



Informatica® Intelligent Cloud Services  
July 2025

**詳細クスタ**

© 著作権 Informatica LLC 2020, 2025

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

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

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

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

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

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

発行日: 2025-12-01

# 目次

<b>序文</b> .....	8
Informatica のリソース.....	8
Informatica マニュアル.....	8
Informatica Intelligent Cloud Services Web サイト.....	8
Informatica Intelligent Cloud Services コミュニティ.....	8
Informatica Intelligent Cloud Services マーケットプレイス.....	9
データ統合のコネクタのドキュメント.....	9
Informatica ナレッジベース.....	9
Informatica Intelligent Cloud Services Trust Center.....	9
Informatica グローバルカスタマサポート.....	9
 <b>第 1 章 : 詳細クラスタ</b> .....	10
詳細クラスタの種類.....	11
フルマネージドクラスタ.....	11
フルマネージドクラスタのクラスタリソースのセットアップ.....	12
フルマネージドクラスタの作成.....	12
フルマネージドクラスタへのジョブの送信.....	13
フルマネージドクラスタの停止.....	13
セルフサービスクラスタ.....	13
ローカルクラスタ.....	14
デフォルトのローカルクラスタ.....	14
デフォルトのステージングとログの場所.....	15
ローカルクラスタのルールとガイドライン.....	15
詳細クラスタのコストの管理.....	16
 <b>第 2 章 : AWS の設定</b> .....	17
手順 1。前提条件の完了.....	18
組織の権限の確認.....	18
AWS サブスクリプションの確認.....	18
AWS 環境でのロールとポリシーの確認.....	19
リソースへのアクセスの詳細.....	20
AWS クラスタの詳細.....	25
手順 2。クラスタファイルの格納場所の作成.....	25
手順 3。VPC とサブネットの作成（オプション）.....	26
十分な数の IP アドレスを含むサブネットの作成.....	26
ルーティング設定の確認.....	26
受信トラフィックの承認.....	26
手順 4。Amazon EC2 のユーザー定義のセキュリティグループの作成.....	27
ELB セキュリティグループの作成.....	27
マスタセキュリティグループの作成.....	28

ワーカーセキュリティグループの作成. . . . .	29
デフォルトのセキュリティグループの使用（代替）. . . . .	30
手順 5. Secure Agent のダウンロードとインストール. . . . .	30
手順 6. AWS のドメインの許可. . . . .	31
手順 7. IAM ロールの作成. . . . .	31
クラスタオペレータのロールを作成する. . . . .	32
クラスタオペレータポリシーの作成. . . . .	32
クラスタオペレータポリシーのアタッチ. . . . .	36
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. . . . .	36
Secure Agent ロールの作成または再利用. . . . .	37
AssumeRole 権限を Secure Agent ロールに追加. . . . .	37
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. . . . .	37
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. . . . .	38
保存時の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）. . . . .	48
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）. . . . .	49
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. . . . .	51
手順 8. 環境変数の設定（オプション）. . . . .	53
手順 9. エラスティックサーバーの設定. . . . .	53
手順 10. プロキシの設定. . . . .	56
CLAIRE を利用した設定に対する追加のセットアップ. . . . .	56
IAM ポリシーリファレンス. . . . .	56
クラスタオペレータロールのアクション. . . . .	57
マスタロールアクション. . . . .	64
ワーカーロールアクション. . . . .	68
マスタとワーカーのロールタイプのリファレンス. . . . .	70
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. . . . .	71

### 第 3 章 : Google Cloud の設定. . . . . 73

手順 1. 前提条件の完了. . . . .	73
組織の権限の確認. . . . .	73
Google Cloud サービスの確認. . . . .	74
リソースへのアクセスの詳細. . . . .	74
Google Cloud クラスタの詳細. . . . .	77
手順 2. クラスタファイルの格納場所の作成. . . . .	77
手順 3. VPC とサブネットの作成（オプション）. . . . .	78
十分な数の IP アドレスを含むサブネットの作成. . . . .	78
Google Cloud NAT ゲートウェイの作成. . . . .	78
VPC ネットワークでのファイアウォールルールの作成. . . . .	79
手順 4. Secure Agent のダウンロードとインストール. . . . .	80
手順 5. Google Cloud でのドメインの許可. . . . .	81
手順 6. クラスタのプロキシの設定（オプション）. . . . .	81
手順 7. ロールとサービスアカウントの作成. . . . .	81
Secure Agent ロールとサービスアカウントの作成. . . . .	82

マスタロールとサービスアカウントの作成. . . . .	85
ワーカーノードロールとサービスアカウントの作成. . . . .	86
手順 8. JAVA_HOME 環境変数の設定. . . . .	87
手順 9. ステージング接続の作成. . . . .	87
<b>第 4 章 : Microsoft Azure の設定. . . . .</b>	<b>88</b>
手順 1. 前提条件の完了. . . . .	88
組織の権限の確認. . . . .	88
Microsoft Azure 製品を確認する. . . . .	89
リソースへのアクセスの詳細. . . . .	89
手順 2. クラスタファイルのストレージアカウントの作成. . . . .	92
手順 3. VNet とサブネットの作成 (オプション) . . . . .	92
十分な数の IP アドレスを含むサブネットの作成. . . . .	93
ルーティング設定の確認. . . . .	93
受信トラフィックの承認. . . . .	93
手順 4. Secure Agent のダウンロードとインストール. . . . .	94
手順 5. Azure のドメインの許可 . . . . .	94
手順 6. クラスタのプロキシの設定 (オプション) . . . . .	95
手順 7. Secure Agent のマネージド ID の作成. . . . .	95
クラスタリソースグループの作成. . . . .	95
マネージド ID の作成. . . . .	95
エージェントロールの作成. . . . .	96
ロールの割り当ての追加. . . . .	99
手順 8. クラスタのサービスプリンシパルの作成. . . . .	99
サービスプリンシパルを作成する. . . . .	99
クラスタロールの作成. . . . .	99
ロールの割り当ての追加. . . . .	101
資格情報の Key Vault への保存. . . . .	101
アクセスポリシーを Key Vault に追加します. . . . .	101
手順 9. ソースとターゲットにアクセスするためのマネージド ID の作成 (オプション) . . . . .	101
手順 10. ユーザー定義のセキュリティグループの作成 (オプション) . . . . .	102
詳細クラスタのデフォルトのネットワークセキュリティグループ. . . . .	102
Azure 上の詳細クラスタ内のユーザー定義のセキュリティグループ. . . . .	104
クラスタの事前検証エラーのトラブルシューティング. . . . .	106
手順 11. JAVA_HOME 環境変数の設定 (オプション) . . . . .	107
手順 12. ステージング接続の作成 (オプション) . . . . .	107
<b>第 5 章 : セルフサービスクラスタの設定. . . . .</b>	<b>108</b>
手順 1. 前提条件の完了. . . . .	108
組織の権限の確認. . . . .	109
リソースへのアクセスの詳細. . . . .	109
手順 2. Secure Agent のダウンロードとインストール. . . . .	112
手順 3. セルフサービスクラスタのドメインの許可. . . . .	112

手順 4. Secure Agent で kubeconfig ファイルをダウンロードして設定する. . . . .	112
注釈と許容の追加（オプション）. . . . .	113
手順 5. Kubernetes ClusterRole および Role の作成. . . . .	113
ロールの権限の設定. . . . .	114
ロールバインディングの作成. . . . .	116
Informatica が管理するサービスアカウントの使用（代替）. . . . .	116
手順 6. ストレージロールの作成. . . . .	117
AWS でのストレージロールの作成. . . . .	117
Microsoft Azure でのストレージロールの作成. . . . .	119
手順 7. データソースへのアクセスの設定. . . . .	120
AWS 上のクラスタの追加設定. . . . .	120
クラスタ認証の設定. . . . .	120
IMDSv2 を使用するクラスタノードの設定. . . . .	121
<b>第 6 章 : ローカルクラスタの設定. . . . .</b>	<b>122</b>
ローカルクラスタ用の準備. . . . .	122
Secure Agent のダウンロードとインストール. . . . .	123
ローカルクラスタのトラブルシューティング. . . . .	124
<b>第 7 章 : 詳細設定. . . . .</b>	<b>125</b>
CLAIRE を利用した設定. . . . .	126
クラスタの予算の見積もり. . . . .	126
CLAIRE の推奨事項. . . . .	128
AWS のプロパティ. . . . .	129
構成の検証. . . . .	133
Amazon Linux 2 イメージ. . . . .	134
GPU ワーカーインスタンスタイプ. . . . .	134
Graviton ワーカーインスタンスタイプ. . . . .	135
スポットインスタンス. . . . .	135
高可用性. . . . .	136
新しいステージングの場所へのアクセス. . . . .	137
クラウドリソースへのタグのプロパゲート. . . . .	137
クラウドリソースのデフォルトタグ. . . . .	138
データ暗号化. . . . .	138
Google Cloud のプロパティ. . . . .	139
構成の検証. . . . .	141
クラウドリソースへのラベルのプロパゲート. . . . .	142
データ暗号化. . . . .	142
Microsoft Azure プロパティ. . . . .	143
構成の検証. . . . .	147
スポットインスタンス. . . . .	147
高可用性. . . . .	148
新しいステージングの場所へのアクセス. . . . .	148

クラウドリソースへのタグのプロパゲート. . . . .	148
クラウドリソースのデフォルトタグ. . . . .	149
データ暗号化. . . . .	149
ローカルクラスタの詳細設定. . . . .	150
ステージングとログの場所の変更（オプション）. . . . .	150
ローカルクラスタのプロパティ. . . . .	151
クラウド権限の設定. . . . .	153
データ暗号化. . . . .	156
セルフサービスクラスタのプロパティ. . . . .	156
ランタイムプロパティ. . . . .	159
構成の検証. . . . .	160
クラスタノードのリソース要件. . . . .	160
リソース要件の再設定. . . . .	161
リソース要件の例. . . . .	162
初期化スクリプト. . . . .	162
初期化スクリプトのエラー. . . . .	163
ランタイム環境またはステージングの場所の更新. . . . .	163
<b>第 8 章: トラブルシューティング. . . . .</b>	<b>165</b>
詳細クラスタのトラブルシューティング. . . . .	165
AWS 上の詳細クラスタのトラブルシューティング. . . . .	167
Microsoft Azure 上の詳細クラスタのトラブルシューティング. . . . .	169
詳細クラスタサブタスクのトラブルシューティング. . . . .	170
セルフサービスクラスタのトラブルシューティング. . . . .	172
Secure Agent マシンとクラウドリソースのシャットダウン. . . . .	173
<b>付録 A: コマンドリファレンス. . . . .</b>	<b>174</b>
generate-policies-for-userdefined-roles.sh. . . . .	174
list-clusters.sh. . . . .	175
delete-clusters.sh. . . . .	176
cluster-operations.sh. . . . .	178
<b>索引. . . . .</b>	<b>180</b>

# 序文

『詳細クラスタ』を使用して、組織がマッピングで高度な機能を開発および実行できるようにするために詳細クラスタをセットアップする方法を学びます。クラウド環境をセットアップし、詳細設定を作成してクラスタを定義するクラウドリソースにアクセスする方法を学びます。

## Informatica のリソース

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

### Informatica マニュアル

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

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

### Informatica Intelligent Cloud Services Web サイト

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

### Informatica Intelligent Cloud Services コミュニティ

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

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

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

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

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



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

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

<https://marketplace.informatica.com/>

## データ統合のコネクタのドキュメント

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

## Informatica ナレッジベース

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

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

## Informatica Intelligent Cloud Services Trust Center

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

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

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

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

## Informatica グローバルカスタマサポート

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

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

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

# 第 1 章

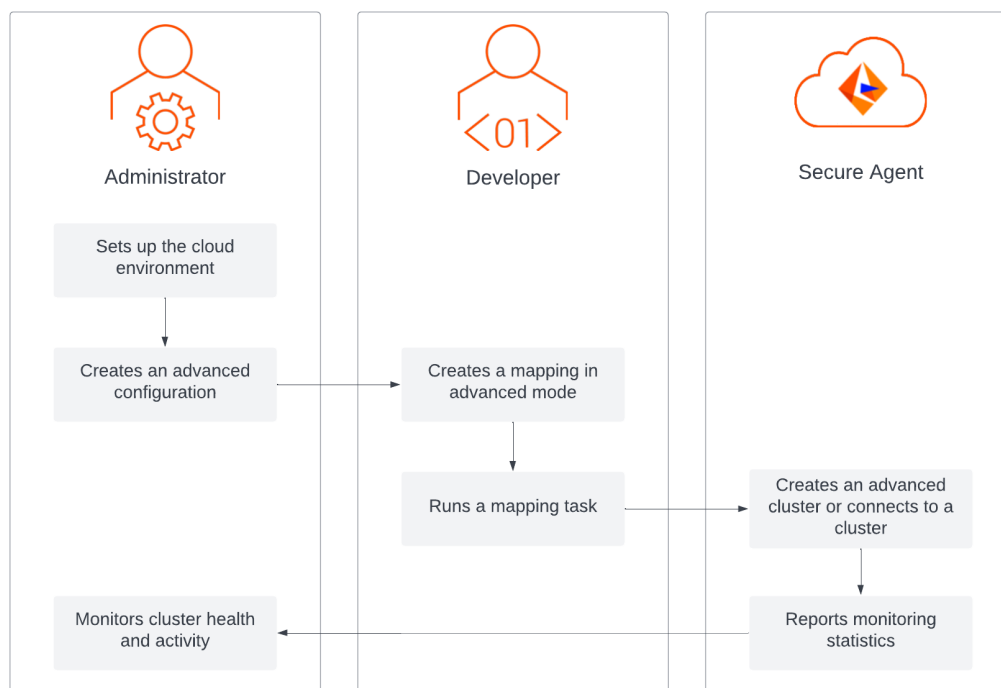
## 詳細クラスタ

詳細クラスタは、クラウド上に分散処理環境を提供する Kubernetes クラスタです。フルマネージド型のセルフサービスクラスタは、スケーラブルなアーキテクチャを使用してデータロジックを実行できますが、ローカルクラスタは単一ノードを使用して、高度な使用方法のためにプロジェクトをすばやくオンボードできます。

詳細クラスタを使用するには、次の手順を実行します。

1. Secure Agent がクラウドリソースに接続してアクセスできるように、クラウド環境をセットアップします。
2. Administrator で、詳細設定を作成してクラスタとクラウドリソースを定義します。
3. Monitor で、組織内の開発者がクラウド上でジョブを作成して実行している間に、クラスタの健全性とアクティビティを監視します。

次の図は、組織内で詳細クラスタを起動して実行するために使用するワークフローを示しています。



# 詳細クラスタの種類

マッピングで高度な機能を有効にし、組織の処理要件を最適にサポートするインフラストラクチャを選択するのに役立つ、さまざまな種類の詳細クラスタを使用できます。

次の種類の詳細クラスタを組織で使用できます。

## フルマネージドクラスタ

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、サーバーレスインフラストラクチャを提供するクラスタ。詳細については、[「フルマネージドクラスタ」\(ページ 11\)](#)を参照してください。

## セルフサービスクラスタ

組織が実行し、マッピングを実行するために再利用する Kubernetes クラスタ。Kubernetes クラスタは、AWS または Microsoft Azure で実行できます。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

Secure Agent マシンで起動できる単純な単一ノードクラスタ。ローカルクラスタを使用して、高度な使用方法のためにプロジェクトをすばやくオンボードできます。詳細については、[「ローカルクラスタ」\(ページ 14\)](#)を参照してください。

## サーバーレスランタイム環境の詳細クラスタ

組織が AWS を使用している場合は、組織が使用するための詳細クラスタを含むサーバーレスランタイム環境を作成できます。詳細については、「ランタイム環境」を参照してください。

次の領域に関して、詳細クラスタのすべてのタイプは類似しています。

- ネットワークプライバシー
- Secure Agent とクラスタ間、Kubernetes ポッド間、Kubernetes ポッドまたはクラスタとインターネット間の通信
- Informatica の Docker イメージとアーティファクトをダウンロードするためのインターネットアクセス
- 外部データソースへのアクセス（データ統合マッピングのソースやターゲットなど）

組織のセキュリティガイドラインに従ってクラウドロールやセキュリティグループなどの機密性の高いリソースを設定することで、Informatica のクラウド環境へのアクセスを制限することができます。例えば、セルフサービスクラスタでは、Informatica と Informatica 以外のアプリケーションおよびユーザーの間で Kubernetes リソースが共有される場合があります。独自の Kubernetes ロールまたはクラスタロールを作成することで、クラスタへの Informatica のアクセスを制限し、Informatica が対話できるリソースを指定することができます。

# フルマネージドクラスタ

フルマネージドクラスタは、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、サーバーレスインフラストラクチャを提供します。

Secure Agent は、クラスタの起動、シャットダウン、自動スケーリング、アップグレードなど、Kubernetes のライフサイクル全体を管理します。エージェントは、コンピューティングインフラストラクチャを管理し、スポットインスタンスを使用して詳細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。

フルマネージドクラスタには、次の機能が含まれます。

- クラスタは、ワークロードのサイズと指定したリソース境界に基づいてスケーリングされます。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、クラスタは処理の負荷の増大に対応します。
- 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、詳細設定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。
- クラスタの 2 番目のチューニングプロセスでは、マッピングのデータサイズとクラスタの容量を分析して、ジョブをさらに自動チューニングします。
- クラスタを使用すると、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。
- 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。

## フルマネージドクラスタのクラスタリソースのセットアップ

フルマネージドクラスタでは、ストレージの場所やロールなどの一部のクラスタリソースを設定し、残りの部分を Informatica が作成します。

次の表に、設定が可能なクラスタリソースを示します。

クラスリソース	必須またはオプション
Secure Agent マシン (Secure Agent がインストールされている EC2 インスタンスや Linux 仮想マシンなど)	必須
Microsoft Azure 上のストレージアカウントリソースグループを含む、ストレージの場所 (ステージングファイルやログファイル用の S3 または ADLS Gen2 上の場所など)	必須
アクセス権限に関連するクラスタリソース (クラスタ管理の IAM ロール、マネージド ID、サービスプリンシパル、Key Vault 内のシークレットなど)	必須
VPC とサブネット、または Microsoft Azure 上の VNet とサブネット	オプション
クラスタノードにアタッチするセキュリティグループ	オプション

Informatica は、ロードバランサ、Auto Scaling グループまたは仮想マシンスケールセット、クラスタノードに接続するボリュームとディスクなど、他のすべてのリソースを作成および管理します。

## フルマネージドクラスタの作成

開発者がジョブを実行するときに、Secure Agent は、フルマネージドクラスタを作成するために、ジョブのランタイム環境に関連付けられている詳細設定を使用します。

このエージェントでは、以下のタスクを実行します。

1. クラスタについての構成情報を含むクラスタ構成設定を作成する。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. 必要なリソースをプロビジョニングしてクラスタを作成する。

**注:** Informatica は、安全なパスイニシャルを使用して、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。

## フルマネージドクラスタへのジョブの送信

フルマネージドクラスタが実行されている場合、Secure Agent はクラスタで実行するジョブを送信します。

ジョブをクラスタに送信するために、Secure Agent は、マッピング内のデータロジックを複数の Spark タスクに分割する実行プランを生成します。クラスタは、Spark ドライバと Spark Executor を起動して、Spark タスクを同時に処理します。

開発者が追加のジョブを実行すると、クラスタはジョブのサイズと数に適応するためにリソースをプロビジョニングおよびプロビジョニング解除します。例えば、クラスタは、バーストの処理中に追加のクラスタノードとクラスタストレージをプロビジョニングできます。

各ジョブは、セッションログ、Spark ドライバログ、Spark Executor ログ、およびエージェントジョブログを生成します。

## フルマネージドクラスタの停止

Secure Agent は、詳細設定で選択したクラスタシャットダウン方法に基づいて、フルマネージドクラスタを停止します。

Secure Agent はアイドルタイムアウト後のクラスタのシャットダウンを待機するか、エージェントが履歴データに基づいたスマートシャットダウンを実行できます。

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。

- 詳細設定でランタイム環境をクリアする場合。
- 詳細設定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。

開発者が同じランタイム環境で別のジョブを実行すると、エージェントはクラスタを再起動します。

## セルフサービスクラスタ

セルフサービスクラスタは、組織が実行し、マッピングを実行するために再利用する Kubernetes クラスタです。

Kubernetes クラスタは、AWS または Microsoft Azure で実行できます。Amazon EC2 インスタンスや Azure Virtual Machines などの自己管理型クラスタを使用するか、Amazon Elastic Kubernetes Service や Azure Kubernetes Service などのサービス管理型クラスタを使用できます。

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、Secure Agent に必要な権限は環境内の最小限の権限で済みます。

フルマネージドクラスタと比較して、セルフサービスクラスタには次の利点があります。

- 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使用したりできます。

Secure Agent をセルフサービスクラスタに接続するには、クラスタ用に生成された kubeconfig ファイルを使用します。kubeconfig ファイルは、クラスタ設定を含む YAML ファイルです。詳細設定で kubeconfig ファイルへのパスを入力して、Secure Agent がセルフサービスクラスタに接続し、ジョブをクラスタに送信できるようにします。

Secure Agent はクラスタを管理しないため、Secure Agent はワークロードに基づいてクラスタをスケールアップしません。クラスタをシャットダウンすると、Secure Agent はすべてのジョブ関連リソースをクラスタから削除します。

## 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して、高度な使用方法のためにプロジェクトをすばやくオンボードできます。ローカルクラスタは、詳細モードのマッピングのみ実行できます。

ローカルクラスタは、オンプレミスまたは次のクラウド環境で実行できます。

- AWS
- Google Cloud
- Microsoft Azure
- Oracle Cloud Infrastructure

最小限の権限とリソース要件で、仮想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。クラスタは、クラウド上またはクラスタノードに接続されているローカルストレージ内のステージングおよびログの場所にアクセスできます。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。

## デフォルトのローカルクラスタ

エージェントは、エージェントマシン上にデフォルトのローカルクラスタを作成できるため、小さなデータセットで高度な機能の開発と実行を開始して、マッピングロジックをテストできます。

詳細設定に関連付けられていないエージェントを使用して詳細モードでマッピングを実行すると、デフォルトの詳細設定が作成され、エージェントに関連付けられます。エージェントは、デフォルト設定を使用して、マッピングを処理できるデフォルトのローカルクラスタを作成できます。

デフォルトの詳細設定は、次の状況で作成されます。

- 詳細モードでマッピングを実行する場合。
- 詳細モードのマッピングに基づいてマッピングタスクを作成し、ランタイム環境を選択する場合。
- 詳細モードでマッピングのデータをプレビューする場合。

Administrator の【詳細クラスタ】 ページでデフォルトクラスタの詳細設定を表示できます。構成を編集して、ステージングの場所、ログの場所、マッピングタスクのタイムアウト、およびランタイムプロパティを変更できます。Monitor の【詳細クラスタ】 ページで、デフォルトのローカルクラスタを監視することもできます。

デフォルトの詳細設定は、エージェントマシンのオペレーティングシステムがローカルクラスタをホストできない場合は作成されません。この場合は、Administrator で詳細設定を手動で作成し、詳細設定をランタイム環境に関連付ける必要があります。

組織がマッピングを実行して本番環境規模のワークロードを処理する準備ができたなら、次のタスクを完了します。

1. クラウド環境をセットアップして、より大規模な詳細クラスタをホストします。
2. 詳細設定をクラスタ用に作成します。
3. デフォルトの詳細設定を編集して、ランタイム環境から切り離します。
4. 新しい詳細設定を編集し、それをランタイム環境に関連付けます。

クラスタを大きくすると、開発者によるテスト中に発生するメモリとパフォーマンスの問題も解決できます。

## デフォルトのステージングとログの場所

デフォルトのローカルクラスタは、クラスタでジョブを実行するときに、ステージングファイルとログファイルをエージェントマシンに保存します。

次の表に、デフォルトのステージングとログの場所を示します。

デフォルトの場所	説明
file:/// \$ADVANCED_MODE_STAGING	エージェントマシンの次のディレクトリにあるデフォルトのステージングの場所: <agent installation directory>/apps/Advanced_Mode_Staging_Dir
file:/// \$ADVANCED_MODE_LOG	エージェントマシンの次のディレクトリにあるデフォルトのログの場所: <agent installation directory>/apps/Advanced_Mode_Log_Dir

エージェントマシンには、ジョブを正常に実行できるように、デフォルトのステージングおよびログの場所に十分なスペースが必要です。クラスタ用に詳細設定を編集して、ステージングとログの場所を変更できます。

データ統合サーバーが詳細モードのマッピングでデータロジックを処理するためのサブタスクをデータ統合で作成する場合、クラスタとデータ統合サーバーはステージングファイルを共有します。ステージングの場所でステージングファイルを読み取りおよび書き込みするために、データ統合サーバーは Hadoop ファイル V2 コネクタを使用します。

## ローカルクラスタのルールとガイドライン

ローカルクラスタを作成するときは、次のルールとガイドラインを考慮してください。

- Oracle Cloud Infrastructure に Secure Agent をインストールすると、ローカルクラスタを作成することはできますが、他のタイプの詳細クラスタは作成できません。
- ローカルクラスタの詳細モードでマッピングを実行する前に、特に Secure Agent がすでに他のジョブを実行している場合は、クラスタを作成してジョブを正常に実行できるように、Secure Agent に十分なリソースがあることを確認してください。Secure Agent に十分なリソースがない場合、Secure Agent ですでに実行されているジョブと詳細モードのマッピングは失敗します。Secure Agent には、少なくとも 8 つのコアと 32GB のメモリを搭載したマシンを使用することをお勧めします。



# 詳細クラスタのコストの管理

Informatica の AI エンジンである CLAIRE は、FinOps 機能を有効にして、詳細クラスタインフラストラクチャのコストを管理、統制、監視し、クラウド支出の透明性を提供します。CLAIRE は、機械学習を使用してインサイトと推奨事項を生成し、コストを削減して、パフォーマンスを最適化し、組織にとって最も重要なデータ管理の取り組みに予算が確実に投入されるようにします。

予算目標に合わせた詳細データ管理プロジェクトの設計を支援するために、CLAIRE は次のようなタスクを実行します。

- 指定した予算に応じて、詳細クラスタインフラストラクチャを選択します。
- 予算内に抑えながら、ワークロードに応じてクラスタインフラストラクチャを動的にスケールアウトおよびスケールインします。
- 詳細クラスタで実行するために適したジョブや SQL ELT の最適化を使用しているジョブを特定して、クラウドインフラストラクチャのコストを節約し、ジョブのパフォーマンスを最適化します。
- コストとパフォーマンスに合わせてランタイムパラメータを微調整します。
- 優先度に基づいて高価値のワークロードをスケジュールし、重要なジョブの期限に間に合うようにします。
- CLAIRE のインテリジェントな最適化によるクラウドインフラストラクチャの推定節約額、その節約に貢献する主要な領域、および追加の財務インサイトについてのレポートを提供します。
- 詳細クラスタで経時的に発生するインフラストラクチャコストを視覚化します。
- 追加のコスト削減やパフォーマンスの向上を実現できる領域を特定するための推奨事項を生成します。

CLAIRE は、詳細クラスタ、マッピング、実行するマッピングタスクなど、詳細データ管理プロジェクトのあらゆる部分を支援します。



## 第 2 章

# AWS の設定

組織で詳細設定を作成する前に、Secure Agent が詳細クラスタを作成できるようにクラウド環境を設定します。

以下のタスクを完了させます。

1. 前提条件を満たしていることを確認します。必要な特権があることを確認し、クラウド環境でのリソースアクセスについて理解します。
2. クラスタファイルの格納場所を作成します。詳細クラスタでは、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ために Amazon S3 ストレージが必要です。
3. 必要に応じて、VPC とサブネットを作成します。VPC とサブネットを作成せず、それらを詳細設定で指定する場合、クラスタでジョブを実行すると、クラスタはデフォルトの 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。セキュリティグループは、ロードバランサ、マスタノード、およびワーカーノードに出入りするトラフィックの受信ルールと送信ルールを定義します。ユーザー定義のセキュリティグループの代わりに、デフォルトのセキュリティグループを使用することもできます。
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。最小リソース要件を満たす仮想マシンにエージェントをセットアップします。
6. AWS でドメインを許可します。クラスタは、特定のドメインにアクセスして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必要があります。
7. IAM ロールを作成します。クラスタオペレータ、Secure Agent、マスタノード、およびワーカーノードは、IAM ロールとポリシーを使用して、クラスタがジョブを実行するときに認証を提供します。
8. 必要に応じて、Secure Agent マシンで環境変数を設定します。シェルコマンドを実行するには、いくつかの環境変数が必要です。
9. エラスティックサーバーを設定します。エラスティックサーバーは詳細クラスタと、そのクラスタで実行するジョブを管理します。
10. Secure Agent にプロキシサーバーを使用する場合は、プロキシ設定を構成します。

詳細クラスタを作成する方法については、[「CLAIRE を利用した設定に対する追加のセットアップ」](#) (ページ 56) を参照してください。

**注:** AWS 環境で、これらのタスクを実行して詳細設定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。

# 手順 1。前提条件の完了

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。
- Secure Agent と詳細クラスタが、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について説明します。
- 詳細クラスタで使用されるパッケージとイメージについて確認します。

## 組織の権限の確認

組織の詳細設定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。

詳細設定に対する特権によって、Administrator および Monitor の【詳細クラスタ】ページへのアクセスレベルは異なります。

詳細設定の表示と詳細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 環境で詳細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。

AWS に次のサービスが必要です。

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 エンジンが詳細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)

詳細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、詳細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 からの受信詳細ジョブを受け入れ、詳細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、詳細クラスタが 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

詳細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)

詳細クラスタは、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、詳細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 と詳細クラスタでは、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、詳細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、詳細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、詳細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、詳細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、[「手順 7.IAM ロールの作成」 \(ページ 31\)](#)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。詳細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。詳細ジョブの Amazon データソースへのアクセスを提供します。

ポリシー	ロールでの使用	説明
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。詳細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。
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 および詳細クラスタは、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、詳細ジョブの一部であるリソースにアクセスします。

次のタスクを実行するために、リソースにアクセスします。

- マッピングの設計
- 詳細クラスタの作成
- データプレビューを含むジョブの実行
- ログのポーリング

### マッピングの設計

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。

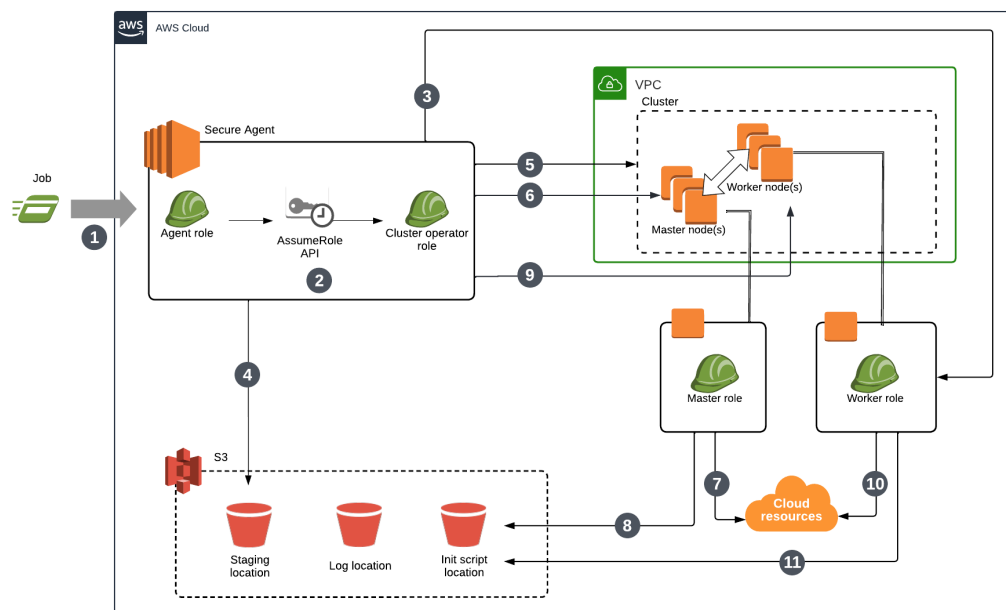
#### Amazon データソースへの直接アクセスがないコネクタ

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。

## 詳細クラスタの作成

詳細クラスタを作成するために、Secure Agent はクラスタオペレータロールを使用してクラスタの詳細をステージング場所に保存し、クラスタの作成を行います。マスターノードとワーカーノードは、マスターロールとワーカーロールを使用してクラウド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ために使用するプロセスを示しています。



次の手順では、Secure Agent がクラスタを作成するために使用するプロセスについて説明します。

1. ジョブを実行します。
2. Secure Agent は、クラスタオペレータロールを引き受けて、AWS で昇格した特権を取得します。クラスタオペレータロールを使用すると、Secure Agent はマスターロールとワーカーロールを引き受けすることができます。
3. ユーザー定義のワーカーロールを作成すると、Secure Agent はワーカーロールを使用して、クラスタがステージングおよびログの場所にアクセスできることを確認します。

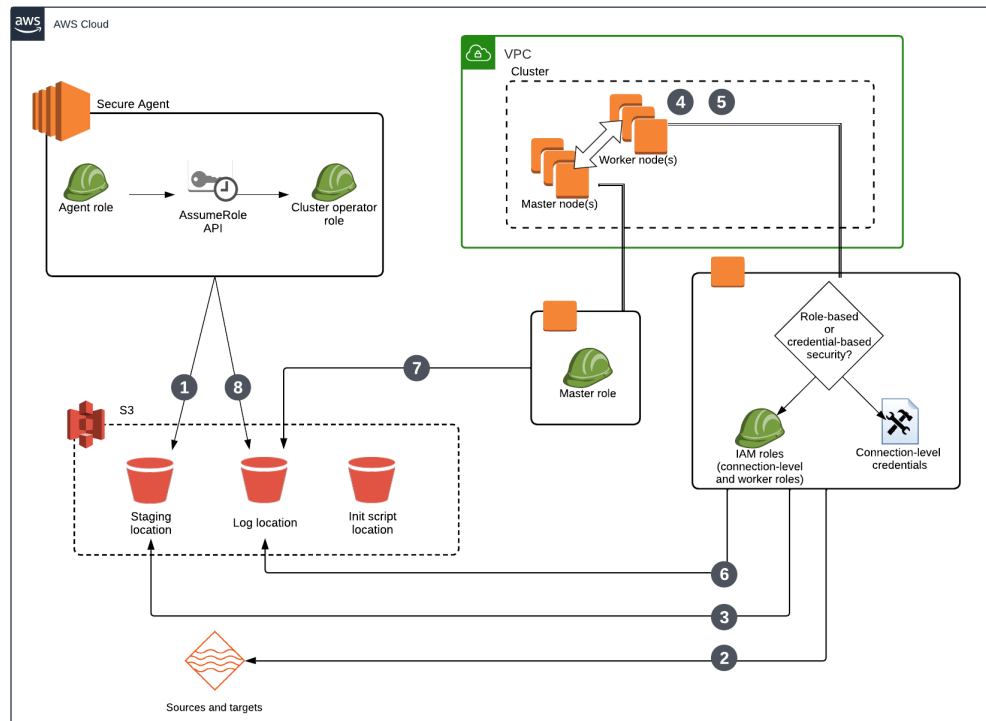
4. Secure Agent は、クラスタオペレータロールを使用してクラスタの詳細をステージング場所に格納します。
5. Secure Agent は、クラスタオペレータロールを使用してクラスタを作成します。
6. Secure Agent は、クラスタオペレータロールを使用して、マスターノードにクラスタリソースを作成します。
7. マスターノードは、マスターロールを使用して、Amazon EC2、AWS Auto Scaling、Elastic Load Balancing などの AWS 上のサービス上のクラウドリソースにアクセスし、ノードの弾性とリソースの最適化を管理します。
8. マスターノードは、マスターロールを使用して初期化スクリプトにアクセスします。
9. Secure Agent は、クラスタオペレータロールを使用してワーカーノードにクラスタリソースを作成し、最小の数のワーカーノードで Auto Scaling グループを作成します。
10. ワーカーノードは、ワーカーロールを使用して、Amazon EC2 や AWS ネットワーキングなどの AWS 上のサービス上のクラウドリソースにアクセスし、コンピューティングおよびネットワーク機能にアクセスします。
11. ワーカーノードは、ワーカーロールを使用して初期化スクリプトにアクセスします。

クラスタオペレータロール、マスターロール、ワーカーロールが詳細クラスタ内のクラウドリソースにアクセスする方法の詳細については、[「IAM ポリシーリファレンス」 \(ページ 56\)](#)を参照してください。

## Amazon データソースへの直接アクセスを持つジョブの実行

Amazon データソースへの直接アクセスを持つコネクタを使用するジョブを実行するために、クラスタ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 Amazon リソースにアクセスします。

次の図は、Secure Agent とクラスタノードがジョブを実行するために使用するプロセスを示しています。



次の手順では、Secure Agent とクラスタノードがジョブを実行するために使用するプロセスについて説明しています。

1. Secure Agent は、クラスタオペレータロールを引き受けて、ジョブの依存関係をステージングの場所に保存します。
2. ワーカーノードは、接続レベルのロール、ワーカーロール、または接続レベルの AWS 資格情報を使用して、ジョブのセキュリティタイプに基づいてソースデータにアクセスします。ロールベースのセキュリティを使用する場合、ワーカーノードは接続レベルのロールまたはワーカーロールを使用します。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資格情報を使用します。接続レベルで構成された認証が優先されます。
3. ワーカーノードは、接続レベルのロール、ワーカーロール、または接続レベルの資格情報を使用してステージングの場所にアクセスし、ジョブの依存関係を取得して一時データをステージングします。
4. ワーカーノードは、ワーカーロールを使用して、ジョブがより多くのストレージ領域を必要とする場合に EBS ボリュームを自動スケーリングします。
5. マスタノードはマスタロールを使用して、リソース要件に基づいてクラスタノードをスケーリングします。
6. 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。
7. マスタノードはマスタロールを使用してログの場所にログを保存します。
8. 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。

## セキュリティの種類

ワーカーノードは、セキュリティの種類に基づいて次の方法で 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

資格情報ベースのセキュリティを設定すると、ワーカーノードは接続レベルの AWS 資格情報を使用して、Amazon データソースやステージングの場所などの Amazon リソースにアクセスします。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アクセスします。

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、ワーカーノードは資格情報を再利用してステージン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、ワーカーノードは、S3 ターゲットにアクセスする AWS 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。

### 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設定すると、ワーカーノードは接続レベルのロールまたはワーカーロールのいずれかを使用して、Amazon データソース、ステージングの場所、ログの場所などの Amazon リソースにアクセスします。接続レベルで構成されたロールは、ワーカーロールよりも優先されます。

**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。

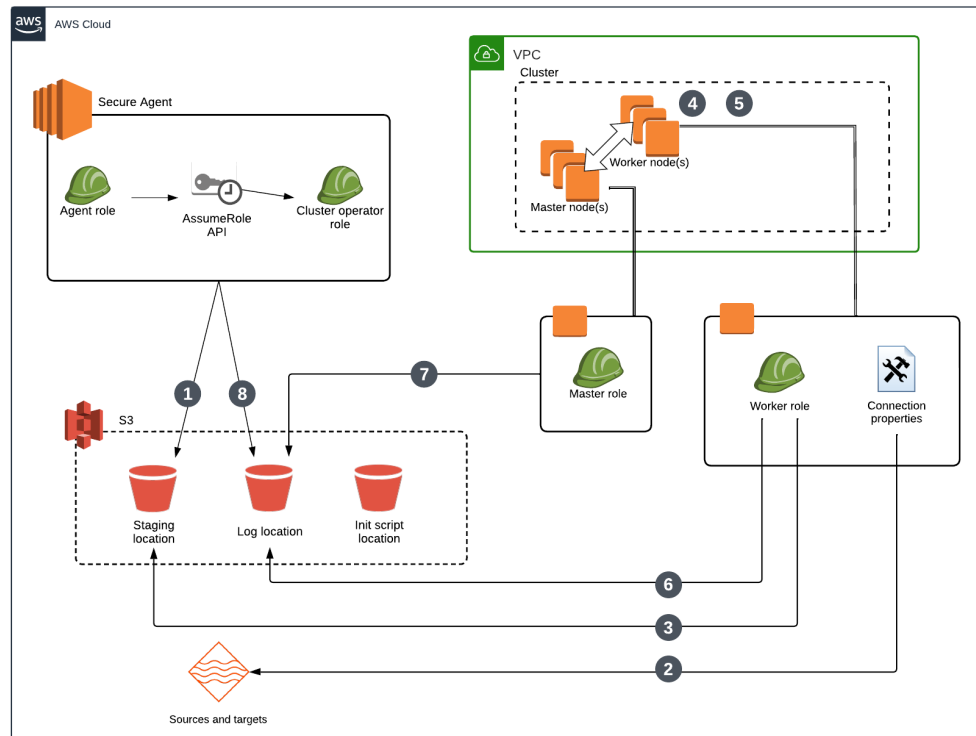
## Amazon データソースへの直接アクセスを持たないジョブの実行

Amazon データソースに直接アクセスできるコネクタを使用しないジョブを実行するために、クラスタは接続プロパティとワーカーロールを使用して Amazon リソースにアクセスします。

例えば、JDBC V2 コネクタは Amazon データソースに直接アクセスできません。JDBC V2 コネクタを使用するジョブを実行するために、クラスタは接続プロパティを使用してデータを読み取り、一時的にステージングしてから、データを処理してターゲットに書き込みます。



次の図は、Secure Agent とクラスターノードがジョブを実行するために使用するプロセスを示しています。



次の手順では、Secure Agent とクラスターノードがジョブを実行するために使用するプロセスについて説明しています。

- Secure Agent は、クラスターオペレーターロールを引き受けて、ジョブの依存関係をステージングの場所に保存します。
- ワーカーノードは、接続プロパティを使用してソースデータにアクセスします。
- 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にアクセスし、ジョブの依存関係を取得して一時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、ジョブがより多くのストレージ領域を必要とする場合に EBS ボリュームを自動スケーリングします。
- マスタノードはマスタロールを使用して、リソース要件に基づいてクラスターノードをスケーリングします。
- 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。
- マスタノードはマスタロールを使用してログの場所にログを保存します。
- 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。

**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、ジョブで使用す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。

## AWS クラスタの詳細

AWS 環境で詳細クラスタを作成すると、そのクラスタは Informatica が管理およびパブリッシュする OS イメージを使用します。

OS イメージには、特定の事前構築済みパッケージと次の追加の yum パッケージが含まれています。

```
device-mapper-persistent-data
docker-ce
gnupg2
gzip
kernel-devel
kernel-headers
kubeadm
kubenet
lvm2
tar
unzip
yum-utils
```

また、OS イメージには、次の Docker イメージが含まれています。

```
calico/kube-controllers
calico/node
calico/cni
calico/pod2daemon-flexvol
coreos/flannel
coreos/flannel-cni
image/jq
kube-scheduler
```

## 手順 2。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詳細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。

## 手順 3。VPC とサブネットの作成（オプション）

詳細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は、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。

- 詳細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に必要な数の 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

詳細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、詳細クラスタで最大 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詳細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。

## 手順 4. 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に、詳細設定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 \(代替\)」 \(ページ 30\)](#) 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は、Kubernetes API サーバーと、詳細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、エージェントが詳細クラスタ用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。

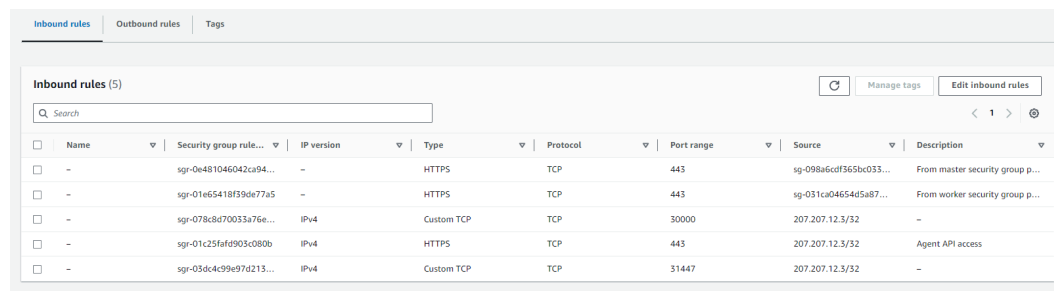
#### 受信ルール

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詳細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。

- 詳細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。
- TCP ポート 31447 を使用した Secure Agent からの受信トラフィック。Secure Agent は、このポートを使用してデータプレビュージョブを実行します。このポート番号を変更する必要がある場合は、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。
- CLAIRE を利用した設定を使用する詳細クラスタの場合は、TCP ポート 30000 を使用して、Secure Agent から Prometheus サーバーへのトラフィックを含めます。

次の図に、必要な受信ルールを示します。



Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-0e481046042ca94...	-	HTTPS	TCP	443	sg-098a6cdf365bc033...	From master security group p...
-	sg-01e65418f39de77a5	-	HTTPS	TCP	443	sg-031ca04654d5a87...	From worker security group p...
-	sg-078cd870033a76e...	IPv4	Custom TCP	TCP	30000	207.207.12.3/32	-
-	sg-01c25fafd903c080b	IPv4	HTTPS	TCP	443	207.207.12.3/32	Agent API access
-	sg-03dc4c99e97d213...	IPv4	Custom TCP	TCP	31447	207.207.12.3/32	-

## 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せんが、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、詳細クラスタ、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

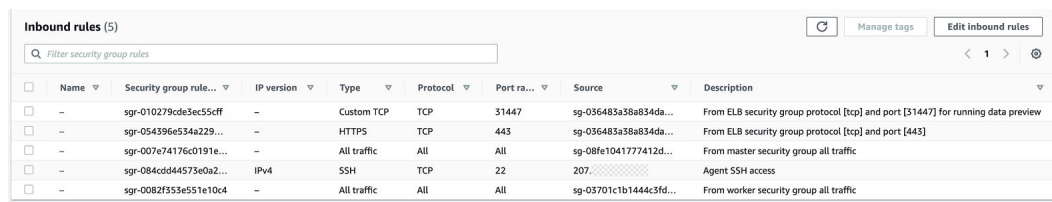
受信ルールでは、次のトラフィックを許可する必要があります。

- 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。
- 同じクラスタ内の ELB セキュリティグループからの、TCP ポート 31447 を使用する受信トラフィック。Secure Agent は、このポートを使用してデータプレビュージョブを実行します。
- CLAIRE を利用した設定を使用する詳細クラスタの場合は、TCP ポート 30000 を使用して、Secure Agent から Prometheus サーバーへのトラフィックを含めます。

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...	IP version	Type	Protocol	Port ra...	Source	Description
<input type="checkbox"/>	-	sgr-010279cde3ec55c5ff	-	Custom TCP	TCP	31447	sg-036483a38a834da...	From ELB security group protocol [tcp] and port [31447] for running data preview
<input type="checkbox"/>	-	sgr-054396e534a229...	-	HTTPS	TCP	443	sg-036483a38a834da...	From ELB security group protocol [tcp] and port [443]
<input type="checkbox"/>	-	sgr-007e74176c0191e...	-	All traffic	All	All	sg-08fe1041777412d...	From master security group all traffic
<input type="checkbox"/>	-	sgr-084cd44575e0a2...	IPv4	SSH	TCP	22	207.171.171.171	Agent SSH access
<input type="checkbox"/>	-	sgr-0082f353e551e10c4	-	All traffic	All	All	sg-03701c1b1444c3fd...	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。

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

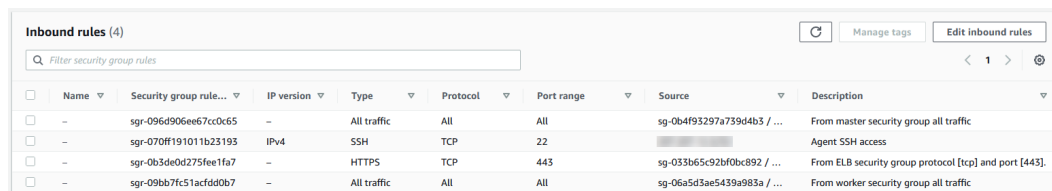
ワーカーセキュリティグループにより、詳細クラスタおよびその他のノードのワーカーノード間の受信ルールと送信ルールを定義します。このセキュリティグループは、クラスタのすべてのワーカーノードにアタッチされます。

## 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。
- TCP ポート 10250、10257、および 10259 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...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-096d906ee67cc0c65	-	All traffic	All	All	sg-0b4f93297a739d4b5 / ...	From master security group all traffic
<input type="checkbox"/>	-	sgr-070ff191011b23193	IPv4	SSH	TCP	22	207.171.171.171	Agent SSH access
<input type="checkbox"/>	-	sgr-0b3de0d275fee1fa7	-	HTTPS	TCP	443	sg-033b65c92bf0bc892 / ...	From ELB security group protocol [tcp] and port [443].
<input type="checkbox"/>	-	sgr-09bb7fc51acdd0b7	-	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、送信ルールによって、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の詳細ジョブの通信を許可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、詳細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、[「手順 7.IAM ロールの作成」](#)（ページ 31）を参照してください。

## 手順 5.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。

## 手順 6.AWS のドメインの許可

Secure Agent が AWS 環境で詳細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。

次のドメインをセキュリティグループの送信許可リストに追加します。

```
.s3.amazonaws.com  
.s3.<staging bucket region>.amazonaws.com  
awscli.amazonaws.com  
artifacthub.informaticacloud.com
```

EMEA POD のいずれかを使用する場合は、次のドメインも許可してください。

```
artifacthubemea.informaticacloud.com
```

[EMEA PODs](#) には、EM West1、EM Central1 Azure、UK、EM SouthEast 1 Azure、ME Central 2 GCP、EM West 2 GCP が含まれます。

**注:** クラスタ作成の一環として AWS CLI をインストールする必要があります。

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、次のドメインも許可します。

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

また、AWS の適切なリージョンを許可します。

```
sts.amazonaws.com
```

リージョナルエンドポイント接続を有効にするには、Informatica グローバルカスタマサポートに連絡して、必要なカスタムプロパティ設定を取得してください。

**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。

## 手順 7.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。

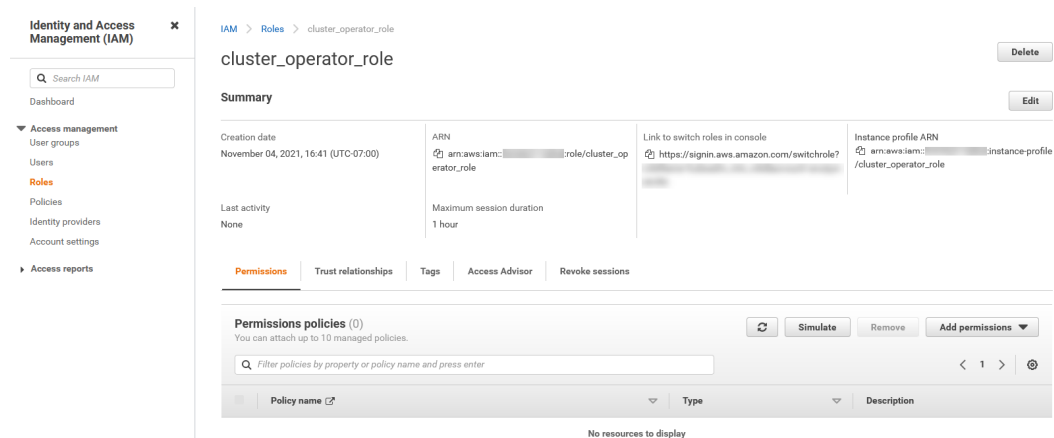
- 必要に応じて、保存時のステージングデータとログファイルを暗号化する。
- 必要に応じて、Amazon データソースのロールベースのセキュリティポリシーを作成する。
- Secure Agent ロールのクラスタストレージアクセスポリシーを作成または再利用する。

**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。

## 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。

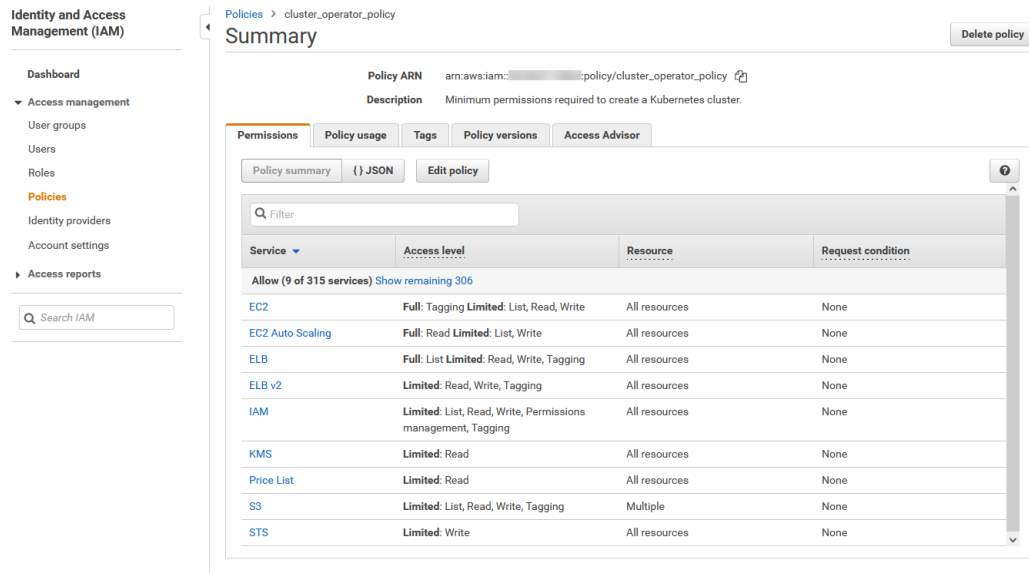
## クラスタオペレータポリシーの作成

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詳細クラスタ用のクラウドリソース



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。クラスタオペレータロールは、kubeadm ロールとも呼ばれます。

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。



以下の JSON ドキュメントは、クラスタオペレータロールポリシーのテンプレートです。必須ではない権限には、「OPTIONAL」というフラグが付きます。

**ヒント:** 保持する行から「OPTIONAL」というテキストを必ず削除するようにしてください。

```
{
  "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:::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/*"
    ]
},
{
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeAccountAttributes",
        "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",

```

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

OPTIONAL

```

        "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", OPTIONAL
        "iam:GetInstanceProfile",
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:ListInstanceProfiles",
        "iam:SimulatePrincipalPolicy",
        "iam:CreateInstanceProfile", OPTIONAL
        "iam:DeleteInstanceProfile", OPTIONAL
        "iam:CreateRole", OPTIONAL
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "iam:ListRolePolicies",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteRole", OPTIONAL
        "iam:TagRole", OPTIONAL
        "iam:GetRolePolicy",
        "iam:AddRoleToInstanceProfile", OPTIONAL
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:PutRolePolicy", OPTIONAL
        "iam:AttachRolePolicy", OPTIONAL
        "iam:DetachRolePolicy", OPTIONAL
        "iam:DeleteRolePolicy", OPTIONAL
        "iam:GetUser",
        "kms:DescribeKey", OPTIONAL
        "kms:Get*",
        "sts:AssumeRole", OPTIONAL
        "sts:DecodeAuthorizationMessage" OPTIONAL
    ],
    "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、[「IAM ポリシーリファレンス」 \(ページ 56\)](#)を参照してください。

クラスタオペレータロールには、Informatica が管理するパブリック Kubernetes クラスタに対する次の権限も必要です。

```

{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
    "ec2:GetLaunchTemplateData",
    "ec2:ModifyLaunchTemplate",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions"
  ],
  "Resource": "arn:aws:ec2:*:543463116864:launch-template/*.k8s.local"
}

```

Amazon S3 でのアクションは、詳細設定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/*"
]
```

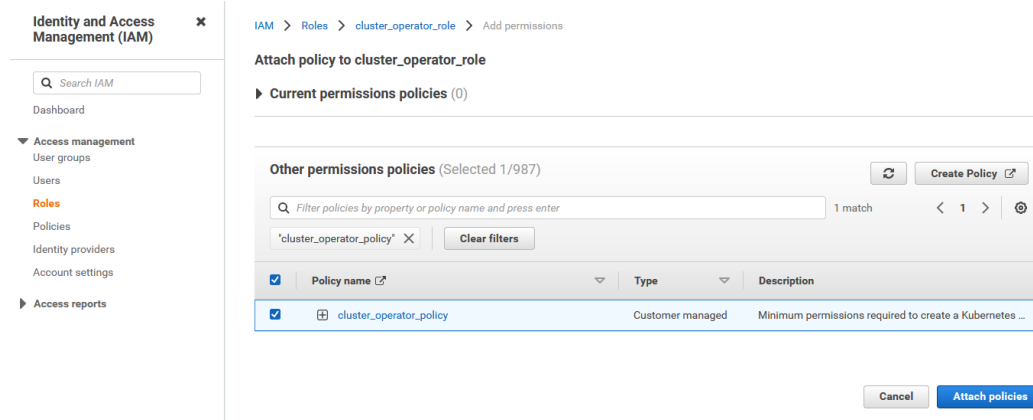
別の詳細設定でステージング、ログ、および初期化スクリプトの場所の異なるセットを使用する場合、これらの場所をリソースとして同じポリシーに追加する必要があります。

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。

## 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。



## 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、詳細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。

## 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。

## AssumeRole 権限を Secure Agent ロールに追加

Secure Agent は、詳細クラスタを管理するための上位の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。

## 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"
        }
      }
    }
  ]
}

```

**注:** ポリシーで設定する外部 ID は、エラスティックサーバーに設定した外部 ID と一致している必要があります。エラスティックサーバーのプロパティの詳細については、「[手順 9.エラスティックサーバーの設定](#)」(ページ 53)を参照してください。

## 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、詳細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、詳細ジョブで 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、詳細設定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 48)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 70)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、詳細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。

## 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詳細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は、さまざまな詳細設定間で同じインスタンスプロファイルを再使用できます。

## 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、[「IAM ポリシーリファレンス」](#)（ページ 56）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 71）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 174）を参照してください。このコマンドにより、出力ファイル `my-userdefined-master-worker-role-policies.json` が作成されます。

### 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", // If enabling CLAIRE, move AttachVolume to the same section as
CreateVolume.
    "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>/*"
        ]
    }
]
}

```

## 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
minimal_worker_policy	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	EBS ボリュームが自動スケールの場合にのみ必要。
staging_log_access_worker_policy	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	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、[「IAM ポリシーリファレンス」](#) (ページ 56)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 71)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 174)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 minimum\_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>/*"
      ]
    }
  ]
}

```

## 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"><li>- minimal_master_policy</li><li>- staging_log_access_master_policy</li><li>- init_script_master_policy</li></ul>
worker_role	<ul style="list-style-type: none"><li>- minimal_worker_policy</li><li>- ebs_autoscaling_worker_policy</li><li>- staging_log_access_worker_policy</li><li>- init_script_worker_policy</li></ul>

## 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

詳細設定を検証するために、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ができるようにする必要があります。

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"
}
```

## 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

詳細設定を検証するために、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ができるようにする必要があります。

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、エージェントが詳細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": [
        "*"
      ]
    }
  ]
}
```

## 保存時の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 バ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。

## 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 \(代替\)」 \(ページ 51\)](#)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詳細ジョブの 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-dir1>/*",
    "arn:aws:s3:::<cluster-logging-dir1>/*"
  ]
}
```

"arn:aws:s3:::<cluster-logging-dir1>/\*"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、「[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 38) 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 51) 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、その資格情報で詳細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。

## 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、詳細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-name>"
      ]
    }
  ],
  {
```

```

        "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、[「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」 \(ページ 38\)](#)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"
    }
  ]
}

```

## 手順 8。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 17 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。

## 手順 9.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 <span>Reset All</span>			
Service:	Elastic Server		
Type:	All Types		
Type	Name	Value	Sensitive
PARAMFILE_CFG	parameterfile_access_flag	'true'	<input type="checkbox"/>  
PARAMFILE_CFG	parameterfile_access_directory	'/\$AGENT_HOME/apps/data/userparameters, /\$AGENT_HOME/apps/Data_Integration_Server/data/userparameters'	<input type="checkbox"/>  
LOG4J_CFG	log4j_app_log_level	'INFO'	<input type="checkbox"/>  
AWS_CFG	agent_role_external_id_key		<input type="checkbox"/>  
AWS_CFG	privileged_role_arn_key	arn:aws:iam::<account id>:role/cluster_operator_role	<input type="checkbox"/>  
AWS_CFG	role_session_duration_secs_key		<input type="checkbox"/>  
AWS_CFG	aws_regional_endpoint_enabled	'false'	<input type="checkbox"/>  
AZURE_CFG	azure_agent_role_identity_client_id		<input type="checkbox"/>  
CONCURRENCY_CFG	allow_queuing	'true'	<input type="checkbox"/>  
CONCURRENCY_CFG	max_concurrent_jobs		<input type="checkbox"/>  

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
PARAMFILE_CFG	parameterfile_access_flag	開発者が、Secure Agent マシンに保存されているパラメータファイルをダウンロードできるかどうかを示します。 デフォルトは'true'です。
PARAMFILE_CFG	parameterfile_access_directory	パラメータファイルのダウンロードを許可する Secure Agent マシン上のディレクトリのリスト。開発者は、指定したディレクトリまたはサブディレクトリのいずれかからパラメータファイルをダウンロードできます。 デフォルトは、' <code>/\$AGENT_HOME/apps/data/userparameters,/\$AGENT_HOME/apps/Data_Integration_Server/data/userparameters</code> 'です。
LOG4J_CFG	log4j_app_log_level	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。  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。 有効な値は次のとおりです。 <ul style="list-style-type: none"><li>- 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。</li><li>- 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。</li><li>- WARNING。修復可能なシステム障害または警告が含まれます。</li><li>- 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。</li><li>- TRACE。ユーザー要求の失敗がログとして記録されます。</li><li>- DEBUG。ユーザー要求がログとして記録されます。</li></ul>
AWS_CFG	agent_role_external_id_key	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。 このプロパティは、AWS 環境でのみ有効です。

タイプ	名前	説明
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>
AZURE_CFG	azure_agent_role_identity_client_id	<p>マネージド ID agent_identity のクライアント ID。agent_identity がユーザー割り当てのマネージド ID であり、Secure Agent マシンに少なくとも 1 つの他のマネージド ID がある場合に必要です。</p> <p>このプロパティは、Azure 環境でのみ有効です。</p>
CONCURRENCY_CFG	allow_queuing	<p>エラスティックサーバーが Spark タスクをキューに格納するかどうかを示します。デフォルトは true です。</p>
CONCURRENCY_CFG	max_concurrent_jobs	<p>エラスティックサーバーが処理できる同時 Spark タスクの最大数。</p>
Tomcat JRE	INFA_MEMORY	<p>最小ヒープサイズと最大ヒープサイズ。</p> <p>エラスティックサーバーの場合、デフォルトは '-Xms256M -Xmx2048M' で、最小メモリは 256MB、最大メモリは 2048MB です。</p> <p>詳細については、「データ統合のパフォーマンスチューニング」および次のナレッジベース記事を参照してください:</p> <p><a href="#">FAQ: What are the guidelines and best practices to increase Java heap size and other memory attributes of the Informatica Cloud Secure Agent?</a></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。

## 手順 10. プロキシの設定

Secure Agent にプロキシサーバーを使用する場合は、エージェントにプロキシ設定を構成します。

プロキシ設定で、インスタンスメタデータサービスの IP アドレスが除外されていることを確認します。プロキシ設定の構成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。

## CLAIRE を利用した設定に対する追加のセットアップ

CLAIRE を利用した設定を使用する詳細クラスタには、CLAIRE がクラスタを予算内に収めることができるようにするための追加のセットアップ要件があります。

CLAIRE を利用した設定を使用するには、次のセットアップタスクを実行します。

- 次の価格ポリシーをクラスタオペレータロールにアタッチします:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts"
      ],
      "Resource": "*"
    }
  ]
}
```

- ELB セキュリティグループを編集し、TCP ポート 30000 を使用して、Secure Agent から Prometheus サーバーへの受信トラフィックを含めます。
- マスタセキュリティグループを編集し、TCP ポート 30000 を使用して Secure Agent から Prometheus サーバーへの受信トラフィックを含めます。
- 最小マスタポリシーを編集し、AttachVolume アクションを CreateVolume アクションと同じセクションに移動して、AttachVolume アクションに条件が設定されないようにします。

ユーザー定義のセキュリティグループまたはユーザー定義のマスタロールとワーカーロールを作成しない場合の手順は、クラスタオペレータロールへの価格ポリシーのアタッチのみです。

CLAIRE を利用した設定の詳細については、「[CLAIRE を利用した設定](#)」(ページ 126)を参照してください。

## IAM ポリシーリファレンス

クラスタオペレータロール、マスタロール、およびワーカーロールには、詳細クラスタでクラウドリソースを作成および管理するための IAM ポリシーが必要です。このセクションでは、IAM ポリシーで各ロールが必要とするアクションについて説明します。



## クラスタオペレータロールのアクション

クラスタオペレータロールの IAM ポリシーにアクションを追加して、ロールがクラウドリソースを作成および管理できるようにします。

クラスタオペレータロールには、AWS の次のサービスによって定義されたアクションが必要です。

- Amazon EC2
- Amazon S3
- AWS Auto Scaling
- AWS Key Management Service
- AWS Security Token Service
- Elastic Load Balancing
- Identity and Access Management
- 価格設定

### Amazon EC2 アクション

Amazon Elastic Compute Cloud (EC2) は、クラウド上でコンピューティングリソースを提供します。Amazon EC2 アクションは、すべての AWS リソースに適用する必要があります。

#### アカウント

クラスタオペレータロールでは、AWS アカウントの属性を取得するために `ec2:DescribeAccountAttributes` アクションが必要です。

#### インターネットゲートウェイ

次の表では、インターネットゲートウェイのアクションについて説明します。

アクション	説明
<code>ec2:CreateInternetGateway</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:AttachInternetGateway</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:DescribeInternetGateway</code>	必須。インターネットゲートウェイを記述します。
<code>ec2:DetachInternetGateway</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2&gt;DeleteInternetGateway</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。

#### 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。クラスタオペレータロールには、キーペアを管理するための次のアクションが必要です。

`ec2:CreateKeyPair`  
`ec2:ImportKeyPair`  
`ec2:DescribeKeyPair`  
`ec2>DeleteKeyPair`

## ネットワーク

クラスタオペレータロールには、ネットワークインタフェースを記述するために `ec2:DescribeNetworkInterfaces` アクションが必要です。

### ルート

クラスタオペレータロールは、Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ、次のアクションを必要とします。

`ec2:CreateRoute`  
`ec2:DeleteRoute`

Secure Agent は、デフォルトで VPC とサブネットを作成します。

### ルートテーブル

次の表では、ルートテーブルのアクションについて説明します。

アクション	説明
<code>ec2:CreateRouteTable</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:DescribeRouteTables</code>	必須。ルートテーブルの詳細を返します。
<code>ec2:ReplaceRouteTableAssociation</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:AssociateRouteTable</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:DisassociateRouteTable</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2&gt;DeleteRouteTable</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。

## VPC

次の表では、VPC のアクションについて説明します。

アクション	説明
<code>ec2:CreateVpc</code>	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
<code>ec2:DescribeVpcs</code>	必須。VPC の詳細を記述します。

アクション	説明
ec2:ModifyVpcAttribute	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
ec2>DeleteVpc	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。

## サブネット

次の表では、サブネットのアクションについて説明します。

アクション	説明
ec2:CreateSubnet	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
ec2:DescribeSubnet	必須。サブネットの詳細を記述します。
ec2>DeleteSubnet	Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。

## セキュリティグループ

次の表では、セキュリティグループのアクションについて説明します。

アクション	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。
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。
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。
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。
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。
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、[「手順 4.Amazon EC2 のユーザー定義のセキュリティグループの作成」 \(ページ 27\)](#)を参照してください。

## タグ

次の表では、タグのアクションについて説明します。

アクション	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は、etcd ボリュームを直接管理します。詳細クラスタでは、etcd ボリュームを使用してメタデータを格納します。クラスタオペレータロールでは、etcd ボリュームを管理するために次のアクションが必要です。

ec2:CreateVolumes  
ec2:DescribeVolumes  
ec2:DeleteVolumes

## イメージ

クラスタオペレータロールには、Amazon EC2 インスタンスから AMI (Amazon Machine Image) の詳細を取得するために ec2:DescribeImages アクションが必要です。

## インスタンス

次の表では、インスタンスのアクションについて説明します。

アクション	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

次の表では、リージョンのアクションについて説明します。

アクション	説明
ec2:DescribeRegions	必須。詳細設定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。クラスタオペレータロールには、起動テンプレートを管理するための次のアクションが必要です。

```
ec2:CreateLaunchTemplate
ec2:DescribeLaunchTemplates
ec2:DeleteLaunchTemplate
ec2:CreateLaunchTemplateVersion
ec2:DescribeLaunchTemplateVersions
ec2:DeleteLaunchTemplateVersions
ec2:GetLaunchTemplateData
ec2:ModifyLaunchTemplate
```

## Amazon S3 アクション

次の表に、クラスタオペレータロールに必要な Amazon S3 アクションと、各アクションを適用する必要があるリソースを示します。

アクション	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>/*"

## AWS Auto Scaling アクション

クラスタオペレータは、自動スケーリンググループを使用して詳細クラスタを管理します。

クラスタオペレータロールには、スケーラブル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 リソースで次のアクションが必要です。

```
autoscaling:AttachLoadBalancers
autoscaling:CreateAutoScalingGroup
autoscaling:DescribeAutoScalingGroups
autoscaling:UpdateAutoScalingGroup
autoscaling>DeleteAutoScalingGroup
autoscaling:DescribeScalingActivities
autoscaling:DescribeTags
autoscaling:TerminateInstanceInAutoScalingGroup
```

## AWS Key Management Service アクション

クラスタオペレータロールでは、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マネージドキー（CMK）が提供されている場合は、`kms:DescribeKey` アクションが必要です。このアクションは、すべての AWS リソースに適用されます。

## AWS Security Token Service アクション

次の表では、STS アクションについて説明します。

アクション	説明
<code>sts:AssumeRole</code>	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。
<code>sts:DecodeAuthorizationMessage</code>	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。

## Elastic Load Balancing アクション

クラスタオペレータは、高可用性、マスタノードアクセス制御、およびその他の機能のためにロードバランサを必要とします。

クラスタオペレータロールには、すべての AWS リソースに対する次の Elastic Load Balancing アクションが必要です。

```
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
```

## Identity and Access Management アクション

Identity and Access Management アクションは、すべての AWS リソースに適用されます。

### インスタンスプロファイル

次の表では、インスタンスプロファイルのアクションについて説明します。

アクション	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。詳細設定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

次の表では、IAM ロールのアクションについて説明します。

アクション	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。
iam:TagRole	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。 Secure Agent によって作成される IAM ロールにタグを付けるために使用されます。

## ポリシー

次の表では、IAM ポリシーのアクションについて説明します。

アクション	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

クラスタオペレータロールでは、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 アクションが必要です。

## Pricing アクション

クラスタオペレータロールには、AWS の価格にアクセスするための Pricing アクションが必要です。クラスタオペレータロールは、AWS の価格を使用してスポットインスタンスを選択し、CLAIRE を利用した設定を使用する詳細クラスタのインフラストラクチャコストの削減額を計算します。

次の表に、Pricing アクションを示します。

アクション	説明
pricing:DescribeServices	CLAIRE を利用した設定を使用する場合は必須です。AWS のサービス製品と価格を取得します。
pricing:GetAttributeValues	CLAIRE を利用した設定を使用する場合は必須です。AWS のサービス製品と価格を取得します。
pricing:GetProducts	スポットインスタンスまたは CLAIRE を利用した設定を使用する場合は必須です。AWS のサービス製品と価格を取得します。

## マスタロールアクション

マスタロールの IAM ポリシーにアクションを追加して、ロールがクラウドリソースにアクセスして管理できるようにします。

マスタロールには、AWS 上の次のサービスによって定義されたアクションが必要です。

- Amazon EC2



- Amazon S3
- AWS Auto Scaling
- AWS Key Management Service
- Elastic Load Balancing
- Identity and Access Management

## Amazon EC2 アクション

Amazon Elastic Compute Cloud (EC2) は、クラウド上でコンピューティングリソースを提供します。Amazon EC2 アクションは、すべての AWS リソースに適用する必要があります。

次の表では、マスタロールに必要なアクションについて説明します。

アクション	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。Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
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。Secure Agent がクラスタの VPC とサブネットを作成する場合にのみ必要です。Secure Agent は、デフォルトで VPC とサブネットを作成します。
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。インスタンスの属性を変更します。
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。E2 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。

アクション	説明
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。

## Amazon S3 アクション

次の表では、マスタロールに必要な Amazon S3 アクションと、各アクションを適用する必要があるリソースについて説明します。

アクション	リソース	説明
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
s3:GetEncryptionConfiguration	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"	必須
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
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

## AWS Auto Scaling アクション

マスタノードは、自動スケーリンググループを管理して、スケーラブルなクラスタノードとノードリカバリを可能にします。

マスタロールには、自動スケーリンググループを管理するために次のアクションが必要です。

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

## AWS Key Management Service アクション

マスタロールには、マスタキーへのアクセスを管理するために、すべての AWS リソースで次のアクションが必要です。

```
kms:Encrypt
kms:Decrypt
kms:ReEncrypt
kms:GenerateDataKey
kms:DescribeKey
```

## Elastic Load Balancing アクション

マスタノードは、詳細クラスタの負荷分散ルールを管理します。

マスタロールには、すべての AWS リソースに対する次のアクションが必要です。

```
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
```

## Identity and Access Management アクション

Identity and Access Management アクションは、すべての AWS リソースに適用されます。

次の表で、アクションについて説明します。

アクション	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。

## ワーカーロールアクション

ワーカーロールの IAM ポリシーにアクションを追加して、ロールがクラウドリソースにアクセスして管理できるようにします。

ワーカーロールには、AWS 上の次のサービスによって定義されたアクションが必要です。

- Amazon EC2
- Amazon S3
- AWS Auto Scaling
- AWS Key Management Service

## Amazon EC2 アクション

Amazon Elastic Compute Cloud (EC2) は、クラウド上でコンピューティングリソースを提供します。

次の表では、ワーカーロールに必要な Amazon EC2 アクションについて説明します。

アクション	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。
ec2:CreateVolume	すべて -- "*"	ストレージのスケーリングに必要です。
ec2:ModifyInstanceAttribute	すべて -- "*"	ストレージのスケーリングに必要です。
ec2:AttachVolume	"arn:aws:ec2:*:*:volume/*" "arn:aws:ec2:*:*:instance/*"	ストレージのスケーリングに必要です。

## Amazon S3 アクション

次の表では、ワーカーロールに必要な Amazon S3 アクションと、各アクションを適用する必要があるリソースについて説明します。

アクション	リソース	説明
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
s3:GetEncryptionConfiguration	"arn:aws:s3:::<cluster-staging-bucket-name>" "arn:aws:s3:::<cluster-logging-bucket-name>"	必須。
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
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。初期化スクリプトを使用してクラスタを起動する場合、アクションを初期化スクリプトの場所に適用する必要があります。
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。

## AWS Auto Scaling アクション

ワーカーロールには、すべての AWS リソースに対する自動スケーリングアクションが必要です。

次の表では、自動スケーリングアクションについて説明します。

アクション	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。

## AWS Key Management Service アクション

ワーカーロールには、マスタキーへのアクセスを管理するために、すべての AWS リソースで次のアクションが必要です。

```
kms:Encrypt  
kms:Decrypt  
kms:ReEncrypt  
kms:GenerateDataKey  
kms:DescribeKey
```

## 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。
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 ロールが両方とも詳細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 ロールが詳細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	複数の詳細設定で同じマスタロールとワーカーロールを使用できる。	詳細設定ごとに別のマスタ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。

領域	ユーザー定義のロール	デフォルトのロール
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、マスタロールとワーカーロールで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。

マスタロールとワーカーロールの使用方法の詳細については、[「リソースへのアクセスの詳細」](#) (ページ 20) 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 は詳細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、[「保存時の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 48) 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징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。

複数の詳細クラスタのステー징ング、ログ、および初期化の場所を指定し、異なる詳細設定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징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

組織で詳細設定を作成する前に、Secure Agent が詳細クラスタを作成できるようにクラウド環境を設定します。

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. 必要に応じて、VPC とサブネットを作成します。
4. 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。
5. Google Cloud で特定のドメインを許可します。
6. オプションで、クラスタのプロキシを設定します。
7. ロールとサービスアカウントを作成します。
8. オプションで、JAVA\_HOME 環境変数を設定する。
9. ステージング接続を作成します。

## 手順 1.前提条件の完了

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。
- Secure Agent と詳細クラスタが、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について説明します。
- 詳細クラスタで使用されるパッケージとイメージについて確認します。

### 組織の権限の確認

組織の詳細設定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。

詳細設定に対する特権によって、Administrator および Monitor の **【詳細クラスタ】** ページへのアクセスレベルは異なります。

詳細設定の表示と詳細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 で詳細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

詳細クラスタおよび詳細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

詳細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 および詳細クラスタは、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、詳細ジョブの一部であるリソースにアクセスします。

次のタスクを実行するために、リソースにアクセスします。

- マッピングの設計
- 詳細クラスタの作成
- データプレビューを含むジョブの実行
- ログのポーリング

### マッピングの設計

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。

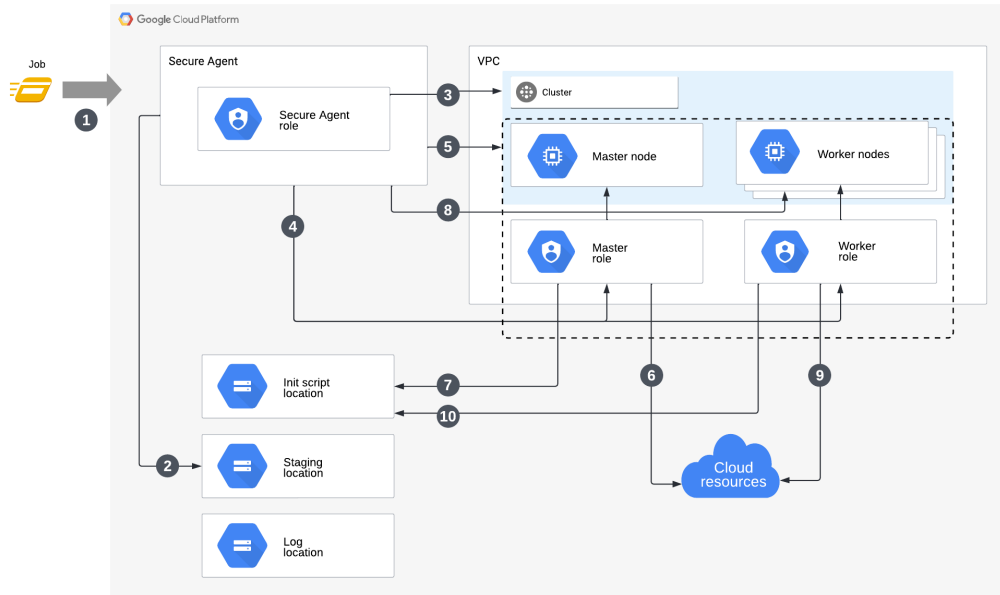
例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで使用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

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。

## 詳細クラスタの作成

詳細クラスタを作成するために、Secure Agent は Secure Agent ロールを使用してクラスタの詳細をステージング場所に保存し、クラスタの作成を行います。マスターノードとワーカーノードは、マスターロールとワーカーロール、または Secure Agent ロールのいずれかを使用して、クラウド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ために使用するプロセスを示しています。



次の手順では、Secure Agent がクラスタを作成するために使用するプロセスについて説明します。

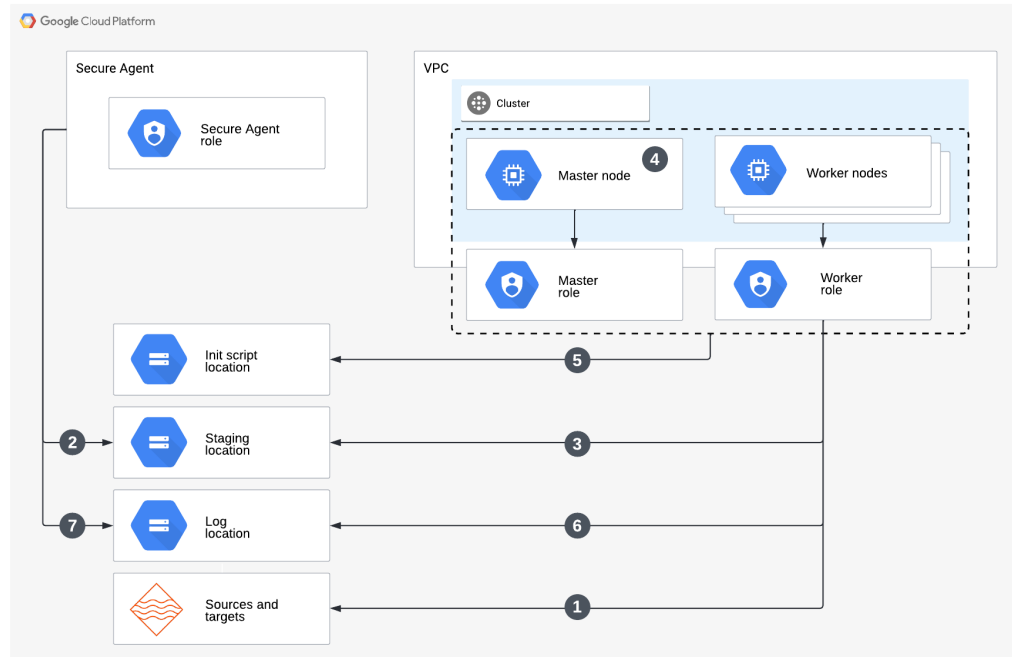
1. ジョブを実行します。
2. Secure Agent は、Secure Agent ロールを使用して、クラスタの詳細をステージングの場所に保存します。
3. Secure Agent は、Secure Agent ロールを使用してクラスタを作成します。
4. マスターロールとワーカーロール、およびサービスアカウントを作成した場合、Secure Agent はサービスアカウントをクラスタノードにアタッチします。
5. Secure Agent は、Secure Agent ロールを使用して、マスターノードにクラスタリソースを作成します。
6. マスターノードは、マスターロールを使用して Google Compute Engine などの Google Cloud 上のサービス上のクラウドリソースにアクセスし、ノードの弾性とリソースの最適化を管理します。
7. マスターノードは、マスターロールを使用して初期化スクリプトにアクセスします。マスターロールとワーカーロール、およびサービスアカウントを作成しなかった場合、マスターノードは Secure Agent ロールを使用します。
8. Secure Agent は、Secure Agent ロールを使用してワーカーノードのクラスタリソースを作成し、最小数のワーカーノードでマネージドインスタンスグループを作成します。
9. ワーカーノードは、ワーカーロールを使用して、Google Compute Engine や Google Cloud ネットワーキングなどの Google Cloud 上のサービス上のクラウドリソースにアクセスし、コンピューティング機能やネットワーク機能にアクセスします。マスターロールとワーカーロールおよびサービスアカウントを作成しなかった場合、ワーカーノードは Secure Agent ロールを使用します。
10. ワーカーノードは、ワーカーロールを使用して初期化スクリプトにアクセスします。マスターロールとワーカーロールおよびサービスアカウントを作成しなかった場合、ワーカーノードは Secure Agent ロールを使用します。

マスタロールとワーカーロールが詳細クラスタ内のクラウドリソースにアクセスする方法の詳細については、[「手順 7.ロールとサービスアカウントの作成」 \(ページ 81\)](#)を参照してください。

## ジョブの実行

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、ソースとターゲット、およびステージング、ログ、および初期化スクリプトの場所にアクセスします。

次の図は、Secure Agent とクラスタノードがジョブを実行するために使用するプロセスを示しています。



次の手順では、Secure Agent とクラスタノードがジョブを実行するために使用するプロセスについて説明しています。

1. ワーカーノード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。
2. 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ジングの場所に保存します。
3. ワーカーノードは、ワーカーロールを使用してジョブの依存関係を取得し、一時データをステージングの場所にステージングします。
4. マスタノードはマスタロールを使用して、クラスタ上のプロセスを調整します。
5. マスタノードはマスタロールを使用して、マスタノード上の初期化スクリプトにアクセスして実行し、ワーカーノードをスケールアップします。追加されたワーカーノードは、ワーカーロールを使用して初期化スクリプトに再度アクセスし、ワーカーノードでスクリプトを実行します。
6. 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。
7. 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。

マスタロールとワーカーロール、およびサービスアカウントを作成した場合、マスタノードとワーカーノードはそれぞれのロールを使用します。それ以外の場合、マスタノードとワーカーノードは Secure Agent ロールを使用します。

## 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。

## Google Cloud クラスタの詳細

Google Cloud クラスタは、Informatica によって公開された Google Cloud CentOS 7 OS イメージを使用します。

OS イメージには、特定の事前構築済みパッケージと次の追加の yum パッケージが含まれています。

```
cloud-init
device-mapper-persistent-data
docker-ce
gnupg2
gzip
kernel-devel
kernel-headers
kubeadm
kubelet
libxml2-python
lvm2
tar
unzip
wget
yum-utils
```

また、OS イメージには、次の Docker イメージが含まれています。

```
calico/kube-controllers
calico/node
calico/cni
calico/pod2daemon-flexvol
coreos/flannel
coreos/flannel-cni
image/jq
kube-scheduler
```

## 手順 2. 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詳細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。

## 手順 3.VPC とサブネットの作成（オプション）

詳細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. 詳細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。

### 十分な数の IP アドレスを含むサブネットの作成

VPC ネットワーク内の詳細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、詳細クラスタで最大 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 11 の IP アドレスをサポートする必要があります。

### 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。

詳細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。

The screenshot shows the 'Create a NAT gateway' page in the Google Cloud Console. The left sidebar lists 'Network services' with 'Cloud NAT' selected. The main content area has a title 'Create a NAT gateway' and a description of Cloud NAT. Below the description are several configuration sections: 'Gateway name' (dev-example-nat), 'Select Cloud Router' (Network: dev-example-vpc, Region: us-west2 (Los Angeles), Cloud Router: new-router), 'NAT mapping' (Source (internal): Primary and secondary ranges for all subnets), and 'NAT IP addresses' (Manual: privateipaddress). The 'Region' and 'Cloud Router' fields are highlighted with orange boxes. The 'NAT mapping' and 'NAT IP addresses' sections are also highlighted with orange boxes.

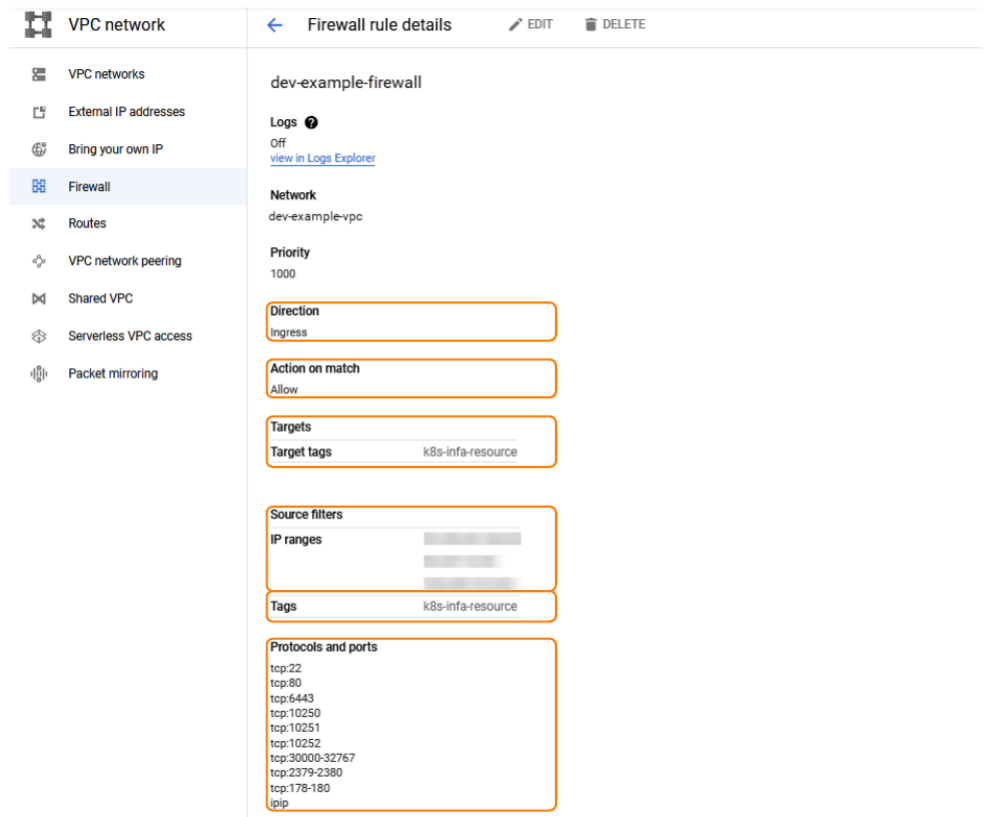
## VPC ネットワークでのファイアウォールルールの作成

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。
- セカンダリソースフィルタをソースタグでフィルタリングするように設定します。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、178-180、5473、6443、2379-2380、10250、10251、10252、10257、10259、30000-32767
  - 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。



## 手順 4.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。



## 手順 5.Google Cloud でのドメインの許可

Secure Agent が Google Cloud で詳細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。

次のドメインをファイアウォールの送信許可リストに追加します。

```
.storage.cloud.google.com  
storage.googleapis.com  
.google.com  
.le100.net  
artifacthub.informaticacloud.com
```

EMEA POD のいずれかを使用する場合は、次のドメインも許可してください。

```
artifacthubemea.informaticacloud.com
```

[EMEA PODs](#) には、EM West1、EM Central1 Azure、UK、EM SouthEast 1 Azure、ME Central 2 GCP、EM West 2 GCP が含まれます。

## 手順 6.クラスタのプロキシの設定（オプション）

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。

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。

プロキシ設定の構成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。

## 手順 7.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 で詳細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。詳細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」 \(ページ 82\)](#)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"><li>- 外部静的 IP アドレスを作成する</li><li>- IP アドレスを削除または解放する</li></ul>	<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"><li>- ターゲットプールを作成する</li><li>- ターゲットプールの詳細を取得する</li><li>- ターゲットプールを削除する</li></ul>	<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"><li>- 転送ルールを作成する</li><li>- ルール作成の詳細を取得する</li><li>- 転送ルールを削除する</li></ul>	<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"> <li>- インスタンステンプレートを作成する</li> <li>- インスタンステンプレートの詳細を取得する</li> <li>- インスタンステンプレートを削除する</li> <li>- インスタンスにディスクを追加する</li> </ul>	<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"> <li>- 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</li> <li>- 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</li> <li>- リージョナルインスタンスグループを削除する</li> </ul>	<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"><li>- 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</li></ul>	<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"><li>- 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</li><li>- 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</li></ul>	<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。

## 手順 8.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 17 と互換性がある必要があります。

## 手順 9.ステージング接続の作成

ステージングの場所へのステージング接続を作成して、詳細クラスタがステージングデータをデータ統合サーバーと共有できるようにします。

1. Administrator で、**接続** ページを開きます。
2. Google Cloud Storage への接続を作成します。  
接続プロパティで、ステージングファイルを保存するために [「手順 2.クラスタファイルの格納場所の作成」](#) (ページ 77) で作成した場所のバケット名を入力します。
3. **詳細クラスタ** ページを開きます。
4. 詳細設定を作成するか、クラスタ用の既存の詳細設定を編集します。
5. **プラットフォーム設定** タブで、接続プロパティに入力したものと同一バケット名を指定するようにステージングの場所を構成します。バケット内のフォルダパスを指定できます。
6. **ランタイムプロパティ** タブで、プロパティ clusterconfig.stagingConnectionName を追加して、値を接続の名前に設定します。

## 第 4 章

# Microsoft Azure の設定

組織で詳細設定を作成する前に、Secure Agent が詳細クラスタを作成できるようにクラウド環境を設定します。

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ストレージアカウントを作成する。
3. 必要に応じて、VNet とサブネットを作成します。
4. 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。
5. Azure で特定のドメインを許可します。
6. オプションで、クラスタのプロキシを設定します。
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、ソースとターゲットにアクセスするためのマネージド ID を作成します。
10. 必要に応じて、ユーザー定義のセキュリティグループを作成します。
11. オプションで、JAVA\_HOME 環境変数を設定する。
12. オプションで、ステージング接続を作成します。

## 手順 1。前提条件の完了

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。
- Secure Agent と詳細クラスタが、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について説明します。

### 組織の権限の確認

組織の詳細設定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。

詳細設定に対する特権によって、Administrator および Monitor の【詳細クラスタ】ページへのアクセスレベルは異なります。

詳細設定の表示と詳細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 環境で詳細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。

Azure Data Lake Storage Gen2

詳細クラスタおよび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)**

詳細クラスタは 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 からの受信ジョブを受け入れ、詳細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 および詳細クラスタは、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、詳細ジョブの一部であるリソースにアクセスします。

次のタスクを実行するために、リソースにアクセスします。

- マッピングの設計
- 詳細クラスタの作成
- データプレビューを含むジョブの実行
- ログのポーリング

### マッピングの設計

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。

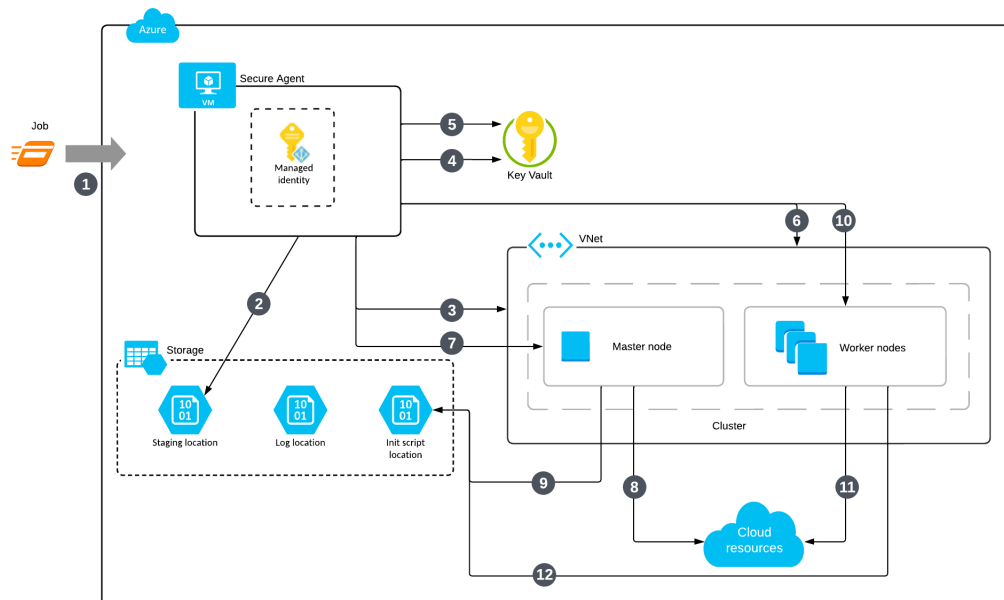
例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで利用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

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。

## 詳細クラスタの作成

詳細クラスタを作成するために、Secure Agent はマネージド ID で認証を行い、クラスタの詳細をステージングの場所に保存し、クラスタを作成します。マスターノードとワーカーノードはサービスプリンシパルを使用してクラウド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ために使用するプロセスを示しています。



次の手順では、Secure Agent がクラスタを作成するために使用するプロセスについて説明します。

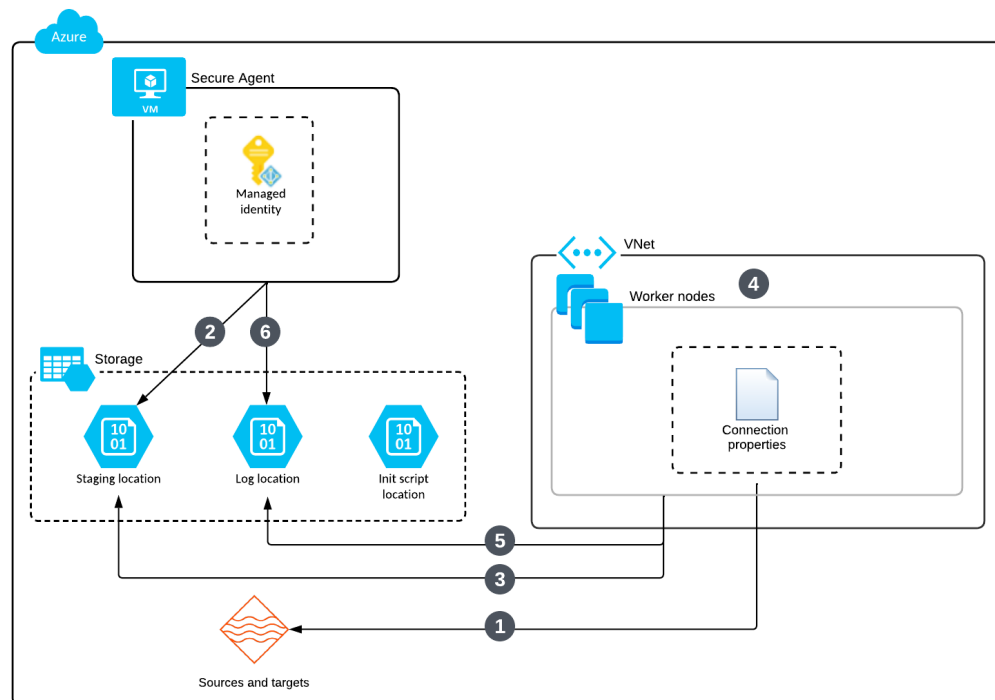
1. ジョブを実行します。
2. Secure Agent はマネージド ID で認証を行い、ステージングの場所にクラスタの詳細を保存します。
3. Secure Agent はマネージド ID を使用して認証を行い、ネットワークセキュリティグループやロードバランサなど、クラスタに必要な前提条件のリソースを作成します。
4. Secure Agent は、マネージド ID で認証を行い、ストレージアカウントへのアクセスキーを取得します。
5. Secure Agent は、マネージド ID で認証を行い、サービスプリンシパルの資格情報を取得します。
6. Secure Agent は、ストレージアカウントへのアクセスキーとサービスプリンシパルの資格情報をクラスタでできるようにします。
7. Secure Agent はマネージド ID を使用して認証を行い、マスタノードのクラスタリソースとマスタノードの仮想マシンスケールセットを作成します。
8. マスタノードは、サービスプリンシパルを使用して Azure コンピューティングなどの Microsoft Azure 上のサービス上のクラウドリソースにアクセスし、ノードの弾性とリソースの最適化を管理します。
9. マスタノードは、Secure Agent がマネージド ID を通じて取得したストレージアカウントキーを使用して初期化スクリプトにアクセスします。
10. Secure Agent は、マネージド ID を使用して認証を行い、ワーカーノードにクラスタリソースを作成して、最小数のワーカーノードで仮想マシンスケールセットを作成します。
11. ワーカーノードは、サービスプリンシパルを使用して Azure コンピューティングなどの Microsoft Azure 上のサービス上のクラウドリソースにアクセスし、コンピューティング機能とネットワーク機能にアクセスします。
12. ワーカーノードは、Secure Agent がマネージド ID を通じて取得したストレージアカウントキーを使用して初期化スクリプトにアクセスします。

マスタロールとワーカーロールが詳細クラスタ内のクラウドリソースにアクセスする方法の詳細については、[「手順 8. クラスタのサービスプリンシパルの作成」](#) (ページ 99) および [「手順 7. Secure Agent のマネージド ID の作成」](#) (ページ 95) を参照してください。

## ジョブの実行

ジョブを実行するために、Secure Agent とワーカーノードは、ソースとターゲット、およびステージングとログの場所にアクセスします。ワーカーノードと Azure ディスクは、リソース要件に従って自動スケールを実行します。

次の図は、Secure Agent とワーカーノードがジョブを実行するために使用するプロセスを示しています。



次の手順では、Secure Agent とワーカーノードがジョブを実行するために使用するプロセスについて説明します。

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。  
接続プロパティは、ストレージアカウントキーまたはマネージド ID を使用してデータにアクセスします。マネージド ID を使用するには、その ID が Secure Agent に割り当てられている必要があり、エージェントロールには、Secure Agent マシンに割り当てられているすべてのユーザー割り当てマネージド ID を検出し、その ID をすべてのクラスタノードに割り当てることができる権限が必要です。
2. Secure Agent は、マネージド ID で認証を行いステージングの場所にジョブの依存関係を保存します。
3. ワーカーノードはジョブの依存関係を取得し、Secure Agent がマネージド ID を通じて取得したストレージアカウントキーを使用して、ステージングの場所に一時データをステージングします。また、Secure Agent はキーを Spark ジョブに渡し、Spark ドライバと Spark エグゼキュータが同じキーを使用してステージングの場所にアクセスできるようにします。
4. ワーカーノードと Azure ディスクは、サービスプリンシパルを使用して自動スケールを実行します。
5. ワーカーノードは、マネージド ID を通じてストレージアカウントキーを取得した後に、ログの場所にログを保存します。

- Secure Agent は、マネージド ID で認証を行い、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。

## 手順 2。クラスタファイルのストレージアカウントの作成

Azure Data Lake Storage Gen2 を使用してデータを格納できます。

Azure で、階層名前空間を使用して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詳細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。

## 手順 3。VNet とサブネットの作成（オプション）

詳細クラスタをホストする固有の VNet およびサブネットを作成する場合は、クラスタの要件に基づいて VNet とサブネットを準備します。

以下のタスクを完了させます。

- 詳細クラスタ内のロードバランサおよびノードに必要な数の IP アドレスをサポートするサブネットを作成します。
- VNet 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。
- クラスタノードが 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受け入れます。

## 十分な数の IP アドレスを含むサブネットの作成

詳細クラスタ内のロードバランサおよびノードに必要な数の 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. 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、8 個の IP アドレスを追加します。
2. マスタノード用に 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は、代わりに 3 個の IP アドレスを追加します。
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、詳細クラスタで最大 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

VNet とサブネットが詳細クラスタで要求をルーティングして、クラスタノードと Secure Agent が相互に通信を行って、インターネットにアクセスできることを確認します。

例えば、クラスタノードはインターネットにアクセスして、Informatica の Docker イメージおよびアーティファクトのダウンロードや Informatica Intelligent Cloud Services 上のサービスへのアクセスを行います。

VNet 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、Microsoft Azure で次の項目を確認します。

- サブネットが、ネットワーク要件に基づいて、NAT ゲートウェイ、ネットワークセキュリティグループおよびルートテーブルに関連付けられている。

NAT ゲートウェイにより、プライベートクラスタノードのインターネットへのアクセスを許可します。ルートテーブルを使用して、ファイアウォールまたはプロキシ経由でトラフィックをルーティングすることができます。また、エンドポイントを VNet レベルで定義して、クラスタノードがクラウドプラットフォーム上の特定のサービスにアクセスするときにインターネット経由でトラフィックがルーティングされないようにすることもできます。

- DNS ホスト名および DNS 解決は有効です。

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。

## 受信トラフィックの承認

クラスタノードが 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受け入れます。シーケンスジェネレーター変換、特定のデータ品質変換、データの暗号化と復号化を行うデータアダプタなどの一部のマッピング機能では、クラスタノードが Secure Agent にアクセスする必要があります。

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 VNet を指定します。

## 手順 4. 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。

## 手順 5. Azure のドメインの許可

Secure Agent が Microsoft Azure 環境で詳細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、マッピングを実行するための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。

次のドメインをネットワークセキュリティグループの送信許可リストに追加します。

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

EMEA POD のいずれかを使用する場合は、次のドメインも許可してください。

```
artifacthubemea.informaticacloud.com
```

[EMEA PODs](#) には、EM West1、EM Central1 Azure、UK、EM SouthEast 1 Azure、ME Central 2 GCP、EM West 2 GCP が含まれます。

**注:** デフォルトの NTP サービス設定を使用するには、ファイアウォールを開き、すべての送信サーバーのデフォルトの NTP サービス UDP ポートを 123 に設定します。この設定を使用しない場合は、カスタム NTP サービス設定を持つカスタムイメージをセットアップできます。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。

## 手順 6. クラスタのプロキシの設定（オプション）

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。マネージド ID 認証を使用して詳細モードのマッピングのソースまたはターゲットに接続するには、インスタンスメタデータサービスの IP アドレスが除外されていることを確認します。

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。

プロキシ設定の構成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。

## 手順 7. Secure Agent 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、詳細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. クラスタリソースグループを作成します。
2. マネージド ID を作成します。
3. エージェントロールを作成します。
4. 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。

### 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。

### マネージド ID の作成

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。ユーザー割り当てマネージド ID を作成し、複数の ID が Secure Agent マシンにアタッチされている場合は、Elastic Server プロパティ azure\_agent\_role\_identity\_client\_id をクライアント ID agent\_identity に設定します。

マネージド ID 作成の詳細については、Microsoft Azure のドキュメントを参照してください。Microsoft Azure は、マネージド ID のベストプラクティスを提供し、システム割り当てマネージド ID またはユーザー割り当てマネージド ID のどちらを使用するかを決定するのに役立ちます。

## エージェントロールの作成

マネージド IDagent\_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.Compute/virtualMachineScaleSets/manualupgrade/action",
          "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.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/publicIPAddresses/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/virtualNetworks/subnets/write",
          "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",
          "Microsoft.Compute/virtualMachines/read",
          "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
        ],
        "notActions": [
        ],
        "dataActions": [
        ],
        "notDataActions": [
        ]
      }
    ]
  }
}
```



次の表に、権限を示します。

権限	説明
Microsoft.Compute/ virtualMachineScaleSets/manualupgrade/ action	必須。仮想マシンでのカスタムスクリプトの実行を許可します。
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詳細設定で指定されていない場合に必要です。 詳細設定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。
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、ストレージ操作を実行します。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リ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.Compute/ virtualMachineScaleSets/virtualMachines/ networkInterfaces/ipConfigurations/ publicIPAddresses/read	Azure パブリッククラスタを開始するためのパブリック IP アドレスを取得するために必要です。Azure プライベートクラスタではいずれのタイプも必須ではありません。
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。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。

権限	説明
Microsoft.Network/virtualNetworks/subnets/join/action	<p>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。</p> <p>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。</p>
Microsoft.Network/virtualNetworks/subnets/read	<p>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。</p>
Microsoft.Network/virtualNetworks/subnets/write	<p>必須。サブネットの作成と更新に使用されます。</p>
Microsoft.Network/networkSecurityGroups/join/action	<p>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。</p>
Microsoft.Network/loadBalancers/backendAddressPools/join/action	<p>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。</p>
Microsoft.Compute/virtualMachineScaleSets/publicIPAddresses/read Microsoft.Compute/virtualMachineScaleSets/networkInterfaces/read	<p>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。</p>
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read Microsoft.Compute/virtualMachines/instanceView/read Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read Microsoft.Compute/virtualMachineScaleSets/instanceView/read	<p>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。</p>
Microsoft.Compute/virtualMachineScaleSets/manualupgrade/action	<p>初期化スクリプトを使用する場合に必要です。</p> <p>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。</p>
Microsoft.Authorization/roleAssignments/read Microsoft.Authorization/roleDefinitions/read	<p>必須。詳細設定を検証します。</p>
Microsoft.Compute/virtualMachines/read Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	<p>マネージド ID 認証を使用してソースまたはターゲットに接続する場合に必要です。Secure Agent はこれらの権限を使用して、エージェントのマネージド ID を検出し、その ID を仮想マシンスケールセットに割り当てます。</p>

## 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マシンに割り当てます。

## 手順 8。クラスタのサービスプリンシパルの作成

詳細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、詳細設定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。

### 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。

### 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>",
      "/subscriptions/<subscription ID>/resourceGroups/<managed_identity_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/virtualNetworks/subnets/write",
        "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write",
        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "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。
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/virtualNetworks/subnets/write	必須。サブネットの作成と更新に使用されます。
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。

権限	説明
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。
Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	マネージド ID 認証を使用してソースまたはターゲットに接続する場合に必要です。 サービスプリンシパルは、この権限を使用して、マネージド ID を仮想マシンスケールセット内の仮想マシンに割り当てます。

## 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。

## 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。

## 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。

# 手順 9. ソースとターゲットにアクセスするためのマネージド ID の作成（オプション）

ソースまたはターゲットに接続するときにマネージド ID 認証を使用するには、データへのアクセスを許可するユーザー割り当てマネージド ID を作成します。

1. `<データソース>_access_identity` という名前のマネージド ID を作成します。

2. Azure 組み込みロールの Storage Blob Data Contributor を<データソース>\_access\_identity に割り当て、データを含むストレージアカウント、リソースグループ、またはリソースへのアクセスの範囲を設定します。
3. <データソース>\_access\_identity を Secure Agent マシンに割り当てます。
4. データを含むリソースグループで、Secure Agent マネージド ID とクラスタサービスプリンシパルがデータにアクセスできるようにします。組み込みロールのマネージド ID オペレータを agent\_identity と cluster\_principal に割り当てます。

または、マネージド ID に付与される権限を制限するために、マネージド ID オペレータを使用するのではなく、カスタムロールを作成できます。次の権限をカスタムロールに割り当てます。

```
"Microsoft.ManagedIdentity/userAssignedIdentities/*/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action",
"Microsoft.Authorization/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/read"
```

**注:** 接続プロパティで、[クライアント ID] を<データソース>\_access\_identity のクライアント ID に必ず設定してください。詳細については、「[接続](#)」を参照してください。

## 手順 10.ユーザー定義のセキュリティグループの作成 (オプション)

デフォルトのセキュリティグループを使用しない場合は、独自のセキュリティグループを作成できます。

Azure で詳細クラスタを作成すると、データ統合では、デフォルトでネットワークセキュリティグループ (NSG) が作成されます。組織で独自の NSG を VNet レベルで管理する場合は、Azure 上の詳細クラスタ用に独自のネットワークセキュリティグループを作成することができます。

### 詳細クラスタのデフォルトのネットワークセキュリティグループ

データ統合は、Azure 上の詳細クラスタに対して、1 つはマスターノード用、もう 1 つはワーカーノード用の 2 つのネットワークセキュリティグループ (NSG) を生成します。これらのデフォルトの NSG のセキュリティルールを理解すると、独自のネットワークセキュリティグループを定義する場合に役立ちます。

#### マスタノードの NSG

独自のカスタム NSG を作成する前に、受信ルールと送信ルールを理解しておくに役立ちます。

次の画像は、デフォルトのマスタノードの NSG を示しています。

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
▼ Inbound Security Rules						
100	ssh-rule	22	Tcp	172.17.0.0/16	Any	Allow
101	ext-access-31447	31447	Tcp	172.17.0.0/16	Any	Allow
110	api-server-rule	6443	Tcp	172.17.0.0/16	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
▼ Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

## 受信ルール

次の表に、NSG の受信ルールとその説明を示します。

ルール	説明
SSH アクセス	このルールには、ソースとして Secure Agent マシンの IP アドレスがあります。デフォルトでは、SSH アクセスはポート 22 を介して実行されます。
Apache Livy サーバーへのアクセス	このルールには、ソースとして Secure Agent マシンの IP アドレスがあります。デフォルトでは、Livy サーバーアクセスルールでは TCP ポート 31447 が使用されます。データプレビューでは、このルールが使用されます。
Kubernetes API サーバーへのアクセス	Secure Agent は、このルールを使用して Kubernetes API サーバーにアクセスし、Kubernetes アプリケーションのデプロイと監視、クラスタリソースの監視などのタスクを実行します。 詳細クラスタの外部にある Kubernetes クライアントであっても、詳細クラスタを使用するためにこのルールが必要です。
その他のデフォルトの受信ルール	次のようなデフォルトの受信ルールも適用されます。 <ul style="list-style-type: none"><li>- VNet 内の通信。ワーカーノードによるマスタノードとの通信を許可します。</li><li>- Kubernetes 要求をマスタノードに分散するためのロードバランサからの受信トラフィック。</li></ul>

## 送信ルール

送信ルールによって、同じ VNet 内の任意のノードとインターネットへの送信トラフィックを許可します。データ統合では、特定のデプロイメントをサポートするためにさまざまな Azure サービスにアクセスする必要があります。

送信ルールを使用してインターネットへの送信トラフィックを制限する代わりに、ファイアウォールポリシーを定義して送信トラフィックを検証することもできます。詳細クラスタが設定されているサブネットを、すべてのトラフィックをファイアウォールにルーティングするルートテーブルに関連付けることができます。

ファイアウォールポリシーの使用は、宛先をドメイン名のドメイン、サブドメイン、またはワイルドカード文字にすることができるため、より柔軟な設定ができます。これにより、パブリック IP アドレスを持つインターネットサービスや、\*.windows.net、\*.azure.net、\*.microsoft.com、\*.azure.com などのさまざまな Azure サービスのアプリケーションルールを作成することができます。

NSG ルールおよびファイアウォールポリシーが存在する場合、データ統合では両方が考慮されます。

## ワーカーノードの NSG

ワーカーノードのデフォルトのネットワークセキュリティグループのルールを使用して、独自のカスタム NSG を作成します。

次の画像は、パブリック IP アドレスを使用するデフォルトのワーカーノード NSG を示しています。

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
▼ Inbound Security Rules						
100	ssh-rule	22	Tcp	172.17.0.0/16	Any	✔ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny
▼ Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✖ Deny

## 受信ルール

次の表に、NSG の受信ルールとその説明を示します。

ルール	説明
SSH アクセス	このルールは、トラブルシューティングの場合にのみ必要になります。データ統合では使用されません。 例えば、このルールを使用して、ワーカーノードからログをプルすることができます。このルールは、「 <a href="#">マスタノードの NSG</a> 」 ( <a href="#">ページ 102</a> )と同じ方法で設定します。
Azure 受信	デフォルトの受信ルールは、「 <a href="#">マスタノードの NSG</a> 」 ( <a href="#">ページ 102</a> )と同じです。
TCP 受信	TCP ポート 10250、10257、および 10259 からの受信トラフィックを許可します。

## 送信ルール

ワーカーノードの送信ルールは、マスタノードの場合と同じです。ワーカーノードは、マスタノードと同じインターネットの場所に加えて、外部データソースなどの追加の場所へのアクセスも行います。

### プライベートクラスタの使用例

次の画像は、プライベートクラスタにデプロイされた、より制限の厳しい権限が割り当てられているワーカーノードの NSG の例を示しています。

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
▼ Inbound Security Rules						
100	AllowCidrBlockSSHInbound	22	TCP	172.17.0.0/16	172.17.0.0/16	✓ Allow
110	AllowCidrBlockCustom6443Inbound	6443	TCP	172.17.0.0/16	172.17.0.0/16	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
▼ Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

## Azure 上の詳細クラスタ内のユーザー定義のセキュリティグループ

デフォルトのネットワークセキュリティグループを使用しない場合は、独自のネットワークセキュリティグループを作成できます。

Azure で独自のネットワークセキュリティグループを作成するには、次のタスクを実行します。

1. ユーザー定義の NSG を設定します。
2. ノードのリカバリに受信ルールが適用されていることを確認します。
3. エージェントロールおよびクラスタロールの権限を更新します。

### ユーザー定義の NSG の設定

データ統合によって生成されたデフォルトの NSG を、詳細クラスタ内のマスタノードおよびワーカーノード用の独自の既存の NSG に置き換えることができます。

デフォルトの NSG を独自の NSG でオーバーライドするには、次の手順を実行します。

1. Administrator を開きます。



2. **【詳細クラスタ】** を選択します。
3. リストからクラスタを選択します。
4. クラスタの **【詳細設定】** タブを選択します。
5. 以下のプロパティを設定します。
  - マスターセキュリティグループ ID
  - ワーカーセキュリティグループ ID

**ヒント:** 詳細設定にクラスタリソースグループが含まれていて、NSG がクラスタリソースグループに属している場合は、値として<NSG 名>を使用できます。

ユーザー定義の NSG を設定する場合は、次のルールとガイドラインを考慮してください。

- NSG は、クラスタと同じリージョンに存在する必要があります。
- NSG には、「[「マスターノードの NSG」 \(ページ 102\)](#)」および「[「ワーカーノードの NSG」 \(ページ 103\)](#)」に記載されているセキュリティールが必要で。
- NSG は、クラスタリソースグループとは異なるリソースグループに配置することができます。
- マスターノードとワーカーノードで同じ NSG を共有することはできますが、これは推奨されません。ワーカーノードの NSG では、通常、必要とする以上の受信トラフィックが許可されます。マスターノードの場合は、ノードを保護するために受信トラフィックを制限することが目標となります。

## ノードのリカバリへの受信ルールの適用の確認

NSG に受信セキュリティールを作成する場合は、これらのルールに他の Secure Agent マシンと互換性があることを確認してください。

独自の NSG を使用する場合、データ統合では NSG 内のルールを変更できません。Secure Agent マシンでエラーが発生し、別のマシンで Secure Agent をリカバリする必要がある場合は、マスターノードの NSG のすべての受信セキュリティールが新しい Secure Agent マシンに適用されていることを確認します。

Secure Agent マシンへの変更に対して NSG が回復性を持つようにするには、クラスタと同じ VNet 内のサブネットに Secure Agent トマシを配置します。サブネットの CIDR アドレスをこれらのルールのソースとして指定することができます。

## エージェントロールおよびクラスタロールの権限の更新

独自のネットワークセキュリティグループを使用する場合、エージェントロールおよびクラスタロールに対する一部の権限は不要になります。

Azure で独自の NSG を使用する場合は、エージェントロールおよびクラスタロールから次の権限を削除できます。

```
Microsoft.Network/networkSecurityGroups/delete  
Microsoft.Network/networkSecurityGroups/write
```

この場合も、NSG のリソースグループのスコープを持つエージェントロールおよびクラスタロールに、次の権限を付与する必要があります。

```
Microsoft.Network/networkSecurityGroups/read  
Microsoft.Network/networkSecurityGroups/join/action
```

NSG を保持するリソースグループがクラスタリソースグループと異なる場合は、NSG リソースグループで、エージェントロールおよびクラスタロールによるセキュリティグループの読み取り、およびクラスタノードへの割り当てが許可されていることを確認します。例えば、リソースグループ QA\_US\_WEST にはいくつかの NSG があるとします。データ統合のエージェントロールには、別のリソースグループ (YX-RESOURCE-GROUP) に詳細クラスタが必要です。

エージェントロールがリソースグループにアクセスできるようにするには、次のロール定義を使用して、QA\_US\_WEST の下に k8s-cluster-resource-read という名前のカスタムロールを作成します。

```
{
  "id": "/subscriptions/<subscription-id>/providers/Microsoft.Authorization/roleDefinitions/<role-def-id>",
  "properties": {
    "roleName": "k8s-cluster-resource-read",
    "description": "For k8s cluster to read/use resources in different resource group",
    "assignableScopes": [
      "/subscriptions/<subscription-id>/resourceGroups/QA_US_WEST"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Network/networkSecurityGroups/read",
          "Microsoft.Network/networkSecurityGroups/join/action",
          "Microsoft.ManagedIdentity/userAssignedIdentities/*/read",
          "Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action",
          "Microsoft.Authorization/*/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

カスタムロールを、エージェントのマネージド ID と QA\_US\_WEST のクラスタサービスプリンシパルに割り当てます。

エージェントロールおよびクラスタロールの権限を更新する場合は、次のガイドラインを考慮してください。

- エージェントのマネージド ID を、Secure Agent マシンレベルでエージェントロールに割り当てます。
- クラスタリソースグループが定義されていない場合は、クラスタリソースグループレベルまたはサブスクリプションレベルで、クラスタサービスプリンシパルをクラスタロールに割り当てます。

## クラスタの事前検証エラーのトラブルシューティング

クラスタの事前検証が失敗する原因となる条件を把握しておく、後々の問題を回避する場合に役立ちます。

クラスタの事前検証は、次のいずれかの条件が発生すると失敗します。

- NSG のリソースグループを識別できない。例えば、NSG がリソースグループなしで設定されており、詳細設定にクラスタリソースグループが定義されていない場合。
- NSG がクラスタと別のリージョンにある。
- NSG がリソースグループに存在しない。
- マスタノードまたはワーカーノードに NSG が定義されていない。
- 読み取りと参加の権限が、エージェントまたはクラスタロールの NSG リソースグループに割り当てられていない。

これらのエラーケースのほとんどでクラスタの作成はすぐに失敗しますが、権限の欠落によるエラーは、クラスタノードが作成されるまで表示されない場合があります。

## 手順 11.JAVA\_HOME 環境変数の設定（オプション）

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 17 と互換性がある必要があります。

## 手順 12.ステージング接続の作成（オプション）

Secure Agent マシンに、クラスタのステージングの場所にアクセスできるシステムによって割り当てられたマネージド ID または単一のユーザーが割り当てたマネージド ID がない場合は、ステージングの場所へのステージング接続を作成して、詳細クラスタがステージングデータをデータ統合サーバーと共有できるようにします。

1. Administrator で、**接続** ページを開きます。
2. Azure Data Lake Storage Gen2 への接続を作成します。  
接続プロパティで、ステージングファイルを保存するために「[手順 2. クラスタファイルのストレージアカウントの作成](#)」(ページ 92)で作成した場所のストレージアカウント名を入力します。
3. **詳細クラスタ** ページを開きます。
4. 詳細設定を作成するか、クラスタ用の既存の詳細設定を編集します。
5. **プラットフォーム設定** タブで、接続プロパティに入力したものと同一ストレージアカウント名を指定するようにステージングの場所を構成します。バケット内のフォルダパスを指定できます。
6. **ランタイムプロパティ** タブで、プロパティ clusterconfig.stagingConnectionName を追加して、値を接続の名前に設定します。

## 第 5 章

# セルフサービスクラスタの設定

Secure Agent が Kubernetes クラスタに接続し、組織内のセルフサービスクラスタとして使用できるように、クラウド環境を設定します。

以下のタスクを完了させます。

1. 前提条件を満たしていることを確認します。必要な特権があることを確認し、クラウド環境でのリソースアクセスについて理解します。
2. Secure Agent をダウンロードしてインストールします。最小リソース要件を満たす仮想マシンにエージェントをセットアップします。
3. ドメインを許可します。クラスタは、特定のドメインにアクセスして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必要があります。
4. Secure Agent で kubconfig ファイルをダウンロードして設定します。
5. Pod や ConfigMap などの Kubernetes クラスタリソースへのアクセスを許可する権限を持つ Kubernetes ClusterRole を作成します。また、ClusterRole と Role を組み合わせて作成し、権限をさらに制限することもできます。
6. Secure Agent とセルフサービスクラスタがステージングデータとログファイルを保存できるようにするためのストレージロールを作成します。
7. データソースへのアクセスを設定して、セルフサービスクラスタがマッピング内のデータの読み取りおよび書き込みを行えるようにします。

AWS でセルフサービスクラスタを使用するには、クラスタ認証の設定などの追加の手順を実行します。

次の YouTube ビデオでは、Amazon EKS で Kubernetes クラスタを作成し、それをデータ統合のセルフサービスクラスタとして登録する方法について説明しています。

[Setting up a Self-Service Cluster on Amazon EKS in Cloud Data Integration](#)

## 手順 1。前提条件の完了

環境をセットアップする前に、前提条件のタスクを実行します。

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。
- Secure Agent とセルフサービスクラスタ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について説明します。

## 組織の権限の確認

組織の詳細設定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。

詳細設定に対する特権によって、Administrator および Monitor の **【詳細クラスタ】** ページへのアクセスレベルは異なります。

詳細設定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징およびログの場所などの、ジョブの一部であるリソースにアクセスします。

エージェントとクラスタはリソースにアクセスして、次のタスクを実行します。

- マッピングの設計。
- セルフサービスクラスタへの接続。
- データプレビュージョブを含むジョブの実行。
- ログのポーリング。

### マッピングの設計

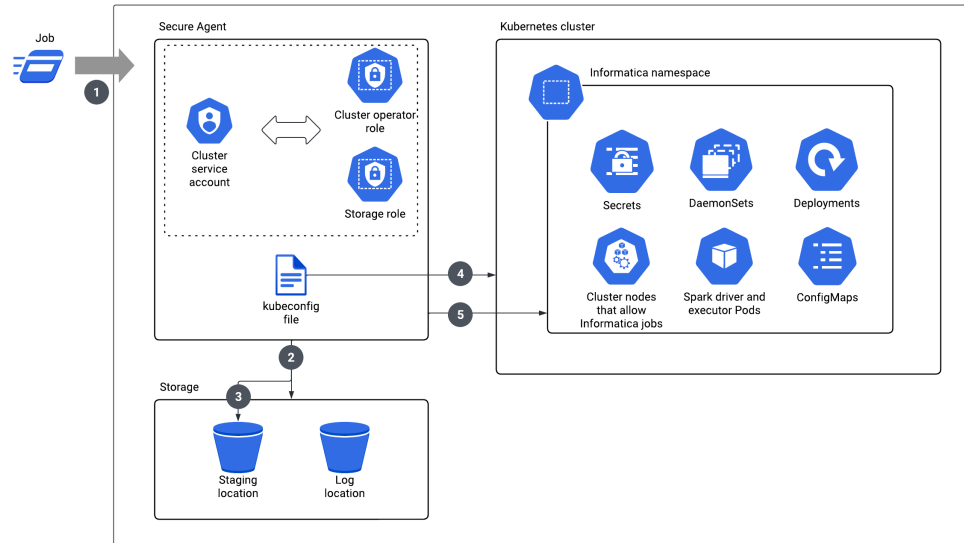
マッピングを設計すると、Secure Agent はソースとターゲットにアクセスするため、ユーザーはデータの読み取りと書き込みができます。例えば、ソーストランスフォーメーションをマッピングに追加する場合、Secure Agent ではソースにアクセスして残りのマッピングで利用できるフィールドを表示します。Secure Agent はデータのプレビュー時にもソースにアクセスします。

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への接続

Kubernetes クラスタをセルフサービスクラスタとして使用するために、Secure Agent は Kubernetes クラスタに接続し、クラスタ内の特定の名前空間内に Informatica 固有の Kubernetes リソースを作成します。

次の画像は、Secure Agent が Kubernetes クラスタとどのように対話するかを示しています。



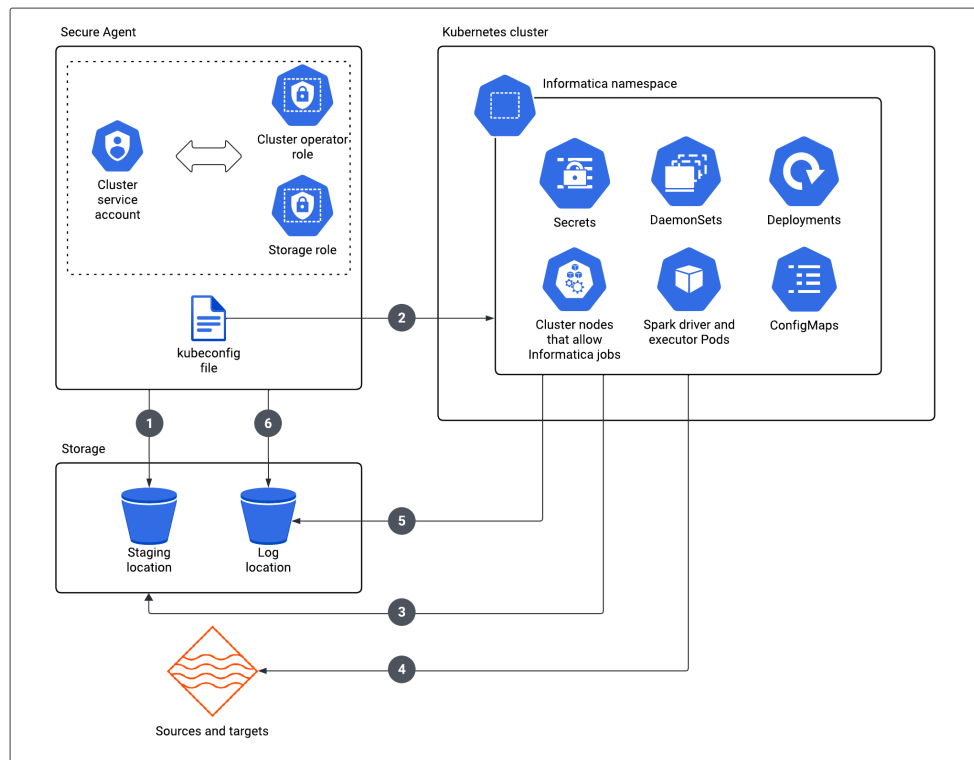
1. ジョブを実行します。
2. Secure Agent は、ストレージロールを使用して、クラスタがステージングおよびログの場所にアクセスできることを確認します。
3. Secure Agent は、ストレージロールを使用してクラスタの詳細をステージング場所に格納します。
4. Secure Agent は、kubeconfig ファイルを使用してクラスタにアクセスします。
5. Secure Agent は、kubeconfig ファイルで Kubernetes ユーザーに定義された権限を使用して、Pod、ConfigMaps、DaemonSet などの Kubernetes リソースを作成します。

## ジョブの実行

ジョブを実行するために、Secure Agent と Kubernetes クラスタの Informatica 固有の名前空間内のリソースは、ステージングとログの場所、およびジョブのソースとターゲットにアクセスします。ジョブ内のデータを処理するために、Informatica は、ノードラベルと許容によって Informatica に割り当てた Kubernetes クラスタ内のノードを使用します。

開発者がデータ統合などのサービスからジョブを実行すると、Spark ジョブからの保留中の Kubernetes Pod によって、Kubernetes クラスタにデプロイした Cluster AutoScaler を介して Kubernetes クラスタがスケールアウトされることもあります。

次の画像は、Secure Agent とセルフサービスクラスタがリソースにアクセスしてジョブを実行する方法を示しています。



1. Secure Agent は、ストレージロールを使用してジョブの依存関係をステージング場所に格納します。ストレージロールの詳細については、「[手順 6.ストレージロールの作成](#)」(ページ 117)を参照してください。
2. Secure Agent は、kubeconfig ファイルを使用してジョブを Kubernetes クラスタに送信し、Informatica 固有のノードで実行します。
3. Spark Pod はストレージロールを使用してステージングの場所にアクセスし、ジョブの依存関係を取得して一時データのステージングを行います。
4. Spark Pod は、接続レベルの権限を使用してソースデータにアクセスします。
5. Spark Pod は、ストレージロールを使用して、ログの場所にログを格納します。
6. Secure Agent は、ストレージロールを使用して、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 はストレージロールを使用します。

## 手順 2。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 インスタンスまたは Azure 仮想マシンにすることができます。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。

## 手順 3。セルフサービスクラスタのドメインの許可

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。

次のドメインを送信許可リストに追加します。

`artifacthub.informaticacloud.com`

EMEA POD のいずれかを使用する場合は、次のドメインも許可してください。

`artifacthubemea.informaticacloud.com`

[EMEA PODs](#) には、EM West1、EM Central1 Azure、UK、EM SouthEast 1 Azure、ME Central 2 GCP、EM West 2 GCP が含まれます。

さらに、データソースを含むすべてのドメインを許可する必要があります。

## 手順 4。Secure Agent で kubeconfig ファイルをダウンロードして設定する

仮想ネットワークに Kubernetes クラスタを作成するか、既存のクラスタを使用します。Secure Agent マシンにアップロードする kubeconfig ファイルを取得します。必要に応じて、サポートされている認証メカニズムおよび承認メカニズムに従ってファイルをカスタマイズします。

サポートされている Kubernetes バージョンを使用しており、クラスタが最小リソース仕様を満たしていることを確認してください。詳細については、

「[Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#)」、および「[クラスタノードのリソース要件](#)」(ページ 160)」を参照してください。



クラスタのネットワークとパフォーマンスを最適化するには、セルフサービスクラスタで Calico プラグインを使用します。詳細については、[Project Calico documentation](#) を参照してください。

## 注釈と許容の追加（オプション）

注釈を定義してクラスタにメタデータをアタッチしたり、許容を定義してクラスタが実行されるノードを制御したりすることができます。

### 注釈

注釈により、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、オブジェクトが最後に更新された日付、オブジェクトを管理するユーザーの名前、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あります。注釈は、リソースに関するコンテキストを提供するための、あらゆる種類の有用な情報を保持します。注釈は通常、マシンによって生成されたデータで構成されます。注釈内のメタデータは小さいものや大きいもの、構造化されているものや構造化されていないものである場合があります、ラベルでは許可されていない文字が含まれる場合もあります。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します。

### 許容

許容（Toleration）とは、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ための Kubernetes ポッドのプロパティです。Taint は、ノードがポッドのセットを排除できるようにするための Kubernetes ノードのプロパティです。許容はポッドに適用されます。Taint と許容は連携して、不適切なノードにポッドがスケジュールされないようにします。

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。

注釈と許容をクラスタにアタッチした後に、詳細設定の【**詳細設定**】タブで、それらの注釈と許容がキーと値のペアとして設定されていることを確認してください。詳細については、「[詳細設定](#)」（[ページ 159](#)）を参照してください。

## 手順 5.Kubernetes ClusterRole および Role の作成

Pod や ConfigMap などの Kubernetes クラスタリソースへのアクセスを許可する権限を持つ Kubernetes ClusterRole を作成します。また、ClusterRole と Role の組み合わせを作成して、Kubernetes クラスタでの Informatica の権限をさらに制限することもできます。

以下のタスクを完了させます。

1. ロールの権限を設定します。
2. ロールバインディングを作成します。

迅速なセットアップが必要な場合は、Informatica が管理するサービスアカウントを使用できます。詳細については、「[Informatica が管理するサービスアカウントの使用（代替）](#)」（[ページ 116](#)）を参照してください。

## ロールの権限の設定

Kubernetes ClusterRole に権限を設定して、Kubernetes クラスタ内のリソースを作成および管理します。

次の表に、ClusterRole がアクセスする必要がある各リソースとその説明を示します。

リソース	説明
サービス	Kubernetes Pod 間の通信に使用されます。
ポッド	Spark ドライバと Spark エグゼキュータを実行するために使用されます。
Secrets	機密性の高いメタデータを Kubernetes Pod に渡すために使用されます。
Configmaps	Spark の設定を Kubernetes Pod に渡すために使用されます。
DaemonSets	Spark シャッフルサービスのデプロイに使用されます。
デプロイ	Kubernetes Pod がキーを使用して Secure Agent にアクセスできるように、クラスタにキーストアをデプロイするために使用されます。

必要な権限は、クラスタが Spark シャッフルサービスを使用してマッピングを実行するかどうかによって異なります。Spark シャッフルサービスは、クラスタが Spark ジョブの動的割り当てを実行する場合に役立ちます。このサービスは、エグゼキュータの存続期間を超えてシャッフルファイルを永続化する責任を負い、計算を失わずにエグゼキュータの数を増減できるようにします。

ClusterRole はグローバルであり、名前空間には関連付けられていません。権限を特定の名前空間に制限する必要がある場合は、ClusterRole の権限を 2 つの異なるロールに分割することができます。

### Spark シャッフルサービスを使用してマッピングを実行するための最小権限

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: ["daemonsets", "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"]
```

このコードスニペットの権限は、すべての名前空間に適用されます。

権限を特定の名前空間のみに制限する必要がある場合は、これらの権限を 2 つのロール（Role と ClusterRole）に分割します。ClusterRole にはグローバルなリソースに対する権限が含まれ、Role には名前空間に固有のリソースに対する権限が含まれます。

次のコードスニペットは、Role の権限を示しています。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
```

```

name: rbac-informatica-np-admin
namespace: informatica
rules:
- apiGroups: [""]
  resources: ["services", "pods", "secrets", "configmaps"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]
- apiGroups: ["apps"]
  resources: ["daemonsets", "deployments"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]

```

次のコードスニペットは、ClusterRole の権限を示しています。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: rbac-informatica-global-admin
rules:
- 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を使用せずにマッピングを実行するための最小権限

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

```

このコードスニペットの権限は、すべての名前空間に適用されます。

権限を特定の名前空間のみに制限する必要がある場合は、これらの権限を 2 つのロール（Role と ClusterRole）に分割します。ClusterRole にはグローバルなリソースに対する権限が含まれ、Role には名前空間に固有のリソースに対する権限が含まれます。

次のコードスニペットは、Role の権限を示しています。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: rbac-informatica-np-admin
  namespace: informatica
rules:
- apiGroups: [""]
  resources: ["services", "pods", "secrets", "configmaps"]
  verbs: ["watch", "list", "get", "create", "update", "patch", "delete", "deletecollection"]

```

次のコードスニペットは、ClusterRole の権限を示しています。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: rbac-informatica-global-admin
rules:
- apiGroups: [""]

```

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

## ジョブの優先度を有効にする権限（オプション）

必要に応じて、ジョブの優先度を有効にして、開発者がデータ統合のマッピングタスクに対して設定したジョブの優先度に従って、クラスタロールがセルフサービスクラスタ上でジョブをスケジュールできるようにすることができます。

ジョブの優先度を有効にするには、次のタスクを実行します。

1. クラスタのロールに次の権限を付与します。
 

```
rules:
- apiGroups: ["scheduling.k8s.io"]
  resources: ["priority classes"]
  verbs: ["list", "create", "update", "patch", "delete"]
```
2. 詳細設定で次のカスタムプロパティを設定します。
 

```
ccs.enable.app.priority=true
```

## ロールバインディングの作成

ロールで定義された権限を付与するには、クラウドユーザーと Kubernetes ClusterRole および Role の間にロールバインディングを作成します。

例えば、Informatica 固有の名前空間にサービスアカウントを作成し、そのサービスアカウントトークンを kubeconfig ファイルに追加できます。次に、サービスアカウントとロールの間にロールバインドを作成します。

**注:** サービスアカウントを使用する場合は、詳細設定の【ランタイム設定】タブを開き、プロパティ `infa.k8s.spark.custom.service.account.name` をサービスアカウント名に設定します。

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。

## Informatica が管理するサービスアカウントの使用（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、デフォルトのサービスアカウント、クラスタロール、およびクラスタロールバインディングを作成します。

Informatica は、Spark ドライバ用に `infa-spark` というサービスアカウントと `infa-spark-role` というクラスタロールバインディングを作成します。このクラスタロールバインディングでは、Kubernetes クラスタで利用できるデフォルトのクラスタロール `edit` を使用します。`edit` 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。`edit` ロールの詳細については、Kubernetes のドキュメントを参照してください。

Spark シャッフルサービスを有効にすると、Informatica は、クラスタ上に個別のサービスアカウント、クラスタロール、およびクラスタロールバインディングを作成します。Informatica は、次のクラスタロール権限をサービスアカウントに割り当てます。

```
---
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"]

```

## 手順 6.ストレージロールの作成

Secure Agent とセルフサービスクラスタがステージングとログの場所にアクセスして、ステージングデータとログファイルを保存できるようにするためのストレージロールを作成します。ストレージロールを設定する手順は、クラウドプラットフォームに応じて異なります。

### AWS でのストレージロールの作成

セルフサービスクラスタが AWS 上にある場合は、ステージングとログの場所にアクセスできる IAM ロールを作成し、そのロールを Kubernetes ユーザー管理サービスアカウントに関連付けます。

Amazon EKS では、クラスタノードのインスタンスプロファイルにストレージロールを追加するか、Informatica に割り当てるサービスアカウントにロールをアタッチできます。

**ヒント:** 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。

1. AWS で、storage\_role という名前の IAM ロールを作成します。
2. 次の IAM ポリシーを storage\_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、ワイルドカード文字を使用できます。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 `storage_policy` を IAM ロール `storage_role` にアタッチします。
4. ストレージロールの信頼関係を設定して、Secure Agent マシンにアタッチされている Secure Agent ロールを含めます。

Secure Agent はストレージロールを引き受ける必要があるため、Secure Agent がストレージロールで信頼済みとみなされている必要があります。

IAM ロール `storage_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 のみがストレージロールを引き受けることができるように外部 ID を設定することができます。

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 でのストレージロールの作成

セルフサービスクラスタが Microsoft Azure 上にある場合は、ステージングとログの場所にアクセスできるストレージロールを持つマネージド ID を作成し、その ID を Secure Agent マシンに関連付けます。

**ヒント:** マネージド ID の作成手順の詳細については、Microsoft Azure のマニュアルを参照してください。

1. Azure で、storage\_identity という名前のマネージド ID を作成します。

システム割り当ての既存のマネージド ID を使用するか、ユーザー割り当てのマネージド ID を作成することができます。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。

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

```

{
  "properties":{
    "roleName":"storage_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":[
        ]
      }
    ]
  }
}

```

3. カスタムロール storage\_role を storage\_identity という名前のマネージド ID に割り当てます。
4. マネージド ID storage\_identity を Secure Agent マシンに割り当てます。

## 手順 7. データソースへのアクセスの設定

セルフサービスクラスタによるデータソースへのアクセスを許可して、マッピング内のデータの読み取りと書き込みを行えるようにします。

セルフサービスクラスタは、組織で設定された接続を使用してデータソースにアクセスします。接続で IAM ロールまたはマネージド ID を作成する必要がある場合は、クラウドプラットフォームに基づいてクラスタによる使用を許可します。

- AWS で、IAM ロールを Kubernetes ユーザー管理サービスアカウントにアタッチします。
- Microsoft Azure で、マネージド ID を Secure Agent マシンに割り当てます。

**注:** Azure ADLSGen2 接続にマネージド ID を設定する場合は、データ統合ジョブを実行できるすべてのクラスタノードにマネージド ID が割り当てられていることを確認してください。

## AWS 上のクラスタの追加設定

AWS でセルフサービスクラスタを使用するには、クラスタ認証の設定やホップ制限の設定などの追加の構成手順を実行します。

### クラスタ認証の設定

AWS でセルフサービスクラスタを作成する場合、AWS CLI を使用して、Secure Agent がクラスタに対して認証できるようにすることができます。クラスタ認証を設定する前に、AWS CLI が Secure Agent マシンにインストールされていることを確認します。

AWS CLI を使用して、kubeconfig ファイルで AWS 資格情報を指定します。AWS CLI を使用して、使用する適切なプロファイルを定義します。exec フローで設定した環境変数は、環境内で設定された環境変数よりも優先されます。

次のサンプルコマンドは、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 を設定する方法を示しています。

```
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
```

Kubernetes 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 でセルフサービス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。

**注:** AWS CLI 認証を使用するクラスタでは、資格情報の有効期間を超えてマッピングが実行されると、失敗する可能性があります。これを防ぐためには、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します。



## IMDSv2 を使用するクラスタノードの設定

Instance Metadata Service Version 2 (IMDSv2) を使用するノードで AWS のセルフサービスクラスタを設定する場合は、クラスタノードのホップ制限が 2 になっていることを確認します。

Amazon EKS でセルフサービスクラスタを作成する場合、デフォルトではクラスタノードのホップ制限は 2 です。

詳細については、AWS のマニュアルを参照してください。

## 第 6 章

# ローカルクラスタの設定

組織で詳細設定を作成する前に、Secure Agent がローカルクラスタを作成できるようにクラウド環境を設定します。

次のタスクを完了して、ローカルクラスタをセットアップします。

1. 準備のための手順を完了します。
2. Secure Agent をダウンロードしてインストールします。
3. ローカルクラスタをトラブルシューティングします。

## ローカルクラスタ用の準備

ローカルクラスタをデプロイする前に、許可リストにドメインを追加したり、OS ファイアウォールを無効化したりするなどの準備手順を完了します。ローカルクラスタは、詳細モードのマッピングを実行します。

ローカルクラスタをデプロイする前に、次の準備手順を完了していることを確認してください。

- 次のドメインをローカルクラスタの送信許可リストに追加し、それらが Secure Agent マシンから到達可能であることを確認します。

```
artifacthub.informaticacloud.com  
rhui3.<region>.<cloud>.ce.redhat.com (RHEL 8.x)
```

例: rhui3.us-west-2.aws.ce.redhat.com

ローカルクラスタは、これらのドメインにアクセスして、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必要があります。

EMEA POD のいずれかを使用する場合は、次のドメインも許可してください。

```
artifacthubemea.informaticacloud.com
```

[EMEA PODs](#) には、EM West1、EM Central1 Azure、UK、EM SouthEast 1 Azure、ME Central 2 GCP、EM West 2 GCP が含まれます。

- Secure Agent マシンで RHEL 9.x を実行しており、ローカルクラスタを使用して詳細マッピングを実行する場合は、Docker バージョン 20 が Secure Agent マシンにインストールされていることを確認してください。ローカルクラスタを実行する場合、Docker バージョン 21 以降を使用することはできません。
- Secure Agent マシンで次のコマンドを実行して、OS ファイアウォールを無効にします。

```
sudo systemctl disable firewalld
```

OS ファイアウォールを無効にすると、ローカルクラスタに送信されるジョブの中断を防ぐことができます。

# Secure Agent のダウンロードとインストール

ローカルクラスタには Secure Agent が必要です。ローカル Linux マシンに Secure Agent をダウンロードしてインストールします。

## 手順 1: ソフトウェアとハードウェアの要件の確認

サポートされているバージョンの Linux を実行していることを確認します。Secure Agent でサポートされている Linux オペレーティングシステムのリストについては、ナレッジベースの [Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#) を参照してください。

マシンがローカルクラスタをセットアップするための最小ハードウェア要件を満たしていることを確認します。

- 8 つの vCPU、32GB のメモリ
- ルートボリューム用に 100GB のディスク容量
- ルートボリュームの/var 用に 20GB のディスク容量
- ルートボリュームの/tmp 用に 30 GB のディスク容量

クラスタが起動時にハングしないようにするには、/var と /tmp のそれぞれに少なくとも 30GB のディスク領域を割り当てます。

## 手順 2: NOPASSWD sudo 特権の確認

Secure Agent でローカルクラスタを実行するには、Secure Agent を起動するユーザーに、Secure Agent マシンでの NOPASSWD sudo 特権が必要です。NOPASSWD 特権を付与できない場合は、次のいずれかの回避策を実行してください。

### pmsuid ファイルを使用する

1. <Secure Agent home>/apps/At\_Scale\_Server/<latest version>/bin/Linux.64/から、pmsuid を <Secure Agent home>/apps/At\_Scale\_Server/ext/にコピーする
2. pmsuid の所有者とグループを root に変更し、ファイルの setgid ビットを設定します。
3. ローカルクラスタのランタイムプロパティセクションで ccs.localcluster.deployment.mode=SUID を設定します。
4. Monitor を使用してローカルクラスタを停止し、ジョブを実行してクラスタを再開します。

### sudoers ファイルの更新

/etc/sudoers ファイルを編集して、次の行を追加します。

```
<user ID> ALL=(ALL) NOPASSWD: /usr/bin/docker, /usr/bin/kubeadm, /usr/bin/tee, /usr/bin/yum, /usr/sbin/modprobe, /usr/sbin/sysctl, /usr/bin/systemctl, /usr/sbin/swapoff, /usr/bin/chown, /usr/bin/cp, /usr/bin/rm
```

<user ID>は、Secure Agent マシンで sudo 特権を持たない非 root ユーザーです。

## 手順 3: Secure Agent のダウンロードとインストール

ローカル Linux マシンに Secure Agent をダウンロードしてインストールします。Secure Agent のインストールの詳細については、「ランタイム環境」の「Linux での Secure Agent のインストール」を参照してください。

# ローカルクラスタのトラブルシューティング

詳細クラスタの起動に失敗したのはなぜですか。

詳細クラスタの起動に失敗した理由をトラブルシューティングするには、Secure Agent マシンの<Secure Agent installation directory>/apps/At\_Scale\_Server/<version>/ccs\_home/ディレクトリにある ccs-operation.log ファイルを調査します。

ccs-operation.log は問題の解決に役立ちませんでした。他にどこを調べればよいですか。

ccs-operation.log ファイルで問題の解決に役立つ情報が十分になかった場合、詳細クラスタのインスタンス専用である cluster-operation.log ファイルを確認してみてください。

外部コマンドセットを実行すると、ccs-operation ログに cluster-operation ログへのパスが表示されます。  
例:

```
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> ; ].
```

実行ログは次の場所にあります。

```
/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。

ジョブがローカルクラスタで処理されないのはなぜですか？

OS ファイアウォールが原因で、ワーカーノードがローカルクラスタにジョブを送信して処理できなくなっている可能性があります。

次のコマンドを使用して、ファイアウォールが実行中かどうかを確認します。

```
sudo firewall-cmd --state
```

このコマンドの出力に「running」と表示されている場合、ファイアウォールはアクティブです。

次のコマンドを使用して OS ファイアウォールデーモンを無効にします。

```
sudo systemctl disable firewalld
```

## 第 7 章

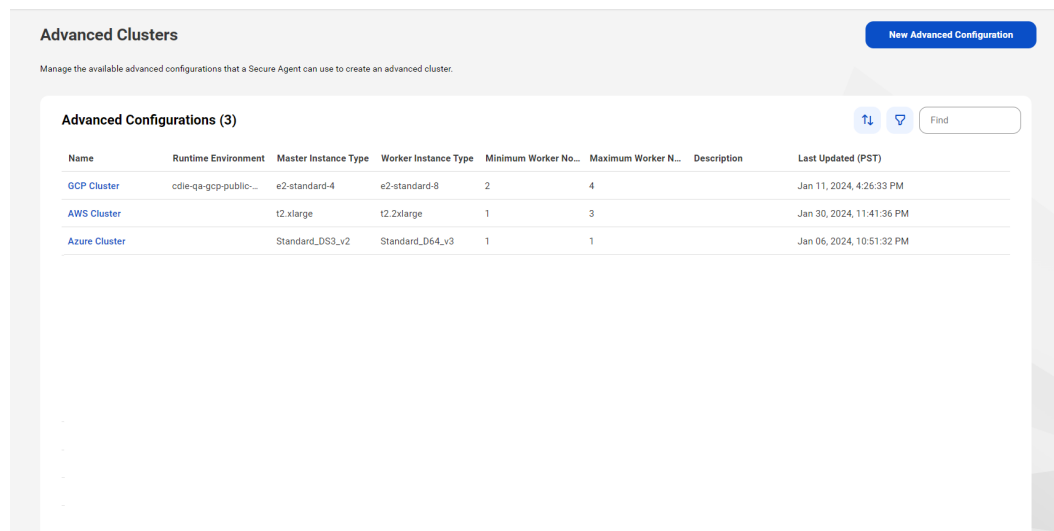
# 詳細設定

詳細設定は、詳細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。詳細設定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。

詳細設定は、**【詳細クラスタ】** ページで作成します。詳細設定でのプロパティの設定時に、設定をランタイム環境と関連付けることができます。既存の設定から詳細設定を作成できます。新しい設定は、既存の設定をテンプレートとして使用します。新しい設定にランタイム環境を指定することができます。また、他のプロパティを編集することもできます。

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、**【詳細クラスタ】** ページを示しています。



The screenshot shows the 'Advanced Clusters' management interface. It features a table titled 'Advanced Configurations (3)' with columns for Name, Runtime Environment, Master Instance Type, Worker Instance Type, Minimum Worker No., Maximum Worker N., Description, and Last Updated (PST). Three configurations are listed: GCP Cluster, AWS Cluster, and Azure Cluster.

Name	Runtime Environment	Master Instance Type	Worker Instance Type	Minimum Worker No.	Maximum Worker N.	Description	Last Updated (PST)
GCP Cluster	cdle-q&gcp-public...	e2-standard-4	e2-standard-8	2	4		Jan 11, 2024, 4:26:33 PM
AWS Cluster		t2.xlarge	t2.2xlarge	1	3		Jan 30, 2024, 11:41:36 PM
Azure Cluster		Standard_DS3_v2	Standard_D64_v3	1	1		Jan 06, 2024, 10:51:32 PM

詳細設定を使用してジョブを実行するには、詳細設定に関連付けられたランタイム環境を使用します。

詳細クラスタの実行時に詳細設定を編集する場合は、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、実行中のジョブが停止します。別のジョブを実行すると、クラスタが再び開始されます。

既存の設定から新しい詳細設定を作成できます。新しい設定は、既存の設定をテンプレートとして使用します。新しい設定では任意のフィールドを変更できますが、デフォルトでは、**【ランタイム環境】** フィールドのみを変更する必要があります。

詳細設定は、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」 \(ページ 174\)](#)」を参照してください。

# CLAIRE を利用した設定

CLAIRE を利用した設定を使用して、予算内に収まる詳細クラスタを作成します。Informatica の AI エンジンである CLAIRE を使用すると、クラスタインフラストラクチャを選択し、クラウドインフラストラクチャの推定節約額をレポートして、長期にわたるインフラストラクチャコストを視覚化し、インサイトと推奨事項を生成できます。これにより、詳細クラスタで発生するコストの透明性が提供され、組織内で FinOps 機能が有効になります。

組織で CLAIRE の推奨事項が有効になっている場合は、CLAIRE を利用した設定を使用して、AWS 環境で詳細クラスタを作成できます。

CLAIRE を利用した設定を使用すると、コストまたはパフォーマンスを考慮してクラスタを最適化できます。次に、時間あたりのターゲット平均コストと時間あたりの最大コストを指定すると、CLAIRE は予算内に収まるようにクラスタを設定します。

コストが最適化されたクラスタの場合、インフラストラクチャのコストが時間あたりの平均コストを超える可能性は低くなりますが、優先度が中および低のジョブの実行には時間がかかる可能性があります。パフォーマンスが最適化されたクラスタの場合、特に大規模なワークロードについては、インフラストラクチャのコストが時間あたりの平均コストを超える可能性が高くなります。ただし、通常、ジョブは短時間で実行され、より短いターゲット期間を達成できます。

CLAIRE は、時間あたりの最大コストが 1.00 米ドルを超えている限り、詳細クラスタを作成できます。時間あたりのターゲット平均コストと最大コストを調整するには、Monitor を使用して、クラスタで発生するインフラストラクチャコストを確認します。実際のインフラストラクチャコストが時間あたりの最大コストに近い場合、またはワークロードの実行時間を短縮したい場合は、最大コストを増やすことができます。実際のインフラストラクチャコストよりもはるかに高い時間あたりの最大コストを設定すると、CLAIRE ではクラスタに必要なクラウドリソースのみが使用されます。

CLAIRE が管理するインフラストラクチャのコストには、コンピューティングインスタンス、ストレージ、エラスティックロードバランサのコストが含まれます。インフラストラクチャのコストを予算内に抑えるために、CLAIRE は次のタスクを実行します。

- 必要に応じて、オンデマンドインスタンスではなくスポットインスタンスを選択します。CLAIRE は、コストが最適化されたクラスタ内でのみスポットインスタンスを選択します。
- クラスタの最適化設定と、クラスタが一般的なワークロードを実行するために使用するリソースに基づいて、インスタンスタイプを選択します。
- 予期されるワークロードに基づいてクラスタとローカルストレージを拡張します。
- クラスタリソースを効率的に使用するためにジョブをスケジュールします。
- クラスタがアイドル状態になると予想される場合、クラスタをシャットダウンします。

CLAIRE は、データ転送コスト、ディスク操作コスト、および IPU コストを管理しません。これらのコストは、クラスタ上で実行するワークロードに応じて異なります。CLAIRE は、ワークロードに依存するコストを削減し、クラスタのパフォーマンスを向上させるための推奨事項を **【推奨事項】** パネルに生成します。

## クラスタの予算の見積もり

CLAIRE は、時間あたりのターゲット平均コストを使用して、クラスタの作成方法とクラスタインフラストラクチャコストの制御方法を決定します。また、時間あたりの最大コストを使用して、クラスタが実行するワークロードに基づいて到達可能なワーカーノードの最大数を最適化します。

CLAIRE は、クラスタが実行するワークロードが不明である場合、クラスタの初めての起動時にワーカーノードのデフォルトの最小数と最大数を使用します。CLAIRE は、クラスタメタデータを収集して処理を行うことで一般的なクラスタワークロードについて学習し、クラスタバジェットに基づいて、到達可能なワーカーノードの最大数までワーカーノードを更新します。ワークロードの数が予想よりも少ない場合、クラスタのワーカーノードの数は開始時よりも少なくなることがあります。

次の表を使用して、予算に基づいてクラスタで使用するワーカーノードの数を見積もることができます。通貨の値は米ドルです。

### コストの最適化

次の表に、特定の予算に基づいてコストが最適化されたクラスタ上のワーカーノードの最小数と最大数を示します。

時間あたりのターゲット平均コスト	時間あたりの最大コスト	ワーカーノードのデフォルトの数	ワーカーノードの最大到達可能数
\$1	\$2	Min: 1 最大: 3	Min: 1 最大: 5
\$1	\$5	Min: 1 最大: 5	Min: 1 最大: 13
\$4	\$10	Min: 1 最大: 14	Min: 1 最大: 28
\$4	\$15	Min: 1 最大: 17	Min: 1 最大: 42

スポットインスタンスが有効になっている場合、クラスタは常に少なくとも 1 つのワーカーノードを使用するため、CLAIRE は必要に応じてスポットインスタンスをクラスタに追加することができます。スポットインスタンスを無効にすると、ワーカーノードの最小数が変更される可能性があります。

### パフォーマンスの最適化

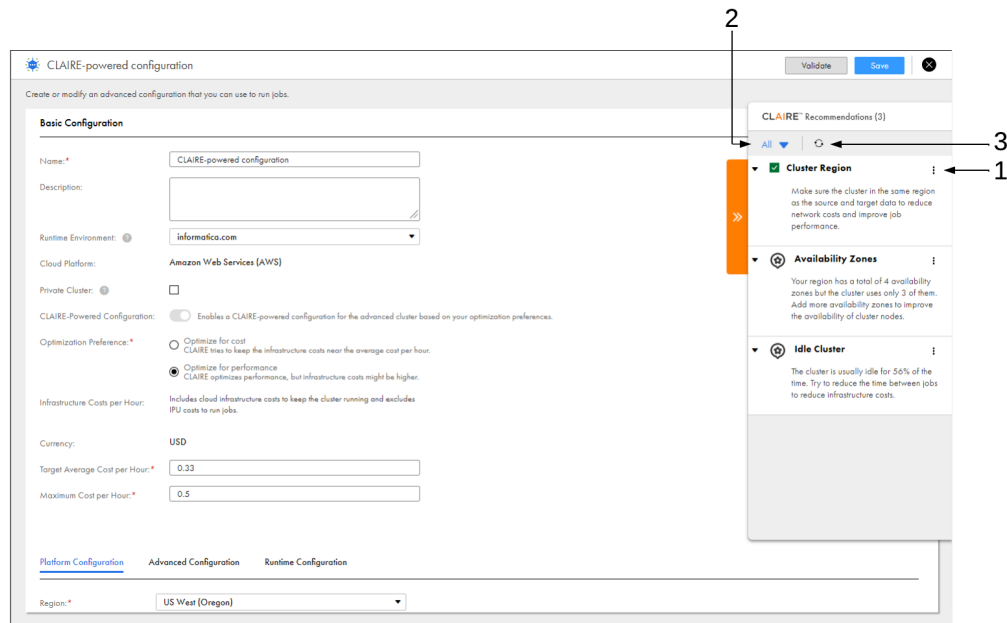
次の表に、特定の予算に基づいてパフォーマンスが最適化されたクラスタ上のワーカーノードの最小数と最大数を示します。

時間あたりのターゲット平均コスト	時間あたりの最大コスト	ワーカーノードのデフォルトの数	ワーカーノードの最大到達可能数
\$1	\$5	Min: 1 最大: 7	Min: 1 最大: 9
\$5	\$10	Min: 5 最大: 15	Min: 9 最大: 18
\$5	\$15	Min: 5 最大: 22	Min: 9 最大: 28
\$10	\$20	Min: 9 最大: 31	Min: 18 最大: 38

## CLAIRE の推奨事項

**【推奨事項】** パネルで、クラスタのパフォーマンスを向上させ、インフラストラクチャのコストを削減するための CLAIRE の推奨事項を表示します。**【推奨事項】** パネルは、CLAIRE を利用した設定で利用できます。

次の図に、**【推奨事項】** パネルを示します。



### 1. 【アクション】メニュー

**【アクション】** メニューを使用して、推奨事項に完了または未完了というマークを付けたり、推奨事項をオプトインおよびオプトアウトしたりすることができます。

CLAIRE は、スポットインスタンスの使用など、一部の推奨事項を自動的に適用します。**【アクション】** メニューを使用して、推奨事項をオプトアウトしたり、再度オプトインしたりすることができます。

クラスタージョンの変更などの他の推奨事項では、手動アクションが必要です。これらの推奨事項は To Do 項目として表示されます。**【アクション】** メニューを使用して、To Do 項目に完了または未完了というマークを付けることができます。推奨事項をオプトアウトしたり、再度オプトインしたりすることもできます。

### 2. 推奨事項のフィルタリング

**【フィルタ】** メニューを使用して、推奨事項をフィルタリングします。次のようなフィルタを使用できます。

- **【すべて】** を使用すると、すべての推奨事項が表示されます。
- **【To Do】** を使用すると、手動アクションが必要な推奨事項が表示されます。
- **【適用済み】** を使用すると、自動的に適用された推奨事項、および完了というマークが付いた推奨事項が表示されます。
- **【オプトアウト】** を使用すると、オプトアウトされた推奨事項が表示されます。

### 3. 推奨事項の更新

**【推奨事項】** パネルの推奨事項を更新したり、Monitor を使用して、組織内の詳細クラスタで新しい推奨事項が利用可能かどうかを確認したりする場合に、推奨事項を更新します。



注: CLAIRE を利用した設定に関連付けられているランタイム環境を変更すると、CLAIRE によって【推奨事項】パネルの推奨事項がクリアされます。

## AWS のプロパティ

詳細設定を作成して、詳細クラスタのプロパティを設定します。プロパティにより、クラウドプラットフォーム上のクラスタを開始する場所と、使用するインフラストラクチャを記述します。

### 基本設定

次の表に、基本プロパティを示します。

プロパティ	説明
名前	詳細設定の名前。
説明	詳細設定の説明。
ランタイム環境	詳細設定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詳細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。

### CLAIRE を利用した設定

CLAIRE を利用した設定を有効にすると、コストの範囲内に収まるようにするためのクラスタの設定、クラスタのパフォーマンスを向上させてインフラストラクチャのコストを削減するための推奨事項の作成を CLAIRE が実行できるようになります。組織で CLAIRE の推奨事項が有効になっている場合は、CLAIRE を利用した設定を使用できます。

以下の表に、CLAIRE を利用した設定のプロパティを示します。

プロパティ	説明
最適化設定	CLAIRE がインフラストラクチャのコストとクラスタのパフォーマンスのバランスを調整するために使用する、コストまたはパフォーマンスの優先度。
時間あたりのターゲット平均コスト (米ドル)	詳細クラスタを実行するための時間あたりのターゲット平均コスト (米ドル)。
時間あたりの最大コスト (米ドル)	詳細クラスタを実行するための時間あたりの最大コスト (米ドル)。

CLAIRE を利用した設定を有効にすると、設定するプラットフォームプロパティが少なくなります。

## 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。 <b>注:</b> リージョンが「アジアパシフィック（ジャカルタ）」の場合は、S3 バケットが同じリージョンにあることを確認してください。
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、現在のリージョンで使用できるインスタンスタイプを表示します。 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。 CLAIRE を利用した設定には適用されません。
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、現在のリージョンで使用できるインスタンスタイプを表示します。 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。 CLAIRE を利用した設定には適用されません。
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。 CLAIRE を利用した設定には適用されません。
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。 CLAIRE を利用した設定には適用されません。
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。 CLAIRE を利用した設定には適用されません。

プロパティ	説明
高可用性の有効化	<p>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。</p> <p>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。</p> <p><b>注:</b> 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。</p> <p>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。</p> <p>CLAIRE を利用した設定には適用されません。</p>
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	<p>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。</p> <p>CLAIRE を利用した設定には適用されません。</p>
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><b>注:</b> 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> <p>CLAIRE を利用した設定には適用されません。</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"> <li>- 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。</li> <li>- 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。</li> </ul> <p>CLAIRE を利用した設定には適用されません。</p>
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>

プロパティ	説明
ステージングの場所	ステージングデータ用の Amazon S3 上の場所。 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。
ログの場所	詳細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。 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。

## 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 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。 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。 <b>注:</b> 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。
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 内の異なる可用性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可用性ゾーンを指定する必要があります。 <b>注:</b> 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。
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 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。 このスクリプトは bash スクリプトでなければなりません。
ELB セキュリティグループ	Kubernetes API サーバーと詳細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 が詳細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します。 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。 セキュリティグループの詳細については、 <a href="#">「手順 4.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 27)</a> を参照してください。
マスタセキュリティグループ ID	詳細クラスタ、ELB セキュリティグループ、Secure Agent 内のマスタ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。 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。 セキュリティグループの詳細については、 <a href="#">「手順 4.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 27)</a> を参照してください。

プロパティ	説明
ワーカーセキュリティグループ ID	<p>詳細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、<a href="#">「手順 4.Amazon EC2 のユーザー定義のセキュリティグループの作成」</a> (ページ 27) 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><b>注:</b> 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"> <li>- 名前</li> <li>- KubernetesCluster</li> <li>- k8s.io/cluster-autoscaler/enabled</li> <li>- k8s.io/cluster-autoscaler/&lt;クラスタインスタンス ID&gt;.k8s.local</li> </ul> <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><b>注:</b> 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、詳細設定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、ランタイム環境を別の詳細設定に関連付けないようしてください。

詳細設定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` を詳細設定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。

## Amazon Linux 2 イメージ

Amazon Linux 2 (AL2) イメージを使用して AWS でフルマネージドクラスタを作成するには、詳細設定で初期化スクリプトを指定し、セキュリティグループの送信許可リストのドメインを更新する必要があります。

詳細については、次のナレッジベースの記事を参照してください:

[HOW TO: Use Amazon Linux 2 images for nodes in a fully-managed cluster in CDI](#)

## GPU ワーカーインスタンスタイプ

詳細設定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、データ統合ヘルプを参照してください。

**注:** 2025 年 2 月リリースから、GPU 対応インスタンスタイプは保留されます。保留された機能は、現在のリリースでは使用できないか、サポートされていません。Informatica では、今後のリリースで復活させる可能性もありますが、市場や技術的な状況の変化に応じて復活しない場合もあります。

## 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、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。

**注:** 2025 年 2 月リリースから、Graviton インスタンスタイプは保留されます。保留された機能は、現在のリリースでは使用できないか、サポートされていません。Informatica では、今後のリリースで復活させる可能性もありますが、市場や技術的な状況の変化に応じて復活しない場合もあります。

## 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。
- 詳細設定ページの EBS ボリュームサイズ構成は、Graviton でストレージスケールリング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詳細クラスタを設定できます。

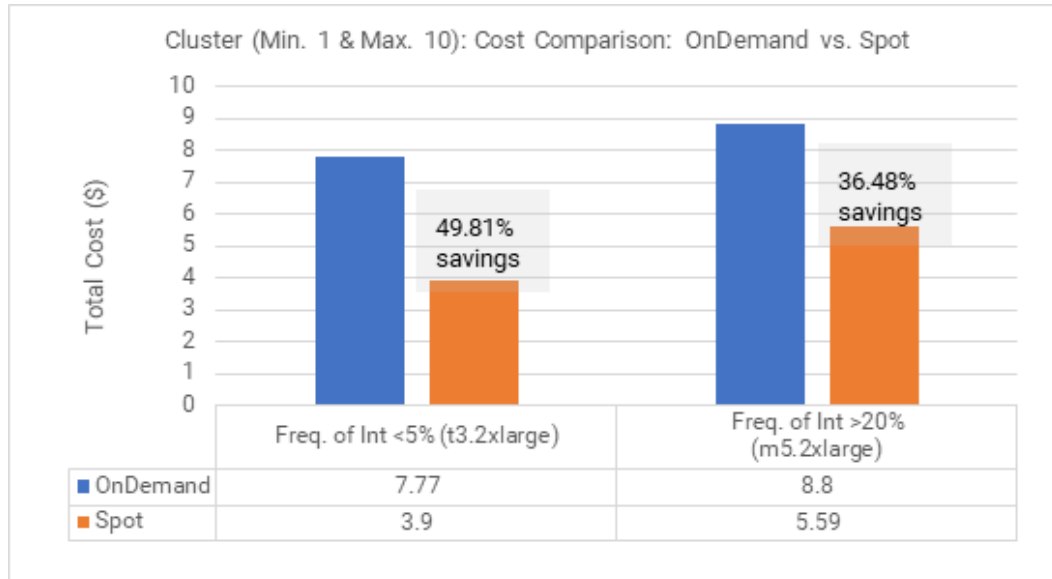
スポットインスタンスは、クラウドプロバイダがオンデマンドインスタンスよりも低価格で提供する予備のコンピューティング容量です。これにより、開発環境や QA 環境で内部テストやデバッグを実行する際に、大幅なコスト削減が可能になります。同じインスタンスタイプのオンデマンドインスタンスとスポットインスタンスのパフォーマンスは似ています。

**注:** スポットインスタンスは常に利用できるとは限らず、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その容量を再利用することができます。したがって、厳密な SLA に制約されたジョブではスポットインスタンスを使用しないでください。



スポットインスタンスは、中断の頻度が5%未満の場合に最も効果的です。AWS で [Spot Instance advisor](#) を使用して、さまざまなレベルの中断のあるインスタンスのリストを表示できます。

次のグラフに、オンデマンドインスタンスとスポットインスタンス間の潜在的な節約コストを示しています。このグラフには、中断頻度のレベルに応じた節約コストの違いも示されています。



このグラフでは、中断の頻度が5%未満の場合、スポットインスタンスはオンデマンドインスタンスと比較して総コストを50%近く節約できることがわかります。ただし、中断の頻度が20%を超えると、節約コストは36%に減少します。

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。

詳細ジョブを実行中のスポットノードをクラウドプロバイダが中断した場合、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

詳細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、最初に詳細設定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、詳細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詳細設定を編集します。
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 はタグを詳細設定で指定する 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、リソースを詳細設定で指定した場合、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、詳細設定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詳細設定の名前。
infa:k8scluster:workdir	クラスタで使用す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、詳細設定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、ジョブの処理に使用されるデータを保護します。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、[「保存時の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 48）](#)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、クラスタノードが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、詳細設定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

詳細設定を作成して、詳細クラスタのプロパティを設定します。プロパティにより、クラウドプラットフォーム上のクラスタを開始する場所と、使用するインフラストラクチャを記述します。

基本プロパティは、詳細設定を記述し、詳細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	詳細設定の名前。
説明	詳細設定の説明。
ランタイム環境	詳細設定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。 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詳細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"><li>- 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。</li><li>- 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。</li></ul>
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	詳細ジョブを実行したときに生成されたログが保存される 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)。VPC は指定したリージョン内に存在する必要があります。 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\u201e および\u201f 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。

## 構成の検証

設定のプロパティを保存する前に、詳細設定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、ランタイム環境を別の詳細設定に関連付けないようにしてください。

**注:** 検証プロセスでは、クラウドロールに必要なすべての権限が割り当てられているどうかといった、クラウドリソースの適切な設定については検証されません。

## クラウドリソースへのラベルのプロパゲート

Secure Agent は、詳細設定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詳細設定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、ジョブの処理に使用されるデータを保護します。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、詳細設定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

詳細設定を作成して、詳細クラスタのプロパティを設定します。プロパティにより、クラウドプラットフォーム上のクラスタを開始する場所と、使用するインフラストラクチャを記述します。

基本プロパティは、詳細設定を記述し、詳細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	詳細設定の名前。
説明	詳細設定の説明。
ランタイム環境	詳細設定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詳細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。
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。

プロパティ	説明
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	<p>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。</p>
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ルされます。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"> <li>- 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。</li> <li>- 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。</li> </ul>
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。リソースグループは最大 90 文字で指定することができます。</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>
ステージングの場所	<p>ジョブの実行時に生成されるステージングデータを格納するための、Azure Data Lake Storage Gen2 上の場所。</p> <p>次の形式を使用します。abfs(s)://&lt;file system&gt;@&lt;storage account&gt;.dfs.core.windows.net/&lt;folder path&gt;</p> <p>暗号化が有効な場合は、ABFSS プロトコルを指定します。有効になっていない場合、ABFS プロトコルを指定します。</p>
ログの場所	<p>ジョブの実行時に生成されるログを格納するための、Azure Data Lake Storage Gen2 上の場所。</p> <p>次の形式を使用します。abfs(s)://&lt;file system&gt;@&lt;storage account&gt;.dfs.core.windows.net/&lt;folder path&gt;</p> <p>暗号化が有効な場合は、ABFSS プロトコルを指定します。有効になっていない場合、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。 リソースグループは最大 90 文字で指定することができます。
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	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。 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。 カスタムネットワークセキュリティグループを使用する場合はオプションです。
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。 カスタムネットワークセキュリティグループを使用する場合はオプションです。
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。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。 例: 10.0.0.0/24 既存の VNet を使用する場合に必要です。IP アドレス範囲は、Kubernetes サービス IP の CIDR として使用され、Kubernetes ネットワークと Azure の VNet インフラストラクチャとの緊密な統合のために必要です。 カスタムネットワークセキュリティグループを使用する場合はオプションです。
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を格納する Azure Data Lake Storage Gen2 上の場所。 次の形式を使用します。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>/file.sh 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。

プロパティ	説明
マスタセキュリティグループ ID	<p>クラスタ内のマスタノードの受信および送信セキュリティルールを定義するセキュリティグループ。Secure Agent は、このセキュリティグループをクラスタ内のすべてのマスタノードにアタッチします。</p> <p>次の形式を使用します: &lt;リソースグループ名&gt;/&lt;NSG 名&gt;</p> <p>マスタセキュリティグループは最大 155 文字で指定することができます。</p> <p><b>注:</b> 詳細設定にクラスタリソースグループが含まれており、NSG（ネットワークセキュリティグループ）がクラスタリソースグループに属している場合は、この値としてネットワークセキュリティグループ名を使用できます。</p> <p>このセキュリティグループは、データ統合によって作成されたデフォルトのマスタセキュリティグループを置き換えます。詳細については、ハウツー記事「<a href="#">Create user defined security groups in Azure</a>」を参照してください。</p> <p>マスタセキュリティグループを指定する場合は、ワーカーセキュリティグループが必要です。</p>
ワーカーセキュリティグループ ID	<p>クラスタ内のワーカーノードの受信および送信セキュリティルールを定義するセキュリティグループ。Secure Agent は、このセキュリティグループをクラスタ内のすべてのワーカーノードにアタッチします。</p> <p>次の形式を使用します: &lt;リソースグループ名&gt;/&lt;NSG 名&gt;</p> <p>ワーカーセキュリティグループは最大 155 文字で指定することができます。</p> <p><b>注:</b> 詳細設定にクラスタリソースグループが含まれており、NSG（ネットワークセキュリティグループ）がクラスタリソースグループに属している場合は、この値としてネットワークセキュリティグループ名を使用できます。</p> <p>このセキュリティグループは、データ統合によって作成されたデフォルトのワーカーセキュリティグループを置き換えます。詳細については、ハウツー記事「<a href="#">Create user defined security groups in Azure</a>」を参照してください。</p> <p>ワーカーセキュリティグループを指定する場合は、マスタセキュリティグループが必要です。</p>
Azure タグ	<p>クラスタノードに適用する Microsoft Azure のタグ。各タグにはキーと値があります。</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><b>注:</b> 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、「<a href="#">クラウドリソースのデフォルトタグ</a>」（<a href="#">ページ 149</a>）を参照してください。</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><b>注:</b> 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、詳細設定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、ランタイム環境を別の詳細設定に関連付けないようにしてください。

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 を詳細設定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

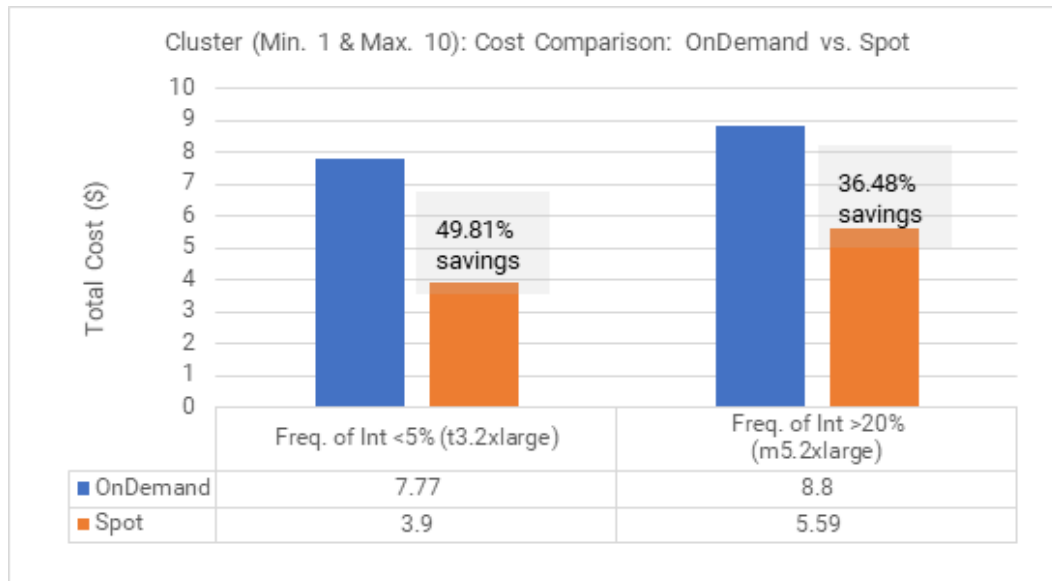
スポットインスタンスを使用してワーカーノードをホストするように詳細クラスタを設定できます。

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。これにより、開発環境や QA 環境で内部テストやデバッグを実行する際に、大幅なコスト削減が可能になります。同じインスタンスタイプのオンデマンドインスタンスとスポットインスタンスのパフォーマンスは似ています。

**注:** スポットインスタンスは常に利用できるとは限らず、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その容量を再利用することができます。したがって、厳密な SLA に制約されたジョブではスポットインスタンスを使用しないでください。

スポットインスタンスは、中断の頻度が 5%未満の場合に最も効果的です。AWS で [Spot Instance advisor](#) を使用して、さまざまなレベルの中断のあるインスタンスのリストを表示できます。

次のグラフに、オンデマンドインスタンスとスポットインスタンス間の潜在的な節約コストを示しています。このグラフには、中断頻度のレベルに応じた節約コストの違いも示されています。



このグラフでは、中断の頻度が 5%未満の場合、スポットインスタンスはオンデマンドインスタンスと比較して総コストを 50%近く節約できることがわかります。ただし、中断の頻度が 20%を超えると、節約コストは 36%に減少します。

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。

詳細ジョブを実行中のスポットノードをクラウドプロバイダが中断した場合、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

詳細クラスタを高可用にして、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、詳細設定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. 詳細設定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 はタグを詳細設定で指定する 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 を作成して詳細設定に 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、詳細設定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詳細設定の名前。
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。
InfraInternalInitDone	内部使用。
KubernetesCluster	詳細クラスタの特定。

一部のデフォルトタグは、名前空間がなく、KubernetesCluster などの詳細設定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、詳細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、ジョブの処理に使用されるデータを保護します。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、Azure 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、クラスターノードが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、詳細設定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、Azure 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。

暗号化が有効になっている場合、詳細設定でステージングの場所とログの場所を設定するときに ABFS 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、ABFS プロトコルを使用する必要があります。

## ローカルクラスタの詳細設定

上級ユーザー向け、または Informatica グローバルカスタマサポートの指示により設定する、ローカルクラスタの追加設定情報。

必要に応じて、次のトピックを参照してください。

- [「ステージングとログの場所の変更（オプション）」（ページ 150）](#)。ステージングの場所とログの場所をローカルファイルシステムからクラウドの場所に移動する場合。
- [「ローカルクラスタのプロパティ」（ページ 151）](#)。ステージングの場所とログの場所をクラウドに移動した場合に変更するプロパティ。ローカルクラスタのその他の詳細プロパティ。
- [「クラウド権限の設定」（ページ 153）](#)。ステージングの場所とログの場所をローカルストレージからクラウドに変更する場合は、クラウド権限を設定します。
- [「データ暗号化」（ページ 156）](#)。暗号化を使用して、保存中のデータ、一時データ、転送中のデータを保護する方法について説明します。
- [Configure custom runtime container storage for local clusters](#): カスタムのランタイムコンテナの保管場所を設定できます。このリンクをクリックすると、Informatica ドキュメントポータルナレッジベースの記事が開きます。

## ステージングとログの場所の変更（オプション）

ローカルクラスタでジョブを実行する場合、Secure Agent マシンのローカルファイルシステムまたはクラウドの場所で、ステージングディレクトリとログディレクトリを選択できます。デフォルトでは、クラウドの接続先を設定していない限り、ローカルクラスタはローカルファイルシステムパスを使用します。

ステージングの場所またはログの場所をクラウドの場所に変更するには、次のタスクを実行します。

1. クラウド環境に場所を作成するには、次の表を参照してください。

クラウド環境	場所の作成
AWS	次の Amazon S3 の場所を作成します。 <ul style="list-style-type: none"><li>- クラスタが実行時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</li><li>- クラスタが、クラスタ上で実行される詳細ジョブのログファイルを保存するために使用する S3 の場所</li></ul>
Microsoft Azure	ステージングの場所とログファイルの場所を指定して、Azure Data Lake Storage Gen2 を使用してストレージアカウントを作成します。階層名前空間を使用します。
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。

2. 詳細クラスタの詳細設定で場所を指定します。ステージングの場所およびログの場所の形式の詳細については、[「ローカルクラスタのプロパティ」（ページ 151）](#)を参照してください

## ローカルクラスタのプロパティ

詳細設定を作成して、詳細クラスタのプロパティを設定します。プロパティにより、クラウドプラットフォーム上のクラスタを開始する場所と、使用するインフラストラクチャを記述します。

基本プロパティは、詳細設定を記述します。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	詳細設定の名前。
説明	詳細設定の説明。
ランタイム環境	詳細設定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	<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の場所。</p> <p>ローカルファイルシステム上のステージングデータの場合は、次の形式で場所を指定します。</p> <p>file://&lt;absolute path to the Secure Agent location&gt;</p> <p>例えば、/home/devbld/staging をステージングの場所として使用するには、次のように入力します。</p> <p>file:///home/devbld/staging</p> <p>ディレクトリが存在しない場合は、データ統合によって作成されます。絶対パスの余分な「/」文字に注意してください。</p> <p>クラウド内のステージングの場所については、次の形式のいずれかでパスを指定します。</p> <ul style="list-style-type: none"><li>- Amazon S3。s3://&lt;バケット名&gt;/&lt;フォルダパス&gt;</li><li>- Google Cloud Storage。gs://&lt;バケット名&gt;/&lt;フォルダパス&gt;&amp;:&lt;プロジェクト ID&gt;/&lt;リージョン&gt;</li><li>- Microsoft Azure Data Lake Storage Gen2。abfs(s)://&lt;ファイルシステム&gt;@&lt;ストレージアカウント&gt;.dfs.core.windows.net/&lt;フォルダパス&gt;&amp;:&lt;リソースグループ&gt;/&lt;リージョン&gt;</li></ul> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"><li>- AWS では、us-west-2 を使用して米国西部（オレゴン）を表します。</li><li>- Google Cloud では、us-west2 を使用してロサンゼルスを表します。</li><li>- Microsoft Azure では、westus2 を使用して米国西部 2 を表します。</li></ul> <p>Secure Agent が Oracle Cloud Infrastructure 上にローカルクラスタを作成する場合、ステージングの場所はローカルファイルシステム上である必要があります。</p>
ログの場所	<p>ログの場所。</p> <p>ローカルファイルシステム上のログの場合、次の形式で場所を指定します。</p> <p>file://&lt;absolute path to the Secure Agent location&gt;</p> <p>例えば、/home/devbld/logging をログの場所として使用するには、次のように入力します。</p> <p>file:///home/devbld/logging</p> <p>ディレクトリが存在しない場合は、データ統合によって作成されます。絶対パスの余分な「/」文字に注意してください。</p> <p>クラウド内のログの場所については、次の形式でパスを指定します。</p> <ul style="list-style-type: none"><li>- Amazon S3。s3://&lt;バケット名&gt;/&lt;フォルダパス&gt;</li><li>- Google Cloud Storage。gs://&lt;バケット名&gt;/&lt;フォルダパス&gt;&amp;:&lt;プロジェクト ID&gt;/&lt;リージョン&gt;</li><li>- Microsoft Azure Data Lake Storage Gen2。abfs(s)://&lt;ファイルシステム&gt;@&lt;ストレージアカウント&gt;.dfs.core.windows.net/&lt;フォルダパス&gt;&amp;:&lt;リソースグループ&gt;/&lt;リージョン&gt;</li></ul> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"><li>- AWS では、us-west-2 を使用して米国西部（オレゴン）を表します。</li><li>- Google Cloud では、us-west2 を使用してロサンゼルスを表します。</li></ul>



プロパティ	説明
	<p>- Microsoft Azure では、westus2 を使用して米国西部 2 を表します。</p> <p>Secure Agent が Oracle Cloud Infrastructure 上にローカルクラスタを作成する場合、ログの場所はローカルファイルシステム上である必要があります。</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	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。

## クラウド権限の設定

ローカルクラスタでは、標準のクラウドデプロイメントと比べて、クラウド権限が簡素化されています。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。

**注:** ステージングの場所とログの場所がローカルファイルシステムにある場合（デフォルト）は、クラウド権限を設定する必要はありません。

### AWS の権限の設定

AWS 環境で、Secure Agent とクラスタオペレータの IAM ロールを構成します。

以下の手順を実行します。

1. AWS で、agent\_role という名前の IAM ロールを作成し、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。または、既存の IAM ロールを Secure Agent ロールに指定することもできます。

**ヒント:** 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. AWS で、cluster\_operator\_role という名前のクラスタオペレータの IAM ロールを作成します。
3. 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、ワイルドカード文字を使用できます。詳細については、AWS のマニュアルを参照してください。

4. IAM ポリシー cluster\_operator\_policy を IAM ロール cluster\_operator\_role にアタッチします。
5. 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"
        }
      }
    }
  ]
}

```

## Google Cloud の権限の設定

Google Cloud 環境で、カスタム IAM ロールを設定します。

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。

## Microsoft Azure の権限の設定

Microsoft Azure 環境で、マネージド ID とカスタムロールを作成します。

以下の手順を実行します。

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。

## データ暗号化

暗号化によって、ジョブの処理に使用されるデータを保護します。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、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、クラスタ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、クラスタノードが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、詳細設定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 で暗号化が有効になっている場合、詳細設定でステージングとログの場所を設定するときに ABFSS 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、ABFS 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

詳細設定を作成して、詳細クラスタのプロパティを設定します。プロパティにより、クラウドプラットフォーム上のクラスタを開始する場所と、使用するインフラストラクチャを記述します。

基本プロパティにより、詳細設定を記述し、セルフサービス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。

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 160) 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	詳細設定の名前。
説明	詳細設定の説明。

プロパティ	説明
ランタイム環境	詳細設定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
Kubeconfig ファイルパス	kubeconfig ファイルのパス。 kubeconfig ファイルにより、クラスタ、ユーザー、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 マシン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。 詳細設定は、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 がリソースをデプロイする名前空間。
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。 最大ノードエントリは、ジョブが多すぎることによってクラスタに負荷がかからないようにし、リソースのデッドロックを発生しにくくするためのものです。ただし、ジョブがクラスタに到達すると、クラスタ自体のポッドスケジューラが、設定された最大ノード数よりも多くのノードを使用してジョブを実行する場合があります。 システムが最大ノード数よりも多くのノードを使用しないようにするには、次の操作を行う必要があります。 1. クラスタで、複数のノードグループを定義します。それぞれに固有のノードラベルが必要です。 2. ノードラベルを詳細クラスタ設定に追加します。そうすることにより、特定のノードグループ内のノードのみにリソースが割り当てられます。
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になってから削除されるまでの時間。クラスタは削除されません。
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。 次のいずれかの形式でパスを指定します。</p> <ul style="list-style-type: none"> <li>- AWS。s3://&lt;バケット名&gt;/&lt;フォルダパス&gt;</li> </ul> <p><b>注:</b> 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> <ul style="list-style-type: none"> <li>- Microsoft Azure。abfs(s)://&lt;ファイルシステム&gt;@&lt;ストレージアカウント&gt;.dfs.core.windows.net/&lt;フォルダパス&gt;&amp;:&lt;リソースグループ&gt;/&lt;リージョン&gt;</li> </ul> <p>リージョンはオプションです。デフォルトのリージョンは westus2 です。</p> <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。 次のいずれかの形式でパスを指定します。</p> <ul style="list-style-type: none"> <li>- AWS。s3://&lt;バケット名&gt;/&lt;フォルダパス&gt;</li> </ul> <p><b>注:</b> 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> <ul style="list-style-type: none"> <li>- Microsoft Azure。abfs(s)://&lt;ファイルシステム&gt;@&lt;ストレージアカウント&gt;.dfs.core.windows.net/&lt;フォルダパス&gt;&amp;:&lt;リソースグループ&gt;/&lt;リージョン&gt;</li> </ul> <p>リージョンはオプションです。デフォルトのリージョンは westus2 です。</p> <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>
ラベル	<p>Informatica がセルフサービスクラスタ内に作成する Kubernetes オブジェクトにアタッチするキーと値のペア。</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>
ノードセレクトラベル	<p>ノードセレクトラベルを使用して、Informatica が Kubernetes オブジェクトを作成できるクラスタ内のノードを識別します。</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
注釈	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。注釈はクラスタ内のポッドに対してのみ定義できます。 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。
許容	ポッドが適切なノードにスケジュールされるようにするために使用するキーと値のペア。 許容の設定時に、次のプロパティを設定します。 <ul style="list-style-type: none"><li>- キー</li><li>- 演算子</li><li>- 値</li><li>- 効果</li><li>- 許容時間（秒）</li></ul> 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。

## 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。 <b>注:</b> 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）。

プロパティ	説明
ccs.app.control.enable	<p>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。</p> <p>アプリケーション送信制御は、次のすべての条件に当てはまる場合にのみ使用できます。</p> <ul style="list-style-type: none"> <li>- すべてのクラスターノードが同種である。</li> <li>- 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。</li> <li>- 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。</li> </ul> <p>クラスターでクォータを定義する場合、クォータ定義で利用でき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。</p>
infacco.job.spark.kubernetes.scheduler.name	<p>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。</p>

## 構成の検証

設定のプロパティを保存する前に、詳細設定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、ランタイム環境を別の詳細設定に関連付けないようになっています。

**注:** 検証プロセスでは、クラウドロールに必要なすべての権限が割り当てられているかどうかといった、クラウドリソースの適切な設定については検証されません。

## クラスターノードのリソース要件

詳細設定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詳細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詳細クラスタが 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詳細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、詳細設定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。
- `script.sh` という名前はシステム用に予約されているため、init スクリプトにこの名前を設定することはできません。

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的パスに配置するか、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、詳細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、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 および詳細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 および詳細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. 詳細設定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、または詳細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」 \(ページ 174\)](#)を参照してください。
2. 詳細設定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 が新しい詳細クラスタを別のクラスタ ID で作成します。

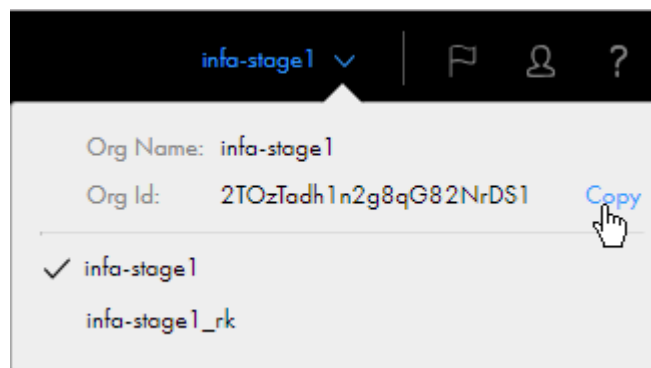
## 第 8 章

# トラブルシューティング

次のセクションを使用して、詳細クラスタのエラーをトラブルシューティングします。

**注:** 詳細クラスタ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。

## 詳細クラスタのトラブルシューティング

詳細クラスタのステータスが不明の場合、どうすればよいですか。

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。

詳細クラスタのトラブルシューティングを行うために `ccs-operation.log` ファイルを調べましたが、十分な情報を得られませんでした。他にどこを調べればよいですか。

詳細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。

## 詳細クラスタの次のエラーメッセージでリソース要件はどのように計算されますか。

```
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。

エーエージェントマシンをシャットダウンすると、エー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 上の詳細クラスタのトラブルシューティング

詳細クラスタの起動に失敗したのはなぜですか。

詳細クラスタが起動に失敗した理由を調べるには、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。

### 詳細クラスタを起動するジョブを実行しましたが、VPC 制限に達しました。

クラスタの詳細設定で VPC を指定しないと、Secure Agent は AWS アカウントに新しい 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 制限に達した場合は、詳細設定を編集し、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。

### 詳細クラスタを起動するジョブを実行しましたが、次のエラーが発生し、クラスタの作成に失敗しました。

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 が詳細クラスタの作成に失敗したのは、Amazon S3 がエージェントの要求を拒否したためです。

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事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、詳細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。

### 詳細クラスタのステージングの場所を更新したら、次のエラーが発生しマッピングに失敗しました。

Error while executing mapping. ExecutionId '`<execution ID>`'. Cause: `[Failed to start cluster for [01000D25000000000005]. Error reported while starting cluster [Cannot apply cluster operation START because the cluster is in an error state.].]`

詳細設定で 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、最初に詳細設定で 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. 詳細設定を編集して S3 ステージングの場所を元に戻します。
3. 設定を保存すると、クラスタが停止します。



4. 設定の 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。

詳細クラスタのステージングの場所を更新したら、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

詳細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。

詳細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、詳細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、ワーカーロールが詳細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 ロールが詳細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、詳細クラスタのステータスがエラーになりました。

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 で詳細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、詳細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 上の詳細クラスタのトラブルシューティング

Secure Agent マシンを再起動したら、詳細クラスタのステータスがエラーになりました。

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 で詳細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、ジョブを実行してクラスタを再起動できます。

詳細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ました。

```
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 ls -l /var/lib/dpkg/lock-frontend)  
do  
  echo "Sleeping 10s"  
  sleep 10  
done  
  
sudo apt-get -y update  
sudo apt-get install -y expect
```

## 詳細クラスタサブタスクのトラブルシューティング

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。

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います。

1. 実行プラン。ジョブの Scala コードをデバッグします。
2. セッションログ。ジョブのコンパイルと Spark 実行ワークフローの生成を行うロジックをデバッグします。
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詳細クラスタにプッシュする方法をデバッグします。
4. Spark ドライバおよびエグゼキュータログ。詳細クラスタがジョブを実行する方法をデバッグします。

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。

失敗したジョブのログファイルが一部見つかりません。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。

ジョブに対して生成されるログは、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、詳細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できません。

ジョブを詳細クラスタにプッシュするとき、Secure Agent は 1 つの Spark ドライバポッドと複数の 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。Spark ドライバポッドは、ジョブが成功または失敗した直後に 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>/services/shared/kubernetes/kubernetes_<version>/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、クラスタインスタンス ID を検索します。
  - セッションログでクラスタインスタンス 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/user-name/cluster/hadoop-tests/cats/edtm/spark/./target/hadoop12345678_InfaSpark0/log4j_infa_spark.properties] to the following shared storage location: [s3a://soki-k8s-local-state-store/k8s-infa/testcluster2.k8s.local/staging/sess12345678/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://abc-k8s-local-state-store/k8s-infa/testcluster2.k8s.local/staging/
```

クラスタインスタンス 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 ファイルでクラスタインスタンス 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>/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_<version>/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 : [16y6xhsvjkdkeybtzdy1dkx.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 マシンから自己管理型 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 マシンから自己管理型 Kubernetes クラスタにアクセスできるにもかかわらず、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。

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、詳細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 で詳細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_<version>/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、[「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」 \(ページ 38\)](#)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	詳細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	詳細クラスタとそのクラスタで実行される詳細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-abfs[s]://> (Azure 環境)

-azsrg | -azure-storage-resource-group

-ac | -azurecpath=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	クラスタの詳細設定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。 - AWS。-staging-dir=<バケット名>/<フォルダ名>。 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。-staging-dir=abfs(s)://<file system>@<storage account>.dfs.core.windows.net/<folder path> 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	クラスタの詳細設定で設定され、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。

オプション	説明
-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 環境には適用されません。 <b>注:</b> 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 環境の詳細クラスタか、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 環境には適用されません。

## delete-clusters.sh

ステージング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-abfs[s]://> (Azure 環境)

-azsrg | -azure-storage-resource-group

-s | -deletable-states=state-1[,state-2,...]

-c | -clusters=cluster1[,cluster2,...]

-f | -force

-ac | -azurecpath=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	クラスタの詳細設定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。 - AWS。-staging-dir=<バケット名>/<フォルダ名>。 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。-staging-dir=abfs(s)://<file system>@<storage account>.dfs.core.windows.net/<folder path> 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。



オプション	説明
-azsrg -azure-storage-resource-group	クラスタの詳細設定で設定され、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	<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"> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> </ul> <p>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。</p> <p>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。</p> <p>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。</p>
-clusters -c	<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>
-force -f	<p>追加のプロンプトをスキップします。</p> <p>-force オプションを使用しない場合は、コマンドに各詳細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。</p> <p>-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。</p>
-azurecpath -ac	<p>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 環境には適用されません。</p> <p><b>注:</b> 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。</p>
-cluster-type -ct	<p>AWS 環境の詳細クラスタか、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 環境には適用されません。</p>

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.local
```

# 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	クラスタの詳細設定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: <i>gs://&lt;bucket&gt;/&lt;folder&gt;</i>
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的識別子。

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	クラスタの詳細設定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"> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> </ul> <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>
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 アプリケーション統合コミュニティ  
URL [8](#)  
Cloud 開発者コミュニティ  
URL [8](#)

## G

Google Cloud カスタムロール [81](#)

## I

Informatica Intelligent Cloud Services  
Web サイト [8](#)  
Informatica グローバルカスタマサポート  
連絡先情報 [9](#)

## W

Web サイト [8](#)

## あ

アップグレード通知 [9](#)

## え

エラスティッククラスタ  
AWS サブスクリプション [18](#)  
CLI/API セッション最長時間 [36](#)  
delete clusters コマンド [176](#)  
generate policies コマンド [174](#)  
Google Cloud NAT ゲートウェイ [78](#)  
Google Cloud サービス [74](#)  
JAVA\_HOME [53](#), [87](#), [107](#)  
list clusters コマンド [175](#)  
Microsoft Azure 製品 [89](#)  
Secure Agent ロール [31](#), [37](#), [51](#)  
VPC [26](#), [78](#), [79](#)  
エージェントのインストール [30](#), [80](#), [94](#)  
エラスティックサーバー [53](#)  
エラスティック構成 [143](#), [156](#)  
クラスタオペレータロール [27](#), [31](#), [32](#), [36](#)  
コマンド [53](#), [87](#), [107](#), [174](#)–[176](#)  
サービスプリンシパル [99](#)  
サブネット [26](#), [78](#)  
ステージングの場所 [137](#), [148](#), [163](#)  
セキュリティ [49](#)–[51](#)  
セキュリティプリンシパル [95](#), [96](#), [99](#), [101](#)  
セルフサービスクラスタ [156](#)

エラスティッククラスタ (続く)

タグ付け [137](#), [138](#), [148](#), [149](#)  
データ暗号化 [48](#), [138](#), [142](#), [149](#)  
デフォルトのロール [48](#), [70](#)  
ファイアウォールルール [79](#)  
マネージド ID [95](#)  
ユーザー定義のロール [38](#), [47](#), [70](#), [71](#)  
ラベリング [142](#)  
ランタイム環境 [163](#)  
リソースへのアクセス [22](#)–[24](#), [76](#), [77](#), [92](#)  
リソース要件 [161](#), [162](#)  
ルーティング [26](#)  
ロールベースのセキュリティ [49](#), [50](#)  
ワーカーロール [70](#)  
高可用性 [136](#), [148](#)  
資格情報ベースのセキュリティ [51](#)  
初期化スクリプト [162](#), [163](#)  
前提条件 [18](#), [73](#), [88](#)  
組織の権限 [18](#), [73](#)

## <

クラウド権限  
AWS [153](#)  
Google Cloud [155](#)  
Microsoft Azure [155](#)  
クラスタ  
クラスタ操作コマンド [178](#)  
コマンド [174](#), [178](#)  
プロキシの設定 [81](#), [95](#)

## し

システムステータス [9](#)

## す

ステータス  
Informatica Intelligent Cloud Services [9](#)

## せ

セキュリティグループ  
ELB セキュリティグループ [27](#)  
マスタセキュリティグループ [27](#)  
ワーカーセキュリティグループ [27](#)  
セルフサービスクラスタ  
AWS CLI 認証 [120](#)  
カスタムプロパティ [159](#)  
ユーザー管理のサービスアカウント [113](#)  
概要 [13](#)  
許容 [113](#)

セルフサービスクラスタ (続く)  
前提条件 [108](#)  
組織の権限 [109](#)  
注釈 [113](#)

## と

トラブルシューティング  
ローカルクラスタ [124](#)  
詳細クラスタ [167](#), [169](#)  
詳細クラスタサブタスク [170](#)

## ふ

プロキシ設定  
クラスタ [81](#), [95](#)

## ま

マスタロール [70](#)

## め

メンテナンスの停止 [9](#)

## ろ

ローカルクラスタ  
AWS [124](#)  
エージェントのインストール [123](#)  
クラウド権限 [153](#), [155](#)  
クラスタプロパティ [151](#)  
ステージングとログの場所 [150](#)  
データ暗号化 [156](#)  
トラブルシューティング [124](#)  
設定 [122](#)  
前提条件 [122](#)