</code> <code>compute.addresses.list</code> <code>compute.addresses.use</code>
<ul style="list-style-type: none">- ターゲットプールを作成する- ターゲットプールの詳細を取得する- ターゲットプールを削除する	<code>compute.targetPools.addInstance</code> <code>compute.targetPools.create</code> <code>compute.targetPools.delete</code> <code>compute.targetPools.get</code> <code>compute.targetPools.list</code> <code>compute.targetPools.removeInstance</code> <code>compute.targetPools.update</code> <code>compute.targetPools.use</code>
<ul style="list-style-type: none">- 転送ルールを作成する- ルール作成の詳細を取得する- 転送ルールを削除する	<code>compute.forwardingRules.create</code> <code>compute.forwardingRules.delete</code> <code>compute.forwardingRules.get</code> <code>compute.forwardingRules.list</code> <code>compute.forwardingRules.setTarget</code> <code>compute.forwardingRules.update</code>

操作	権限
<ul style="list-style-type: none"> - インスタンステンプレートを作成する - インスタンステンプレートの詳細を取得する - インスタンステンプレートを削除する - インスタンスにディスクを追加する 	<pre>compute.instanceTemplates.create compute.instanceTemplates.delete compute.instanceTemplates.get compute.instanceTemplates.list compute.instanceTemplates.useReadOnly compute.disks.create compute.disks.delete compute.disks.get compute.disks.list compute.disks.resize compute.disks.setLabels compute.disks.update compute.disks.use</pre>
<ul style="list-style-type: none"> - リージョナルグループおよびゾーングループを作成する - リージョナルのインスタンスグループの詳細または説明を取得する - リージョナルインスタンスグループを削除する 	<pre>compute.addresses.create compute.addresses.delete compute.addresses.get compute.addresses.list compute.addresses.use compute.instanceGroupManagers.create compute.instanceGroupManagers.delete compute.instanceGroupManagers.get compute.instanceGroupManagers.list compute.instanceGroupManagers.update compute.instanceGroupManagers.use compute.instanceGroups.create compute.instanceGroups.delete compute.instanceGroups.get compute.instanceGroups.list compute.instanceGroups.update compute.instanceGroups.use compute.instances.addAccessConfig compute.instances.attachDisk compute.instances.create compute.instances.delete compute.instances.deleteAccessConfig compute.instances.detachDisk compute.instances.get compute.instances.getEffectiveFirewalls compute.instances.list compute.instances.osAdminLogin compute.instances.osLogin compute.instances.reset compute.instances.resume compute.instances.setDiskAutoDelete compute.instances.setLabels compute.instances.setMachineResources compute.instances.setMachineType compute.instances.setMetadata compute.instances.setMinCpuPlatform compute.instances.setServiceAccount compute.instances.setTags compute.instances.start compute.instances.startWithEncryptionKey compute.instances.stop compute.instances.suspend compute.instances.update compute.instances.updateAccessConfig compute.instances.updateNetworkInterface compute.instances.updateSecurity compute.instances.use compute.subnetworks.use compute.subnetworks.useExternalIp compute.subnetworks.get</pre>

操作	権限
- Google Cloud Storage のメタデータとログを削除、アップロード、一覧表示する	storage.objects.create storage.objects.delete storage.objects.get storage.objects.list storage.objects.update storage.buckets.get
- VPC およびサブネット内のリソースを作成、使用、および削除する	compute.subnetworks.get compute.subnetworks.use compute.subnetworks.useExternalIp
- プロジェクトで作業する	resourcemanager.projects.get
- サービスアカウントを使用する	iam.serviceAccounts.actAs
- 内部 IP アドレスを作成、使用、および削除する	compute.addresses.createInternal compute.addresses.deleteInternal compute.addresses.useInternal
- リージョンバックエンドサービスを作成、使用、削除する	compute.regionBackendServices.create compute.regionBackendServices.delete compute.regionBackendServices.get compute.regionBackendServices.list compute.regionBackendServices.update compute.regionBackendServices.use
- リージョンのヘルスチェックを作成、使用、および削除する	compute.regionHealthChecks.create compute.regionHealthChecks.delete compute.regionHealthChecks.get compute.regionHealthChecks.list compute.regionHealthChecks.update compute.regionHealthChecks.use compute.regionHealthChecks.useReadOnly

Secure Agent が VPC ネットワークとサブネットを作成できるようにするには、Secure Agent ロールに次の権限を追加します。

操作	権限
- VPC ネットワークを作成、使用、および削除する	compute.networks.access compute.networks.create compute.networks.delete compute.networks.get compute.networks.list compute.networks.use
- サブネットワークを作成、使用、および削除する	compute.subnetworks.create compute.subnetworks.delete compute.subnetworks.get compute.subnetworks.list compute.subnetworks.update compute.subnetworks.use compute.subnetworks.useExternalIp

操作	権限
- Cloud Router を作成、使用、削除する	compute.routers.create compute.routers.delete compute.routers.get compute.routers.list compute.routers.use
- ファイアウォールルールを作成、使用、および削除する - VPC ネットワークにファイアウォールルールを追加する	compute.firewalls.create compute.firewalls.delete compute.firewalls.get compute.firewalls.list compute.firewalls.update compute.networks.updatePolicy

クラスタノードに個別のロールとサービスアカウントを作成しない場合は、次の権限を Secure Agent ロールに追加します。

ノードタイプ	操作	権限
マスタ	- ワーカーノードのインスタンスグループをスケールアップまたはスケールダウンする	compute.regions.get compute.instanceGroups.list compute.instanceGroups.update compute.instanceGroups.use compute.instanceGroups.get
ワーカー	- 初期化スクリプト通知をステージングの場所にアップロードする - 初期化スクリプトログをログの場所にアップロードする	storage.objects.create storage.objects.delete storage.objects.get storage.objects.list storage.objects.update

マスタロールとサービスアカウントの作成

必要に応じて、別のマスタロールとサービスアカウントを作成して、Secure Agent ロールに割り当てる権限の数を減らすことができます。マスタロールは、マスタノードにのみ権限を付与します。

マスタロールの作成

マスタロールを作成して、マスタノードの権限のセットを定義します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[ロール]** に移動します。
2. ロールを作成します。
3. ロールのタイトル、説明、および ID を入力します。
ID の形式には<username-master-role>を使用できます。
4. ロールに権限を追加します。

次の表に、ロールに必要な権限を示します。

操作	権限
<ul style="list-style-type: none">- ワーカーノードのインスタンスグループをスケールアップまたはスケールダウンする	<code>compute.regions.get</code> <code>compute.instanceGroups.list</code> <code>compute.instanceGroups.update</code> <code>compute.instanceGroups.use</code> <code>compute.instanceGroups.get</code>

マスタサービスアカウントを作成する

マスタロールを使用するマスタサービスアカウントを作成します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[サービスアカウント]** に移動します。
2. サービスアカウントを作成します。
3. 名前、ID、説明などのサービスアカウントの詳細を入力します。
4. プロジェクトへのサービスアカウントアクセスの詳細を入力します。
5. マスタロール<username-master-role>を選択します。

ワーカーノードロールとサービスアカウントの作成

必要に応じて、別のワーカーノードロールとサービスアカウントを作成して、Secure Agent ロールに割り当てる権限の数を減らすことができます。ワーカーロールは、ワーカーノードにのみ権限を付与します。

ワーカーロールの作成

ワーカーロールを作成して、ワーカーノードの権限のセットを定義します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[ロール]** に移動します。
2. ロールを作成します。
3. ロールのタイトル、説明、および ID を入力します。
ID の形式には<username-worker-role>を使用できます。
4. ロールに権限を追加します。

次の表に、ロールに必要な権限を示します。

操作	権限
<ul style="list-style-type: none">- 初期化スクリプト通知をステージングの場所にアップロードする- 初期化スクリプトログをログの場所にアップロードする	<code>storage.objects.create</code> <code>storage.objects.delete</code> <code>storage.objects.get</code> <code>storage.objects.list</code> <code>storage.objects.update</code>

ワーカーサービスアカウントを作成する

ワーカーロールを使用するワーカーサービスアカウントを作成します。

1. Google Cloud Web コンソールで、**[IAM と管理]** > **[サービスアカウント]** に移動します。
2. サービスアカウントを作成します。
3. 名前、ID、説明などのサービスアカウントの詳細を入力します。
4. プロジェクトへのサービスアカウントアクセスの詳細を入力します。

5. ワーカーロール<username-worker-role>を選択します。

VPC およびサブネットの準備

エラスティッククラスタをホストする固有の VPC およびサブネットを作成する場合、クラスタの要件に基づいて VPC ネットワークおよびサブネットを準備します。

ネットワークとサブネットを準備するには、VPC を作成した後に次のタスクを完了します。

1. エラスティッククラスタ内のノードに対して、十分な数の IP アドレスをサポートするサブネットを作成します。
2. Google Cloud NAT ゲートウェイを作成します。
3. TCP トラフィックを許可するために、VPC ネットワークにファイアウォールルールを作成します。

手順 1.十分な数の IP アドレスを含むサブネットの作成

VPC ネットワーク内のエラスティッククラスタのすべてのノードに対して、十分な数の IP アドレスをサポートするサブネットを作成します。

次のガイドラインに従って、必要な IP アドレスの数を計算します。

- マスターノード用に IP アドレスを 1 つ追加します。
- ワーカーノードの最大数と同数の IP アドレスを追加します。

例えば、エラスティッククラスタで最大 10 個のワーカーノードを使用できるようにする場合は、各サブネットですでに少なくとも 11 個の IP アドレスがサポートされている必要があります。

手順 2.Google Cloud NAT ゲートウェイの作成

外部 IP アドレスを持たないプライベートノードからインターネットに接続する必要がある場合は、Google Cloud Network Address Translator (NAT) ゲートウェイを作成します。

Google Cloud NAT で、次の設定を使用して VPC ネットワークに NAT ゲートウェイを作成します。

- サブネットと同じリージョンを使用します。
- デフォルト設定を使用するクラウドルーターを使用します。
- NAT マッピングソースのデフォルト値を使用します。
- NAT IP アドレスに使用する新しい静的パブリック IP アドレスを手動で作成します。

エラスティックジョブを実行する前に、NAT ゲートウェイが実行されていることを確認してください。

次の図は、Google Cloud Console での NAT ゲートウェイ設定の例を示しています。

Network services

- Load balancing
- Cloud DNS
- Cloud CDN
- Cloud NAT**
- Traffic Director
- Service Directory
- Cloud Domains
- Private Service Connect

Create a NAT gateway

Cloud NAT lets your VM instances and container pods communicate with the internet using a shared, public IP address.

Cloud NAT uses NAT gateway to manage those connections. A NAT gateway is region and VPC network specific. If you have VM instances in multiple regions, you'll need to create a NAT gateway for each region. [Learn more](#)

Gateway name *
dev-example-nat
Lowercase letters, numbers, hyphens allowed

Select Cloud Router

Network *
dev-example-vpc

Region *
us-west2 (Los Angeles)
One subnet

Cloud Router *
new-router

NAT mapping

Source (internal)
Primary and secondary ranges for all subnets
Select which subnets to map to the NAT gateway. Primary IP addresses are used by VM instances and secondary IP addresses are used by container pods. [Learn more](#)

NAT IP addresses
Manual

IP address
privateipaddress

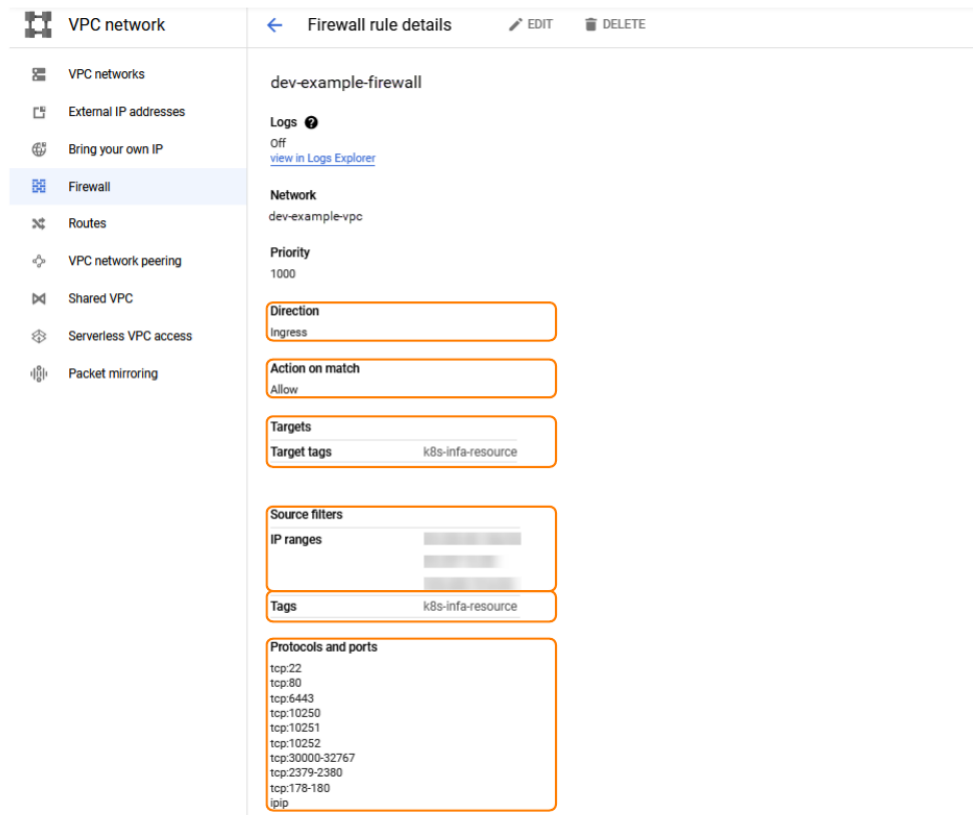
手順 3.VPC ネットワークでのファイアウォールルールの作成

VPC ネットワークのファイアウォールルールを作成して、Secure Agent マシンの IP アドレスと NAT ゲートウェイからの TCP トラフィックを許可します。

Google Cloud で、次の設定を使用して VPC ネットワークのファイアウォールルールを作成します。

- トラフィックの方向を入力トラフィックに設定します。
- 一致を許可します。
- 次のターゲットタグを追加します: k8s-infa-resource
- IP 範囲でフィルタするようにプライマリソースフィルタを設定します。CIDR 表記を使用して、ソース IP 範囲を Secure Agent マシンの静的 IP アドレスと手順 2 で作成した NAT ゲートウェイに設定します。
- ソースタグでフィルタするようにセカンダリソースフィルタを設定し、次のソースタグを追加します: k8s-infa-resource
- 次のプロトコルとポートを指定します。
 - TCP ポート: 22、80、6443、10250、10251、10252、30000-32767、2379-2380、178-180
 - その他のプロトコル: *ipip*

次の図は、ファイアウォールルールが Google Cloud Console にどのように表示されるかを示しています。



JAVA_HOME 環境変数の設定

cluster-operations.sh などのコマンドを実行するには、Secure Agent マシンで JAVA_HOME 環境変数を設定する必要があります。

Secure Agent マシンの Java バージョンは、JDK 8 と互換性がある必要があります。

第 4 章

Microsoft Azure の設定

エラスティック構成の作成を組織内で開始する前に、Microsoft Azure をセットアップして Data Integration Elastic と連携します。

以下のタスクを完了させます。

1. 環境の要件を確認する。
2. Secure Agent をダウンロードし、Azure クラウドにある Linux 仮想マシンにインストールします。
3. Azure のドメインをホワイトリストに登録します。
4. オプションで、クラスタのプロキシを設定します。
5. クラスタファイルのストレージアカウントを作成する。
6. クラスタリソースグループの作成
7. Secure Agent のマネージド ID を作成する。
8. クラスタ用のサービスプリンシパルを作成する。
9. オプションで、JAVA_HOME 環境変数を設定する。

始める前に

環境をセットアップする前に、環境とクラウドプラットフォームの要件を確認してください。

以下のタスクを完了させます。

- 組織で正しい特権を持っていることを確認してください。
- 必要な Microsoft Azure 製品があることを確認します。
- Data Integration Elastic がクラウドプラットフォーム上のリソースにアクセスする方法を学びます。

組織の権限の確認

組織のエラスティック構成に対する適切な特権が割り当てられていることを確認します。

エラスティック構成に対する特権によって、Administrator および Monitor の【エラスティッククラスタ】ページへのアクセスレベルは異なります。

エラスティック構成の表示とエラスティッククラスタの監視を行うには、少なくとも読み取り権限が必要です。

Microsoft Azure 製品を確認する

Azure 環境でエラスティッククラスタを作成するために必要な Microsoft Azure 製品があることを確認します。

Azure アカウントで次の製品が必要です。

Microsoft Azure Blob Storage **または** Azure Data Lake Storage Gen2

エラスティッククラスタおよびエラスティックジョブのステージングデータとログファイルは、Azure クラウドに保存されます。

Linux **仮想マシン**

Linux 仮想マシンは Secure Agent をホストします。

仮想ネットワーク (VNet)

エラスティッククラスタは VNet に作成されます。既存の VNet を指定するか、または指定したリージョンに基づき Secure Agent が VNet を作成することができます。

Key Vault

クラスタ操作を実行するためのサービスプリンシパルを作成する場合、Key Vault にサービスプリンシパルの資格情報が保存されます。Secure Agent は Key Vault にアクセスして資格情報を取得します。

ロードバランサ

ロードバランサは、Secure Agent からの受信エラスティックジョブを受け入れ、エラスティッククラスタへのジョブのエントリポイントを提供します。

リソースへのアクセスの詳細

データを処理するために、Secure Agent およびエラスティッククラスタは、クラウドプラットフォーム上のリソース、ソースおよびターゲットデータ、ステージングおよびログの場所などの、エラスティックジョブの一部であるリソースにアクセスします。

リソースへのアクセスは実行されるタスクによって異なります。

- エラスティックマッピングの設計
- エラスティッククラスタの作成
- エラスティックジョブの実行
- ログのポーリング

エラスティックマッピングの設計

エラスティックマッピングの設計は、データ統合でのエラスティックマッピング以外のマッピングの設計に似ています。マッピングを設計すると、Secure Agent はソースとターゲットにアクセスするため、ユーザーはデータの読み取りと書き込みができます。

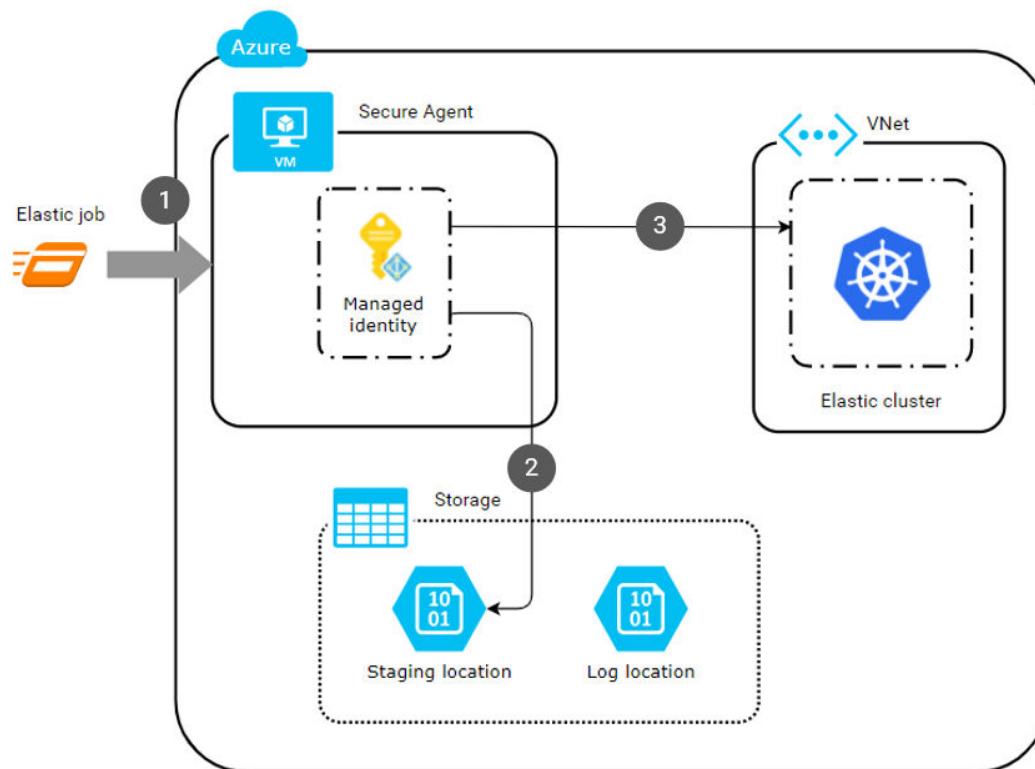
例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで利用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

ソースまたはターゲットにアクセスするために、Secure Agent は接続プロパティを使用します。例えば、Secure Agent は接続プロパティ内に指定するユーザー名およびパスワードを使用してデータベースにアクセスすることがあります。

エラスティッククラスタの作成

エラスティッククラスタを作成するには、Secure Agent がステージングの場所にクラスタ情報を保存して、クラスタを作成するのと同じリソースにアクセスします。

次の図は、Secure Agent がクラスタを作成するときの一連のイベントを示しています。

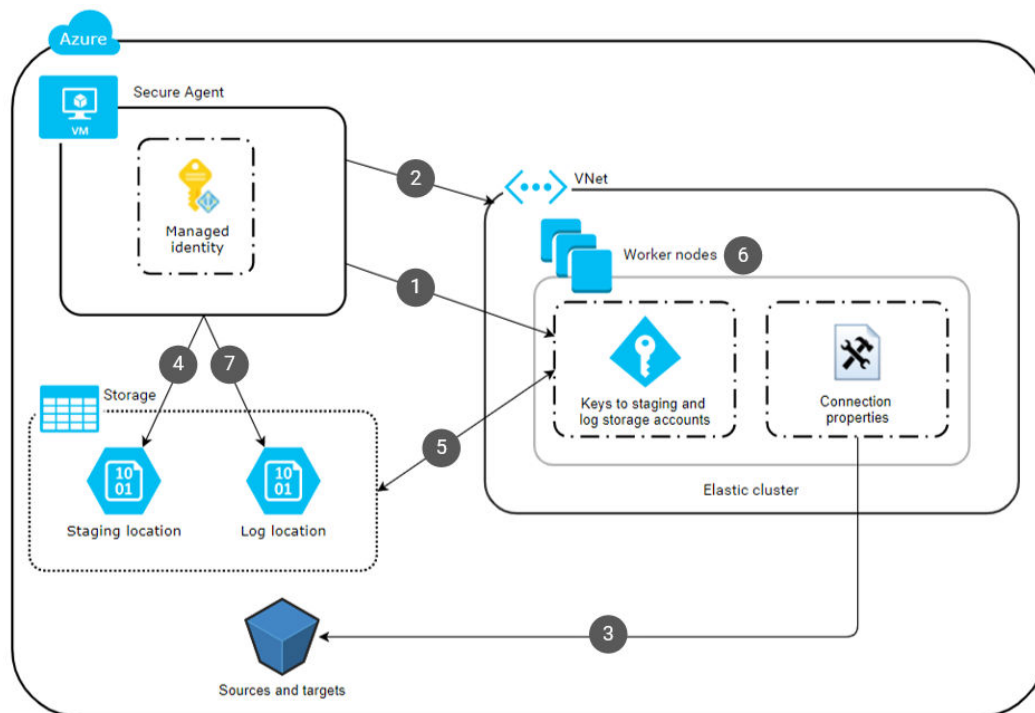


1. エラスティックジョブを実行します。
2. Secure Agent が、マネージド ID の権限を使用してステージングの場所にクラスタ情報を保存します。
3. Secure Agent が、マネージド ID の権限を使用してクラスタリソースを作成し、エラスティッククラスタを開始します。

ジョブの実行

エラスティックジョブを実行するために、Secure Agent およびワーカーノードはソースおよびターゲット、ステージングの場所およびログの場所にアクセスします。一方、ワーカーノードと Azure ディスクは、必要に応じて自動スケールを行います。

次の画像に、ジョブをエラスティッククラスターで実行するときのリソースへのアクセス方法について示します。



1. Secure Agent は、マネージド ID を使用してステージングおよびログストレージアカウントにアクセスキーを収集し、セキュアチャネルを使用してワーカーノードでキーを使用できるようにします。
2. Secure Agent によってクラスターへのサービスプリンシパルの資格情報が使用可能になります。
3. ワーカーノードは接続プロパティを使用してソースおよびターゲットデータにアクセスします。
4. Secure Agent は、マネージド ID を使用してステージングの場所にジョブの依存関係を保存します。
5. ワーカーノードはステージングおよびログストレージアカウントへのアクセスキーを使用して、ステージングの場所からジョブの依存関係を取得し、ステージングの場所のデータをステージングし、ログの場所にログを保存します。
6. ワーカーノードと Azure ディスクは、サービスプリンシパルの権限を使用して自動スケールを行います。
7. Secure Agent は、マネージド ID を使用してエージェントジョブのログをログの場所にアップロードします。

ログのポーリング

Monitor を使用すると、Secure Agent はログの場所にアクセスしてログをポーリングします。

ログの場所からログをポーリングするために、Secure Agent は Secure Agent マシンに割り当てられたマネージド ID の権限を使用します。

Secure Agent のダウンロードとインストール

Secure Agent をダウンロードし、Azure クラウドにある Linux 仮想マシンにインストールします。この VM は、Secure Agent マシンと呼ばれます。

次の表に、Secure Agent マシンの最小リソース要件を一覧表示します。

コンポーネント	最小要件
CPU あたりのコア数	4 以上
メモリ	16GB
ディスク空き容量	100GB

Secure Agent をインストールした後、Secure Agent マシンに OpenSSL をインストールします。

Secure Agent のインストールに関する詳細については、「ランタイム環境」を参照してください。

Azure のドメインのホワイトリスト登録

Secure Agent が Microsoft Azure でエラスティッククラスタを作成する場合、クラスタノードは、マシンイメージなどのアーティファクトを取得し、ソースとターゲットにアクセスするために、特定のドメインにアクセスする必要があります。

次のドメインをホワイトリストに登録します。

```
infacloud.jfrog.io
infacloud-ct-cdie-docker.jfrog.io
infacloud-discale-docker-stable.jfrog.io
discale-docker-stable.artifacts.cloudtrust.rocks
```

```
*.azure.com
*.azure.net
*.database.windows.net
*.microsoft.com
*.microsoftonline.com
*.microsoftonline.com
*.windows.net
azure.com
azure.net
ifconfig.me
microsoft.com
microsoftonline.com
microsoftonline.com
windows.net
```

クラスタのプロキシの設定

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

クラスタにプロキシサーバーを使用するには、Secure Agent のプロキシサーバーを編集します。クラスタに割り当てられる予定の IP アドレスを除外します。

次のファイルでプロキシサーバーの詳細を編集できます。

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

InfAgent.NonProxyHost プロパティを設定して、IP アドレスを除外します。

以下の手順を実行します。

1. proxy.ini ファイルを開きます。
2. InfAgent.NonProxyHost の値を更新して、クラスタ IP アドレスを除外します。

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 のクラスタ IP アドレスが除外されます。

```
InfAgent.NonProxyHost=localhost|127.[\:\:1]|123.432.|172.16.*|172.16.0.0/16
```

注: パイプ文字 (|) は、ホスト名と IP アドレスのリストを結合する区切り文字です。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。

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。

変更が有効になると、Secure Agent はプロキシを通過せずにクラスタと通信しますが、クラスタと通信するコマンドはプロキシを通過する必要があります。

非プロキシホストを除外するようにプロキシを設定する方法の詳細については、「ランタイム環境」を参照してください。

クラスタファイルのストレージアカウントの作成

データは、Microsoft Azure Blob Storage または Azure Data Lake Storage Gen2 を使用して保存できます。

Azure で、次のストレージアカウントを作成します。

- 次の場所を使用したストレージアカウント:
 - クラスタがランタイムにステージングファイルを保存するために使用する場所
 - クラスタ上で実行されるエラスティックジョブ用のログファイルを保存するためにクラスタが使用する場所
- オプションで、クラスタに追加のソフトウェアをインストールするためにクラスタノードが実行する初期化スクリプトを格納できるストレージアカウント

次に、これらのストレージアカウントを storage_resource_group という名前のリソースグループに追加します。

ステージングの場所には、クラスタがクラスタノード全体に配布するアーティファクトやマッピングでプレビューするデータなどの一時データが格納されます。エラーにより、マッピングでステージングの場所のプレビューデータをクリアできない可能性があるため、ステージングの場所にアクセスできるユーザーがソースデータの表示を許可されていることを確認してください。

初期化スクリプトを作成する場合は、スクリプトを適切な場所に追加します。

Microsoft Azure Blob

Azure Blob ストレージを使用する場合は、クラスタファイルを保持するための BLOB データのストレージアカウントを作成します。階層型名前空間が無効になっていることを確認してください。

Azure Data Lake Storage Gen2

Azure Data Lake Storage Gen2 を使用する場合は、階層型名前空間を持つストレージアカウントを作成します。

クラスタリソースグループの作成

Azure で、`cluster_resource_group` という名前のリソースグループを作成します。

Secure Agent は、このリソースグループを使用して、マスタノードとワーカーノードの VM、仮想マシンのスケールセット、ネットワークインタフェース、ロードバランサなどのクラスタリソースを格納します。

Secure Agent 向けのマネージド ID の作成

Secure Agent はマネージド ID を使用して Microsoft Azure クラウドにログインし、エラスティッククラスタを作成します。`list-clusters.sh` および `delete-clusters.sh` コマンドを実行している場合は、Secure Agent ではマネージド ID を使用して Azure CLI を認証します。

Azure で、以下のタスクを実行します。

1. マネージド ID を作成します。
2. エージェントロールを作成します。
3. ロールの割り当てを追加して、エージェントロールをマネージド ID に割り当て、マネージド ID を Secure Agent マシンに割り当てます。

手順 1. マネージド ID を作成する

`agent_identity` という名前でマネージド ID を作成します。

システムによって割り当てられた既存のマネージド ID を使用することも、ユーザーによって割り当てられたマネージド ID を作成することもできます。ユーザーが割り当てたマネージド ID を作成する場合は、システムが割り当てたマネージド ID を無効にします。

マネージド ID の作成手順については、Microsoft Azure のドキュメントを参照してください。

手順 2. エージェントロールの作成

マネージド ID `agent_identity` の権限を定義するエージェントロールを作成します。

次のロール定義を使用して、`agent_role` という名前のカスタムロールを作成します。

```
{
  "properties": {
    "roleName": "agent_role",
    "description": ""
  }
}
```

```

"assignableScopes":[
  "/subscriptions/<subscription ID>/resourceGroups/<cluster_resource_group>",
  "/subscriptions/<subscription ID>/resourceGroups/<storage_resource_group>",
  "/subscriptions/<subscription ID>/resourceGroups/<vnet_resource_group>"
],
"permissions":[
  {
    "actions":[
      "Microsoft.Resources/subscriptions/resourcegroups/read",
      "Microsoft.Storage/storageAccounts/read",
      "Microsoft.Storage/storageAccounts/write",
      "Microsoft.Storage/storageAccounts/listKeys/action",
      "Microsoft.Compute/virtualMachineScaleSets/delete",
      "Microsoft.Compute/virtualMachineScaleSets/write",
      "Microsoft.Compute/virtualMachineScaleSets/read",
      "Microsoft.Network/loadBalancers/delete",
      "Microsoft.Network/loadBalancers/write",
      "Microsoft.Network/loadBalancers/read",
      "Microsoft.Network/networkSecurityGroups/delete",
      "Microsoft.Network/networkSecurityGroups/write",
      "Microsoft.Network/networkSecurityGroups/read",
      "Microsoft.Network/virtualNetworks/delete",
      "Microsoft.Network/virtualNetworks/write",
      "Microsoft.Network/virtualNetworks/read",
      "Microsoft.Network/publicIPAddresses/delete",
      "Microsoft.Network/publicIPAddresses/write",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Network/publicIPAddresses/join/action",
      "Microsoft.Network/virtualNetworks/subnets/join/action",
      "Microsoft.Network/networkSecurityGroups/join/action",
      "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
      "Microsoft.Compute/virtualMachineScaleSets/publicIPAddresses/read",
      "Microsoft.Compute/virtualMachineScaleSets/networkInterfaces/read",
      "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
      "Microsoft.Compute/virtualMachines/instanceView/read",
      "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read",
      "Microsoft.Compute/virtualMachineScaleSets/instanceView/read",
      "Microsoft.Authorization/roleAssignments/read",
      "Microsoft.Authorization/roleDefinitions/read"
    ],
    "notActions":[
    ],
    "dataActions":[
    ],
    "notDataActions":[
    ]
  }
]
}
}
}

```

次の表に、権限を示します。

権限	説明
Microsoft.Resources/subscriptions/resourcegroups/read	必須。クラスタリソースグループが存在するかどうかを確認します。
Microsoft.Resources/subscriptions/resourcegroups/write Microsoft.Resources/subscriptions/resourcegroups/delete	クラスタリソースグループがエラスティック構成指定されていない場合に必要です。 エラスティック構成でクラスタリソースグループを指定していない場合、Secure Agent は、<cluster-instance-id>-rg という名前でサブスクリプションに新しいリソースグループを作成します。

権限	説明
Microsoft.Storage/storageAccounts/read Microsoft.Storage/storageAccounts/write Microsoft.Storage/storageAccounts/listKeys/action	必須。ストレージアカウントキーを一覧表示し、Blob 操作を実行します。これらのアクションは、ステージングストレージアカウントがクラスターソースグループ内にあることを前提としています。
Microsoft.Compute/virtualMachineScaleSets/delete Microsoft.Compute/virtualMachineScaleSets/write Microsoft.Compute/virtualMachineScaleSets/read	必須。マスタノードとワーカーノードの仮想マシンスケールセット (VMSS) を検出して管理します。
Microsoft.Network/loadBalancers/delete Microsoft.Network/loadBalancers/write Microsoft.Network/loadBalancers/read	必須。API サーバーエンドポイントに使用されるロードバランサを検出して管理します。
Microsoft.Network/networkSecurityGroups/delete Microsoft.Network/networkSecurityGroups/write Microsoft.Network/networkSecurityGroups/read	必須。マスタノードとワーカーノード用に作成されたネットワークセキュリティグループを検出して管理します。ネットワークセキュリティグループ (NSG) がサブネットに接続されている場合、これらの権限は、サブネットで指定されたルールを上書きします。
Microsoft.Network/virtualNetworks/read	必須。エラスティッククラスタの VNet を検出します。
Microsoft.Network/virtualNetworks/delete Microsoft.Network/virtualNetworks/write	クラスタアセットで VNet が指定されていない場合に必要です。
Microsoft.Network/publicIPAddresses/delete Microsoft.Network/publicIPAddresses/write Microsoft.Network/publicIPAddresses/read Microsoft.Network/publicIPAddresses/join/action	必須。クラスタエンドポイントに関連付けられているパブリック IP アドレスを検出して管理します。ロードバランサがこのパブリック IP アドレスを使用できるようにするには、参加アクションが必要です。
Microsoft.Network/virtualNetworks/subnets/join/action	必須。マスタノードとワーカーノードが特定のサブネットに参加できるようにします。この権限は、あらゆる形式の VNet 設定に必要です。 既存の VNet を使用する場合、この権限の範囲には、VNet を保持するリソースグループが含まれている必要があります。
Microsoft.Network/virtualNetworks/subnets/read	既存の VNet を使用する場合に必要です。この権限の範囲には、VNet を保持するリソースグループが含まれている必要があります。
Microsoft.Network/networkSecurityGroups/join/action	必須。マスタノードとワーカーノードが事前に作成されたネットワークセキュリティグループ (NSG) を接続できるようにします。
Microsoft.Network/loadBalancers/backendAddressPools/join/action	必須。マスタノードとワーカーノードをクラスタエンドポイントに追加できるようにします。マスタノードは、クラスタのプロビジョニング中にクラスタエンドポイントに追加されます。

権限	説明
Microsoft.Compute/ virtualMachineScaleSets/ publicIPAddresses/read Microsoft.Compute/ virtualMachineScaleSets/ networkInterfaces/read	必須。Secure Agent がマスタノードとワーカーノードに割り当てられた IP アドレスを取得するために使用します。Secure Agent は、これらの権限を使用して、SSH を使用してマスタノードに接続し、特定のクラスタの kubeconfig ファイルをダウンロードします。
Microsoft.Compute/ virtualMachineScaleSets/virtualMachines/ read Microsoft.Compute/virtualMachines/ instanceView/read Microsoft.Compute/ virtualMachineScaleSets/virtualMachines/ instanceView/read Microsoft.Compute/ virtualMachineScaleSets/instanceView/read	必須。マスタノードとワーカーノードのステータスを確認します。
Microsoft.Compute/ virtualMachineScaleSets/manualupgrade/ action	初期化スクリプトを使用する場合に必要です。 また、スクリプト拡張を適用するためにはマスタノードとワーカーノードを手動で更新する必要があります。
Microsoft.Authorization/roleAssignments/ read Microsoft.Authorization/roleDefinitions/read	必須。エラスティック構成を検証します。

手順 3. ロールの割り当ての追加

ロールの割り当てを追加して、エージェントロールをマネージド ID に割り当てます。次に、マネージド ID を Secure Agent マシンに割り当てます。

以下のタスクを完了させます。

1. カスタムロール agent_role を agent_identity という名前のマネージド ID に割り当てます。
2. マネージド ID agent_identity を、Secure Agent がインストールされている VM に割り当てます。

クラスタ用のサービスプリンシパルの作成

エラスティッククラスタでクラスタ操作を実行するサービスプリンシパルを作成します。このサービスプリンシパルを使用して、エラスティック構成にデータを取り込みます。

Azure で、以下のタスクを実行します。

1. サービスプリンシパルを作成します。
2. クラスタロールを作成します。
3. ロールの割り当てを追加して、クラスタロールをサービスプリンシパルに割り当てます。
4. サービスプリンシパル資格情報を Key Vault に保存します。
5. アクセスポリシーを Key Vault に追加します。

手順 1。サービスプリンシパルを作成する

cluster_principal という名前のサービスプリンシパルを作成します。

サービスプリンシパルの作成手順については、Microsoft Azure のドキュメントを参照してください。

手順 2。クラスタロールの作成

クラスタロールを作成して、サービスプリンシパル cluster_principal の権限を定義します。

次のロール定義を使用して、cluster_role という名前のカスタムロールを作成します。

```
{
  "properties": {
    "roleName": "cluster_role",
    "description": "",
    "assignableScopes": [
      "/subscriptions/<subscription ID>/resourceGroups/<cluster_resource_group>",
      "/subscriptions/<subscription ID>/resourceGroups/<storage_resource_group>",
      "/subscriptions/<subscription ID>/resourceGroups/<vnet_resource_group>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
          "Microsoft.Compute/virtualMachineScaleSets/read",
          "Microsoft.Compute/virtualMachineScaleSets/delete/action",
          "Microsoft.Compute/virtualMachines/instanceView/read",
          "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read",
          "Microsoft.Compute/virtualMachineScaleSets/instanceView/read",
          "Microsoft.Compute/virtualMachineScaleSets/write",
          "Microsoft.Network/networkSecurityGroups/join/action",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
          "Microsoft.Compute/disks/delete",
          "Microsoft.Compute/disks/write",
          "Microsoft.Compute/disks/read",
          "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

次の表に、権限を示します。

権限	説明
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read Microsoft.Compute/virtualMachineScaleSets/write Microsoft.Network/loadBalancers/backendAddressPools/join/action Microsoft.Network/networkSecurityGroups/join/action	必須。Secure Agent がクラスタリソースを検出するために使用します。
Microsoft.Network/virtualNetworks/subnets/join/action	必須。Secure Agent がクラスタリソースを検出するために使用します。 既存の VNet を使用する場合、この権限の範囲には、VNet を保持するリソースグループが含まれている必要があります。

権限	説明
Microsoft.Network/virtualNetworks/subnets/read	既存の VNet を使用する場合に必要です。 この権限の範囲には、VNet を保持するリソースグループが含まれている必要があります。
Microsoft.Compute/virtualMachineScaleSets/read Microsoft.Compute/virtualMachines/instanceView/read Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read Microsoft.Compute/virtualMachineScaleSets/instanceView/read	必須。Secure Agent が、Azure で実行されているマスタノードとワーカーノードを検出するために使用します。
Microsoft.Network/virtualNetworks/subnets/join/action Microsoft.Compute/virtualMachineScaleSets/write Microsoft.Network/networkSecurityGroups/join/action	クラスタにワーカーノードを追加するためにクラスタが自動スケールを実行する場合に必要です。
Microsoft.Compute/disks/write Microsoft.Compute/disks/read Microsoft.Compute/disks/delete	ストレージが自動スケールを実行する場合に必要です。 これらの権限によって、Azure 上のディスクを管理します。
Microsoft.Compute/virtualMachineScaleSets/virtualmachines/write	ストレージとクラスタが自動スケールを実行する場合に必要です。 これらの権限によって、Azure ディスクをワーカーノードに接続します。
Microsoft.Network/virtualNetworks/subnets/join/action	ストレージとクラスタが自動スケールを実行する場合に必要です。
Microsoft.Network/networkSecurityGroups/join/action	ストレージとクラスタが自動スケールを実行する場合に必要です。 Secure Agent は、この権限を使用して、マスタノードとワーカーノードにアタッチされるメタデータを更新します。

手順 3. ロールの割り当ての追加

ロールの割り当てを追加して、カスタムロール `cluster_role` をサービスプリンシパル `cluster_principal` に割り当てます。

手順 4. 資格情報の Key Vault への保存

新しい Key Vault を作成し、サービスプリンシパル `cluster_principal` の資格情報を保存するためのシークレットを生成します。

手順 5. アクセスポリシーを Key Vault に追加します。

マネージド ID `agent_identity` にサービスプリンシパル `cluster_principal` の資格情報へのアクセスを許可するアクセスポリシーを、Key Vault に追加します。

1. アクセスポリシーを Key Vault に追加します。

2. アクセスポリシーで、サービスプリンシパル `cluster_principal` 用に生成したシークレットを選択します。
3. マネージド ID `agent_identity` にシークレットの権限を付与します。

JAVA_HOME 環境変数の設定

`list-clusters.sh`、`delete-clusters.sh` などのコマンドを実行するには、Secure Agent マシンで `JAVA_HOME` 環境変数を設定する必要があります。

Secure Agent マシンの Java バージョンは、JDK 8 と互換性がある必要があります。

第 5 章

セルフサービスクラスタの設定

エラスティック構成の作成を組織内で開始する前に、セルフサービスクラスタをセットアップして Data Integration Elastic と連携します。

始める前に

環境をセットアップする前に、環境とクラウドプラットフォームの要件を確認してください。Amazon Virtual Private Cloud (VPC) 上に Kubernetes クラスタを作成したことを確認してください。

以下のタスクを完了させます。

- 組織で正しい特権を持っていることを確認してください。
- Data Integration Elastic がクラウドプラットフォーム上のリソースにアクセスする方法を学びます。

エラスティックマッピングを実行するようにセルフサービスクラスタをセットアップするために必要な最小リソース仕様については、[「クラスタノードのリソース要件」 \(ページ 134\)](#)を参照してください。

組織の権限の確認

組織のエラスティック構成に対する適切な特権が割り当てられていることを確認します。

エラスティック構成に対する特権によって、Administrator および Monitor の **【エラスティッククラスタ】** ページへのアクセスレベルは異なります。

エラスティック構成の表示とセルフサービスクラスタの監視を行うための読み取り権限があることを確認してください。

リソースへのアクセスの詳細

データを処理するために、Secure Agent およびセルフサービスクラスタは、クラウドプラットフォーム上のリソース、ソースおよびターゲットデータ、ステージングおよびログの場所などの、エラスティックジョブの一部であるリソースにアクセスします。

リソースへのアクセスは実行されるタスクによって異なります。

- エラスティックマッピングの設計
- セルフサービスクラスタの作成
- エラスティックマッピングを実行するためのクラスタロールの最適化
- エラスティックジョブの実行
- ログのポーリング

エラスティックマッピングの設計

エラスティックマッピングの設計は、データ統合でのエラスティックマッピング以外のマッピングの設計に似ています。マッピングを設計すると、Secure Agent はソースとターゲットにアクセスするため、ユーザーはデータの読み取りと書き込みができます。

例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで利用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

ソースまたはターゲットにアクセスするために、Secure Agent は接続プロパティを使用します。例えば、Secure Agent は接続プロパティ内に指定するユーザー名およびパスワードを使用してデータベースにアクセスすることがあります。

セルフサービスクラスタの作成

Virtual Private Cloud (VPC) に Kubernetes クラスタを作成し、構成を含む生成された kubeconfig ファイルを使用して Secure Agent にデータを入力します。

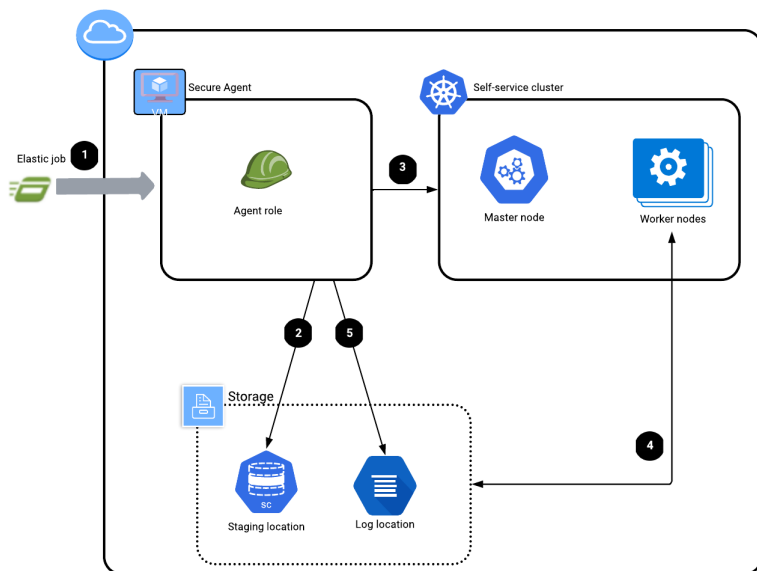
Secure Agent は、クラスタ情報をステージングの場所に保管し、同じリソースにアクセスしてクラスタに接続します。

Informatica では、クラスタネットワーキングとパフォーマンスの向上のために、セルフサービスの Kubernetes クラスタで Calico プラグインを使用することをお勧めします。詳細については、[Kubernetes cluster networking with Calico plug-in](#) を参照してください。

ジョブの実行

エラスティックジョブを実行するために、Secure Agent およびワーカーノードはソースおよびターゲット、ステージングの場所およびログの場所にアクセスします。

次の図に、ジョブをセルフサービスクラスタで実行するときのリソースへのアクセス方法について示します。



1. エラスティックジョブを実行します。
2. Secure Agent は、Secure Agent ロールの権限を使用して、クラスタ情報をステージングの場所に保存します。
3. Secure Agent は、kubeconfig ファイルを使用してクラスタにアクセスし、セルフサービスクラスタにジョブを送信します。
4. ワーカーノードはステージングおよびログストレージアカウントへのアクセス情報を使用して、ステージングの場所からジョブの依存関係を取得し、ステージングの場所のデータをステージングし、ログの場所にログを保存します。
5. Secure Agent は、Secure Agent ロールを使用して、エージェントジョブログをログの場所にアップロードします。

ログのポーリング

Monitor を使用すると、Secure Agent はログの場所にアクセスしてログをポーリングします。

ログの場所からログをポーリングするために、Secure Agent は Secure Agent マシンに割り当てられたロールを使用します。

Secure Agent のダウンロードとインストール

Linux 仮想マシンに Secure Agent をダウンロードしてインストールします。仮想マシンは Amazon EC2 インスタンスに配置できます。この仮想マシンは、Secure Agent マシンと呼ばれます。

次の表に、Secure Agent マシンの最小リソース要件を一覧表示します。

コンポーネント	最小要件
CPU あたりのコア数	4 以上
メモリ	16GB
ディスク空き容量	100GB

Secure Agent のインストールに関する詳細については、「ランタイム環境」を参照してください。

ユーザー管理のサービスアカウントの作成

Kubernetes セルフサービスクラスタでエラスティックマッピングを実行するには、サービスアカウントユーザーに必要なクラスタロール権限を定義する必要があります。

次のサービスアカウントに基づいて権限を定義できます。

- ユーザー管理のサービスアカウント
- Informatica が管理するサービスアカウント

ユーザー管理のサービスアカウント用に、クラスタでサービスアカウントを作成します。サービスアカウントは、任意の名前空間で作成できます。サービスアカウントトークンを kubeconfig ファイルに追加します。

Kubernetes セルフサービスクラスタで管理するサービスアカウント用に次のリソースを作成します。

最適化されたクラスタロールの作成

次の権限を持つクラスタロールを作成します。クラスタロールは、どの名前空間とも関連付けられていません。

Spark シャッフルサービスを使用してエラスティックマッピングを実行するために必要な最小権限

次のコードスニペットは、Spark シャッフルサービスを使用してエラスティックマッピングを実行するために必要な最小権限を示しています。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: optimized-cluster-role
rules:
- apiGroups: [""]
  resources: ["services", "pods", "secrets", "configmaps"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]
- apiGroups: ["apps"]
  resources: ["deployments"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]
```

```
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["watch", "list", "get", "patch"]
- apiGroups: [""]
  resources: ["namespaces", "persistentvolumeclaims"]
  verbs: ["watch", "list", "get"]
```

Spark シャッフルサービスなしでエラスティックマッピングを実行するために必要な最小権限

次のコードスニペットは、Spark シャッフルサービスなしでエラスティックマッピングを実行するために必要な最小権限を示しています。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: optimized-cluster-role
rules:

- apiGroups: [""]
  resources: ["pods/exec", "pods/log"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["watch", "list", "get"]
- apiGroups: [""]
  resources: ["namespaces", "persistentvolumeclaims"]
  verbs: ["watch", "list", "get"]
```

クラスタロールの作成バインディング

サービスアカウントとクラスタロールを参照して、クラスタロールバインディングを作成します。

エラスティック構成でのサービスアカウントの設定

サービスアカウント名を使用して、Administrator でエラスティック構成を作成できます。

［ランタイム設定］ タブで、`infa.k8s.spark.custom.service.account.name` プロパティをサービスアカウント名に設定します。Spark エンジンで、Spark ドライバと Spark シャッフルサービス（有効になっている場合）のサービスアカウントが使用されるようになります。

Self_Service_Cluster

Create or modify an elastic configuration that you can use to run elastic jobs.

Basic Configuration

Name: * Self_Service_Cluster

Description:

Runtime Environment: ? agent_discale_aws ▼

Cloud Platform: * Self Service Cluster ▼

Platform Configuration Advanced Configuration Runtime Configuration

Encrypt Data: ? ☐

Runtime Properties (1): ?

Key ▲	Value
infa.k8s.spark.custom.service.account.name	infa-spark-service-account

Informatica が管理するサービスアカウントの作成（代替）

infa.k8s.spark.custom.service.account.name プロパティを使用してサービスアカウント名を指定しない場合、Informatica は、デフォルトでサービスアカウント、クラスターロール、およびクラスターロールバインディングを作成します。

infa-spark サービスアカウントは、Spark ドライバの infa-spark-role クラスターロールバインディングと一緒に作成されます。このクラスターロールは Kubernetes クラスターにすでに存在するため、このクラスターロールバインディングは「編集」クラスターロールを使用します。「編集」ロールを使用すると、ポッドのデプロイなどの基本的なアクションを実行できます。詳細については、Kubernetes のマニュアルを参照してください。

Spark シャッフルサービスを有効にすると、個別のサービスアカウント、クラスターロール、およびクラスターロールバインディングがクラスター上に作成されます。Spark シャッフルサービスを使用するには、ユーザーまたはサービスアカウントに次のクラスターロール権限が必要です。

```
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: spark-shuffle
  labels:
    {{- range $index, $value := .Values.shuffleDsServiceAccountLabels }}
    {{ $index }}: {{ $value }}
    {{- end }}
rules:
- apiGroups: [""]
  resources: ["events", "endpoints"]
```

```

    verbs: ["create", "patch"]
  - apiGroups: [""]
    resources: ["pods/eviction"]
    verbs: ["create"]
  - apiGroups: [""]
    resources: ["pods/status"]
    verbs: ["update"]
  - apiGroups: [""]
    resources: ["nodes"]
    verbs: ["watch", "list", "get", "update", "patch"]
  - apiGroups: [""]
    resources: ["pods", "services", "replicationcontrollers", "persistentvolumeclaims", "persistentvolumes"]
    verbs: ["watch", "list", "get"]
  - apiGroups: ["apps"]
    resources: ["replicasets", "daemonsets"]
    verbs: ["watch", "list", "get"]
  - apiGroups: ["policy"]
    resources: ["poddisruptionbudgets"]
    verbs: ["watch", "list"]
  - apiGroups: ["apps"]
    resources: ["statefulsets"]
    verbs: ["watch", "list", "get"]
  - apiGroups: ["storage.k8s.io"]
    resources: ["storageclasses"]
    verbs: ["watch", "list", "get"]

```

注釈と許容

セルフサービスクラスタの設定中に、注釈と許容を定義できます。

注釈

注釈（Kubernetes ではアノテーションと呼ばれる）を使用すると、識別用途でないメタデータを Kubernetes オブジェクトに追加できます。注釈の例としては、最終更新日時、管理者、オブジェクトの責任者の電話番号、デバッグ目的のツール情報などが挙げられます。注釈内のメタデータは大小さまざまで、構造化されているものや、そうでないものも設定でき、ラベルでは許可されていない文字も含むことができます。ツールやライブラリなどのクライアントは、このメタデータを取得できます。

注釈は、リソースに関するコンテキストを提供できるあらゆる種類の有用な情報を保持できます。注釈は通常、マシンにより生成されたデータで構成されます。

許容

許容（Kubernetes では Toleration と呼ばれる）は、一致する Taint が設定されている場合に Kubernetes スケジューラがポッドをスケジュールできるようにする Kubernetes ポッドプロパティです。Taint は、ノードがポッドのセットを排除できるようにする Kubernetes ノードプロパティです。許容はポッドに適用されます。Taint と許容は連携して機能し、ポッドが適切でないノードにスケジュールされないようにします。

許容は、**【セルフサービスクラスタ】** 設定の **【詳細設定】** タブでキーと値のペアとして定義するようにします。詳細については、[「詳細設定」](#)（[ページ 131](#)）を参照してください。

注釈と許容の詳細については、Kubernetes のドキュメントを参照してください。

Amazon EKS クラスタ認証

Amazon EKS は、IAM を使用して Kubernetes クラスタに認証を提供します。

Amazon EKS クラスタの kubeconfig ファイルを作成する場合、有効な IAM エンティティに対して次のいずれかの認証方法を使用できます。

- AWS CLI
- AWS IAM 認証システム

AWS CLI または AWS IAM 認証システムを使用して、kubeconfig ファイルで AWS 資格情報を指定できます。クラスタ認証方法を使用すると、使用する適切なプロファイルを定義できます。「exec」フローの一環として設定された環境変数はすべて、環境内ですでに設定されているものよりも優先されます。AWS CLI が Secure Agent と同じ VM にインストールされていることを確認してください。

AWS CLI

AWS CLI 認証によって提供される認証トークンを使用するように kubectl を設定するサンプルコマンド:

```
users:
- name: eks_cdie-eks-GT3YbtNg
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1alpha1
      command: aws-iam-authenticator
      args:
        - "token"
        - "-i"
        - "cdie-eks-GT3YbtNg"
```

AWS CLI 認証を使用するクラスタでは、長時間実行されるマッピングが失敗する可能性があります。認証メカニズムをサービスアカウントトークン認証システムに切り替えて、マッピングを再実行できます。

AWS IAM 認証システム

AWS IAM 認証システムによって提供される認証トークンを使用するように kubectl を設定するサンプルコマンド:

```
users:
- name: arn:aws:eks:ap-southeast-1:543463116864:cluster/cdie-eks-GT3YbtNg
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1alpha1
      args:
        - --region
        - ap-southeast-1
        - eks
        - get-token
        - --cluster-name
        - cdie-eks-GT3YbtNg
      command: aws
```

上記の認証タイプのほかに、Kubernetes のクライアント証明書とサービスアカウントトークンを使用して AWS EKS クラスタを認証することもできます。Kubernetes 認証ストラテジの詳細については、Kubernetes のドキュメントを参照してください。

シーケンスジェネレータトランスフォーメーション

セルフサービスクラスタ上のエラスティックマッピングでシーケンスジェネレータトランスフォーメーションを使用できます。

シーケンスジェネレータトランスフォーメーションは、数値を生成する、接続されたパッシブトランスフォーメーションです。一意なプライマリキー値の作成、欠落しているプライマリキーの置き換え、連続した数値のでサイクル動作を実行する場合、Sequence Generatorを使用します。

セルフサービスクラスタでは、シーケンスジェネレータトランスフォーメーションによるパブリックキーとプライベートキーの生成に失敗する場合があります。セッションログにエラーメッセージが記録されます。このログメッセージは無視してかまいません。

セルフサービスクラスタのドメインのホワイトリスト登録

セルフサービスクラスタを使用する場合、クラスタノードは、アーティファクトを取得し、ソースとターゲットにアクセスするために、特定のドメインにアクセスする必要があります。

次のドメインをホワイトリストに登録します。

```
infacloud.jfrog.io
infacloud-ct-cdie-docker.jfrog.io
infacloud-discale-docker-stable.jfrog.io
discale-docker-stable.artifacts.cloudtrust.rocks
https://storage.googleapis.com
```

第 6 章

ローカルクラスタの設定

エラスティック構成の作成を組織内で開始する前に、ローカルクラスタをセットアップして Data Integration Elastic と連携します。

以下のタスクを完了させます。

1. 組織の権限を確認します。
2. ステージングとログの場所を作成します。
3. Secure Agent をダウンロードしてインストールします。
4. クラウド権限を設定します。

組織の権限の確認

組織のエラスティック構成に対する適切な特権が割り当てられていることを確認します。

エラスティック構成に対する特権によって、Administrator および Monitor の **【エラスティッククラスタ】** ページへのアクセスレベルは異なります。

エラスティック構成の表示とエラスティッククラスタの監視を行うには、少なくとも読み取り権限が必要です。

ステージングとログの場所の作成

お使いのクラウドプラットフォームに基づいて、ステージングファイルとログファイルの場所を作成します。

AWS

AWS 環境では、次の Amazon S3 の場所を作成します。

- クラスタがランタイムにステージングファイルを保存するために使用する S3 の場所
- クラスタ上で実行されるエラスティックジョブ用のログファイルを保存するためにクラスタが使用する S3 の場所

Microsoft Azure

Microsoft Azure 環境では、ステージングファイルとログファイルの場所を使用してストレージアカウントを作成します。

次のいずれかのストレージタイプを使用できます。

- Microsoft Azure Blob ストレージにリードを挿入するように同期タスクを設定します。階層型名前空間が無効になっていることを確認してください。
- Azure Data Lake Storage Gen2。階層型名前空間を持つストレージアカウントを作成します。

Google Cloud

Google Cloud 環境では、Google Cloud Storage 上にステージングファイルとログファイルの場所を作成します。

Secure Agent のダウンロードとインストール

Secure Agent をダウンロードしてローカルマシンにインストールします。このマシンは、Secure Agent マシンと呼ばれます。

Secure Agent は、RHEL 7.x および AMD64 を実行するローカルマシンにインストールします。Secure Agent を起動するユーザーには、クラスタに対する NOPASSWD sudo 権限が必要です。

次の表に、Secure Agent マシンの最小リソース要件を一覧表示します。

コンポーネント	最小要件
CPU あたりのコア数	8
メモリ	32GB
ディスク空き容量	100GB

Secure Agent をインストールした後、Secure Agent マシンに OpenSSL をインストールします。

Secure Agent のインストールに関する詳細については、「ランタイム環境」を参照してください。

ローカルクラスタのドメインのホワイトリスト登録

Secure Agent がローカルクラスタを作成する場合、クラスタノードは、マシンイメージなどのアーティファクトを取得し、ソースとターゲットにアクセスするために、特定のドメインにアクセスする必要があります。

ローカルクラスタの次のドメインをホワイトリストに登録します。

```
infacloud.jfrog.io
infacloud-ct-cdie-docker.jfrog.io
infacloud-discale-docker-stable.jfrog.io
discale-docker-stable.artifacts.cloudtrust.rocks
```

さらに、ローカルクラスタのクラウド環境に基づいて、適切なドメインをホワイトリストに登録します。

AWS

AWS の場合、次のドメインをホワイトリストに登録します。

```
.s3.amazonaws.com
sts.amazonaws.com
sts.<staging bucket region>.amazonaws.com
```



```
.s3.<staging bucket region>.amazonaws.com
informatica.snowflakecomputing.com
```

また、AWS の適切なリージョンをホワイトリストに登録します。

```
sts.us-east-2.amazonaws.com
sts.us-west-2.amazonaws.com
```

Microsoft Azure

Microsoft Azure の場合、次のドメインをホワイトリストに登録します。

```
*.azure.com
*.azure.net
*.database.windows.net
*.microsoft.com
*.microsoftonline.com
*.microsoftonline.com
*.windows.net
azure.com
azure.net
ifconfig.me
microsoft.com
microsoftonline.com
microsoftonline.com
windows.net
```

Google Cloud

Google Cloud の場合、次のドメインをホワイトリストに登録します。

```
.storage.cloud.google.com
.google.com
.le100.net
https://storage.googleapis.com
```

クラウド権限の設定

ローカルクラスタでは、簡素化されたクラウド権限を使用します。お使いのクラウドプラットフォームに適した設定手順に従ってください。

AWS の設定

AWS 環境では、IAM ロールを設定します。

IAM ロールを設定するには、以下のタスクを実行します。

1. AWS で、クラスタオペレータの IAM ロールを作成します。ロールに `cluster_operator_role` という名前を付けます。IAM ロールの作成手順については、AWS のドキュメントを参照してください。AWS は、AWS マネジメントコンソールや AWS CLI を使用するなど、IAM ロールを作成する方法をいくつか提供しています。
2. 次の IAM ポリシーを `cluster_operator_policy` という名前で作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
```

```

        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::<cluster-staging-dir1>/*",
        "arn:aws:s3:::<cluster-logging-dir1>/*"
      ]
    }
  ]
}

```

<cluster-staging-dir1>と<cluster-logging-dir1>を、それぞれお使いのステージングとログの場所に置き換えます。頻繁に変更される S3 の場所に対応するために、ワイルドカードを使用できます。詳細については、AWS のマニュアルを参照してください。

3. IAM ポリシー cluster_operator_policy を IAM ロール cluster_operator_role にアタッチします。
4. Secure Agent ロールを含めるようにクラスタオペレータロールの信頼関係を設定します。Secure Agent はクラスタオペレータロールを引き受ける必要があるため、クラスタオペレータロールは Secure Agent を信頼する必要があります。

IAM ロール cluster_operator_role の信頼関係を編集し、次の IAM 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"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{{account-id}}:role/agent_role"
      },
      "Action": "sts:AssumeRole",
    }
  ]
}

```

注: Principal 要素の値は Secure Agent ロールの ARN です。

必要に応じて、Secure Agent のみがクラスタオペレータロールを引き受けることができるように外部 ID を設定できます。

例えば、次のポリシーを使用して外部 ID 「123」を設定できます。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{{account-id}}:role/agent_role"
      },
      "Action": "sts:AssumeRole",
    }
  ]
}

```

```

        "Condition": {
          "StringEquals": {
            "sts:ExternalId": "123"
          }
        }
      ]
    }
  ]
}

```

Microsoft Azure の設定

Azure 環境では、以下のタスクを実行します。

1. Secure Agent マシンでファイアウォールを無効にします。
2. Azure で、agent_identity という名前でマネージド ID を作成します。システムによって割り当てられた既存のマネージド ID を使用することも、ユーザーによって割り当てられたマネージド ID を作成することもできます。ユーザーが割り当てたマネージド ID を作成する場合は、システムが割り当てたマネージド ID を無効にします。
マネージド ID の作成手順については、Microsoft Azure のドキュメントを参照してください。
3. 次のロール定義を使用して、agent_role という名前のカスタムロールを作成します。

```

{
  "properties": {
    "roleName": "agent_role",
    "description": "",
    "assignableScopes": [
      "/subscriptions/<subscription ID>/resourceGroups/<storage_resource_group>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",
          "Microsoft.Storage/storageAccounts/listKeys/action"
        ],
        "notActions": [
        ],
        "dataActions": [
        ],
        "notDataActions": [
        ]
      }
    ]
  }
}

```

4. カスタムロール agent_role を agent_identity という名前のマネージド ID に割り当てます。
5. マネージド ID agent_identity を、Secure Agent がインストールされている VM に割り当てます。

Google Cloud の設定

Google Cloud 環境では、次の権限を持つ IAM ロールを設定します。

```

storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update

```

Google VM を作成するときに、必要なロールが関連付けられているサービスアカウントを指定します。

第 7 章

エラスティック構成

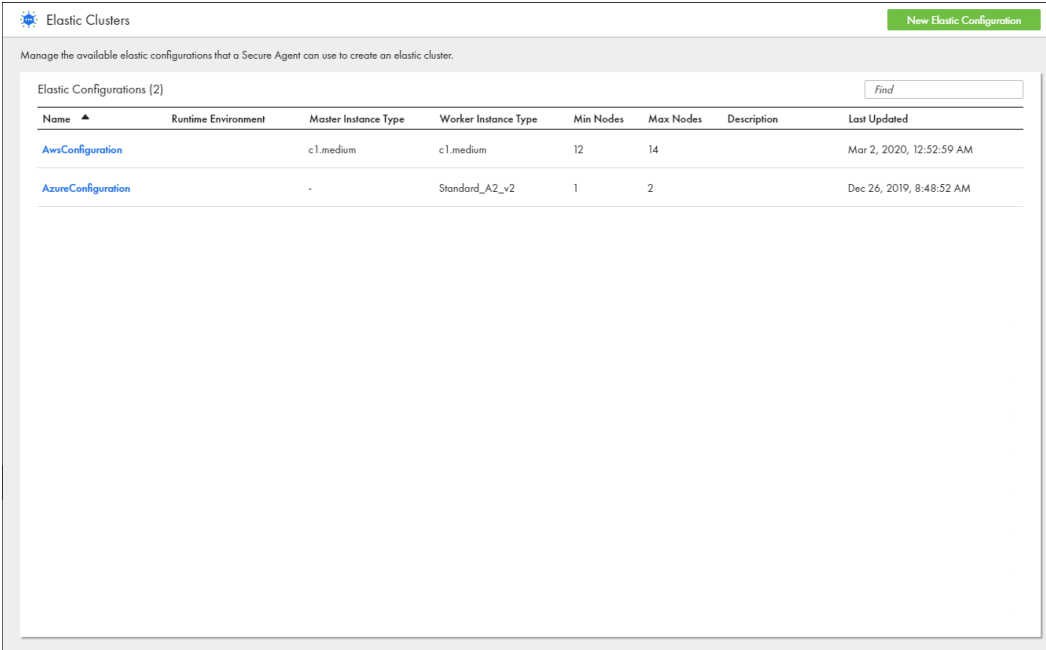
エラスティック構成は、エラスティッククラスタを作成するためにプロビジョニングするリソースを定義する一連のプロパティです。エラスティック構成で設定するプロパティは、クラウドプラットフォームによって決まります。

エラスティック構成は、**【エラスティッククラスタ】** ページで作成します。エラスティック構成でのプロパティの設定時に、追加で設定をランタイム環境と関連付けます。Secure Agent がクラスタを停止するタイミングを決定するために使用するクラスタシャットダウン方法を選択することもできます。次のクラスタシャットダウン方法のいずれかを選択できます。

- スマートシャットダウン。Secure Agent は、履歴データに基づいて、定義されたアイドルタイムアウト中にジョブがないことが予測される場合にクラスタを停止します。
- アイドルタイムアウト。Secure Agent は、定義したアイドル時間の後にクラスタを停止します。

この構成を作成した後、ページを使用して、組織で利用できる構成のサマリを確認します。サマリには、ノードのインスタンスタイプや、クラスタで利用できるノードの最小/最大数などをすばやく参照することができる情報が含まれています。

次の図は、**【エラスティッククラスタ】** ページを示しています。



Name	Runtime Environment	Master Instance Type	Worker Instance Type	Min Nodes	Max Nodes	Description	Last Updated
AwsConfiguration		c1.medium	c1.medium	12	14		Mar 2, 2020, 12:52:59 AM
AzureConfiguration	-		Standard_A2_v2	1	2		Dec 26, 2019, 8:48:52 AM

エラスティック構成を使用してエラスティックジョブを実行するには、エラスティック構成に関連付けられたランタイム環境を使用します。

エラスティッククラスタの実行時にエラスティック構成を編集する場合は、構成の変更を有効にするためにクラスタを停止する必要があります。クラスタを停止すると、クラスタが削除され、実行中のエラスティックジョブが停止します。別のエラスティックジョブを実行すると、クラスタが再び開始されます。

エラスティック構成は、Secure Agent が実行されている場合にのみ削除できます。構成を削除すると、プロビジョニングされたすべてのリソースが自動的に削除されます。エージェントが実行されていないときにプロビジョニングされたリソースを削除する場合は、コマンドを実行してクラスタの一覧表示と削除を行います。コマンドの詳細については、「[付録 A, 「コマンドリファレンス」 \(ページ 148\)](#)」を参照してください。

AWS のプロパティ

エラスティック構成でプロパティを設定するには、**[新規エラスティック構成]** をクリックするか、**[エラスティッククラスタ]** ページで編集する構成の名前をクリックします。

基本プロパティは、エラスティック構成を記述し、エラスティッククラスタをホストするクラウドプラットフォームを定義します。クラスタを設定するには、プラットフォームプロパティ、詳細プロパティ、およびランタイムプロパティを設定します。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	エラスティック構成の名前。
説明	エラスティック構成の説明。
ランタイム環境	エラスティック構成に関連付けるランタイム環境。ランタイム環境に含めることができる Secure Agent は 1 つのみです。ランタイム環境を複数の構成と関連付けることはできません。 ランタイム環境を選択しない場合、検証プロセスは Secure Agent への通信リンクを検証できず、Secure Agent にクラスタを開始するための最小ランタイム要件があることを確認できません。
クラウドプラットフォーム	クラスタをホストするクラウドプラットフォーム。 Amazon Web Services (AWS) を選択します。
プライベートクラスタ	クラスタリソースがプライベート IP アドレスのみを持つエラスティッククラスタを作成します。 プライベートクラスタを作成する場合は、詳細プロパティで VPC とサブネットを指定する必要があります。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
リージョン	クラスタを作成するリージョン。ドロップダウンメニューを使用して、使用できるリージョンを表示します。
マスタインスタンスタイプ	マスタノードをホストするインスタンスのタイプ。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。 使用できるインスタンスタイプは、選択するアベイラビリティゾーンとお使いの AWS アカウントによって異なります。 ドロップダウンメニューから選択するインスタンスタイプが選択したアベイラビリティゾーンおよびお使いの AWS アカウントでサポートされているかどうかを確認するには、AWS のマニュアルを参照してください。
マスタインスタンスプロファイル	マスタノードにアタッチされるインスタンスプロファイル。名前はスペースなしの英数字である必要があります。次の文字を含めることもできます: _+=,.@- マスタインスタンスプロファイルを指定する場合は、ワーカーインスタンスプロファイルも指定する必要があります。
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。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。 使用できるインスタンスタイプは、選択するアベイラビリティゾーンとお使いの AWS アカウントによって異なります。 ドロップダウンメニューから選択するインスタンスタイプが選択したアベイラビリティゾーンおよびお使いの AWS アカウントでサポートされているかどうかを確認するには、AWS のマニュアルを参照してください。
ワーカーインスタンスプロファイル	ワーカーノードにアタッチされるインスタンスプロファイル。名前はスペースなしの英数字である必要があります。次の文字を含めることもできます: _+=,.@- ワーカーインスタンスプロファイルを指定する場合は、マスタインスタンスプロファイルも指定する必要があります。
ワーカーノードの数	クラスタ内のワーカーノードの数。ワーカーノードの最小数と最大数を指定します。
スポットインスタンスの有効化	ワーカーノードにスポットインスタンスを使用するかどうかを示します。
スポットインスタンスの料金比率	スポットインスタンスに支払うオンデマンドインスタンス価格の最大パーセンテージ。1 から 100 までの整数値を指定します。 スポットインスタンスを有効にする場合は必須です。スポットインスタンスを有効にしない場合、このプロパティは無視されます。
高可用性の有効化	クラスタが高可用性かどうかを示します。指定するアベイラビリティゾーンまたはサブネットに基づいて、奇数のマスタノードが作成されます。少なくとも 3 つのアベイラビリティゾーンまたはサブネットを指定する必要があります。 例えば、6 つのアベイラビリティゾーンを指定すると、5 つのマスタノードが作成され、各マスタノードは異なるアベイラビリティゾーンに配置されます。 注: 複数のアベイラビリティゾーンまたはサブネットを指定すると、ワーカーノードの可用性が高くなります。高可用性が有効になっているかどうかに関係なく、アベイラビリティゾーンまたはサブネットに対してワーカーノードが作成されます。 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。

プロパティ	説明
可用性ゾーン	<p>クラスタノードが作成される AWS アベイラビリティゾーンのリスト。マスタノードがリスト内の最初の可用性ゾーンに作成されます。ゾーンが複数指定されている場合、クラスタノードは指定した複数のゾーンに作成されます。</p> <p>アベイラビリティゾーンを指定する場合、そのゾーンは一意であり指定したリージョン内に存在する必要があります。</p> <p>使用できるアベイラビリティゾーンは、お使いの AWS アカウントによって異なります。お使いのアカウントで使用できるゾーンを確認するには、AWS のマニュアルを参照してください。</p> <p>VPC を指定しない場合は必須です。VPC を指定すると、アベイラビリティゾーンを指定できません。アベイラビリティゾーンではなくサブネットを指定する必要があります。</p>
EBS ボリュームタイプ	Amazon EC2 インスタンスにローカルストレージとしてアタッチする Amazon EBS ボリュームのタイプ。EBS 汎用 SSD (gp2) のみ使用できます。
EBS ボリュームサイズ	<p>データ処理中の一時ストレージ用にワーカーノードにアタッチする EBS ボリュームのサイズ。ボリュームサイズは、ジョブの要件に基づいて最小から最大までスケーリングされます。サイズは 50 GB から 16 TB の範囲にする必要があります。</p> <p>デフォルトでは、ボリュームサイズの最小/最大値は 100 GB です。</p> <p>Graviton はストレージのスケーリングをサポートしていないため、この設定プロパティは Graviton 対応クラスタには適用されません。</p> <p>注: ボリュームサイズを縮小すると、クラスタで現在実行しているジョブを完了するまでの時間が長くなる可能性があります。</p>
クラスタシャットダウン	<p>クラスタのシャットダウン方法。次のクラスタシャットダウン方法のいずれかを選択できます。</p> <ul style="list-style-type: none"> - スマートシャットダウン。Secure Agent は、履歴データに基づいて、定義されたアイドルタイムアウト中にジョブがないことが予測される場合にクラスタを停止します。 - アイドルタイムアウト。Secure Agent は、定義したアイドル時間の後にクラスタを停止します。
マッピング	<p>マッピングタスクが完了するまで待機する時間。この時間が経過した後、マッピングタスクは強制終了となります。デフォルトでは、マッピングタスクにはタイムアウトはありません。</p> <p>タイムアウトを指定する場合は、10 分以上の値をお勧めします。マッピングタスクが Secure Agent にサブミットされると、タイムアウトが開始されます。</p>
ステージングの場所	<p>ステージングデータ用の Amazon S3 上の場所。</p> <p>バケット内のフォルダを含めるパスを使用できます (<bucket name>/<folder name>など)。同じリージョン内の S3 バケットをクラスタとして指定すると、待ち時間を減らすことができます。</p>
ログの場所	<p>エラスティックジョブを実行したときに生成されるログを保存する Amazon S3 上の場所。</p> <p>バケット内のフォルダを含めるパスを使用できます (<bucket name>/<folder name>など)。同じリージョン内の S3 バケットをクラスタとして指定すると、待ち時間を減らすことができます。</p>

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
VPC	<p>クラスタを作成する Amazon Virtual Private Cloud (VPC)。VPC は指定したリージョン内に存在する必要があります。</p> <p>プライベートクラスタを作成しない場合は、VPC を指定する必要はありません。この場合、エージェントでは、選択したリージョンとゾーンに基づいて AWS アカウント上に VPC が作成されます。</p> <p>注: シーケンスジェネレータトランスフォーメーションを使用する場合、VPC とサブネットを指定する必要があります。</p>
サブネット	<p>クラスタノードを作成するサブネット。サブネットを指定するには、カンマ区切りのリストを使用します。</p> <p>VPC が指定されている場合は必須です。各サブネットは、指定された VPC 内の異なる可用性ゾーンに存在する必要があります。</p> <p>VPC を指定しない場合は、サブネットを指定できません。サブネットではなく可用性ゾーンを指定する必要があります。</p> <p>注: シーケンスジェネレータトランスフォーメーションを使用する場合、VPC とサブネットを指定する必要があります。</p>
初期化スクリプトパス	<p>ノードの作成時に各クラスタノードで実行する初期化スクリプトの Amazon S3 ファイルパス。<bucket name>/<folder name>という形式を使用します。このスクリプトで、同じフォルダ内またはサブフォルダ内の他の初期化スクリプトを参照できます。</p> <p>このスクリプトは bash スクリプトでなければなりません。</p>
ELB セキュリティグループ	<p>Kubernetes API サーバーとエラスティッククラスタの外部にあるクライアント間の受信ルールを定義します。また、Kubernetes API サーバーとクラスタノード間の送信ルールも定義します。このセキュリティグループは、Secure Agent がエラスティッククラスタにプロビジョニングするロードバランサにアタッチされます。</p> <p>セキュリティグループを指定する場合、VPC とサブネット情報が必要です。</p> <p>セキュリティグループの詳細については、「Amazon EC2 のユーザー定義のセキュリティグループの作成」 (ページ 23) を参照してください。</p>
マスタセキュリティグループ	<p>エラスティッククラスタ、ELB セキュリティグループ、Secure Agent 内のマスターノードとワーカーノード間の受信ルール、および他のノードへの送信ルールを定義します。このセキュリティグループは、クラスタのすべてのマスターノードにアタッチされます。</p> <p>セキュリティグループを指定する場合、VPC とサブネット情報が必要です。</p> <p>セキュリティグループの詳細については、「Amazon EC2 のユーザー定義のセキュリティグループの作成」 (ページ 23) を参照してください。</p>

プロパティ	説明
ワーカーセキュリティグループ	<p>エラスティッククラスタ内のワーカーノードと他のノード間の受信および送信ルールを定義します。このセキュリティグループは、クラスタのすべてのワーカーノードにアタッチされます。</p> <p>セキュリティグループを指定する場合、VPC とサブネット情報が必要です。</p> <p>セキュリティグループの詳細については、「Amazon EC2 のユーザー定義のセキュリティグループの作成」 (ページ 23) を参照してください。</p>
AWS タグ	<p>クラスタノードに適用する AWS タグ。各タグにはキーと値があります。キーの長さは最大 127 文字です。値の長さは最大 256 文字です。</p> <p>最大 30 個のタグを表示できます。Secure Agent は、クラスタリソースにデフォルトタグも割り当てます。デフォルトタグは、タグの表示制限数 (30 個) には含まれません。</p> <p>注: デフォルトタグを上書きすると、問題が発生する可能性があります。次のデフォルトタグは上書きしないでください。</p> <ul style="list-style-type: none"> - 名前 - KubernetesCluster - k8s.io/cluster-autoscaler/enabled - k8s.io/cluster-autoscaler/<クラスタインスタンス ID>.k8s.local <p>AWS はこのフレーズを使用するために予約しているため、キーを「aws:」で始めることはできません。</p> <p>タグには、ASCII 制御文字 30 および 31 で表されるレコードおよび単位の区切り文字に対応する、UTF-8 文字 \u241e および \u241f を含めることはできません。</p>

ランタイム設定

次の表に、ランタイムプロパティを示します。

プロパティ	説明
暗号化データ	<p>クラスタ上の一時データが暗号化されるかどうかを示します。</p> <p>注: 一時データの暗号化によってジョブのパフォーマンスが低下する可能性があります。</p>
ランタイムプロパティ	<p>クラスタとそのクラスタで実行するジョブをカスタマイズするためのカスタムプロパティ。</p>

構成の検証

設定のプロパティを保存する前に、エラスティック構成を作成または更新するために必要な情報を検証できます。

検証プロセスでは、次の検証を実行します。

- 設定ページで必要な情報を指定している。
- 指定した情報は有効であるか、正しい形式である。例えば、指定したランタイム環境が別のクラスタ設定に関連付けられているかどうか。
- 指定した情報は有効であるか、正しい形式である。例えば、指定したランタイム環境が別のクラスタ設定に関連付けられているかどうか。

エラスティック構成の検証時にコンテキストキーに関連するエラーが発生した場合、キー `ccs.k8s.policy.context.key` をエラスティック構成のランタイムプロパティに追加します。次の値構造を使用して、コンテキストキーを追加できます。

```
"ContextKeyName-'keyName1',ContextKeyValues-'keyValue1',ContextKeyType-(string|stringList|
numeric|numericList|boolean|booleanList|ip|ipList|binary|binaryList|date|
dateList)&infaContextKeyName-'keyName2',ContextKeyValues-'keyValue2',ContextKeyType-(string|
stringList|numeric|numericList|boolean|booleanList|ip|ipList|binary|binaryList|date|dateList)"
```

以下に例を示します。

```
ccs.k8s.policy.context.key=ContextKeyName-'aws:username',ContextKeyValues-'kops',ContextKeyType-
string&infaContextKeyName-'ec2:ResourceTag/CREATED_BY',ContextKeyValues-'SFA-TDS',ContextKeyType-string
```

コンテキストキーの詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

GPU ワーカーインスタンスタイプ

エラスティック構成のワーカーインスタンスタイプの設定時に、GPU 対応のインスタンスタイプを選択できます。GPU 対応のインスタンスタイプを選択すると、GPU 対応クラスタが作成されます。GPU は大規模な並列アーキテクチャを使用して並行処理を高速化するため、多くの場合、パフォーマンスが向上します。

g4 および p3 インスタンスファミリーでワーカーインスタンスタイプを選択できます。これらのインスタンスタイプの詳細については、AWS のドキュメントを参照してください。

組織で送信プロキシサーバーを使用している場合は、Secure Agent マシンから次のドメインへのトラフィックを許可します。

```
.docker.io
.docker.com
.nvidia.com
.nvidia.github.io
```

GPU 対応クラスタを作成する場合、Spark Executor はそれぞれデフォルトで 1 つの GPU と 4 つの Spark Executor コアを使用します。Spark セッションプロパティ `spark.executor.cores` を使用して Spark Executor コアの数を変更できます。

GPU で実行できるクラスタに送信されたすべてのマッピングは、GPU で実行されます。GPU で実行できないマッピングの Spark タスクは、代わりに CPU で実行されます。GPU で実行される Spark ジョブと CPU で実行されるジョブを確認するには、ジョブの完了後に Spark イベントログを確認してください。

注: GPU で実行されるタスクの出力は、タスクが CPU で実行された場合の出力とは異なる場合があります。例えば、浮動小数点値の四捨五入が異なる場合があります。処理の違いに関する詳細については、Spark RAPIDS のドキュメントを参照してください。

GPU 対応クラスタで実行されるマッピングのルールとガイドラインについては、データ統合ヘルプの「マッピング」を参照してください。

Graviton ワーカーインスタンスタイプ

AWS Graviton 2 をワーカーインスタンスタイプとして選択して、エラスティックマッピングを実行できます。Graviton は、高度な RISC マシン（ARM）Neoverse N1 コアを使用して計算テクノロジーを提供する CPU ベースのインスタンスタイプです。

以下のいずれかのワーカーインスタンスタイプを選択できます。

- T4g
- M6g
- M6gd
- C6g

- C6gd
- C6gn
- R6g
- R6gd

これらのインスタンスタイプの詳細については、AWS のマニュアルを参照してください。

Graviton のガイドラインと制限

以下のガイドラインと制限は、Graviton ワーカーインスタンスタイプに適用されます。

- Graviton ワーカーインスタンスタイプでは、rand などの数値関数や is_date などの特殊関数といった一部の式関数がサポートされていません。
- エラスティック構成ページの EBS ボリュームサイズ構成は、Graviton でストレージスケールアップがサポートされないため、Graviton ワーカーインスタンスタイプには適用されません。
- Graviton ワーカーインスタンスタイプで Java トランスフォーメーションまたは Python トランスフォーメーションを使用することはできません。
- エスケープ文字、複数のカラム区切り文字、複数の文字による引用符、\n 以外の改行、およびスキップする先頭の行数が複数に設定されたフラットファイルを含むマッピングを実行することはできません。
- Graviton ワーカーインスタンスタイプでスナッピー圧縮された Parquet ソースを使用することはできません。
- マッピングの複雑さによっては、libs の非互換性エラーが発生する場合があります。Spark ドライバのログを確認し、java.lang.UnsatisfiedLinkError を検索することで、根本的な原因を確認できます。

スポットインスタンス

スポットインスタンスを使用してワーカーノードをホストするようにエラスティッククラスタを設定できます。

スポットインスタンスは、クラウドプロバイダがオンデマンドインスタンスよりも低価格で提供する予備のコンピューティング容量です。スポットインスタンスは常に利用できるとは限りません。クラウドプロバイダは実行中のスポットインスタンスを中断して容量を再利用できます。

スポットインスタンスを使用する場合は、スポットインスタンスの価格比率を設定します。スポットインスタンスの料金比率は、オンデマンドインスタンスの料金のうち、スポットインスタンスに支払う最大料金をパーセンテージで表したものです。例えば、オンデマンドインスタンスの料金が 1 時間あたり 0.68 ドルで、スポットインスタンスの価格比率を 50 に設定した場合、価格が 1 時間あたり 0.34 ドル以下である限り、現在のスポットインスタンスの価格を支払うことになります。

Secure Agent は、設定するワーカーノードの最小数に等しい数のオンデマンドワーカーノードを常に作成します。スポットインスタンスを有効にしてクラスタをスケールアップすると、エージェントはスポットインスタンス上にワーカーノードの最大数まで追加のワーカーノードを作成しようとします。スポットインスタンスが利用できない場合、または設定した最大料金を超える場合、クラスタはワーカーノード用にオンデマンドインスタンスを使用します。

例えば、ワーカーノードの最小数を 5 に設定し、最大数を 8 に設定すると、エージェントはオンデマンドインスタンスに 5 つのノードを作成し、スポットインスタンスに 3 つのノードを作成しようとします。ワーカーノードの最大数を最小数と等しく設定すると、クラスタはオンデマンドインスタンスのみを使用します。

クラウドプロバイダがエラスティックジョブを実行中のスポットノードを中断した場合、エージェントはオンデマンドノードを使用してジョブを完了します。

高可用性

エラスティッククラスタを高可用性にして、マスタ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つのマスタノードがダウンしても、他のマスタノードを使用でき、クラスタでジョブを引き続き実行できます。

クラスタが高可用性の場合、次のシナリオでのジョブの失敗に注意します。

- 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。

新しいステージングの場所へのアクセス

新しいステージングの場所を使用する場合、最初にエラスティック構成でステージングの場所を変更してから、AWS でステージングの場所に対する権限を変更する必要があります。

ロールベースのセキュリティを使用する場合は、Secure Agent マシンでステージングの場所に対する権限を変更する必要もあります。

構成でステージングの場所を変更する前に権限を変更すると、エラスティックジョブは次のエラーが発生して失敗します。

```
Error while executing mapping. ExecutionId '<execution ID>'. Cause: [Failed to start cluster for [01000D250000000000005]. Error reported while starting cluster [Cannot apply cluster operation START because the cluster is in an error state.].].
```

エラーを修正するには、次のタスクを実行します。

1. ステージングの場所の権限に対する変更を元に戻します。
2. ステージングの場所を元に戻すようにエラスティック構成を編集します。
3. 構成を保存すると、クラスタが停止します。
4. 構成でステージングの場所を更新してから、AWS でステージングの場所に対する権限を変更します。

クラウドリソースへのタグのプロパゲート

Secure Agent はタグをエラスティック構成で指定する AWS タグに基づいてクラウドリソースにプロパゲートします。

エージェントによって、次のリソースにタグがプロパゲートされます。

- 自動スケーリンググループ
- EBS ボリューム
- EC2 インスタンス
- IAM ロール*
- 起動テンプレート
- ロードバランサ*
- パブリックキー
- セキュリティグループ
- サブネット
- VPC

* タグのキーまたは値に特殊文字が含まれている場合、エージェントはタグをこのリソースにプロパゲートしません。

注: Secure Agent は、エージェントを作成するクラウドリソースにのみタグをプロパゲートします。VPC およびサブネットを作成し、リソースをエラスティック構成で指定した場合、エージェントは AWS タグを VPC およびサブネットにプロパゲートしません。

エンタープライズがタグ付けポリシーに従う場合、タグを次のリソースに手動で割り当ててください。

- インターネットゲートウェイ
- ネットワーク ACL
- ルートテーブル

クラウドリソースのデフォルトタグ

Secure Agent は、エラスティック構成で指定するクラウドプラットフォームのタグに加えて、複数のデフォルトタグをリソースに割り当てます。デフォルトタグでは、クラスタオペレータ、クラウドプラットフォームでのサービス、およびデータガバナンスがサポートされます。デフォルトタグは上書きしないでください。

次の表で、クラスタに関する情報をレポートするために、エージェントがクラスタノードに割り当てるタグについて説明します。

クラウドプラットフォームのタグ	説明
infa:ccs:hostname	クラスタを開始した Secure Agent マシンのホスト名。 Secure Agent マシンが予期せず停止し、Secure Agent が別のマシンで再び開始される場合、ホスト名は元の Secure Agent マシンです。
infa:k8scluster:configname	クラスタの作成に使用されるエラスティック構成の名前。
infa:k8scluster:workdir	クラスタで使用されるステージングディレクトリ。

一部のデフォルトタグは、名前空間がなく、エラスティック構成で指定したユーザー定義タグと競合する可能性があります。例えば、クラスタオペレータでは名前タグおよび KubernetesCluster タグがすべてのリソースに自動で追加されますが、これらのタグには名前空間がありません。KubernetesCluster など同じ名前のユーザー定義のタグを指定すると、クラスタオペレータではユーザー定義のタグをデフォルトタグで上書きします。

注: デフォルトタグを上書きすると、問題が発生する可能性があります。次のデフォルトタグは上書きしないでください。

- 名前
- KubernetesCluster
- k8s.io/cluster-autoscaler/enabled
- k8s.io/cluster-autoscaler/<クラスタインスタンス ID>.k8s.local

データ暗号化

暗号化によってエラスティックジョブの処理に使用されるデータが保護されます。暗号化は、保存データ、一時データ、転送中のデータの保護に使用できます。

暗号化は、以下のタイプのデータで使用できます。

保存データ

Amazon S3 でサーバーサイド暗号化オプションを使用し、次の保存データを暗号化できます。

- Amazon S3 上のステージングデータ
- Amazon S3 上のログファイル

ステージングデータとログファイルの暗号化の詳細については、[「手順 9.保存ステージングデータとログファイルの暗号化（オプション）」（ページ 43）](#)を参照してください。

ソースデータおよびターゲットデータの暗号化について詳しくは、データ統合のヘルプで該当するコネクタのヘルプを参照してください。

注: Amazon S3 V2 接続内の暗号化関係のカスタムプロパティを設定する場合、Spark エンジンではステージングデータの読み取りと書き込みに同じカスタムプロパティを使用します。

一時データ

一時データには、サーバーレス Spark エンジンがクラスターノード上で生成するキャッシュデータとシャッフルデータが含まれます。

一時データを暗号化するには、エラスティック構成で暗号化を有効にします。暗号化を有効にする場合、一時データはデフォルトで HMAC-SHA1 アルゴリズムを使用して暗号化されます。別のアルゴリズムを使用するには、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。

転送中のデータ

デフォルトでは、ステージングデータとログファイルを含む Amazon S3 との間で転送中のデータは、Transport Layer Security (TLS) プロトコルを使用して暗号化されます。

Google Cloud のプロパティ

エラスティック構成でプロパティを設定するには、**[新規エラスティック構成]** をクリックするか、**[エラスティッククラスタ]** ページで編集する構成の名前をクリックします。

基本プロパティは、エラスティック構成を記述し、エラスティッククラスタをホストするクラウドプラットフォームを定義します。クラスタを設定するには、プラットフォームプロパティ、詳細プロパティ、およびランタイムプロパティを設定します。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	エラスティック構成の名前。
説明	エラスティック構成の説明。
ランタイム環境	エラスティック構成に関連付けるランタイム環境。ランタイム環境に含めることができる Secure Agent は 1 つのみです。ランタイム環境を複数の構成と関連付けることはできません。

プロパティ	説明
クラウドプラットフォーム	クラスタをホストするクラウドプラットフォーム。 Google Cloud Platform (GCP) を選択します。
プライベートクラスタ	クラスタリソースがプライベート IP アドレスのみを持つエラスティッククラスタを作成します。 プライベートクラスタを作成する場合は、詳細プロパティで VPC とサブネットを指定する必要があります。Secure Agent は、同じ VPC ネットワークまたは詳細プロパティで指定した VPC に接続できる VPC ネットワークに存在する必要があります。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
リージョン	クラスタを作成するリージョン。ドロップダウンメニューを使用して、使用できるリージョンを表示します。
マスタインスタンスタイプ	マスタノードをホストするインスタンスのタイプ。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。
マスタサービスアカウント	マスタノードにアタッチするサービスアカウント。
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。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。
ワーカーノードの数	クラスタ内のワーカーノードの数。ワーカーノードの最小数と最大数を指定します。
ワーカーサービスアカウント	ワーカーノードにアタッチするサービスアカウント。
可用性ゾーン	クラスタノードが作成される可用性ゾーンのリスト。マスタノードがリスト内の最初のゾーンに作成されます。ゾーンが複数指定されている場合、クラスタノードは指定した複数のゾーンに作成されます。 ゾーンは一意であり、指定されたリージョン内に存在する必要があります。
ディスクサイズ	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永続ディスクのサイズ。ディスクサイズは 50 GB から 16 TB の範囲にする必要があります。
クラスタシャットダウン	クラスタのシャットダウン方法。次のクラスタシャットダウン方法のいずれかを選択できます。 <ul style="list-style-type: none"> - スマートシャットダウン。Secure Agent は、履歴データに基づいて、定義されたアイドルタイムアウト中にジョブがないことが予測される場合にクラスタを停止します。 - アイドルタイムアウト。Secure Agent は、定義したアイドル時間の後にクラスタを停止します。

プロパティ	説明
マッピング	マッピングタスクが完了するまで待機する時間。この時間が経過した後、マッピングタスクは強制終了となります。デフォルトでは、マッピングタスクにはタイムアウトはありません。 タイムアウトを指定する場合は、10 分以上の値をお勧めします。マッピングタスクが Secure Agent にサブミットされると、タイムアウトが開始されます。
ステージングの場所	データをステージングするための Google Cloud Storage 上の場所。 場所の名前は gs:// で始まる必要があります。
ログの場所	エラスティックジョブを実行したときに生成されるログを保存する Google Cloud Storage 上の場所。 場所の名前は gs:// で始まる必要があります。

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
VPC	クラスタを作成する Google Cloud Virtual Private Cloud (VPC)。 プライベートクラスタを作成しない場合は、VPC を指定する必要はありません。この場合、エージェントでは、選択したリージョンとゾーンに基づいて Google Cloud アカウント上に VPC が作成されます。
サブネット	クラスタノードを作成するサブネット。サブネットを指定するには、カンマ区切りのリストを使用します。 VPC が指定されている場合は必須です。各サブネットは、指定された VPC 内の異なるゾーンに存在する必要があります。 VPC を指定しない場合は、サブネットを指定できません。サブネットではなくゾーンを指定する必要があります。
IP アドレス範囲	クラスタが使用できる IP アドレス範囲を指定する CIDR ブロック。 例: 10.0.0.0/24
初期化スクリプトパス	ノードの作成時に各クラスタノードで実行する初期化スクリプトの Google Cloud Storage ファイルパス。<bucket name>/<folder name>という形式を使用します。スクリプトは、同じバケット内、または同じサブディレクトリ内のその他の初期化スクリプトを参照します。 このスクリプトは bash スクリプトでなければなりません。
クラスタラベル	クラスタノードに適用するラベル。各ラベルにはキーと値があります。キーの長さは最大 63 文字です。 最大 55 個のラベルを列挙できます。Secure Agent は、クラスタリソースにデフォルトラベルも割り当てます。デフォルトラベルは、ラベルの上限 (55 個) には含まれません。 ラベルには、ASCII 制御文字 30 および 31 で表されるレコードおよび単位の区切り文字に対応する、UTF-8 文字 \u241e および \u241f を含めることはできません。

ランタイム設定

次の表に、ランタイムプロパティを示します。

プロパティ	説明
暗号化データ	クラスタ上の一時データが暗号化されるかどうかを示します。
ランタイムプロパティ	クラスタとそのクラスタで実行するジョブをカスタマイズするためのカスタムプロパティ。

クラウドリソースへのラベルのプロパゲート

Secure Agent は、エラスティック構成で指定したクラスタラベルに基づいて、ラベルをクラウドリソースにプロパゲートします。

エージェントによって、次のリソースにラベルがプロパゲートされます。

- Compute Engine インスタンス
- Compute Engine インスタンステンプレート

企業でタグ付けポリシーを使用している場合は、ラベルを他のクラウドリソースに手動で割り当ててください。

注: Secure Agent は、エージェントが作成するクラウドリソースにのみラベルをプロパゲートします。例えば、ネットワークを作成してエラスティック構成でネットワークを指定した場合、エージェントはクラスタラベルをネットワークにプロパゲートしません。

データ暗号化

暗号化によってエラスティックジョブの処理に使用されるデータが保護されます。暗号化は、保存データ、一時データ、転送中のデータの保護に使用できます。

暗号化は、以下のタイプのデータで使用できます。

保存データ

デフォルトでは、Google Cloud Storage はステージングデータおよびログファイルを暗号化します。詳細については、Google Cloud のマニュアルを参照してください。

ソースデータおよびターゲットデータの暗号化について詳しくは、データ統合のヘルプで該当するコネクタのヘルプを参照してください。

一時データ

一時データには、Spark エンジンがクラスタノード上で生成するキャッシュデータとシャッフルデータが含まれます。

一時データを暗号化するには、エラスティック構成で暗号化を有効にします。暗号化を有効にする場合、一時データはデフォルトで HMAC-SHA1 アルゴリズムを使用して暗号化されます。別のアルゴリズムを使用するには、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。

転送中のデータ

デフォルトでは、Google Cloud Storage は、Transport Layer Security (TLS) プロトコルを使用して、Google Cloud Storage に対して送受信されるデータ（ステージングデータ、ログファイルなど）を暗号化します。

Microsoft Azure プロパティ

エラスティック構成でプロパティを設定するには、**【新規エラスティック構成】** をクリックするか、**【エラスティッククラスタ】** ページで編集する構成の名前をクリックします。

基本プロパティは、エラスティック構成を記述し、エラスティッククラスタをホストするクラウドプラットフォームを定義します。クラスタを設定するには、プラットフォームプロパティ、詳細プロパティ、およびランタイムプロパティを設定します。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	エラスティック構成の名前。
説明	エラスティック構成の説明。
ランタイム環境	エラスティック構成に関連付けるランタイム環境。ランタイム環境に含めることができる Secure Agent は 1 つのみです。ランタイム環境を複数の構成と関連付けることはできません。
クラウドプラットフォーム	クラスタをホストするクラウドプラットフォーム。 Microsoft Azure を選択します。
プライベートクラスタ	クラスタリソースがプライベート IP アドレスのみを持つエラスティッククラスタを作成します。 プライベートクラスタを作成する場合は、詳細プロパティで VNet とサブネットを指定する必要があります。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
リージョン	クラスタを作成するリージョン。ドロップダウンメニューを使用して、使用できるリージョンを表示します。
マスタインスタンスタイプ	マスタノードをホストするインスタンスのタイプ。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。 使用できるインスタンスタイプのリストは、クラスタで必要とされるリソースの最小数に基づいてフィルタされます。
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。ドロップダウンメニューを使用して、使用できるインスタンスタイプを表示します。 使用できるインスタンスタイプは、ご使用の Azure アカウントによって異なります。 ドロップダウンメニューから選択するインスタンスタイプがご使用のアカウントでサポートされているか確認するには、Microsoft Azure のドキュメントを参照してください。
ワーカーノードの数	クラスタ内のワーカーノードの数。ワーカーノードの最小数と最大数を指定します。

プロパティ	説明
スポットインスタンスの有効化	ワーカーノードにスポットインスタンスを使用するかどうかを示します。
スポットインスタンスの価格比率	<p>スポットインスタンスに支払うオンデマンドインスタンス価格の最大パーセンテージ。1 から 100 までの整数値を指定します。</p> <p>スポットインスタンスを有効にする場合は必須です。スポットインスタンスを有効にしない場合、このプロパティは無視されます。</p>
高可用性の有効化	クラスタが高可用性かどうかを示します。リージョンに可用性ゾーン 1、2、および 3 がある場合にのみ高可用性を有効にできます。可用性ゾーンごとに、マスタノードが 1 つ作成されます。
可用性ゾーン	<p>クラスタノードが作成される可用性ゾーンのリスト。可用性ゾーンのリストは、リージョンに基づいて自動的に取り込まれます。</p> <p>リージョンに可用性ゾーン 1、2、および 3 がある場合は、ワーカーノードがゾーン全体に作成されます。</p>
Azure ディスクサイズ	<p>データ処理中の一時ストレージ用にワーカーノードにアタッチする Azure ディスクのサイズ。ディスクサイズは、ジョブの要件に基づいて最小から最大までスケーリングされます。サイズは 80 GB から 16 TB の範囲にする必要があります。</p> <p>デフォルトでは、ディスクサイズの最小/最大値は 100 GB です。</p> <p>注: ディスクサイズを縮小すると、クラスタで現在実行しているジョブを完了するまでの時間が長くなる可能性があります。</p>
クラスタシャットダウン	<p>クラスタのシャットダウン方法。次のクラスタシャットダウン方法のいずれかを選択できます。</p> <ul style="list-style-type: none"> - スマートシャットダウン。Secure Agent は、履歴データに基づいて、定義されたアイドルタイムアウト中にジョブがないことが予測される場合にクラスタを停止します。 - アイドルタイムアウト。Secure Agent は、定義したアイドル時間の後にクラスタを停止します。
マッピング	<p>マッピングタスクが完了するまで待機する時間。この時間が経過した後、マッピングタスクは強制終了となります。デフォルトでは、マッピングタスクにはタイムアウトはありません。</p> <p>タイムアウトを指定する場合は、10 分以上の値をお勧めします。マッピングタスクが Secure Agent にサブミットされると、タイムアウトが開始されます。</p>
リソースグループ (ストレージ)	<p>ステージングおよびログストレージアカウントを保持するストレージリソースグループ。</p> <p>初期化スクリプトのパスを指定する場合、初期化スクリプトを保持するストレージアカウントが同じリソースグループに属している必要があります。</p>

プロパティ	説明
ステージングの場所	<p>Microsoft Azure Blob Storage または Azure Data Lake Storage Gen2 上のステージングデータの場所。</p> <p>次の形式を使用します。</p> <ul style="list-style-type: none"> - Microsoft Azure Blob Storage: wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<ステージングの場所のパス> - Azure Data Lake Storage Gen2: abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<ステージングの場所のパス> <p>暗号化が有効になっている場合は、ストレージタイプに基づいて WASBS または ABFS プロトコルを指定します。それ以外の場合は、WASB または ABFS プロトコルを指定します。</p>
ログの場所	<p>エラスティックジョブを実行するときに生成されるログを格納する、Microsoft Azure Blob Storage または Azure Data Lake Storage Gen2 上の場所。</p> <p>次の形式を使用します。</p> <ul style="list-style-type: none"> - Microsoft Azure Blob Storage: wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<ログの場所のパス> - Azure Data Lake Storage Gen2: abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<ログの場所のパス> <p>暗号化が有効になっている場合は、ストレージタイプに基づいて WASBS または ABFS プロトコルを指定します。それ以外の場合は、WASB または ABFS プロトコルを指定します。</p>

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
リソースグループ (クラスタ)	クラスタリソースを保存するクラスタリソースグループ。リソースグループを指定しない場合、エージェントでリソースグループが作成され、クラスタリソースが入力されます。
サービスプリンシパルのクライアント ID	エージェントが Azure リソースの管理に使用するサービスプリンシパル。
Key Vault	サービスプリンシパルの資格情報を保存する Key Vault。
シークレット名	サービスプリンシパルの資格情報を保存するシークレットの名前。
VNet	<p>クラスタを作成する Azure VNet。resourceGroup/VNet という形式を使用します。VNet は指定したリージョン内に存在する必要があります。</p> <p>プライベートクラスタを作成しない場合は、VNet を指定する必要はありません。この場合、エージェントでは、選択したリージョンに基づいて Azure アカウント上に VNet が作成されます。</p>
サブネット	VNet が指定されている場合は必須。クラスタノードを作成するサブネット。
IP アドレス範囲	<p>クラスタが使用できる IP アドレス範囲を指定する CIDR ブロック。IP アドレス範囲は、サブネットの IP アドレスと重複することはできません。</p> <p>例: 10.0.0.0/24</p>

プロパティ	説明
初期化スクリプトパス	ノードの作成時に各クラスターノードで実行する初期化スクリプトの Microsoft Azure Blob Storage または Azure Data Lake Storage Gen2 ファイルパス。 Blob ストレージで、スクリプトを Blob ストレージコンテナ内のフォルダ内に配置し、 <code>https://storageAccount.blob.core.windows.net/container/folder/file.sh</code> の形式を使用します。 スクリプトは bash スクリプトである必要があり、同じフォルダ内の他の init スクリプトを参照できます。
Azure タグ	クラスターノードに適用する Microsoft Azure のタグ。各タグにはキーと値があります。 最大 30 個のタグを表示できます。Secure Agent は、クラスターリソースにデフォルトタグも割り当てます。デフォルトタグは、タグの表示制限数（30 個）には含まれません。 注: デフォルトタグを上書きすると、問題が発生する可能性があります。詳細については、「 クラウドリソースのデフォルトタグ 」(ページ 127)を参照してください。 タグには、ASCII 制御文字 30 および 31 で表されるレコードおよび単位の区切り文字に対応する、UTF-8 文字 <code>\u241e</code> および <code>\u241f</code> を含めることはできません。

ランタイム設定

次の表に、ランタイムプロパティを示します。

プロパティ	説明
暗号化データ	クラスター上の一時データが暗号化されるかどうかを示します。 注: 一時データの暗号化によってジョブのパフォーマンスが低下する可能性があります。
ランタイムプロパティ	クラスターとそのクラスターで実行するジョブをカスタマイズするためのカスタムプロパティ。

構成の検証

設定のプロパティを保存する前に、エラスティック構成を作成または更新するために必要な情報を検証できます。

検証プロセスでは、次の検証を実行します。

- 設定ページで必要な情報を指定している。
- 指定した情報は有効であるか、正しい形式である。例えば、指定したランタイム環境が別のクラスター設定に関連付けられているかどうか。
- 指定した情報は有効であるか、正しい形式である。例えば、指定したランタイム環境が別のクラスター設定に関連付けられているかどうか。

マネージド ID を Secure Agent 資格情報として使用する場合は、キー `ccs.azure.k8s.prevalidation.agent.clientid` をエラスティック構成のランタイムプロパティに追加する必要があります。

スポットインスタンス

スポットインスタンスを使用してワーカーノードをホストするようにエラスティッククラスターを設定できます。

スポットインスタンスは、クラウドプロバイダがオンデマンドインスタンスよりも低価格で提供する予備のコンピューティング容量です。スポットインスタンスは常に利用できるとは限りません。クラウドプロバイダは実行中のスポットインスタンスを中断して容量を再利用できます。

スポットインスタンスを使用する場合は、スポットインスタンスの価格比率を設定します。スポットインスタンスの料金比率は、オンデマンドインスタンスの料金のうち、スポットインスタンスに支払う最大料金をパーセンテージで表したものです。例えば、オンデマンドインスタンスの料金が 1 時間あたり 0.68 ドルで、スポットインスタンスの価格比率を 50 に設定した場合、価格が 1 時間あたり 0.34 ドル以下である限り、現在のスポットインスタンスの価格を支払うことになります。

Secure Agent は、設定するワーカーノードの最小数に等しい数のオンデマンドワーカーノードを常に作成します。スポットインスタンスを有効にしてクラスタをスケールアップすると、エージェントはスポットインスタンス上にワーカーノードの最大数まで追加のワーカーノードを作成しようとします。スポットインスタンスが利用できない場合、または設定した最大料金を超える場合、クラスタはワーカーノード用にオンデマンドインスタンスを使用します。

例えば、ワーカーノードの最小数を 5 に設定し、最大数を 8 に設定すると、エージェントはオンデマンドインスタンスに 5 つのノードを作成し、スポットインスタンスに 3 つのノードを作成しようとします。ワーカーノードの最大数を最小数と等しく設定すると、クラスタはオンデマンドインスタンスのみを使用します。

クラウドプロバイダがエラスティックジョブを実行中のスポットノードを中断した場合、エージェントはオンデマンドノードを使用してジョブを完了します。

高可用性

エラスティッククラスタを高可用性にして、マスタノードがダウンしたときに単一障害点とし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 つのマスタノードがダウンしても、他のマスタノードを使用でき、クラスタでジョブを引き続き実行できます。

クラスタが高可用性の場合、次のシナリオでのジョブの失敗に注意します。

- 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。

新しいステージングの場所へのアクセス

新しいステージングの場所を使用する場合、エラスティック構成で場所を更新する前に、Secure Agent がその場所にアクセスできるようにする必要があります。

新しいステージングの場所を使用するには、次のタスクを完了します。

1. Secure Agent マシンに割り当てられているマネージド ID の権限を更新します。
2. エラスティック構成でステージングの場所を編集します。

クラウドリソースへのタグのプロパゲート

Secure Agent はタグをエラスティック構成で指定する Azure タグに基づいてクラウドリソースにプロパゲートします。

エージェントによって、次のリソースにタグがプロパゲートされます。

- Azure ディスク
- ロードバランサ
- ネットワークセキュリティグループ
- パブリック IP アドレス

- リソースグループ
- 仮想マシンスケールセット
- VNet

エンタープライズがタグ付けポリシーに従う場合、タグを他のクラウドリソースに手動で割り当ててください。

注: Secure Agent は、エージェントを作成するクラウドリソースにのみタグをプロパゲートします。例えば、VNet を作成してエラスティック構成に VNet を指定する場合、エージェントでは Azure タグを VNet にプロパゲートしません。

クラウドリソースのデフォルトタグ

Secure Agent は、エラスティック構成で指定するクラウドプラットフォームのタグに加えて、複数のデフォルトタグをクラスターリソースに割り当てます。デフォルトタグは上書きしないでください。

以下の表で、エージェントがクラスターリソースに割り当てるタグについて説明します。

クラウドプラットフォームのタグ	説明
infa:ccs:hostname	クラスタを開始した Secure Agent マシンのホスト名。 Secure Agent マシンが予期せず停止し、Secure Agent が別のマシンで再び開始される場合、ホスト名は元の Secure Agent マシンです。
infa:k8scluster:configname	クラスタの作成に使用されるエラスティック構成の名前。
infa:k8scluster:workdir	クラスタで使用されるステージングディレクトリ。
InfaInternalInitDone	内部使用。
KubernetesCluster	エラスティッククラスタの特定。

一部のデフォルトタグは、名前空間がなく、KubernetesCluster などのエラスティック構成で指定したユーザー定義タグと競合する可能性があります。ユーザー定義タグと同じ名前を指定すると、タグが上書きされ、エラスティッククラスタで問題が発生する可能性があります。

データ暗号化

暗号化によってエラスティックジョブの処理に使用されるデータが保護されます。暗号化は、保存データ、一時データ、転送中のデータの保護に使用できます。

暗号化は、以下のタイプのデータで使用できます。

保存データ

デフォルトでは、Microsoft Azure Blob Storage はステージングデータおよびログファイルを暗号化します。詳細については、Microsoft Azure のドキュメントを参照してください。

ソースデータおよびターゲットデータの暗号化について詳しくは、データ統合のヘルプで該当するコネクタのヘルプを参照してください。

一時データ

一時データには、サーバーレス Spark エンジンがクラスタノード上で生成するキャッシュデータとシャッフルデータが含まれます。

一時データを暗号化するには、エラスティック構成で暗号化を有効にします。暗号化を有効にする場合、一時データはデフォルトで HMAC-SHA1 アルゴリズムを使用して暗号化されます。別のアルゴリズムを使用するには、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。

転送中のデータ

デフォルトでは、Microsoft Azure Blob Storage は、Transport Layer Security (TLS) プロトコルを使用して、Blob Storage に対して送受信されるデータ（ステージングデータ、ログファイルなど）を暗号化します。

Blob Storage で暗号化が有効になっている場合、エラスティック構成でステージングとログの場所を設定するときに WASBS プロトコルを指定できます。暗号化が有効になっていない場合、WASB プロトコルを使用する必要があります。

セルフサービスクラスタのプロパティ

エラスティック構成でプロパティを設定するには、**【新規エラスティック構成】** をクリックするか、**【エラスティッククラスタ】** ページで編集する構成の名前をクリックします。

基本プロパティは、エラスティック構成を記述し、エラスティッククラスタをホストするクラウドプラットフォームを定義します。クラスタを設定するには、プラットフォームプロパティおよびランタイムプロパティを設定します。

エラスティックマッピングを実行するようにセルフサービスクラスタをセットアップするために必要な最小リソース仕様については、[「クラスタノードのリソース要件」 \(ページ 134\)](#)を参照してください。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	エラスティック構成の名前。
説明	エラスティック構成の説明。
ランタイム環境	エラスティック構成に関連付けるランタイム環境。ランタイム環境に含めることができる Secure Agent は 1 つのみです。ランタイム環境を複数の構成と関連付けることはできません。 ランタイム環境を選択しない場合、検証プロセスは Secure Agent への通信リンクを検証できず、Secure Agent にクラスタを開始するための最小ランタイム要件があることを確認できません。
クラウドプラットフォーム	クラスタをホストするクラウドプラットフォーム。 セルフサービスクラスタを選択します。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
Kube 設定ファイルパス	kubeconfig ファイルのパス。 kubeconfig ファイルを使用して、クラスタ、ユーザー、および認証メカニズムに関する情報を整理します。 例: <ディレクトリ名>/<ファイル名>.yaml YAML ファイルは Secure Agent VM の任意のディレクトリに保存できます。
Kube コンテキスト名	クラスタコンテキスト名。 コンテキストは、指定された認証情報を使用して指定されたクラスタに要求を送信するために使用される、名前付きクラスタとユーザータプルを定義します。
クラスタバージョン	Kubernetes クラスタサーバーのバージョン。 エラスティック構成は、Kubernetes クラスタサーバーのメジャーバージョンとマイナーバージョンを検証しますが、パッチリリースのバージョン番号は検証しません。
名前空間	Informatica が作成したリソースがデプロイされる名前空間。
ワーカーノードの数	クラスタ内のワーカーノードの数。ワーカーノードの最小数と最大数を指定します。
クラスタのアイドルタイムアウト	Informatica が作成したクラスタリソースオブジェクトが非アクティブであるために削除されるまでの時間。
マッピングタスクタイムアウト	マッピングタスクが完了するまで待機する時間。この時間が経過した後、マッピングタスクは強制終了となります。デフォルトでは、マッピングタスクにはタイムアウトはありません。 タイムアウトを指定する場合は、10 分以上の値をお勧めします。マッピングタスクが Secure Agent にサブミットされると、タイムアウトが開始されます。

プロパティ	説明
ステージングの場所	<p>クラウド上のステージングデータの場所の完全なパス。 お使いのクラウド環境に基づいて、次の形式で場所を指定します。</p> <ul style="list-style-type: none"> - AWS。s3://<バケット名>/<フォルダパス> ファイルパスに S3 のプレフィックスを付ける必要があります。 同じリージョン内の S3 バケットをクラスタとして指定すると、待ち時間を減らすことができます。 - Microsoft Azure。 <ファイルシステム>://<コンテナ>@<ストレージアカウント>.dfs.core.windows.net/<フォルダパス>:<リソースグループ>/<リージョン>または <ファイルシステム>://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<フォルダパス>:<リソースグループ>/<リージョン> 次のファイルシステムを使用できます。 <ul style="list-style-type: none"> - abfs - abfss - wasb - wasbs <リソースグループ>の入力は必須です。<リージョン>はオプションです。デフォルトは westus2 です。 <p>Secure Agent には、ランタイムにステージングファイルを保存するために、ステージングの場所にアクセスできる権限が必要です。ステージングの場所にアクセスするには、クラスタで実行されている Secure Agent マシンとワーカーノードの両方に適切な IAM アクセス権限を提供する必要があります。</p>
ログの場所	<p>クラウド上のログの格納場所の完全なパス。 お使いのクラウド環境に基づいて、次の形式で場所を指定します。</p> <ul style="list-style-type: none"> - AWS。s3://<バケット名>/<フォルダパス> ファイルパスに S3 のプレフィックスを付ける必要があります。 同じリージョン内の S3 バケットをクラスタとして指定すると、待ち時間を減らすことができます。 - Microsoft Azure。 <ファイルシステム>://<コンテナ>@<ストレージアカウント>.dfs.core.windows.net/<フォルダパス>:<リソースグループ>/<リージョン>または <ファイルシステム>://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<フォルダパス>:<リソースグループ>/<リージョン> 次のファイルシステムを使用できます。 <ul style="list-style-type: none"> - abfs - abfss - wasb - wasbs <リソースグループ>の入力は必須です。<リージョン>はオプションです。デフォルトは westus2 です。 <p>Secure Agent には、ランタイムにステージングファイルを保存するために、ステージングの場所にアクセスできる権限が必要です。ステージングの場所にアクセスするには、クラスタで実行されている Secure Agent マシンとワーカーノードの両方に適切な IAM アクセス権限を提供する必要があります。</p>

プロパティ	説明
ラベル	<p>セルフサービスクラスタで Informatica によって作成された Kubernetes オブジェクトにアタッチされているキーと値のペア。</p> <p>ラベルを使用して、オブジェクトのサブセットを整理および選択できます。各オブジェクトには、キーと値のラベルのセットを定義できます。各キーは、特定のオブジェクトに対して一意である必要があります。</p> <p>ラベルに@記号を使用することはできません。サポートされている構文と文字セットの詳細については、Kubernetes のドキュメントを参照してください。</p>
ノードセクタラベル	ノードセクタラベルを使用して、Informatica が Kubernetes オブジェクトを作成できるセルフサービスクラスタ内のノードを識別します。

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
注釈	<p>識別用途でない任意のメタデータをオブジェクトに割り当てるために使用されるキーと値のペア。</p> <p>注: 注釈は、クラスタ内の POD オブジェクトに対してのみ定義できます。</p> <p>注釈の詳細については、Kubernetes のドキュメントを参照してください。</p>
許容	<p>ポッドが適切でないノードにスケジュールされないようにするために使用されるキーと値のペア。</p> <p>次のいずれかの演算子を選択します。</p> <ul style="list-style-type: none"> - 等しい - 既存 <p>次のいずれかの Taint 効果を選択します。</p> <ul style="list-style-type: none"> - NoSchedule - PreferNoSchedule - NoExecute <p>【許容時間 (秒)】 フィールドに、ノードから POD を削除することが必要になるまでの時間を秒単位で入力します。</p> <p>許容の詳細については、Kubernetes のドキュメントを参照してください。</p>

ランタイム設定

次の表に、ランタイムプロパティを示します。

プロパティ	説明
暗号化データ	<p>クラスタ上の一時データが暗号化されるかどうかを示します。</p> <p>注: 一時データの暗号化によってジョブのパフォーマンスが低下する可能性があります。</p>
ランタイムプロパティ	クラスタとそのクラスタで実行するジョブをカスタマイズするためのカスタムプロパティ。

ランタイムプロパティ

次の表に、セルフサービスクラスタとそのクラスタで実行するジョブをカスタマイズするために使用できるランタイムプロパティを示します。

プロパティ	説明
infa.k8s.deploy.clusterkeygen.enable	clusterkeygen デプロイメントを管理します。デプロイメントを無効にするには、このプロパティを <code>false</code> に設定します。
infa.k8s.custom.quota.name	クォータ名を指定します（クラスタで定義されている場合）。
ccs.app.control.enable	アプリケーション送信制御を管理します。送信制御を無効にするには、このプロパティを <code>false</code> に設定します。 アプリケーション送信制御は、次の条件に当てはまる場合にのみ使用できます。 <ul style="list-style-type: none">- すべてのクラスタノードが同種である。- 名前空間またはノードが Informatica 用に予約されている。Informatica がノードの詳細を読み取ることができる。- 名前空間のクォータが存在する場合はそれが適用され、カスタムフラグを使用してクォータ名を設定できます。 クラスタでクォータを定義する場合、クォータ定義で使用するのは要求のみです。デプロイするリソースの制限を定義すると、リソースがスケジュールされないため、クォータ定義で制限は使用しないでください。
infacco.job.spark.kubernetes.scheduler.name	ドライバポッドとエグゼキュータポッドのカスタムスケジューラ名を指定します。 複数の同時マッピングを実行する場合は、より適切なポッドスケジューラをデプロイする必要があります。

ローカルクラスタのプロパティ

エラスティック構成でプロパティを設定するには、**【新規エラスティック構成】** をクリックするか、**【エラスティッククラスタ】** ページで編集する構成の名前をクリックします。

基本プロパティは、エラスティック構成を記述します。クラスタを設定するには、プラットフォームプロパティおよびランタイムプロパティを設定します。

基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	エラスティック構成の名前。
説明	エラスティック構成の説明。

プロパティ	説明
ランタイム環境	エラスティック構成に関連付けるランタイム環境。ランタイム環境に含めることができる Secure Agent は 1 つのみです。ランタイム環境を複数の構成と関連付けることはできません。
クラウドプラットフォーム	クラスタをホストするクラウドプラットフォーム。 [ローカル] を選択します。

プラットフォーム設定

次の表に、プラットフォームプロパティを示します。

プロパティ	説明
マッピング	マッピングタスクが完了するまで待機する時間。この時間が経過した後、マッピングタスクは強制終了となります。デフォルトでは、マッピングタスクにはタイムアウトはありません。 タイムアウトを指定する場合は、10 分以上の値をお勧めします。マッピングタスクが Secure Agent にサブミットされると、タイムアウトが開始されます。
ステージングの場所	クラウド上のステージングデータの場所の完全なパス。お使いのクラウド環境に基づいて、次の形式で場所を指定します。 <ul style="list-style-type: none"> - AWS。s3://<バケット名>/<フォルダパス> - Microsoft Azure。ストレージタイプに基づき、次のいずれかの形式を使用します。 <ul style="list-style-type: none"> - Microsoft Azure Blob Storage: wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<フォルダパス>&:<リソースグループ>/<リージョン> - Azure Data Lake Storage Gen2: abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<フォルダパス>&:<リソースグループ>/<リージョン> - Google Cloud。gs://<バケット名>/<フォルダパス>&:<プロジェクト ID>/<リージョン> リージョンはオプションです。有効なリージョンのリストについては、クラウドプロバイダのマニュアルを参照してください。 次の例は、リージョン形式が各クラウドプラットフォームでどのように異なるかを示しています。 <ul style="list-style-type: none"> - AWS では、us-west-2 を使用して米国西部（オレゴン）を表します。 - Google Cloud では、us-west2 を使用してロサンゼルスを表します。 - Microsoft Azure では、westus2 を使用して米国西部 2 を表します。
ログの場所	クラウド上のログの場所の完全なパス。お使いのクラウド環境に基づいて、次の形式で場所を指定します。 <ul style="list-style-type: none"> - AWS。s3://<バケット名>/<フォルダパス> - Microsoft Azure。ストレージタイプに基づき、次のいずれかの形式を使用します。 <ul style="list-style-type: none"> - Microsoft Azure Blob Storage: wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<フォルダパス>&:<リソースグループ>/<リージョン> - Azure Data Lake Storage Gen2: abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<フォルダパス>&:<リソースグループ>/<リージョン> - Google Cloud。gs://<バケット名>/<フォルダパス>&:<プロジェクト ID>/<リージョン> リージョンはオプションです。有効なリージョンのリストについては、クラウドプロバイダのマニュアルを参照してください。 次の例は、リージョン形式が各クラウドプラットフォームでどのように異なるかを示しています。 <ul style="list-style-type: none"> - AWS では、us-west-2 を使用して米国西部（オレゴン）を表します。 - Google Cloud では、us-west2 を使用してロサンゼルスを表します。 - Microsoft Azure では、westus2 を使用して米国西部 2 を表します。

ランタイム設定

次の表に、ランタイムプロパティを示します。

プロパティ	説明
暗号化データ	クラスタ上の一時データが暗号化されるかどうかを示します。
ランタイムプロパティ	クラスタとそのクラスタで実行するジョブをカスタマイズするためのカスタムプロパティ。

データ暗号化

暗号化によってエラスティックジョブの処理に使用されるデータが保護されます。暗号化は、保存データ、一時データ、転送中のデータの保護に使用できます。

暗号化は、以下のタイプのデータで使用できます。

保存データ

デフォルトでは、各クラウドプラットフォームでステージングファイルとログファイルが暗号化されます。詳細については、クラウドプロバイダのマニュアルを参照してください。

ソースデータおよびターゲットデータの暗号化について詳しくは、データ統合のヘルプで該当するコネクタのヘルプを参照してください。

注: Amazon S3 V2 接続内の暗号化関係のカスタムプロパティを設定する場合、Spark エンジンではステージングデータの読み取りと書き込みに同じカスタムプロパティを使用します。

一時データ

一時データには、サーバーレス Spark エンジンがクラスタノード上で生成するキャッシュデータとシャッフルデータが含まれます。

一時データを暗号化するには、エラスティック構成で暗号化を有効にします。暗号化を有効にする場合、一時データはデフォルトで HMAC-SHA1 アルゴリズムを使用して暗号化されます。別のアルゴリズムを使用するには、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。

転送中のデータ

デフォルトでは、クラウドプロバイダは、Transport Layer Security (TLS) プロトコルを使用して、クラウドストレージに対して送受信されるデータ（ステージングデータ、ログファイルなど）を暗号化します。

注: Microsoft Azure の Blob Storage で暗号化が有効になっている場合、エラスティック構成でステージングとログの場所を設定するときに WASBS プロトコルを指定できます。暗号化が有効になっていない場合、WASB プロトコルを使用する必要があります。

クラスタノードのリソース要件

エラスティック構成でインスタンスタイプを選択する場合、マスタノードとワーカーノードにエラスティックジョブを正常に実行するのに十分なリソースがあることを確認してください。

マスタノード

マスタノードでは、少なくとも 8 GB のメモリと 4 個の CPU を使用することをお勧めします。

注: マスターノードでの処理はネットワーク負荷が高いため、AWS 環境では T インスタンスタイプは避けてください。

ワーカーノード

ワーカーノードには、少なくとも 16 GB のメモリと 8 個の CPU を使用することをお勧めします。

次の表に、ワーカーノードのデフォルトのリソース要件の一覧を示します。

コンポーネント	デフォルトのメモリ要件	デフォルトの CPU 要件
Kubernetes システム	ワーカーノードあたり 1 GB	ワーカーノードあたり 0.5 CPU、およびクラスタに対して追加で 0.5 CPU
Spark シャッフルサービス	ワーカーノードあたり 2 GB	ワーカーノードあたり 1 CPU
Spark ドライバ	4 GB	0.75 CPU
Spark Executor	Spark Executor コアあたり 6 Gb または 3 GB	Spark Executor コアあたり 1.5 CPU または 0.75 CPU

デフォルトのリソース要件に基づいて、1 つのワーカーノードを持つクラスタには、13 GB のメモリと 4.25 個の CPU が必要です。

ワーカーノードがクラスタに追加されると、各ワーカーノードは、Kubernetes システムおよび Spark シャッフルサービス用に 3 GB のメモリと 1.5 個の CPU を追加で予約します。したがって、2 つのワーカーノードを持つクラスタには、16 GB のメモリと 5.75 個の CPU が必要です。

リソース要件の再設定

デフォルトの要件を満たすための十分なリソースを用意できない場合は、一部の要件を再設定できます。

以下のコンポーネントの要件を再設定できます。

Spark シャッフルサービス

シャッフルサービスを無効にすると、Spark エンジンで動的割り当てを使用出来なくなります。詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

Spark ドライバ

Spark ドライバのメモリ量を再設定するには、マッピングタスクで Spark セッションプロパティ `spark.driver.memory` を使用します。GB 単位でメモリを設定する場合は、「2G」などの値を使用します。MB 単位でメモリを設定する場合は、「1500m」などの値を使用します。

Spark ドライバの CPU 要件の再設定の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

Spark Executor

Spark Executor のメモリ量を再設定するには、マッピングタスクで Spark セッションプロパティ `spark.executor.memory` を使用します。Spark ドライバのメモリ値と同様に、メモリを GB または MB 単位で指定できます。

また、Spark セッションプロパティ `spark.executor.cores` を使用して Spark Executor コアの数を変更することもできます。GPU 対応クラスタのデフォルトのコア数は 4 です。他のすべてのクラスタのデフォルトのコア数は 2 です。

コア数を編集する場合は、同時に実行する Spark タスクの数を変更します。例えば、`spark.executor.cores=2` と設定すると、2 つの Spark タスクを各 Spark Executor 内部で同時に実行できます。

Spark Executor の CPU 要件の再設定の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

注: Spark ドライバおよび Spark Executor に対して設定したメモリが少なすぎると、これらのコンポーネントで `OutOfMemoryException` が発生する場合があります。

Kubernetes システムのリソース要件を編集することはできません。リソースは、機能的な Kubernetes システムを維持するために必要です。

Spark セッションプロパティの詳細については、データ統合のヘルプの「タスク」を参照してください。

リソース要件の例

1 台のワーカーノードにエラスティッククラスタが 1 つあります。ワーカーノードに 16 GB メモリと 4 CPU が搭載されています。

デフォルトの要件を使用してエラスティックジョブを実行すると、ジョブは失敗します。Kubernetes システムおよび Spark シャッフルサービスで 3 GB および 2 CPU を確保するため、クラスタでジョブを実行するための残量は 13 GB および 2 CPU となります。クラスタが Spark ドライバと Spark Executor を起動するために 10 GB のメモリと 2.25 CPU が必要となるため、ジョブを実行できません。

大きなインスタンスタイプをプロビジョニングできない場合は、マッピングタスクで以下の詳細なセッションプロパティを設定して CPU 要件を減らすことができます。

```
spark.executor.cores=1
```

Spark Executor コアの数 が 1 の場合、Spark Executor では 1.5 CPU ではなく 0.75 CPU のみ必要となります。

少量のデータを処理する場合、Spark ドライバおよび Spark Executor では数百 MB しか必要とならないため、ドライバと Executor のメモリ要件を減らすことも検討できます。要件は次の方法で減らすことができます。

```
spark.driver.memory=1G
```

```
spark.executor.memory=500M
```

リソース要件を再設定した後も、クラスタに 5 GB メモリ、3.5 CPU 以上が残っている必要があります。16 GB および 4 CPU の 1 台のワーカーノードは、ジョブを正常に実行するための要件を満たしています。

初期化スクリプト

クラスタノードは、エラスティック構成で指定したスクリプトパスに基づいて初期化スクリプトを実行できます。ノードが作成されると各ノードはスクリプトを実行します。スクリプトは他の初期化スクリプトを参照できます。

クラスタに追加ソフトウェアをインストールするために初期化スクリプトを実行したい場合があります。例えば、企業のポリシーにより、データを保護するための監視ソフトウェアやアンチウイルスソフトウェアを各クラスタノードに組み込む必要がある場合があります。

初期化スクリプトを作成する場合、次のガイドラインを考慮してください。

- 初期化スクリプトには、ファイルシステム上のすべての設定を変更する特権があります。このため、ファイルシステムからオブジェクトが削除されないようにしてください。
- Secure Agent は、初期化スクリプトの構文を検証しません。

初期化スクリプトのパスはクラウドストレージ内になければなりません。スクリプトは、クラウドストレージシステムの一意のパスに配置するか、ステージングの場所に配置することができます。

初期化スクリプトのエラー

クラスタノードで初期化スクリプトが失敗した場合、エラスティッククラスタに深刻な影響が及ぶ可能性があります。初期化スクリプトが失敗すると、クラスタをスケールアップできなくなります。または、Secure Agent によってクラスタが強制終了させられます。

次の状況で初期化スクリプトが失敗した場合は、その影響に注意してください。

クラスタ作成中の失敗

クラスタ作成中にノードで初期化スクリプトが失敗した場合、Secure Agent はクラスタを強制終了します。

ジョブを実行してクラスタを再び開始する前に、初期化スクリプトに関する問題を解決してください。

スケールアップイベント中の失敗

スケールアップイベント中にクラスタに追加されるノードで初期化スクリプトが失敗した場合、ノードは開始できず、クラスタのスケールアップは失敗します。クラスタがスケールアップを再試行し、ノードを引き続き開始できない場合、Secure Agent がクラスタを強制終了するまで、ノードの累積失敗数は増えた状態となります。

マスタノードのリカバリ中の失敗

AWS 環境で高可用性を有効にし、リカバリ対象のマスタノードで初期化スクリプトが失敗した場合、ノードは開始できず、クラスタのライフサイクル中、ノードの累積失敗数は増えた状態となります。

クラスタのライフサイクル中の累積失敗数

クラスタのライフサイクル中、Secure Agent は、特定のタイムフレーム内に初期化スクリプトが原因で発生したノードの失敗の累積数を追跡します。失敗の数が非常に多い場合、エージェントはクラスタを強制終了します。

ジョブを実行してクラスタを再び開始する前に、初期化スクリプトが失敗したノードのログファイルを見つければ、そのログファイルを使用して失敗を解決してください。

ランタイム環境またはステージングの場所の更新

ランタイム環境またはステージングの場所を更新するには、Secure Agent およびエラスティッククラスタのステータスに基づき、次のタスクのいずれかを実行します。

Secure Agent およびエラスティッククラスタが稼働している。

エージェントおよびクラスタが稼働している場合は、以下のタスクを実行します。

1. エラスティック構成でランタイム環境またはステージングの場所を更新します。
2. 構成を保存すると、クラスタが停止します。

Secure Agent を使用できない、またはエラスティッククラスタにアクセスできない。

エージェントを使用できない、またはクラスタにアクセスできない場合は、次のすべてのタスクを完了します。

1. コマンドを実行してクラスタを削除するか、クラウドプラットフォームのアカウントにログインしてすべてのクラスタリソースが削除されていることを確認します。コマンドについては、[付録 A, 「コマンドリファレンス」 \(ページ 148\)](#)を参照してください。
2. エラスティック構成でランタイム環境またはステージングの場所を更新します。
3. 構成を保存する場合は、クラスタを無効にします。

注: ランタイム環境を更新する場合、新しい Secure Agent が新しいエラスティッククラスタを別のクラスタ ID で作成します。

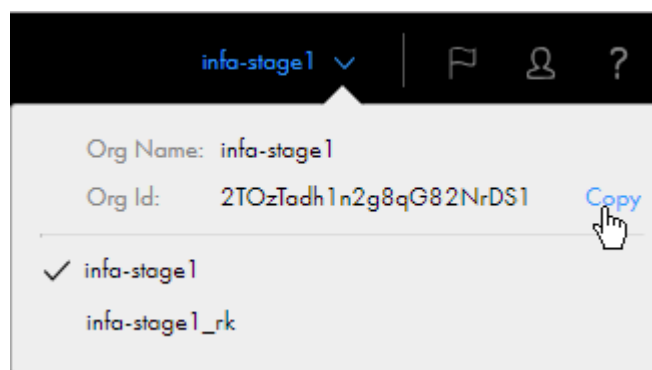
第 8 章

トラブルシューティング

次のセクションを使用して、エラスティッククラスタのエラーをトラブルシューティングします。

注: Data Integration Elastic のサポートを受けるには、組織 ID を Informatica グローバルカスタマサポートに伝える必要があります。組織 ID は、右上隅にある【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 をコピーするには、【組織 ID】フィールドの右側にカーソルを置くと表示される【コピー】オプションをクリックします。

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。

エラスティッククラスタのトラブルシューティング

エラスティッククラスタのステータスが不明の場合に実行すべきこと。

クラスタのステータスが不明の場合は、最初に Secure Agent が稼働している事を確認します。エージェントが稼働していない場合は、エージェントを有効にして、クラスタの稼働開始を確認します。

クラスタが始動しない場合は、管理者がクラスタをリストするコマンドを実行できます。コマンド出力が一部または使用中のクラスタ状態を返す場合、管理者はクラスタを削除するコマンドを実行する事ができます。

コマンドの詳細については、Administrator ヘルプを参照してください。

ccs-operation.log ファイルを調べてエラスティッククラスタのトラブルシューティングを行ったが、情報が不十分であった。他にどこを調べればよいか。

エラスティッククラスタのインスタンス専用の cluster-operation ログを確認できます。外部コマンドセットの実行が開始されると、ccs-operation ログに cluster-operation ログへのパスが表示されます。

以下に例を示します。

```
2020-06-15 21:22:36.094 [reqid:] [T:000057] INFO : c.i.c.s.c.ClusterComputingService [CCS_10400]
Starting to run command set [<command set>] which contains the following commands: [
  <commands> ;
]. The execution log can be found in the following location: [/data2/home/cldagnt/SystemAgent/apps/
At_Scale_Server/35.0.1.1/ccs_home/3xukm9iqp5zeahyrb7rqoz.k8s.local/infa/cluster-operation.log].
```

指定されたフォルダには、クラスタのインスタンスに属するすべての cluster-operation ログが含まれます。ログを使用して、コマンドセットの完全な stdout および stderr 出力ストリームを表示できます。

ログ名の数字はログの生成を示し、各 cluster-operation ログは最大 10 MB です。例えば、外部コマンドの実行中にクラスタインスタンスが 38 MB のログメッセージを生成した場合、フォルダには 4 つの cluster-operation ログが含まれます。最新のログのファイル名では 0 で、最も古いログのファイル名では 3 です。cluster-operation0.log ファイルのメッセージを表示して、最新のエラーを表示できます。

エラスティックサーバーのログレベルを DEBUG に設定すると、ccs-operation ログに cluster-operation ログと同じ詳細レベルが表示されます。

init スクリプトが失敗したノードの初期化スクリプトログを見つける方法

init スクリプトログを見つけるには、次のタスクを実行します。

1. Secure Agent マシンの次のディレクトリに、ccs-operation.log ファイルがあります。
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/ccs_home/
2. ccs-operation.log ファイルで、次のようなメッセージを見つけます。
Failed to run the init script for cluster [<cluster instance ID>] on the following nodes: [<cluster node IDs>]. Review the log in the following S3 file path: [<cloud platform location>].
3. メッセージで示されているクラウドプラットフォームの場所に移動します。
4. クラスタノード ID を、init スクリプトが失敗したノードの init スクリプトログファイル名と一致させます。

次のエラーメッセージでのエラスティッククラスタのリソース要件の計算方法

```
2019-04-26T19:04:11.762+00:00 <Thread-16> SEVERE: java.lang.RuntimeException: [java.lang.RuntimeException: The
Cluster Computing System rejected the Spark task [InfaSpark0] due to the following error: [[CCS_10252] Cluster
[6bjwune8v4bkt3vneoki9.k8s.local] doesn't have enough resources to run the application [spark--
infaspark0e6674748-b038-4e39-a2a9-3fd49e63f289infaspark0-driver] which requires a minimum resource of [(KB
memory, mCPU)]. The cluster must have enough nodes, and each node must have at least [(KB memory, mCPU)] to
run this job.].]
```

最初のリソース要件は、Spark ドライバと Spark エグゼキュータが必要とするリソースの総数です。

2 番目のリソース要件は、最低 1 つの Spark プロセスを実行するための各ワーカーノードの最小リソース要件に基づいて計算されます。

リソースは次の式を使用して計算されます。

```
Memory: MAX(driver_memory, executor_memory)
CPU: MAX(driver_CPU, executor_CPU)
```

Spark プロセスは、Spark ドライバプロセスまたは Spark 実行者プロセスのいずれかです。クラスタでは、各ノードがドライバまたは実行者のいずれかを実行するための最小要件を満たすノードを 2 つ使用するか、ドライバと実行者の両方を実行するために十分なリソースを持つ 1 つのノードを使用する必要があります。

注: ドライバおよびエグゼキュータのリソース要件は、マッピングタスクの次の詳細セッションプロパティを設定する方法に応じて異なります。

spark.driver.memory

```
spark.executor.memory
spark.executor.cores
```

最小リソース要件の詳細については、Administrator ヘルプで *Data Integration Elastic* 管理に関するヘルプを参照してください。

クラウドプラットフォームで Secure Agent マシンをシャットダウンしたが、一部のジョブはまだ実行されている。

エージェントマシンをシャットダウンすると、エージェントは新しいマシンで起動しますが、ジョブは新しいマシンに引き継がれません。

Monitor で、ジョブをキャンセルして再度実行します。新しいマシンのエージェントがジョブの処理を開始します。

この問題を回避するには、Administrator ヘルプのエージェントマシンをシャットダウンする手順を参照してください。

AWS 上のエラスティッククラスタのトラブルシューティング

エラスティッククラスタが起動しない理由

エラスティッククラスタが起動に失敗した理由を見つけるには、Secure Agent マシンの次のディレクトリにある `ccs-operation.log` ファイルを使用します。

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

次のテーブルに、クラスタが起動しないいくつかの理由を示します。

理由	考えられる原因
クラスタオペレータはクラスタの更新に失敗しました。	AWS アカウントで VPC 制限に到達した。
マスターノードの起動に失敗した。	マスターインスタンスタイプは、指定されたリージョンまたは可用性ゾーン、または AWS アカウントではサポートされていません。
すべてのワーカーノードを起動できなかった。	ワーカーインスタンスタイプは、指定されたリージョンまたは可用性ゾーン、または AWS アカウントではサポートされていません。
Kubernetes API サーバーが起動できなかった。	ユーザー定義のマスターロールでエラーが発生しました。

これらの理由の少なくとも 1 つが原因でクラスタが起動に失敗すると、`ccs-operation.log` ファイルに `BadClusterConfigException` が表示されます。

例えば、次のようなエラーが発生する可能性があります。

```
2019-06-27 00:50:02.012 [T:000060] SEVERE : [CCS_10500] [Operation of <cluster instance ID>: start_cluster-
<cluster instance ID>]: com.informatica.cloud.service.ccs.exception.BadClusterConfigException: [[CCS_10207]
```

The cluster configuration for cluster [<cluster instance ID>] is incorrect due to the following error: [No [Master] node has been created on the cluster. Verify that the instance type is supported.]. The Cluster Computing System will stop the cluster soon.]

クラスタで `BadClusterConfigException` が発生した場合、エージェントはすぐにクラスタを停止して、追加のリソースコストの発生を防ぎ、潜在的なリソースリークを回避します。エージェントは、設定エラーが解決されるまで、クラスタの回復を試みません。

エラスティッククラスタを開始するジョブを実行したが、VPC 制限に到達した。

クラスタのエラスティック構成で VPC を指定していない場合は、Secure Agent が AWS アカウントで新しい VPC を作成します。AWS アカウントの VPC の数が各リージョンで制限されているため、VPC 制限に到達した可能性があります。

VPC 制限に到達した場合は、エラスティック構成を編集し、次のいずれかのタスクを実行します。

- それぞれのリージョンを指定します。
- 可用性ゾーンを削除します。次に、既存の VPC および使用するクラスタの VPC 内の特定のサブネットを指定します。

クラスタでプロビジョニングされたクラウドリソースは、クラスタが新しいリージョンまたは既存の VPC で起動する場合に再利用されます。例えば、Secure Agent が VPC 制限のエラーを受信する前に Amazon EBS ボリュームをプロビジョニングしたとします。EBS ボリュームは削除されず、次の起動時に再利用されます。

エラスティッククラスタを起動するジョブを実行したが、次のエラーが発生し、クラスタの作成に失敗した。

Failed to create cluster [<cluster instance ID>] due to the following error: [[CCS_10302] Failed to invoke AWS SDK API due to the following error: [Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied; Request ID: <request ID>; S3 Extended Request ID: <S3 extended request ID>)].].]

Secure Agent は、Amazon S3 がエージェントの要求を拒否したためにエラスティッククラスタの作成に失敗しました。

S3 バケットポリシーが、クライアントによる暗号化ヘッダーを含む要求の送信を求めていることを確認してください。

起動に失敗した Kubernetes API サーバーをトラブルシューティングする方法

Kubernetes API サーバーの起動に失敗すると、エラスティッククラスタの起動に失敗します。この失敗をトラブルシューティングするには、代わりに Kubernetes API サーバーログを使用します。

Kubernetes API サーバーログを見つけるには、次のタスクを実行します。

1. Secure Agent マシンからマスターノードに接続します。
2. マスターノードで、ディレクトリ `/var/log/` にある Kubernetes API Server ログファイルを見つけます。

エラスティッククラスタのステージング場所を更新したら、エラスティックマッピングに次のエラーが発生し、失敗するようになった。

Error while executing mapping. ExecutionId '<execution ID>'. Cause: [Failed to start cluster for [01000D2500000000000005]. Error reported while starting cluster [Cannot apply cluster operation START because the cluster is in an error state.].].]

エラスティック構成で S3 ステージングの場所を変更する前にステージングの場所に対する権限を変更すると、このエラーが発生してマッピングが失敗します。

ステージングの場所を更新する場合は、最初にエラスティック構成で S3 ステージングの場所を変更してから、AWS のステージングの場所に対する権限を変更します。ロールベースのセキュリティを使用した場合は、Secure Agent マシンでステージングの場所に対する権限を変更する必要もあります。

エラーを修正するには、次のタスクを実行します。

1. ステージングの場所の権限に対する変更を元に戻します。
2. S3 ステージングの場所を元に戻すようにエラスティック構成を編集します。
3. 構成を保存すると、クラスタが停止します。
4. 構成の S3 ステージングの場所を更新してから、AWS でステージングの場所に対する権限を変更します。

エラスティッククラスタのステージング場所を更新したら、エージェントジョブログに次のエラーメッセージが表示されるようになった。

```
Could not find or load main class com.informatica.compiler.InfaSparkMain
```

このエラーメッセージは、クラスタノードがアクセス権限のためにステージングの場所から Spark バイナリをダウンロードできない場合に表示されます。

ジョブが使用するコネクタのタイプに基づいて、ステージングの場所のアクセス権限を確認します。

Amazon データソースへの直接アクセスを持つコネクタ

エラスティックジョブで資格情報ベースのセキュリティを使用する場合は、Amazon S3 V2 および Amazon Redshift V2 接続の資格情報がステージングの場所へのアクセスに使用できることを確認します。

エラスティックジョブでロールベースのセキュリティを使用する場合は、エラスティッククラスタおよびステージングの場所が同じ AWS アカウント内に存在することを確認します。

Amazon データソースへの直接アクセスがないコネクタ

ユーザー定義のワーカーロールを使用する場合は、ワーカーロールがエラスティックジョブのステージングの場所とデータソースの両方にアクセスできることを確認します。

デフォルトのワーカーロールを使用する場合は、Secure Agent ロールがエラスティックジョブのステージングの場所とデータソースの両方にアクセスできることを確認します。

Secure Agent マシンを再起動したら、エラスティッククラスタのステータスがエラーになった。

Secure Agent マシンおよび Secure Agent が稼働していることを確認します。次に、Monitor でエラスティッククラスタを停止します。AWS 環境では、クラスタの停止に 3~4 分かかる場合があります。クラスタが停止したら、エラスティックジョブを実行してクラスタを再起動できます。

カスタム AMI を使用してクラスタノードを作成する前に行う必要があること

カスタム AMI (Amazon マシンイメージ) を使用してクラスタノードを作成する場合は、AMI に AWS CLI のインストールが含まれていることを確認します。

Secure Agent は AWS CLI を使用して、タグを Amazon リソースにプロパゲートし、ログを集計します。また、クラスタノードは AWS CLI を使用して初期化スクリプトを実行します。

カスタム AMI の使用方法については、Informatica グローバルカスタマーサポートにお問い合わせください。

Microsoft Azure 上のエラスティッククラスタのトラブルシューティング

Blob Storage にステージングとログの場所を設定した後、エラスティックマッピングが失敗し、セッションログに次のエラーメッセージが表示される。

```
20-02-11T00:52:43.273+00:00 <WorkflowExecutorThread20> INFO: [LDTM_0075] Total time to perform the LDTM operation: 84,962 ms
2020-02-11T00:52:43.305+00:00 <InfaDisnextHadoopMappingExecutor-3-64> SEVERE: java.lang.RuntimeException: java.lang.RuntimeException: Failed to upload the local file in the path [/mnt/resource/informatica/secureagent/apps/At_Scale_Server/33.0.1.1/metadata/0100edc7-f043-43f7-a5e1-a39f0774c2c7InfaSpark0/submit_InfaSpark0_staticCode.jar] to the following shared storage location: [<Blob Storage location>] due to the following error: [java.lang.RuntimeException: [org.apache.hadoop.fs.azure.AzureException: com.microsoft.azure.storage.StorageException: The account being accessed does not support http.]].
2020-02-11T00:52:43.306+00:00 <InfaDisnextHadoopMappingExecutor-3-64> INFO: Spark Mapping Ended with state: Failed
```

Blob Storage では HTTPS 経由でリクエストを行う必要があるため、エラーが表示されます。エラーを解決するには、Azure ポータルを使用して、ステージングとログの場所を保持するストレージアカウントの [Secure transfer required (セキュア転送が必要)] オプションを無効にします。

Secure Agent マシンを再起動したら、エラスティッククラスタのステータスがエラーになった。

Secure Agent マシンおよび Secure Agent が稼働していることを確認します。次に、Monitor でエラスティッククラスタを停止します。Azure 環境では、クラスタの停止に 10 分かかる場合があります。クラスタが停止したら、エラスティックジョブを実行してクラスタを再起動できます。

エラスティッククラスタの一部のノードで、次の標準エラーが発生して init スクリプトが失敗した。

```
Created symlink from /etc/systemd/system/apt-daily.service to /dev/null.
Created symlink from /etc/systemd/system/apt-daily-upgrade.service to /dev/null.
Removed symlink /etc/systemd/system/timers.target.wants/apt-daily.timer.
Removed symlink /etc/systemd/system/timers.target.wants/apt-daily-upgrade.timer.
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is another process using it?
```

ノードが init スクリプトと同時に内部プロセスを実行していたため、init スクリプトが失敗しました。エラーが引き続き表示される場合は、init スクリプトに必要な期間だけスリープコマンドを配置して、内部プロセスが完了するまで待ちます。

例えば、次のようにスリープコマンドを使用できます。

```
#!/bin/sh

while(sudo lsof /var/lib/dpkg/lock-frontend)
do
echo "Sleeping 10s"
sleep 10
done

sudo apt-get -y update
sudo apt-get install -y expect
```


エラスティックジョブのトラブルシューティング

エラスティックジョブが失敗しましたが、表示できるログがたくさんあります。どこから始めればよいですか。

エラスティックジョブが失敗した場合、次の順序でログを調べてジョブのトラブルシューティングを行うことができます。

1. 実行プラン。ジョブの Scala コードをデバッグするのに使用します。
2. セッションログ。ジョブをコンパイルし、Spark 実行ワークフローを生成するロジックをデバッグするのに使用します。
3. エージェントジョブログ。Secure Agent が Spark 実行ワークフローを処理するためにエラスティッククラスタにプッシュする方法をデバッグするのに使用します。
4. Spark ドライバおよびエグゼキュータログ。サーバーレス Spark エンジンのジョブの実行方法をデバッグするのに使用します。

Monitor で、実行プラン、セッションログ、エージェントジョブログ、および Spark ドライバログをダウンロードできます。

Spark 実行ログを見つけるには、失敗した特定の Spark タスクの詳細ログの場所をコピーします。次に、クラウドプラットフォームのログの場所に移動し、ログをダウンロードします。

失敗したエラスティックジョブのすべてのログファイルを見つけることができない。
Monitor とクラウドプラットフォームのログの場所の両方からログをダウンロードしようとした。

エラスティックジョブの使用可能なログは、処理中にジョブが失敗したステップによって異なります。

例えば、ジョブがエラスティッククラスタにプッシュされる前にジョブが失敗した場合、Spark ドライバおよびエグゼキュータログはログの場所には生成されず、Monitor がクラウドプラットフォームからログをクエリすることもできません。

一部のログファイルはリカバリできますが、ジョブをトラブルシューティングするには、別のタイプのログを使用する必要がある場合があります。

Spark ドライバおよび Spark エグゼキュータログが見つかりません。これらをリカバリできますか。

Spark ドライバログをユーザーインターフェースからダウンロードできない場合、Spark ドライバポッドを使用してログをリカバリできます。Spark エグゼキュータログはリカバリ出来ません。

Secure Agent がエラスティックジョブをクラスタにプッシュするときに、Secure Agent は 1 つの Spark ドライバポッドおよび複数の Spark エグゼキュータポッドを作成して Spark タスクを実行します。Spark ドライバポッドを使用して Spark ドライバログをリカバリできますが、Spark エグゼキュータログはリカバリできません。エラスティックジョブが成功または失敗したらすぐに、Spark ドライバポッドは Spark エグゼキュータポッドを削除します。

注: ジョブが成功または失敗したとき、Spark ドライバポッドはデフォルトでは 5 分後に削除されます。トラブルシューティングの支援のためにこの上限を増やす必要がある場合は、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。

Spark ドライバログをリカバリするには、次のタスクを実行します。

1. エージェントジョブログで Spark ドライバポッドの名前を検索します。例えば、次のメッセージに、Spark ドライバポッドの名前があります。

```
2019/04/09 11:10:15.511 : INFO :Spark driver pod [spark-passthroughparquetmapping-veryvery-longlongname-1234567789-infaspark02843891945120475434-driver] was successfully submitted to the cluster.  
Monitor でエージェントジョブログをダウンロードできない場合、ログは Secure Agent マシンの次のディレクトリで入手できます。
```

```
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/logs/job-logs/
```

エージェントジョブログのファイル名は、*AgentLog-<Spark job ID>.log* の形式を使用します。Spark ジョブ ID はセッションログで見つける事ができます。例えば、セッションログの次のメッセージで、Spark ジョブ ID は *0c2c5f47-5f0b-43af-a867-da011452c19dInfaSpark0* です。

```
2019-05-09T03:07:52.129+00:00 <LdtmWorkflowTask-pool-1-thread-9> INFO: Registered job to status checker with Id 0c2c5f47-5f0b-43af-a867-da011452c19dInfaSpark0
```

2. Spark ドライバポッドが存在することを確認します。ドライバポッドが削除された場合、Spark ドライバログを取得できません。

ドライバポッドが存在することを確認するには、Secure Agent マシンの次のディレクトリに移動します。

```
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/mercury/services/shared/kubernetes/kubernetes_1.11/bin
```

そのディレクトリで、以下のコマンドを実行します。

```
./kubectl get pods
```

3. 次のいずれかの方法で、クラスティンスタンス ID を検索します。

- セッションログでクラスティンスタンス ID を探します。例えば、表示される可能性のあるメッセージには次のようなものがあります。

```
2019/05/07 16:22:00.20 : INFO :[SPARK_2005] Uploading the local file in the path [/export/home/builds/ws/yxiao_hadoopvm_ML/Mercury/platformdiscle/main/components/cluster/hadoop-tests/cats/edtm/spark/.target/hadoop3a0b1db6-76ea-4317-8272-5b3a8dfd2171_InfaSpark0/log4j_infa_spark.properties] to the following shared storage location: [s3a://soki-k8s-local-state-store/k8s-infa/testcluster2.k8s.local/staging/sess4280021555102778947/log4j_infa_spark.properties].
```

メッセージに表示される次のクラウドストレージの場所に注意してください。

```
s3a://soki-k8s-local-state-store/k8s-infa/testcluster2.k8s.local/staging/
```

クラスティンスタンス ID は「k8s-infa」の後に続くエントリです。この場合、ID は testcluster2.k8s.local です。

- ccs-operation.log ファイルでクラスティンスタンス ID を探します。ファイルは Secure Agent マシンの次のディレクトリにあります。

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

4. Secure Agent マシンにエージェントを開始した sudo ユーザーとしてログインします。

5. Secure Agent マシンの環境変数 KUBECONFIG に次の値を設定します。

```
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/ccs_home/<cluster ID>/k8s_infa/kubeconfig.yaml
```

6. Spark ドライバログを取得するには、Secure Agent マシンの次のディレクトリに移動します。

```
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/mercury/services/shared/kubernetes/kubernetes_1.11/bin
```

そのディレクトリで、以下のコマンドを実行します。

```
./kubectl logs <Spark driver pod name>
```

セルフサービスクラスタのトラブルシューティング

自己管理型 Kubernetes クラスタにアクセスできない場合、セルフサービスクラスタで実行されるエラスティックマッピングが失敗する。

マッピングが失敗して、次のエラーが表示されます。

```
2022-06-23T04:42:10.872+00:00 <getThreadPoolTaskExecutor-502> INFO: Waiting for cluster with Cluster Instance ID : [16y6xhsvjkdeybtzdy1dkx.k8s.local] to start. 2022-06-23T04:42:13.394+00:00 <getThreadPoolTaskExecutor-502> SEVERE: WES_internal_error_An unexpected error occurred during execution.
```

Secure Agent ノードから自己管理型 Kubernetes クラスタにアクセスできるかどうかを確認します。

Secure Agent ノードから自己管理型 Kubernetes クラスタにアクセスできるにもかかわらず、エラスティックマッピングが失敗する場合は、クラスタのアイドルタイムアウト（30 分）を待って、クラスタの状態を監視します。クラスタの状態が STOP に変わったら、クラスタを起動してからマッピングを実行します。

クラスタのアイドルタイムアウトを待たないようにするには、Secure Agent プロセスを再起動してからマッピングを実行します。

エラスティックマッピングを実行したときに、途中でセルフサービスクラスタを停止すると、クラスタの再起動後に次のエラーでマッピングが失敗します。

```
<SparkTaskExecutor-pool-1-thread-11> SEVERE: Reattemptable operation failed with error: Failure executing: POST at: https://35.84.220.154:6443/api/v1/namespaces/default/pods. Message: pods "spark-infaspark0229e35d4-d9d1-4203-a2b1-d4692ace052finfaspark0-driver" is forbidden: error looking up service account default/infa-spark: serviceaccount "infa-spark" not found, metadata=ListMeta(_continue=null, remainingItemCount=null, resourceVersion=null, selfLink=null, additionalProperties={}), reason=Forbidden, status=Failure, additionalProperties={}
```

エラーを解決するには、Secure Agent プロセスを再起動してから、マッピングを実行します。

Secure Agent マシンとクラウドリソースのシャットダウン

Secure Agent マシンをシャットダウンする場合は、エラスティッククラスタにプロビジョニングされたすべてのクラウドリソースが削除されていることを確認してください。

Secure Agent マシンを適切にシャットダウンするには、以下のタスクを実行します。

1. クラスタが実行中の場合は、Monitor でエラスティッククラスタを停止します。
2. Administrator で Secure Agent を停止します。
3. クラウドプラットフォームで、Secure Agent マシンをシャットダウンします。

クラスタの実行中に Secure Agent マシンをシャットダウンすると、クラスタノードのみシャットダウンされます。ネットワーク、ステージングデータとログファイル、ストレージデバイスなど、その他のリソースはクラウドに残ります。

クラスタを停止する前または Secure Agent を停止する前に Secure Agent マシンをシャットダウンした場合、Secure Agent マシンを再起動して、Secure Agent が実行していることを確認します。次に、モニタを使用してクラスタを停止します。クラスタが停止したら、Secure Agent を停止して Secure Agent マシンをシャットダウンします。

注: Secure Agent マシンを再起動すると、クラスタのステータスがモニタでエラーになります。

付録 A

コマンドリファレンス

提供されたシェルコマンドを使用すると、クラスタデプロイメントの設定および管理に役立ちます。例えば、完全には停止しなかったクラスタを削除するためにコマンドを実行できます。

コマンドを実行する前に

コマンドを実行する前に、JAVA_HOME 環境変数が Secure Agent マシンで設定されていること、および Secure Agent マシンの Java バージョンが JDK 8 と互換性があることを確認します。

コマンドの実行

Secure Agent マシンの次のディレクトリで、コマンドを実行します。

```
<Secure Agent installation directory>/apps/At_Scale_Server/<version>/mercury/services/shared/kubernetes/  
kubernetes_1.11/scripts/
```

バージョンは、エラスティックサーバーのバージョン番号です。

注: コマンドを実行するとき、現在のディレクトリは、スクリプトがあるディレクトリでなければなりません。

generate-policies-for-userdefined-roles.sh

AWS 環境で、マスタロールとワーカーロールのポリシーコンテンツを生成します。

出力は my-userdefined-master-worker-role-policies.json ファイルに保存されます。ポリシーコンテンツ内の特定の要素を制限し、コンテンツをポリシーとしてマスタロールおよびワーカーロールにアタッチできます。詳細については、[「手順 8.ユーザー定義のマスタロールおよびワーカーロールの作成」 \(ページ 33\)](#)を参照してください。

コマンドでは、以下のオプションを使用します。

```
-h | -help  
-sd | -staging-dir=<cluster-staging-directory>  
-ld | -logging-dir=<cluster-logging-directory>
```

次の表に、各オプションを示します。

オプション	説明
-help -h	コマンドのヘルプにアクセスします。
-staging-dir -sd	エラスティッククラスタのステージングディレクトリ。 -staging-dir=bucket/folder という形式を使用します。 ディレクトリには少なくともバケット名を含める必要があります。プレフィックス s3://は含めないでください。
-logging-dir -ld	エラスティッククラスタとそのクラスタで実行されるエラスティックジョブのログを保存するログディレクトリ。 -logging-dir=bucket/folder という形式を使用します。 ディレクトリには少なくともバケット名を含める必要があります。プレフィックス s3://は含めないでください。

list-clusters.sh

ステージングディレクトリ内のクラスタをすべて一覧表示します。

コマンドでは、以下のオプションを使用します。

-h | -help

-d | -staging-dir=<cluster-bucket-location-without-prefix-s3://> (AWS 環境) または<staging-location-with-prefix-wasb[s]-or-abfs[s]://> (Azure 環境)

-azsrg | -azure-storage-resource-group

-ac | -azurecrepath=azcredfilepath

-ct | -cluster-type

次の表に、各オプションを示します。

オプション	説明
-help -h	コマンドのヘルプにアクセスします。
-staging-dir -d	クラスタのエラスティック構成で設定されるステー징ディレクトリ。 ご使用のクラウドプラットフォームに基づき、次のいずれかの形式を使用します。 <ul style="list-style-type: none">- AWS 環境では、-staging-dir=<バケット名>/<フォルダ名>を使用します。 ディレクトリには少なくともバケット名を含める必要があります。プレフィックス s3:// は含めないでください。Microsoft Azure Blob Storage を使用する Azure 環境では、-staging-dir=wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<ステー징ディレクトリパス>を使用します。 格納場所で暗号化が有効になっている場合は、WASBS プロトコルを指定します。Azure Data Lake Storage Gen2 を使用する Azure 環境では、-staging-dir=abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<ステー징ディレクトリパス>を使用します。 格納場所で暗号化が有効になっている場合は、ABFSS プロトコルを指定します。
-azsrg -azure-storage-resource-group	クラスタのエラスティック構成で設定され、ステー징ストレージアカウントを保持するストレージリソースグループ。
-azurecpath -ac	APPID、TENANTID、SERVICE PRINCIPAL、および SUBSCRIPTION を含む、Secure Agent マシンでの Azure 資格情報ファイルの場所。AWS 環境では、このオプションは無視してください。 注: このオプションを含むスクリプトは失敗します。Informatica グローバルカスタマサポートによって指示された場合のみ、Microsoft Azure 環境でこのオプションを使用します。
-cluster-type -ct	AWS 環境のエラスティッククラスタか、AWS 環境または Microsoft Azure 環境のローカルクラスタのクラスタタイプ。local、kubeadm、または kops を指定できます。デフォルトでは、コマンドは kubeadm によって管理されているクラスタで実行されます。Azure 環境のエラスティッククラスタの場合、このオプションは無視してください。

delete-clusters.sh

ステー징ディレクトリでクラスタを削除します。

コマンドでは、以下のオプションを使用します。

```
-h | -help  
  
-d | -staging-dir=<cluster-bucket-location-without-prefix-s3://> (AWS 環境) または <staging-location-with-prefix-wasb[s]-or-abfs[s]://> (Azure 環境)  
  
-azsrg | -azure-storage-resource-group  
  
-s | -deletable-states=state-1[,state-2,...]  
  
-c | -clusters=cluster1[,cluster2,...]  
  
-f | -force
```

-ac | -azurecrepath=azcredfilepath

-ct | -cluster-type

次の表に、各オプションを示します。

オプション	説明
-help -h	コマンドのヘルプにアクセスします。
-staging-dir -d	クラスタのエラスティック構成で設定されるステージングディレクトリ。 ご使用のクラウドプラットフォームに基づき、次のいずれかの形式を使用します。 <ul style="list-style-type: none">- AWS 環境では、-staging-dir=<バケット名>/<フォルダ名>を使用します。 ディレクトリには少なくともバケット名を含める必要があります。プレフィックス s3:// は含めないでください。- Microsoft Azure Blob Storage を使用する Azure 環境では、-staging-dir=wasb(s)://<コンテナ>@<ストレージアカウント>.blob.core.windows.net/<ステージングディレクトリパス>を使用します。 格納場所で暗号化が有効になっている場合は、WASBS プロトコルを指定します。- Azure Data Lake Storage Gen2 を使用する Azure 環境では、-staging-dir=abfs(s)://<ファイルシステム>@<ストレージアカウント>.dfs.core.windows.net/<ステージングディレクトリパス>を使用します。 格納場所で暗号化が有効になっている場合は、ABFSS プロトコルを指定します。
-azsrg -azure-storage-resource-group	クラスタのエラスティック構成で設定され、ステージングストレージアカウントを保持するストレージリソースグループ。
-deletable-states -s	クラスタの状態を表すカンマ区切りのリスト。表示されたいずれかの状態とクラスタの状態が一致する場合、そのクラスタは削除されます。 次のいずれかの状態を一覧表示できます。 <ul style="list-style-type: none">- 削除。クラウド上のいずれのリソースも使用していないクラスタを削除します。AWS 環境でクラウドに保存された残りの情報は、Amazon S3 の履歴メタデータです。このコマンドによってクラスタのストレージが消去され、クラスタの状態、作成履歴、ステージングディレクトリが削除されます。- メタデータのみ。開始されていないクラスタを削除します。AWS 環境では、このコマンドによって、クラスタに保存された Kubernetes の状態のみが削除されます。- 一部。開始出来なかったクラスタ、または開始したが完全に停止しなかったクラスタが削除されます。AWS 環境では、このコマンドによって Kubernetes の delete コマンドが実行され、クラスタにプロビジョニングされたクラウドリソースが削除されます。- 使用中。仮想マシンが実行中である可能性が高いクラスタが削除されますが、このクラスタではジョブが実行されていない可能性があります。AWS 環境では、このコマンドによって Kubernetes の delete コマンドが実行され、クラスタにプロビジョニングされたクラウドリソースが削除されます。- すべて。上記の状態にあるすべてのクラスタが削除されます。 Microsoft Azure 環境では、クラスタを削除するとステージングディレクトリからすべてのクラスタ情報が消去されます。 例えば、-deletable-states=metadata-only,partial を使用すると、まだ開始していないクラスタと開始出来なかったクラスタが削除されます。 上記の状態にあるすべてのクラスタを削除するには、-deletable-states=all を使用します。

オプション	説明
-clusters -c	コマンドを実行するクラスタのカンマ区切りのリスト。 例えば、同じステージングディレクトリを使用する開発環境とテスト環境があるとし ます。開発環境ではなくテスト環境で一部または使用中の状態にあるクラスタを削除する 必要があります。テスト環境のクラスタのみを削除するには、テスト環境のクラスタを 一覧表示します。
-force -f	追加のプロンプトをスキップします。 -force オプションを使用しない場合は、コマンドに各エラスティッククラスタが一覧表 示され、クラスタの削除を確認するよう求められます。「Yes」または「No」のいずれかを 入力できます。 -force オプションを使用する場合は、クラスタが自動的に削除されます。
-azurecrepath -ac	APPID、TENANTID、SERVICE PRINCIPAL、および SUBSCRIPTION を含む、Secure Agent マシンでの Azure 資格情報ファイルの場所。AWS 環境では、このオプションは無視して ください。 注: このオプションを含むスクリプトは失敗します。Informatica グローバルカスタマサ ポートによって指示された場合のみ、Microsoft Azure 環境でこのオプションを使用しま す。
-cluster-type -ct	AWS 環境のエラスティッククラスタか、AWS 環境または Microsoft Azure 環境のローカ ルクラスタのクラスタタイプ。local、kubeadm、または kops を指定できます。デフォ ルトでは、コマンドは kubeadm によって管理されているクラスタで実行されます。 Azure 環境のエラスティッククラスタの場合、このオプションは無視してください。

例えば、次のコマンドは、ステージングディレクトリ *autodeploy/devbld* 内の特定のクラスタを調べて、ス
テータスが *deleted*、*metadata-only*、または *in-use* になっているクラスタを削除します。

```
delete-clusters.sh -d=autodeploy/devbld -deletable-states=deleted,metadata-only,in-use -  
c=testcluster.k8s.local,testcluster.k8s.local,testcluster2.k8s.local,testcluster3.k8s.local,testcluster4.k8s.lo  
cal
```

cluster-operations.sh

クラスタの一覧表示やクラスタの削除など、ステージングディレクトリ内のクラスタに対する操作を実行しま
す。

コマンドでは、以下の構文を使用します。

```
cluster-operations.sh <cloud environment> <operation> <argument1> <argument2> [<argument3>...]
```

Google Cloud のクラウド環境として *gcp* を使用します。Google Cloud 上のローカルクラスタのクラウド環境
として *local* を使用します。

使用する引数は、操作によって異なります。以下の操作を使用できます。

list

ステージングディレクトリ内のクラスタを一覧表示します。

リスト操作を使用するときは、次の構文を使用してください。

```
cluster-operations.sh <cloud environment> list <staging location> <project ID>
```


次の表に、リスト操作で使用する引数を示します。

引数	説明
ステージングの場所	クラスタのエラスティック構成で設定されるステージングディレクトリ。 Google Cloud 環境では、次の構文を使用します: gs://<bucket>/<folder>
プロジェクト ID	クラスタリソースを含む Google Cloud プロジェクトの一意の識別子。

例えば、次のコマンドは、プロジェクト *myproject1* のステージングフォルダ内のクラスタを一覧表示します。

```
cluster-operations.sh gcp list gs://mybucket/cluster/staging myproject1
```

delete

ステージングディレクトリでクラスタを削除します。

削除操作を使用する場合は、次の構文を使用してください。

```
cluster-operations.sh <cloud environment> delete <staging location> <project ID> <deletable states>  
<clusters> [force]
```

次の表に、削除操作で使用する引数を示します。

引数	説明
ステージングの場所	クラスタのエラスティック構成で設定されるステージングディレクトリ。 Google Cloud 環境では、次の構文を使用します: gs://<bucket>/<folder>
プロジェクト ID	クラスタリソースを含む Google Cloud プロジェクトの一意の識別子。
削除可能な状態	<p>クラスタの状態を表すカンマ区切りのリスト。表示されたいずれかの状態とクラスタの状態が一致する場合、そのクラスタは削除されます。</p> <p>次のいずれかの状態を一覧表示できます。</p> <ul style="list-style-type: none">- 削除。クラウド上のいずれのリソースも使用していないクラスタを削除します。- メタデータのみ。開始されていないクラスタを削除します。- 一部。開始出来なかったクラスタ、または開始したが完全に停止しなかったクラスタが削除されます。- 使用中。仮想マシンが実行中である可能性が高いクラスタが削除されますが、このクラスタではジョブが実行されていない可能性があります。- すべて。上記の状態にあるすべてのクラスタが削除されます。 <p>Google Cloud 環境では、クラスタを削除するとステージングディレクトリからすべてのクラスタ情報が消去されます。</p>

引数	説明
クラス タ	<p>コマンドを実行するクラスタのカンマ区切りのリスト。</p> <p>例えば、同じステージングディレクトリを使用する開発環境とテスト環境があるとします。開発環境ではなくテスト環境で一部または使用中の状態にあるクラスタを削除する必要があります。テスト環境のクラスタのみを削除するには、テスト環境のクラスタを一覧表示します。</p> <p>all を使用して、ステージングディレクトリ内のすべてのクラスタを調べることもできます。</p>
強制	<p>オプション。force を使用して、追加のプロンプトをスキップします。</p> <p>force 引数を使用しない場合は、コマンドを実行すると各クラスタが一覧表示され、クラスタの削除を確認するメッセージが表示されます。「Yes」または「No」のいずれかを入力できます。</p> <p>force 引数を使用する場合は、クラスタが自動的に削除されます。</p>

例えば、次のコマンドは、各クラスタの確認を求めるプロンプトを表示せずに、プロジェクト *myproject1* 内の削除されたクラスタと部分的なクラスタをすべて削除します。

```
cluster-operations.sh gcp delete gs://mybucket/cluster/staging myproject1 deleted,partial all force
```

索引

C

Cloud Application Integration コミュニティ
URL [7](#)
Cloud 開発者コミュニティ
URL [7](#)

D

Data Integration Elastic
エラスティッククラスタ [11](#)
概要 [9](#)

G

Google Cloud カスタムロール [72](#)

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](#)

W

Web サイト [7](#)

あ

アップグレード通知 [8](#)

え

エラスティッククラスタ
AWS [141](#)
AWS サブスクリプション [15](#)
CLI/API セッション最長時間 [32](#)
delete clusters コマンド [150](#)
generate policies コマンド [148](#)
Google Cloud NAT ゲートウェイ [78](#)
Google Cloud サービス [67](#)
Google Cloud 統合タスク [67](#)
JAVA_HOME [48](#), [80](#), [93](#)
list clusters コマンド [149](#)
Microsoft Azure [144](#)
Microsoft Azure 製品 [82](#)
Secure Agent ロール [27](#), [32](#), [33](#), [46](#)
VPC [22](#), [23](#), [78](#), [79](#)
エージェントのインストール [26](#), [71](#), [85](#), [97](#)

エラスティッククラスタ (続く)
エラスティックサーバー [48](#)
エラスティック構成 [13](#), [108](#), [109](#), [118](#), [122](#), [128](#)
クラスタオペレータポリシー [28](#)
クラスタオペレータロール [23](#), [27](#), [28](#), [31](#), [33](#)
コマンド [48](#), [80](#), [93](#), [148-150](#)
サービスプリンシパル [90](#)
サブネット [22](#), [23](#), [78](#)
ステージングの場所 [116](#), [126](#), [137](#)
セキュリティ [44-46](#)
セキュリティプリンシパル [87](#), [90-92](#)
セルフサービスクラスタ [128](#)
タグ付け [116](#), [117](#), [126](#), [127](#)
データ暗号化 [43](#), [117](#), [121](#), [127](#)
デフォルトのロール [43](#), [64](#)
トラブルシューティング [141](#), [144](#)
ファイアウォールルール [79](#)
マネージド ID [87](#)
ユーザー定義のロール [34](#), [42](#), [64](#), [65](#)
ライフサイクル [11](#)
ラベリング [121](#)
ランタイム環境 [137](#)
リソースへのアクセス [17](#), [18](#), [20](#), [21](#), [68-70](#), [82-84](#), [95](#)
リソース要件 [135](#), [136](#)
ルーティング [23](#)
ロールベースのセキュリティ [44-46](#)
ワーカーロール [64](#)
概要 [11](#)
高可用性 [116](#), [126](#)
資格情報ベースのセキュリティ [46](#)
初期化スクリプト [136](#), [137](#)
前提条件 [14](#), [67](#), [81](#)
組織の権限 [14](#), [67](#)
統合タスク [14](#), [81](#), [94](#)
エラスティックジョブ
AWS [145](#)
Microsoft Azure [145](#)
トラブルシューティング [145](#)

く

クラスタ
クラスタ操作コマンド [152](#)
コマンド [148](#), [152](#)
プロキシの設定 [72](#), [86](#)

し

システムステータス [8](#)

す

ステータス

Informatica Intelligent Cloud Services [8](#)

せ

セキュリティグループ

ELB セキュリティグループ [23](#)

マスタセキュリティグループ [23](#)

ワーカーセキュリティグループ [23](#)

セルフサービスクラスタ

EKS 認証 [101](#)

カスタムプロパティ [132](#)

ユーザー管理のサービスアカウント [97](#)

リソースへのアクセス [95](#), [96](#)

概要 [13](#)

許容 [100](#)

前提条件 [94](#)

組織の権限 [94](#)

注釈 [100](#)

て

データ統合エラスティック

セルフサービスクラスタ [13](#)

と

トラブルシューティング

エラスティッククラスタ [141](#), [144](#)

トラブルシューティング (続く)

エラスティックジョブ [145](#)

ふ

プロキシ設定

クラスタ [72](#), [86](#)

ま

マスタロール [64](#)

め

メンテナンスの停止 [8](#)

ろ

ローカルクラスタ

エージェントのインストール [104](#)

クラウド権限 [105](#)

クラスタプロパティ [132](#)

ステージングとログの場所 [103](#)

データ暗号化 [134](#)

権限の確認 [103](#)

設定 [103](#)