OpenShift Dedicated 4

Google Cloud 上の OpenShift Dedicated クラスター

Google Cloud 上に OpenShift Dedicated クラスターをインストールする

Last Updated: 2025-12-11

OpenShift Dedicated 4 Google Cloud 上の OpenShift Dedicated クラスター

Google Cloud 上に OpenShift Dedicated クラスターをインストールする

Legal Notice

Abstract

このドキュメントでは、Google Cloud 上に OpenShift Dedicated クラスターをインストールする方法を説明します。このドキュメントでは、クラスターの設定方法も詳しく説明します。

Table of Contents

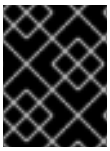
第1章 PRIVATE SERVICE CONNECT の概要

Google Cloud のセキュリティー強化ネットワーク機能である Private Service Connect (PSC) を使用して、Google Cloud 上にプライベート OpenShift Dedicated クラスターを作成できます。

1.1. PRIVATE SERVICE CONNECT について

Google Cloud のネットワーク機能である Private Service Connect (PSC) を使用すると、Google Cloud 内の異なるプロジェクトや組織にまたがるサービス間のプライベート通信が可能になります。ネットワーク接続の一部として PSC を実装するユーザーは、パブリックに公開されるクラウドリソースを使用せずに、Google Cloud 内のプライベートでセキュアな環境に OpenShift Dedicated クラスターをデプロイできます。

PSC の詳細は、Private Service Connect を参照してください。



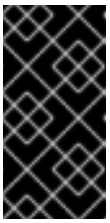
重要

PSC は OpenShift Dedicated バージョン 4.17 以降でのみ使用可能であり、Customer Cloud Subscription (CCS) インフラストラクチャータイプでのみサポートされます。

1.2. 前提条件

Google Cloud 上の OpenShift Dedicated クラスターをデプロイする前に必要な前提条件に加えて、Private Service Connect (PSC) を使用してプライベートクラスターをデプロイするには、以下の前提条件も完了している必要があります。

- クラスターがデプロイされる同じ Google Cloud リージョン内に、次のサブネットを持つ Virtual Private Cloud (VPC) が事前に作成されている。
  - コントロールプレーンサブネット
  - ワーカーサブネット
  - 目的を Private Service Connect に設定した、PSC サービスアタッチメントに使用するサブネット。

    重要

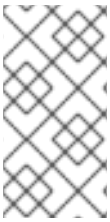
    PSC サービスアタッチメントのサブネットマスクは /29 以上で、1 つの OpenShift Dedicated クラスター専用である必要があります。さらに、サブネットは、OpenShift Dedicated クラスターのプロビジョニング中に使用されるマシン CIDR 範囲内に含まれている必要があります。

    Google Cloud で VPC を作成する方法は、Google Cloud ドキュメントの Create and manage VPC networks を参照してください。

- **関連情報** セクションの **Google Cloud ファイアウォールの前提条件** に記載されているドメインとポートに、OpenShift Dedicated クラスターからインターネットへのパスを提供する。
- Google Cloud プロジェクトレベルで Cloud Identity-Aware Proxy API を有効にしました。

上記の要件に加えて、**Service Account 認証タイプ** で設定されたクラスターでは、**osd-ccs-admin** サービスアカウントに **IAP-Secured Tunnel User** ロールを付与する必要があります。

OpenShift Dedicated を Google Cloud にデプロイする前に満たす必要がある前提条件の詳細は、**お客様の要件** を参照してください。



注記

PSC は、Customer Cloud Subscription (CCS) インフラストラクチャータイプでのみサポートされます。PSC を使用して Google Cloud 上に OpenShift Dedicated を作成するには、**Workload Identity Federation 認証を使用した Google Cloud 上でのクラスターの作成** を参照してください。

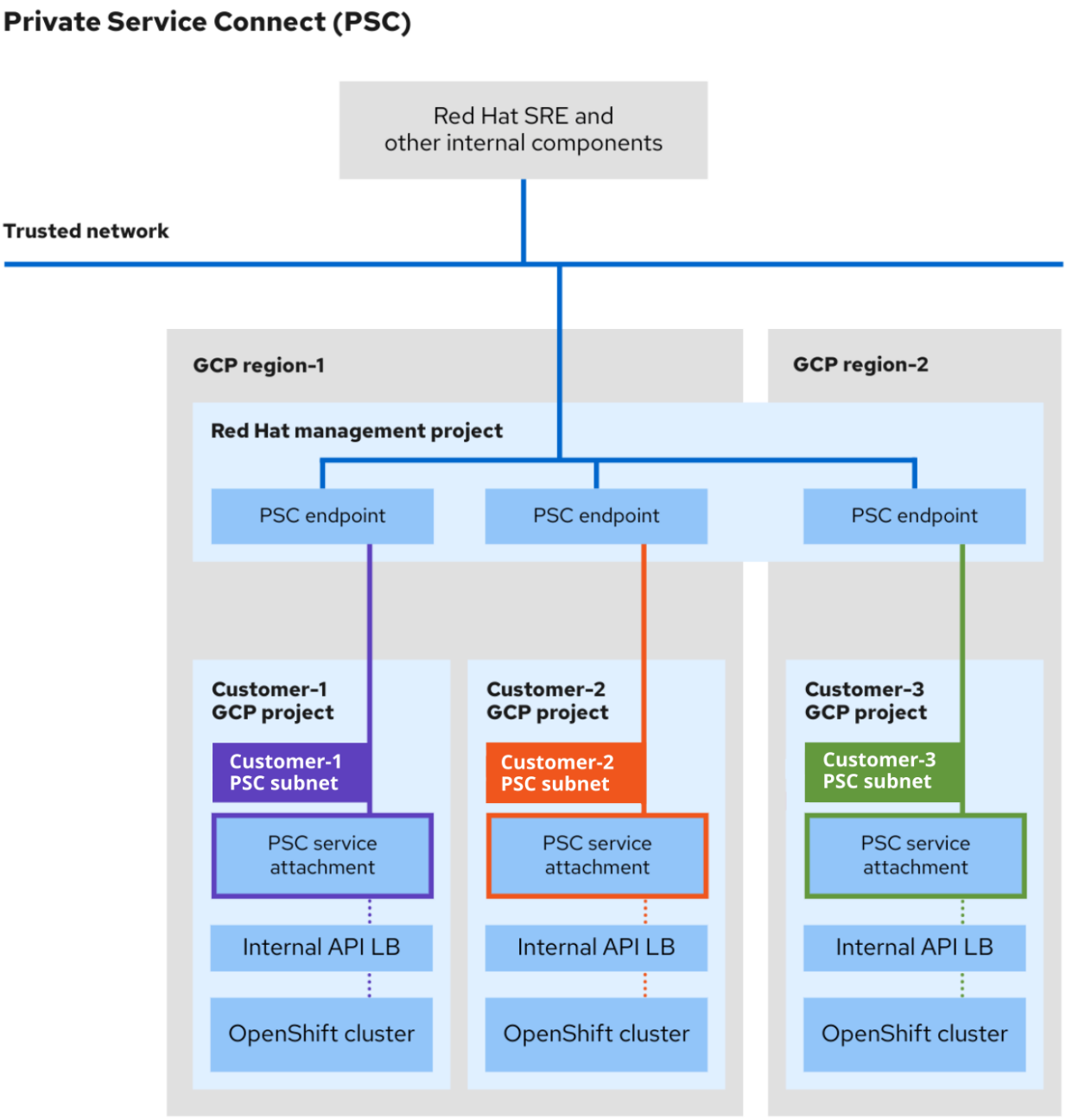
1.3. PRIVATE SERVICE CONNECT のアーキテクチャー

PSC のアーキテクチャーには、プロデューサーサービスとコンシューマーサービスが含まれています。PSC を使用すると、コンシューマーは VPC ネットワーク内からプロデューサーサービスにプライベートにアクセスできます。同様に、プロデューサーは独自の個別の VPC ネットワークでサービスをホストし、コンシューマーにプライベート接続を提供できます。

次の図は、Red Hat SRE およびその他の内部リソースが PSC を使用して作成されたクラスターにアクセスし、サポートする方法を示しています。

- お客様の Google Cloud プロジェクト内の OSD クラスターごとに、一意の PSC サービスアタッチメントが作成されます。PSC サービスアタッチメントは、お客様の Google Cloud プロジェクトに作成されたクラスター API サーバーロードバランサーを参照します。
- サービスアタッチメントと同様に、各 OSD クラスターに対して、Red Hat Management Google Cloud プロジェクトに一意の PSC エンドポイントが作成されます。
- お客様の Google Cloud プロジェクト内のクラスターのネットワークに、Google Cloud Private Service Connect 専用のサブネットが作成されます。これは特別なサブネットタイプであり、このサブネットタイプを使用してプロデューサーサービスが PSC サービスアタッチメントを介して公開されます。このサブネットは、クラスター API サーバーへの受信要求に対してソース NAT (SNAT) を実行するために使用されます。さらに、PSC サブネットは、マシン CIDR 範囲内にある必要があり、複数のサービスアタッチメントで使用することはできません。
- Red Hat の内部リソースと SRE は、PSC エンドポイントとサービスアタッチメント間の接続を使用してプライベート OSD クラスターにアクセスします。トラフィックは複数の VPC ネットワークを通過しますが、完全に Google Cloud 内に留まります。
- PSC サービスアタッチメントへのアクセスは、Red Hat Management プロジェクト経由でのみ可能です。

図1.1 PSC のアーキテクチャーの概要



1.4. 次のステップ

- Google Cloud 上の OpenShift Dedicated クラスターの前提条件に関する詳細は、お客様の要件を参照してください。
- ファイアウォールを設定するには、Google Cloud ファイアウォールの前提条件 を参照してください。
- PSC と Workload Identity Federation 認証タイプを使用して Google Cloud 上に OpenShift Dedicated を作成するには、Workload Identity Federation 認証を使用した Google Cloud 上でのクラスターの作成 を参照してください。

第2章 WORKLOAD IDENTITY FEDERATION 認証を使用した GOOGLE CLOUD 上でのクラスターの作成

システム管理者またはクラウドエンジニアは、Workload Identity Federation (WIF)を使用して、Google Cloud に OpenShift Dedicated クラスターをプロビジョニングできます。この機能は、クラスターのコントロールプレーンとワークロードが必要な Google Cloud ロールと必要なサービスにアクセスできるようにする信頼関係を確立します。このアプローチにより、有効期間の長い Google Cloud サービスアカウントキーの管理およびローテーションに関連するセキュリティーリスクと操作のオーバーヘッドを排除できます。

2.1. WORKLOAD IDENTITY FEDERATION の概要

Workload Identity Federation (WIF) は、Google Cloud のアイデンティティーおよびアクセス管理 (IAM) 機能であり、お客様のクラウドアカウント上のリソースにセキュアにアクセスする方法をサードパーティーに提供するものです。WIF を使用するとサービスアカウントキーが不要になります。これは Google Cloud の推奨される認証情報の認証方法です。

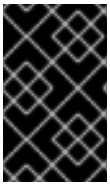
サービスアカウントキーを使用すると、Google Cloud リソースへの強力なアクセスが可能になります。しかし、サービスアカウントキーは、ユーザーが管理する必要があり、適切に管理されていない場合、セキュリティーリスクになる可能性があります。WIF では、Google Cloud リソースのアクセス方法としてサービスキーを使用しません。代わりに、WIF は外部アイデンティティープロバイダーからの認証情報を使用してワークロード用の有効期間が短い認証情報を生成することでアクセスを許可します。ワークロードはこの認証情報を使用して、一時的にサービスアカウントの権限を借用し、Google Cloud リソースにアクセスします。これにより、サービスアカウントキーを適切に管理する負担がなくなり、権限のないユーザーがサービスアカウントキーにアクセスするリスクもなくなります。

以下に、Workload Identity Federation のプロセスの基本的な概要を箇条書きで示します。

- Google Cloud プロジェクトの所有者が、アイデンティティープロバイダーを使用してワークロードアイデンティティープールを設定します。これにより、OpenShift Dedicated が有効期間の短い認証情報を使用してプロジェクトの関連サービスアカウントにアクセスできるようになります。
- このワークロードアイデンティティープールは、ユーザーが定義するアイデンティティープロバイダー (IP) を使用して要求を認証するように設定されます。
- アプリケーションがクラウドリソースにアクセスするために、まず Google の Security Token Service (STS) に認証情報を渡します。STS は指定されたアイデンティティープロバイダーを使用して認証情報を検証します。
- 認証情報が検証されると、STS は呼び出し元に一時的なアクセストークンを返します。これにより、アプリケーションがそのアイデンティティーにバインドされたサービスアカウントの権限を借用できるようになります。

Operator もクラウドリソースへのアクセスを必要とします。このアクセスを許可するためにサービスアカウントキーの代わりに WIF を使用すると、サービスアカウントキーがクラスターに保存されなくなるため、クラスターのセキュリティーがさらに強化されます。代わりに、Operator にはサービスアカウントの権限を借用する一時的なアクセストークンが付与されます。これらのトークンは有効期間が短く、定期的にローテーションされます。

Workload Identity Federation の詳細は、Google Cloud のドキュメント を参照してください。



重要

Workload Identity Federation (WIF) は、OpenShift Dedicated バージョン 4.17 以降でのみ使用可能であり、Customer Cloud Subscription (CCS) インフラストラクチャータイプでのみサポートされます。

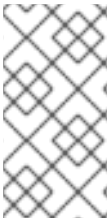
2.2. 前提条件

- Google Cloud アカウントで、クラスターのリソース要件に基づいて、目的のクラスターサイズをサポートするために必要なリソースのクォータおよび制限が設定されていることを確認した。リソースのクォータと制限の詳細は、**関連情報** を参照してください。
- OpenShift Dedicated の概要 と アーキテクチャーの概念 に関するドキュメントを確認した。
- OpenShift Dedicated クラウドデプロイメントオプション を確認した。
- 必要なお客様の手順 を読んで完了した。
- OpenShift Cluster Manager の ダウンロード ページから、オペレーティングシステムの OpenShift Cluster Manager CLI (**ocm**)の最新バージョンをダウンロードしている。https://console.redhat.com/openshift/downloads

重要

ocm は開発者プレビューのみの機能です。Red Hat 開発者プレビュー機能のサポート範囲の詳細は、開発者プレビューのサポート範囲 を参照してください。

- ワークロード ID フェデレーション 設定を作成している。詳細については、ワークフォース ID **フェデレーション設定の作成 を** 参照してください。



注記

WIF は、Private Service Connect (PSC) を使用した Google Cloud クラスター上のプライベート OpenShift Dedicated のデプロイをサポートしています。Red Hat は、プライベートクラスターをデプロイする際に PSC を使用することを推奨します。PSC の前提条件の詳細は、Private Service Connect の前提条件 を参照してください。

2.3. ワークロード ID フェデレーション設定の作成

ocm CLI では、**auto** モードまたは **manual** モードを使用して WIF 設定を作成できます。

auto モードでは、OpenShift Dedicated コンポーネントやその他の IAM リソース用のサービスアカウントを自動的に作成できます。

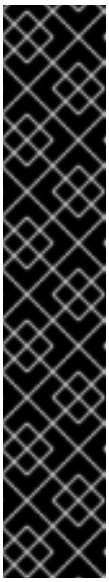
または、**manual** モードを使用することもできます。**manual** モードでは、**script.sh** ファイル内にコマンドが提供されます。このコマンドを使用して、OpenShift Dedicated コンポーネントやその他の IAM リソース用のサービスアカウントを手動で作成します。

手順

- 選択したモードに応じて、次のいずれかのコマンドを実行して WIF 設定を作成します。
  - auto モードで WIF 設定を作成するには、次のコマンドを実行します。

```
$ ocm gcp create wif-config --name <wif_name> \ 1
  --project <gcp_project_id> \ 2
  --version <osd_version> 3
  --federated-project <gcp_project_id> 4
```

1. **<wif_name>** は、WIF 設定の名前に置き換えます。
2. **<gcp_project_id>** は、WIF 設定が実装される Google Cloud プロジェクトの ID に置き換えます。
3. オプション: **<osd_version>** は、wif-config のサポートが必要な OpenShift Dedicated バージョンに置き換えます。バージョンを指定しない場合、wif-config は最新の OpenShift Dedicated y-stream バージョンと、その直前のサポート対象の OpenShift Dedicated y-stream バージョン 3 つ (バージョン 4.17 以降) をサポートします。
4. オプション: **<gcp_project_id>** は、ワークロードアイデンティティープールとプロバイダーが作成および管理される専用プロジェクトの ID に置き換えます。**--federated-project** フラグが指定されていない場合、ワークロードアイデンティティープールとプロバイダーは、**--project** フラグで指定されたプロジェクト内で作成および管理されます。



重要

Google Cloud では、専用プロジェクトを使用してワークロードアイデンティティープールとプロバイダーを作成および管理することが推奨されています。専用プロジェクトを使用すると、ワークロードアイデンティティープールとプロバイダーの設定に対する一元的なガバナンスを確立し、すべてのプロジェクトとアプリケーションにわたって均一な属性マッピングと条件を適用し、許可されたアイデンティティープロバイダーだけが WIF で認証できるようにすることが可能です。

専用プロジェクトでのワークロードアイデンティティープールとプロバイダーの作成と管理は、WIF 設定の初期作成時にのみ可能です。**--federated-project** フラグは既存の **wif-configs** には適用できません。

詳細は、専用プロジェクトを使用したワークロードアイデンティティープールとプロバイダーの管理 を参照してください。

出力例

```
2024/09/26 13:05:41 Creating workload identity configuration...
2024/09/26 13:05:47 Workload identity pool created with name
2e1kcps6jtgla8818vqs8tbjjls4oeub
2024/09/26 13:05:47 workload identity provider created with name oidc
2024/09/26 13:05:48 IAM service account osd-worker-oeub created
2024/09/26 13:05:49 IAM service account osd-control-plane-oeub created
2024/09/26 13:05:49 IAM service account openshift-gcp-ccm-oeub created
2024/09/26 13:05:50 IAM service account openshift-gcp-pd-csi-driv-oeub created
2024/09/26 13:05:50 IAM service account openshift-image-registry-oeub created
2024/09/26 13:05:51 IAM service account openshift-machine-api-gcp-oeub created
2024/09/26 13:05:51 IAM service account osd-deployer-oeub created
2024/09/26 13:05:52 IAM service account cloud-credential-operator-oeub created
```

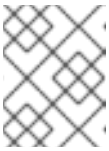
```
2024/09/26 13:05:52 IAM service account openshift-cloud-network-c-oeub created
2024/09/26 13:05:53 IAM service account openshift-ingress-gcp-oeub created
2024/09/26 13:05:55 Role "osd_deployer_v4.19" updated
```

- manual モードで WIF 設定を作成するには、次のコマンドを実行します。

```
$ ocm gcp create wif-config --name <wif_name> \ 1
  --project <gcp_project_id> \ 2
  --mode=manual
```

1. **<wif_name>** は、WIF 設定の名前に置き換えます。
2. **<gcp_project_id>** は、WIF 設定が実装される Google Cloud プロジェクトの ID に置き換えます。

WIF を設定すると、次のサービスアカウント、ロール、およびグループが作成されます。



注記

Red Hat カスタムロールは、OpenShift y-stream リリースごとにバージョン管理されます (例: 4.19)。

表2.1 WIF 設定のサービスアカウント、グループ、およびロール

サービスアカウント/グループ	Google Cloud の事前定義ロールと Red Hat のカスタムロール
osd-deployer	osd_deployer_v<y-stream-version>
osd-control-plane	■ compute.instanceAdmin ■ compute.networkAdmin ■ compute.securityAdmin ■ compute.storageAdmin
osd-worker	■ compute.storageAdmin ■ compute.viewer
cloud-credential-operator-gcp-ro-creds	cloud_credential_operator_gcp_ro_creds_v<y-stream-version>
openshift-cloud-network-config-controller-gcp	openshift_cloud_network_config_controller_gcp_v<y-stream-version>
openshift-gcp-ccm	openshift_gcp_ccm_v<y-stream-version>

サービスアカウント/グループ	Google Cloud の事前定義ロールと Red Hat のカスタムロール
openshift-gcp-pd-csi-driver-operator	■ compute.storageAdmin ■ iam.serviceAccountUser ■ resourcemanager.tagUser ■ openshift_gcp_pd_csi_driver_operator_v<y-stream-version>
openshift-image-registry-gcp	openshift_image_registry_gcs_v<y-stream-version>
openshift-ingress-gcp	openshift_ingress_gcp_v<y-stream-version>
openshift-machine-api-gcp	openshift_machine_api_gcp_v<y-stream-version>
SRE グループ経由のアクセス: sd-sre-platform-gcp-access	sre_managed_support

WIF 設定ロールとそれらに割り当てられた権限の完全なリストについては、managed-cluster-config を参照してください。

2.4. OPENSHIFT CLUSTER MANAGER を使用した WORKLOAD IDENTITY FEDERATION クラスターの作成

以下の手順に従って、OpenShift Cluster Manager Web コンソールを使用した認証用の Workload Identity Federation (WIF)を使用して Google Cloud に OpenShift Dedicated クラスターを作成します。

前提条件

- WIF 設定を作成している。詳細については、「ワークロード ID フェデレーション設定の作成」を参照してください。
- OpenShift Cluster Manager Web コンソールにアクセスできる。詳細は、関連情報 セクションの **OpenShift Cluster Manager** へのアクセス を **参照し** てください。

手順

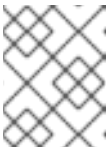
1. OpenShift Cluster Manager にログインし、OpenShift Dedicated カードで **Create cluster** をクリックします。
2. **Billing model** で、サブスクリプションタイプとインフラストラクチャータイプを設定します。
   a. サブスクリプションのタイプを選択します。OpenShift Dedicated サブスクリプションオプションは、OpenShift Cluster Manager ドキュメントの クラスターのサブスクリプションと登録 を参照してください。
   b. **Customer cloud subscription** インフラストラクチャータイプを選択します。
   c. **Next** をクリックします。

3. **Run on Google Cloud** を選択します。
4. 認証タイプとして **Workload Identity Federation** を選択します。

注記

Workload Identity Federation (WIF)は、OpenShift Dedicated インストールの認証用の Google Cloud の推奨方法です。有効期間が短く、最小権限の認証情報を使用することで、クラスターの耐性が大幅に向上し、静的なサービスアカウントキーが不要になります。

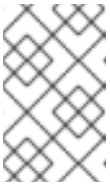
   a. 必要な前提条件をすべて読んで完了します。
   b. 必要な前提条件をすべて読んで完了したことを示すチェックボックスをクリックします。
5. **WIF configuration** ドロップダウンリストから設定済みの WIF 設定を選択します。
6. **Next** をクリックします。
7. **Details** ページで、クラスターの名前を入力し、クラスターの詳細を指定します。
   a. **Cluster name** フィールドに、クラスターの名前を入力します。
   b. オプション: クラスターを作成すると、**openshiftapps.com** にプロビジョニングされたクラスターのサブドメインとしてドメイン接頭辞が生成されます。クラスター名が 15 文字以下の場合は、その名前がドメイン接頭辞に使用されます。クラスター名が 15 文字を超える場合、ドメイン接頭辞は 15 文字の文字列としてランダムに生成されます。
   サブドメイン接頭辞をカスタマイズするには、**Create custom domain prefix**チェックボックスをオンにし、**Domain prefix** フィールドにドメイン接頭辞名を入力します。ドメイン接頭辞は 15 文字を超えてはならず、組織内で一意である必要があり、クラスターの作成後に変更できません。
   c. **Version** ドロップダウンメニューからクラスターバージョンを選択します。



注記

Workload Identity Federation (WIF) は、OpenShift Dedicated バージョン 4.17 以降でのみサポートされています。

   d. **Channel group** ドロップダウンメニューからチャネルグループを選択します。



注記

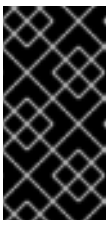
チャネルグループオプションには、**Stable** (デフォルトオプション) と **EUS** が含まれます。Stable および EUS チャネルグループオプションの詳細は、更新チャネルとリリースについて を参照してください。

   e. **Region** ドロップダウンメニューからクラウドプロバイダーのリージョンを選択します。
   f. **Single zone** または **Multi-zone** 設定を選択します。
   g. オプション: クラスターのインストール時に Shielded VM を使用するには、**Enable Secure Boot support for Shielded VMs** を選択します。クラスターを作成すると、**Enable Secure Boot support for Shielded VMs** 設定を変更できなくなります。詳細は、Shielded VMs を

参照してください。

重要

組織でポリシー制約 **constraints/compute.requireShieldedVm** が有効になっている場合、クラスターを正常に作成するには、**Enable Secure Boot support for Shielded VMs** を選択する必要があります。Google Cloud 組織ポリシーの制約に関する詳細は、組織ポリシーの制約 を参照してください。



重要

ベアメタルインスタンスタイプを使用して作成された Google Cloud 上の OpenShift Dedicated クラスターでは、**Enable Secure Boot support for Shielded VMs** はサポートされていません。詳細は、Google Cloud ドキュメントの Limitations を参照してください。

h. **Enable user workload monitoring** を選択したままにして、Red Hat サイト信頼性エンジニアリング (SRE) プラットフォームメトリクスから切り離して独自のプロジェクトをモニターします。このオプションはデフォルトで有効になっています。

8. オプション: **Advanced Encryption** を展開して、暗号化設定を変更します。

a. カスタム KMS キーを使用するには、**Use custom KMS keys** を選択します。カスタム KMS キーを使用しない場合は、デフォルト設定 **Use default KMS Keys** のままにしておきます。

b. **Use Custom KMS keys** を選択した場合は、以下を実行します。

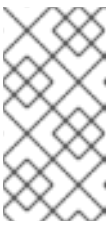
i. **Key ring location** ドロップダウンメニューからキーリングの場所を選択します。

ii. **Key ring** ドロップダウンメニューからキーリングを選択します。

iii. **Key name** ドロップダウンメニューからキー名を選択します。

iv. **KMS Service Account** を指定します。

c. オプション: クラスターで FIPS 検証を必須にする場合は、**Enable FIPS cryptography** を選択します。



注記

Enable FIPS cryptography を選択すると、**Enable additional etcd encryption** がデフォルトで有効になり、無効にできなくなります。**Enable FIPS cryptography** を選択しなくても、**Enable additional etcd encryption** は選択できます。

d. オプション: etcd キー値の暗号化が必要な場合は、**Enable additional etcd encryption** を選択します。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。このオプションは、デフォルトで OpenShift Dedicated クラスターの etcd ボリュームを暗号化するコントロールプレーンのストレージ暗号化に追加されます。

注記

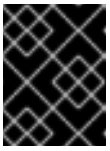
etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。お客様のユースケースで特に etcd 暗号化が必要な場合にのみ、暗号化を有効にすることを検討してください。

9. **Next** をクリックします。
10. **Machine pool** ページで、**Compute node instance type**および **Compute node count** を選択します。利用可能なノードの数およびタイプは、OpenShift Dedicated のサブスクリプションによって異なります。複数のアベイラビリティーゾーンを使用している場合、コンピュートノード数はゾーンごとに設定されます。
11. オプション: **Add node labels** を展開してラベルをノードに追加します。さらにノードラベルを追加するには、**Add additional label** をクリックします。

重要

このステップのラベルは、Google Cloud ではなく Kubernetes 内のラベルを指しています。Kubernetes のラベルの詳細は、ラベルとセレクター を参照してください。

12. **Next** をクリックします。
13. **Cluster privacy** ダイアログボックスで、**Public** または **Private** を選択し、クラスターのパブリックまたはプライベート API エンドポイントおよびアプリケーションルートを使用します。**Private** を選択した場合は、**Use Private Service Connect**がデフォルトで選択され、無効にすることはできません。Private Service Connect (PSC) は、Google Cloud のセキュリティー強化ネットワーク機能です。
14. オプション: 既存の Google Cloud Virtual Private Cloud (VPC) にクラスターをインストールする場合:
    a. **Install into an existing VPC**を選択します。



重要

Private Service Connect は、**既存の VPC へのインストール** でのみサポートされています。

    b. 既存の VPC にインストールし、クラスターの HTTP または HTTPS プロキシーを有効にする場合は、**Configure a cluster-wide proxy**を参照してください。

重要

クラスターのクラスター全体のプロキシーを設定するには、まず Cloud ネットワークアドレス変換 (NAT) と Cloud ルーターを作成する必要があります。詳細は、**関連情報** セクションを参照してください。

15. デフォルトのアプリケーション Ingress 設定を受け入れます。または、独自のカスタム設定を作成するには、**Custom Settings** を選択します。

a. オプション: ルートセレクターを指定します。

b. オプション: 除外する namespace を指定します。

c. namespace の所有権ポリシーを選択します。

d. ワイルドカードポリシーを選択します。
カスタムアプリケーションの Ingress 設定の詳細は、各設定に用意されている情報アイコンをクリックしてください。

16. **Next** をクリックします。

17. オプション: クラスターを Google Cloud 共有 VPC にインストールするには、次の手順に従います。

注記

別のクラスター用にインストーラーによって自動的に作成された VPC に新しい OpenShift Dedicated クラスターをインストールすることはサポートされていません。

重要

ホストプロジェクトの VPC 所有者は、クラスターをインストールする前に、Google Cloud コンソールでプロジェクトをホストプロジェクトとして有効にし、**Computer Network Administrator**、**Compute Security Administrator**、および **DNS Administrator** ロールを次のサービスアカウントに追加する必要があります。

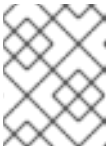
- **osd-deployer**
- **osd-control-plane**
- **openshift-machine-api-gcp**

これを行わないと、クラスターが "Installation Waiting" 状態になります。これが発生した場合は、ホストプロジェクトの VPC 所有者に連絡して、上記のサービスアカウントにロールを割り当てる必要があります。ホストプロジェクトの VPC オーナーが 30 日以内に上記の権限を付与しないと、クラスターの作成が失敗します。詳細は、Enable a host project と Provision Shared VPC を参照してください。

a. **Install into Google Cloud Shared VPC**を選択します。

b. **Host project ID** を指定します。指定したホストプロジェクト ID が間違っていると、クラスターの作成が失敗します。

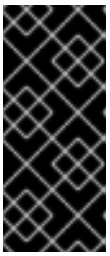
c. クラスターを既存の Google Cloud VPC にインストールする場合、**Virtual Private Cloud (VPC) サブネット設定** を指定して、**Next** を選択します。Cloud ネットワークアドレス変換 (NAT) と Cloud ルーターを作成しておく必要があります。Cloud NAT と Google VPC の詳細は、**関連情報** を参照してください。



注記

クラスターを共有 VPC にインストールする場合、VPC 名とサブネットはホストプロジェクトから共有されます。

18. **Next** をクリックします。
19. クラスター全体のプロキシーを設定することを選択した場合は、**Cluster-wide proxy** ページでプロキシー設定の詳細を指定します。
    a. 次のフィールドの少なくとも 1 つに値を入力します。
        - 有効な **HTTP proxy URL** を指定します。
        - 有効な **HTTPS proxy URL** を指定します。
        - **Additional trust bundle** フィールドに、PEM でエンコードされた X.509 証明書バンドルを指定します。このバンドルはクラスターノードの信頼済み証明書ストアに追加されます。TLS 検査プロキシーを使用する場合は、プロキシーのアイデンティティー証明書が Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルからの認証局によって署名されない限り、追加の信頼バンドルファイルが必要です。この要件は、プロキシーが透過的であるか、**http-proxy** 引数および **https-proxy** 引数を使用して明示的な設定を必要とするかに関係なく適用されます。
    b. **Next** をクリックします。
    OpenShift Dedicated でのプロキシーの設定に関する詳細は、**クラスター全体のプロキシーの設定** を参照してください。
20. **CIDR ranges** ダイアログで、カスタムの Classless Inter-Domain Routing (CIDR) 範囲を設定するか、提供されるデフォルトを使用します。



重要

CIDR 設定は後で変更することはできません。続行する前に、ネットワーク管理者と選択内容を確認してください。

クラスターのプライバシーが **Private** に設定されている場合は、クラウドプロバイダーでプライベート接続を設定するまでクラスターにアクセスできません。

21. **Cluster update strategy** ページで、更新設定を行います。
    a. クラスターの更新方法を選択します。
        - 各更新を個別にスケジュールする場合は、**Individual updates** を選択します。以下はデフォルトのオプションになります。
        - **Recurring updates** を選択して、更新が利用可能な場合に、希望の曜日と開始時刻にクラスターを更新します。

注記

OpenShift Dedicated の更新ライフサイクルのドキュメントでライフサイクルの終了日を確認できます。詳細は、OpenShift Dedicated update life cycle を参照してください。

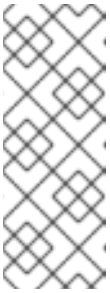
b. クラスターの更新方法に基づいて管理者の承認を提供します。

- 個別の更新: 承認が必要な更新バージョンを選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。
- 定期的な更新: クラスターの定期的な更新を選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。OpenShift Cluster Manager が、管理者承認なしでマイナーバージョンのスケジュールされた y-stream 更新を開始することはありません。

c. 繰り返し更新を選択した場合は、ドロップダウンメニューから希望の曜日およびアップグレード開始時刻 (UTC) を選択します。

d. オプション: クラスターのアップグレード時における **ノード drain (Pod の退避)** の猶予期間を設定できます。デフォルトで **1 時間** の猶予期間が設定されています。

e. **Next** をクリックします。



注記

クラスターのセキュリティーまたは安定性に大きく影響する重大なセキュリティー問題がある場合、Red Hat サイト信頼性エンジニアリング (SRE) は、影響を受けない最新の z ストリームバージョンへの自動更新をスケジュールする場合があります。更新は、お客様に通知された後、48 時間以内に適用されます。重大な影響を及ぼすセキュリティー評価の説明は、Red Hat セキュリティー評価について を参照してください。

22. 選択の概要を確認し、**Create cluster** をクリックしてクラスターのインストールを開始します。インストールが完了するまで約 30 - 40 分かかります。

23. オプション: **Overview** タブで、**Delete Protection: Disabled** のすぐ下にある **Enable** を選択して、削除保護機能を有効にできます。これにより、クラスターが削除されなくなります。削除保護を無効にするには、**Disable** を選択します。デフォルトでは、クラスターは削除保護機能が無効になった状態で作成されます。

検証

- クラスターの **Overview** ページで、インストールの進捗をモニターできます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。

重要

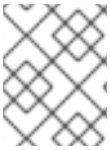
インストール中にクラスターのデプロイメントが失敗すると、インストールプロセス中に作成された特定のリソースが Google Cloud アカウントから自動的に削除されません。Google Cloud アカウントからこれらのリソースを削除するには、障害が発生したクラスターを削除する必要があります。

関連情報

- OpenShift Cluster Manager へのアクセス

2.5. OCM CLI を使用した WORKLOAD IDENTITY FEDERATION クラスターの作成

OpenShift Cluster Manager CLI (**ocm**) を使用すると、interactive モードまたは non-interactive モードで、Workload Identity Federation (WIF) を使用する Google Cloud 上の OpenShift Dedicated クラスターを作成できます。



注記

既存の非 WIF クラスターを WIF 設定に移行することはサポートされていません。この機能は、新しいクラスターの作成時にのみ有効にできます。

手順

WIF クラスターは、**interactive** モードまたは **non-interactive** モードを使用して作成できます。

interactive モードでは、クラスターの作成中にクラスター属性がプロンプトとして自動的に表示されます。指定された要件に基づいて、表示されるフィールドにプロンプトの値を入力します。

non-interactive モードでは、コマンド内の特定パラメーターの値を指定します。

- 選択したモードに応じて、次のコマンドのいずれかを実行して、WIF 設定を使用して Google Cloud 上に OpenShift Dedicated クラスターを作成します。
  - interactive モードでクラスターを作成するには、次のコマンドを実行します。

```
$ ocm create cluster --interactive 1
```

1 **interactive** モードでは、インタラクティブプロンプトで設定オプションを指定できます。

  - non-interactive モードでクラスターを作成するには、次のコマンドを実行します。

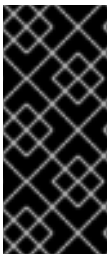
注記

次の例は、オプションおよび必須のパラメーターで構成されており、**non-interactive** モードのコマンドとは異なる場合があります。オプションと記載されていないパラメーターは必須です。これらのパラメーターやその他のパラメーターの詳細を確認するには、ターミナルウィンドウで **ocm create cluster --help flag** コマンドを実行してください。

```
$ ocm create cluster <cluster_name> \ 1
--provider=gcp \ 2
--ccs=true \ 3
--wif-config <wif_name> \ 4
--region <gcp_region> \ 5
--subscription-type=marketplace-gcp \ 6
--marketplace-gcp-terms=true \ 7
--version <version> \ 8
--multi-az=true  \ 9
--enable-autoscaling=true \ 10
--min-replicas=3 \ 11
```

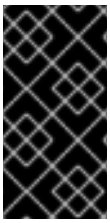
```
--max-replicas=6 \ 12
--secure-boot-for-shielded-vms=true 13
--channel-group <channel_group_name> 14
```

1. **<cluster_name>** は、クラスターの名前に置き換えます。
2. 値を **gcp** に設定します。
3. 値を **true** に設定します。
4. **<wif_name>** は、WIF 設定の名前に置き換えます。
5. **<gcp_region>** は、新しいクラスターがデプロイされる Google Cloud リージョンに置き換えます。
6. オプション: クラスターのサブスクリプション請求モデル。
7. オプション: **subscription-type** パラメーターに **marketplace-gcp** の値を指定した場合、**marketplace-gcp-terms** は **true** である必要があります。
8. オプション: 必要な OpenShift Dedicated バージョン。
9. オプション: 複数のデータセンターにデプロイします。
10. オプション: コンピュートノードの自動スケーリングを有効にします。
11. オプション: コンピュートノードの最小数。
12. オプション: コンピュートノードの最大数。
13. オプション: セキュアブートにより、Google Cloud で Shielded 仮想マシンを使用できるようになります。
14. オプション: **<channel_group_name>** は、クラスターを割り当てるチャネルグループの名前に置き換えます。チャネルグループのオプションには **stable** と **eus** が含まれます。



重要

OpenShift Dedicated バージョンが指定されている場合、バージョンも割り当てられた WIF 設定でサポートされる必要があります。割り当てられた WIF 設定でサポートされていないバージョンが指定されている場合、クラスターの作成に失敗します。作成に失敗した場合に、割り当てられた WIF 設定を任意のバージョンに更新するか、--version <osd_version> フィールドに任意のバージョンを指定して新しい WIF 設定を作成します。



重要

インストール中にクラスターのデプロイメントが失敗すると、インストールプロセス中に作成された特定のリソースが Google Cloud アカウントから自動的に削除されません。Google Cloud アカウントからこれらのリソースを削除するには、障害が発生したクラスターを削除する必要があります。

2.6. ワークロード ID フェデレーションクラスターの一覧表示

OpenShift Cluster Manager CLI (**ocm**)を使用して、Workload Identity Federation (WIF)認証を使用してデプロイされた OpenShift Dedicated クラスターを一覧表示できます。

手順

- WIF 認証タイプを使用してデプロイされたすべての OpenShift Dedicated クラスターを一覧表示するには、次のいずれかのコマンドを実行します。
  - **search** オプションで-- **parameter** フラグを使用します。

```
$ ocm list clusters --parameter search="gcp.authentication.wif_config_id != ""
```

  - 特定の wif-config ID を使用して、その設定に関連付けられたクラスターをフィルタリングします。

```
$ ocm list clusters --parameter search="gcp.authentication.wif_config_id =
'<wif_config_id>'" 1
```

1 **<wif_config_id>** を WIF 設定の ID に置き換えます。

2.7. ワークロード ID フェデレーション設定の更新

既存の Workload Identity Federation (WIF)設定を更新して、新しい OpenShift Dedicated y-stream バージョンをサポートし、最新のセキュリティーのベストプラクティスに合わせることができます。

注記

WIF 設定の更新は、y-stream の更新にのみ適用されます。バージョンセマンティクスに関する詳細を含む更新プロセスの概要は、The Ultimate Guide to OpenShift Release and Upgrade Process for Cluster Administrators を参照してください。

WIF 対応の OpenShift Dedicated クラスターを新しいバージョンに更新する前に、wif-config もそのバージョンにアップグレードする必要があります。クラスターバージョンの更新を試みる前に wif-config バージョンをアップグレードしないと、クラスターバージョンのアップグレードが失敗します。

Red Hat が継続的に取り組んでいる最小権限の原則の一環として、WIF 設定において **osd-deployer** サービスアカウントに以前割り当てられていた特定の権限が削除されました。これらの変更により、サービスアカウントには機能を実行するために必要な権限のみが付与されるようになり、クラスターのセキュリティーが強化されます。

WIF 設定ロールとそれらに割り当てられた権限の完全なリストについては、managed-cluster-config を参照してください。

既存の WIF 設定をこれらの更新された権限に合わせるには、**ocm gcp update wif-config** コマンドを実行します。このコマンドは、最適な操作に必要な最新の権限とロールを含むように WIF 設定を更新します。

wif-config を更新するか、新しい wif-config を作成する場合は、OpenShift Cluster Manager CLI (**ocm**)が最新であることを確認してください。**ocm** を最新バージョンに更新しないと、エラーメッセージが表示され、サービスが中断される可能性があります。

出力例

> Error: failed to create wif-config: failed to create wif-config: status is 400, identifier is '400', code is 'CLUSTERS-MGMT-400', at '2025-10-06T15:18:37Z' and operation identifier is 'f9551d63-a58a-4e3c-b847-5f99ba1b0b74': Client version is out of date for WIF operations. Please update from vOCM-CLI/1.0.7 to v1.0.8 and try again.

また、すでに WIF を使用している既存の OpenShift Dedicated クラスターを更新することもできます。そのためには、the- **federated-project フラグを使用してワークロード ID プールおよびプロバイダーを管理する専用のプロジェクト** を追加します。このベストプラクティスモデルでは、ワークロード ID プールとプロバイダーが専用の集中化された Google Cloud プロジェクトに分割されます。

the- **federated-project** フラグを使用して設定を更新すると、関連付けられたワークロード ID プールは、指定した新しいフェデレーションされたプロジェクトに移動します。一方、既存の IAM サービスアカウントとカスタムロールは、元のクラスターアソシエーションされたプロジェクトに残ります。

手順

1. **ocm** のバージョンを確認するには、次のコマンドを実行します。

```
$ ocm version
```

2. オプション: **ocm** バージョンが最新でない場合は、OpenShift Cluster Manager の ダウンロード ページから、最新バージョンをダウンロードしてインストールします。

3. 次のコマンドを実行し、wif-config を特定の OpenShift Dedicated バージョンに更新します。

```
ocm gcp update wif-config <wif_name> \ 1
--version <version> 2
--federated-project <gcp_project_id> 3
```

1. **<wif_name>** は、更新する WIF 設定の名前に置き換えます。
2. オプション: **<version>** は、クラスターの更新先の OpenShift Dedicated y-stream バージョンに置き換えます。バージョンを指定しない場合、wif-config は最新の OpenShift Dedicated y-stream バージョンと、その直前のサポート対象の OpenShift Dedicated y-stream バージョン 3 つ (バージョン 4.17 以降) をサポートするように更新されます。
3. オプション: **<gcp_project_id>** は、ワークロードアイデンティティープールとプロバイダーが作成および管理される専用プロジェクトの ID に置き換えます。the- **federated-project** フラグが指定されていない場合、ワークロード ID プールおよびプロバイダーはクラスターに関連付けられたプロジェクトに残ります。

次のステップ

osd-deployer サービスアカウントに以前割り当てられた古い権限セットは、wif-config を更新した後もアカウントに残ります。手動でロールにアクセスし、古い権限を削除する必要があります。

WIF 設定によって管理されるサービスアカウントからの古いデプロイパーミッションの削除と WIF 設定によって管理されているサービスアカウントからの古いサポートパーミッションの削除の手順に従い、これらの古いパーミッションを削除します。

さらに、the- **federated-project** フラグを使用してワークロード ID プールを新しい専用プロジェクトに移動した場合は、古いワークロード ID プールを元のクラスター関連付けられたプロジェクトから手動で削除できます。詳細は、Google Cloud ドキュメント の プールの削除 を参照し てください。

2.7.1. WIF 設定によって管理されるサービスアカウントから古いデプロイヤー権限を削除する

WIF 設定が管理するサービスアカウントから古いデプロイヤーパーミッションを削除するには、サービスアカウントをホストする Google Cloud プロジェクトにアクセスできるターミナルで以下のコマンドを実行します。

手順

1. 既存のロール定義を取得し、**PROJECT_ID** 環境変数が Google Cloud プロジェクトを指していることを確認します。

```
$ gcloud iam roles describe \
  osd_deployer_v4.18 \
  --project $PROJECT_ID \
  --format=yaml > /tmp/role.yaml
```

2. 不要な権限を削除します。これを行うには、ロール定義ファイルから不要な権限を除外し、更新された定義を新しいファイルに保存します。

```
$ cat /tmp/role.yaml | \
grep -v "resourcemanager.projects.setIamPolicy" | \
grep -v "iam.serviceAccounts.signBlob" | \
grep -v "iam.serviceAccounts.actAs" > /tmp/updated_role.yaml
```

3. 元のロール定義と更新されたロール定義の間の出力の変更を確認し、不要な権限のみが削除されていることを確認します。

```
$ diff /tmp/role.yaml /tmp/updated_role.yaml
```

4. 更新されたロール定義ファイルを使用して Google Cloud のロールを更新し、**PROJECT_ID** 環境変数が Google Cloud プロジェクトを指していることを確認します。

```
$ gcloud iam roles update \
  osd_deployer_v4.18 \
  --project=$PROJECT_ID \
  --file=/tmp/updated_role.yaml
```

2.7.2. WIF 設定によって管理されるサービスアカウントから古いサポート権限を削除する

古くなったサポート権限を削除するには、サービスアカウントをホストしている Google Cloud プロジェクトへのアクセス権を持つターミナルで次のコマンドを実行します。

手順

1. 既存のロール定義を取得し、**PROJECT_ID** 環境変数が Google Cloud プロジェクトを指していることを確認します。

```
$ gcloud iam roles describe sre_managed_support --project $PROJECT_ID --format=yaml >
/tmp/role.yaml
```

2. 不要な権限を削除します。これを行うには、ロール定義ファイルから不要な権限を除外し、更新された定義を新しいファイルに保存します。

```
$ cat /tmp/role.yaml | grep -v "compute.firewalls.create"  > /tmp/updated_role.yaml
```

3. 元のロール定義と更新されたロール定義の間の出力の変更を確認し、不要な権限のみが削除されていることを確認します。

```
$ diff /tmp/role.yaml /tmp/updated_role.yaml
```

4. 更新されたロール定義ファイルを使用して Google Cloud のロールを更新し、**PROJECT_ID** 環境変数が Google Cloud プロジェクトを指していることを確認します。

```
$ gcloud iam roles update sre_managed_support --project $PROJECT_ID --
file=/tmp/updated_role.yaml
```

2.8. ワークロード ID フェデレーション設定の確認

ocm gcp verify wif-config コマンドを実行すると、WIF 設定に関連付けられたリソースの設定が正しいことを確認できます。誤った設定が見つかった場合、出力には誤った設定の詳細が提供され、WIF 設定を更新するよう推奨されます。

検証を行うには、検証対象の WIF 設定の名前と ID が必要です。アクティブな WIF 設定の名前と ID を取得するには、次のコマンドを実行します。

```
$ ocm gcp list wif-configs
```

検証対象の WIF 設定が正しく設定されているかどうかを確認するには、次のコマンドを実行します。

```
$ ocm gcp verify wif-config <wif_config_name>|<wif_config_id> 1
```

1 **<wif_config_name>** と **<wif_config_id>** を、それぞれ WIF 設定の名前と ID に置き換えます。

出力例

```
Error: verification failed with error: missing role 'compute.storageAdmin'.
Running 'ocm gcp update wif-config' may fix errors related to cloud resource misconfiguration.
exit status 1.
```

2.9. 関連情報

- お客様の要件
- プロジェクトごとのリソースクォータ
- Google Cloud アカウントの制限
- 必要なお客様の手順
- ワークロード ID プールおよびプロバイダーの管理
- ロールと権限

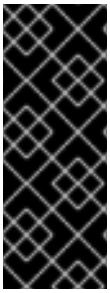
- クラスターの最大値
- アイデンティティープロバイダーの設定
- OpenShift Dedicated クラスターへのアクセスおよび権限の取り消し

第3章 サービスアカウント認証を使用して GOOGLE CLOUD 上にクラスターを作成する

3.1. サービスアカウント認証の概要

サービスアカウント認証タイプでは、認証のために秘密鍵が使用されます。サービスアカウントは、RSA キーペアを使用します。RSA キーペアは公開鍵と秘密鍵で構成され、秘密鍵はサービスアカウントキーになります。キーペアの公開部分は Google Cloud に保存され、秘密鍵はユーザーが保管します。秘密鍵により、ユーザーはサービスアカウントとして認証され、そのサービスアカウントに関連付けられたアセットやリソースにアクセスできるようになります。

サービスアカウントキーは、慎重に管理しなければセキュリティー上のリスクになり得ます。キーの漏洩や盗難のリスクを軽減するために、ユーザーはサービスアカウントキーを定期的にローテーションする必要があります。



重要

サービスアカウント認証タイプを使用する場合の潜在的なセキュリティーリスクを考慮して、Google Cloud 上にデプロイされた OpenShift Dedicated クラスターのインストールとインタラクションに使用する認証タイプとして、セキュリティーが強化された Google Cloud Workload Identity Federation (WIF) を使用することを Red Hat は推奨しています。詳細は、**関連情報** セクションの **Workload Identity Federation 認証を使用した Google Cloud 上でのクラスターの作成** を参照してください。

3.2. 前提条件

- OpenShift Dedicated の概要 と、アーキテクチャーの概念 に関するドキュメントを確認している。
- OpenShift Dedicated クラウドデプロイメントオプション を確認している。
- 必要なお客様の手順 を確認し、手順を完了した。

3.3. OPENSHIFT CLUSTER MANAGER でサービスアカウント認証を使用してクラスターを作成する

手順

1. OpenShift Cluster Manager にログインし、**Create cluster** をクリックします。
2. **Create an OpenShift cluster** ページの **Red Hat OpenShift Dedicated** 行で **Create cluster** を選択します。
3. **Billing model** セクションで、サブスクリプションのタイプおよびインフラストラクチャーのタイプを設定します。
    a. サブスクリプションのタイプを選択します。OpenShift Dedicated サブスクリプションオプションは、OpenShift Cluster Manager ドキュメントの クラスターのサブスクリプションと登録 を参照してください。

注記

利用可能なサブスクリプションタイプは、OpenShift Dedicated のサブスクリプションおよびリソースクォータに応じて異なります。Red Hat では、Google Cloud Marketplace を通じて購入したオンデマンドサブスクリプションタイプを使用してクラスターをデプロイすることを推奨しています。この方法を使用すると、消費ベースの柔軟な請求モデルを利用できます。追加容量の消費がスムーズで、Red Hat の介入が不要です。

詳細は、営業担当者または Red Hat サポートにお問い合わせください。

b. **Customer Cloud Subscription** インフラストラクチャータイプを選択し、OpenShift Dedicated を所有している既存のクラウドプロバイダーアカウントにデプロイします。

c. **Next** をクリックします。

4. **Run on Google Cloud** を選択します。

5. 認証タイプとして **Service Account** を選択します。

注記

Red Hat では、認証タイプとして Workload Identity Federation を使用することを推奨しています。詳細は、**関連情報** セクションの **Workload Identity Federation 認証を使用した Google Cloud 上でのクラスターの作成** を参照してください。

6. 記載されている **Prerequisites** (前提条件) を確認して完了します。

7. チェックボックスを選択して、すべての前提条件を読み、完了したことを確認します。

8. Google Cloud サービスアカウントの秘密鍵を JSON 形式で提供します。**Browse** をクリックし、JSON ファイルを探して添付するか、**Service account JSON** フィールドに詳細を追加できます。

9. **Next** をクリックしてクラウドプロバイダーアカウントを検証し、**Cluster details** ページに移動します。

10. **Cluster details** ページで、クラスターの名前を指定し、クラスターの詳細を指定します。

a. **Cluster name** を追加します。

b. オプション: クラスターを作成すると、**openshiftapps.com** にプロビジョニングされたクラスターのサブドメインとしてドメイン接頭辞が生成されます。クラスター名が 15 文字以下の場合は、その名前がドメイン接頭辞に使用されます。クラスター名が 15 文字を超えると、ドメイン接頭辞が 15 文字の文字列にランダムに生成されます。
サブドメインをカスタマイズするには、**Create customize domain prefix** チェックボックスをオンにし、**Domain prefix** フィールドにドメイン接頭辞名を入力します。ドメイン接頭辞は 15 文字を超えてはならず、組織内で一意である必要があり、クラスターの作成後に変更できません。

c. **Version** ドロップダウンメニューからクラスターバージョンを選択します。

重要

Private Service Connect (PSC) で設定されたクラスターは、OpenShift Dedicated バージョン 4.17 以降でのみサポートされます。PSC の詳細は、**関連情報** セクションの **Private Service の概要** を参照してください。

d. **Channel group** ドロップダウンメニューからチャネルグループを選択します。

注記

チャネルグループオプションには、**Stable** (デフォルトオプション) と **EUS** が含まれます。Stable および EUS チャネルグループオプションの詳細は、更新チャネルとリリースについて を参照してください。

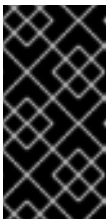
e. **Region** ドロップダウンメニューからクラウドプロバイダーのリージョンを選択します。

f. **Single zone** または **Multi-zone** 設定を選択します。

g. オプション: クラスターのインストール時に Shielded VM を使用するには、**Enable Secure Boot for Shielded VMs** を選択します。クラスターを作成すると、**Enable Secure Boot for Shielded VMs** 設定を変更できなくなります。詳細は、Shielded VMs を参照してください。

重要

組織でポリシー制約 **constraints/compute.requireShieldedVm** が有効になっている場合、クラスターを正常に作成するには、**Enable Secure Boot support for Shielded VMs** を選択する必要があります。Google Cloud 組織ポリシーの制約に関する詳細は、組織ポリシーの制約 を参照してください。



重要

ベアメタルインスタンスタイプを使用して作成された Google Cloud 上の OpenShift Dedicated クラスターでは、**Enable Secure Boot support for Shielded VMs** はサポートされていません。詳細は、Google Cloud ドキュメントの Limitations を参照してください。

h. **Enable user workload monitoring** を選択したままにして、Red Hat サイト信頼性エンジニアリング (SRE) プラットフォームメトリクスから切り離して独自のプロジェクトをモニターします。このオプションはデフォルトで有効になっています。

11. オプション: **Advanced Encryption** を展開して、暗号化設定を変更します。

a. カスタム KMS キーを使用するには、**Use custom KMS keys** を選択します。カスタム KMS キーを使用しない場合は、デフォルト設定 **Use default KMS Keys** のままにしておきます。

重要

カスタム KMS キーを使用するには、IAM サービスアカウント **osd-ccs-admin** に **Cloud KMS CryptoKey Encrypter/Decrypter** ロールを付与する必要があります。リソースに対するロールの付与の詳細は、Granting roles on a resource を参照してください。

b. **Use Custom KMS keys**を選択した場合は、以下を実行します。

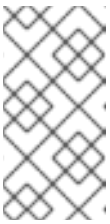
i. **Key ring location** ドロップダウンメニューからキーリングの場所を選択します。

ii. **Key ring** ドロップダウンメニューからキーリングを選択します。

iii. **Key name** ドロップダウンメニューからキー名を選択します。

iv. **KMS Service Account**を指定します。

c. オプション: クラスターで FIPS 検証を必須にする場合は、**Enable FIPS cryptography**を選択します。



注記

Enable FIPS cryptographyを選択すると、**Enable additional etcd encryption** がデフォルトで有効になり、無効にできなくなります。**Enable FIPS cryptography** を選択しなくても、**Enable additional etcd encryption** は選択できます。

d. オプション: etcd キー値の暗号化が必要な場合は、**Enable additional etcd encryption**を選択します。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。このオプションは、デフォルトで OpenShift Dedicated クラスターの etcd ボリュームを暗号化するコントロールプレーンのストレージ暗号化に追加されます。

注記

追加の etcd 暗号化を有効にすると、約 20% のパフォーマンスオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。お客様のユースケースで特に etcd 暗号化が必要な場合にのみ、暗号化を有効にすることを検討してください。

e. **Next** をクリックします。

12. **Default machine pool** ページで、ドロップダウンメニューから **Compute node instance type** を選択します。

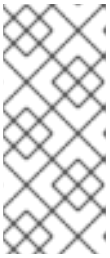
13. オプション: 自動スケーリングを有効にするには、**Enable autoscaling** チェックボックスを選択します。

a. 自動スケーリング設定を変更するには、**Edit cluster autoscaling settings**をクリックします。

b. 必要な変更を行ったら、**Close** をクリックします。

c. 最小および最大のノード数を選択します。利用可能なプラス記号とマイナス記号を使用するか、数値入力フィールドに必要なノード数を入力することで、ノード数を選択できます。

14. ドロップダウンメニューから **Compute node count** を選択します。



注記

複数のアベイラビリティーゾーンを使用している場合、コンピュートノード数はゾーンごとに設定されます。クラスターの作成後、クラスター内のコンピュートノード数は変更できますが、マシンプールのコンピュートノードインスタンスのタイプは変更できません。利用可能なノード数および種類は、OpenShift Dedicated のサブスクリプションに応じて異なります。

15. オプション: **Add node labels** を展開してラベルをノードに追加します。**Add additional label** をクリックし、ノードラベルをさらに追加して、**Next** を選択します。

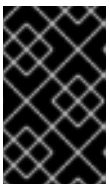
重要

このステップのラベルは、Google Cloud ではなく Kubernetes 内のラベルを指しています。Kubernetes のラベルの詳細は、ラベルとセレクター を参照してください。

16. **Network configuration** ページで **Public** または **Private** を選択し、クラスターのパブリックまたはプライベート API エンドポイントおよびアプリケーションルートを使用します。
Private を選択し、クラスターバージョンとして OpenShift Dedicated バージョン 4.17 以降を選択した場合は、**Use Private Service Connect** がデフォルトで選択されます。Private Service Connect (PSC) は、Google Cloud のセキュリティー強化ネットワーク機能です。**Use Private Service Connect** チェックボックスをクリックすると、PSC を無効にできます。

注記

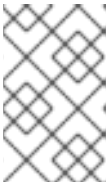
Red Hat では、Google Cloud にプライベート OpenShift Dedicated クラスターをデプロイする場合に、Private Service Connect を使用することを推奨しています。Private Service Connect は、Red Hat インフラストラクチャー、Site Reliability Engineering (SRE)、およびプライベート OpenShift Dedicated クラスター間のセキュアなプライベート接続を実現します。



重要

プライベート API エンドポイントを使用している場合は、クラウドプロバイダーアカウントのネットワーク設定を更新するまでクラスターにアクセスできません。

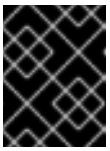
17. オプション: 既存の Google Cloud Virtual Private Cloud (VPC) にクラスターをインストールする場合:



注記

別のクラスター用にインストーラーによって自動的に作成された VPC に新しい OpenShift Dedicated クラスターをインストールすることはサポートされていません。

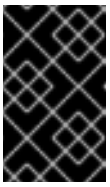
a. **Install into an existing VPC** を選択します。



重要

Private Service Connect は、**既存の VPC へのインストール** でのみサポートされています。

b. 既存の VPC にインストールし、クラスターの HTTP または HTTPS プロキシーを有効にする場合は、**Configure a cluster-wide proxy**を参照してください。



重要

クラスターのクラスター全体のプロキシーを設定するには、まず Cloud ネットワークアドレス変換 (NAT) と Cloud ルーターを作成する必要があります。詳細は、**関連情報** セクションを参照してください。

18. デフォルトのアプリケーション Ingress 設定を受け入れます。または、独自のカスタム設定を作成するには、**Custom Settings** を選択します。

a. オプション: ルートセレクターを指定します。

b. オプション: 除外する namespace を指定します。

c. namespace の所有権ポリシーを選択します。

d. ワイルドカードポリシーを選択します。
カスタムアプリケーションの Ingress 設定の詳細は、各設定に用意されている情報アイコンをクリックしてください。

19. **Next** をクリックします。

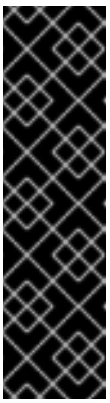
20. オプション: クラスターを Google Cloud 共有 VPC にインストールする場合:

重要

クラスターを共有 VPC にインストールするには、OpenShift Dedicated バージョン 4.13.15 以降を使用する必要があります。さらに、ホストプロジェクトの VPC オーナーが、Google Cloud コンソールでプロジェクトをホストプロジェクトとして有効にする必要があります。詳細は、Enable a host project を参照してください。

a. **Install into Google Cloud Shared VPC**を選択します。

b. **Host project ID** を指定します。指定したホストプロジェクト ID が間違っていると、クラスターの作成が失敗します。



重要

クラスター設定ウィザード内の手順を完了し、**Create Cluster** をクリックすると、クラスターが "Installation Waiting" の状態になります。この時点で、ホストプロジェクトの VPC オーナーに連絡する必要があります。オーナーは動的に生成されたサービスアカウントに、**Compute Network Administrator**、**Compute Security Administrator**、**Project IAM Admin**、および **DNS Administrator** ロールを割り当てる必要があります。ホストプロジェクトの VPC オーナーが 30 日以内に上記の権限を付与しないと、クラスターの作成が失敗します。共有 VPC の権限の詳細は、Provision Shared VPC を参照してください。

21. クラスターを既存の Google Cloud VPC にインストールする場合、**Virtual Private Cloud (VPC) サブネット設定** を指定して、**Next** を選択します。Cloud ネットワークアドレス変換 (NAT) と Cloud ルーターを作成しておく必要があります。Cloud NAT と Google VPC は、「関

連情報」のセクションを参照してください。

注記

クラスターを共有 VPC にインストールする場合、VPC 名とサブネットはホストプロジェクトから共有されます。

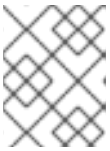
22. クラスター全体のプロキシーを設定することを選択した場合は、**Cluster-wide proxy** ページでプロキシー設定の詳細を指定します。

    a. 次のフィールドの少なくとも 1 つに値を入力します。

    - 有効な **HTTP proxy URL** を指定します。
    - 有効な **HTTPS proxy URL** を指定します。
    - **Additional trust bundle** フィールドに、PEM でエンコードされた X.509 証明書バンドルを指定します。このバンドルはクラスターノードの信頼済み証明書ストアに追加されます。TLS 検査プロキシーを使用する場合は、プロキシーのアイデンティティー証明書が Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルからの認証局によって署名されない限り、追加の信頼バンドルファイルが必要です。この要件は、プロキシーが透過的であるか、**http-proxy** 引数および **https-proxy** 引数を使用して明示的な設定を必要とするかに関係なく適用されます。

    b. **Next** をクリックします。
    OpenShift Dedicated でのプロキシーの設定に関する詳細は、**クラスター全体のプロキシーの設定** を参照してください。

23. **CIDR ranges** ダイアログで、カスタムの Classless Inter-Domain Routing (CIDR) 範囲を設定するか、提供されるデフォルトを使用します。



注記

VPC にインストールする場合は、**Machine CIDR** 範囲を VPC サブネットに一致させる必要があります。

重要

CIDR 設定は後で変更することはできません。続行する前に、ネットワーク管理者と選択内容を確認してください。

24. **Cluster update strategy** ページで、更新設定を行います。

    a. クラスターの更新方法を選択します。

    - 各更新を個別にスケジュールする場合は、**Individual updates** を選択します。以下はデフォルトのオプションになります。
    - **Recurring updates** を選択して、更新が利用可能な場合に、希望の曜日と開始時刻にクラスターを更新します。

注記

OpenShift Dedicated の更新ライフサイクルのドキュメントでライフサイクルの終了日を確認できます。詳細は、OpenShift Dedicated 更新ライフサイクル を参照してください。

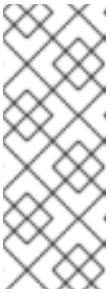
b. クラスターの更新方法に基づいて管理者の承認を提供します。

- 個別の更新: 承認が必要な更新バージョンを選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。
- 定期的な更新: クラスターの定期的な更新を選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。OpenShift Cluster Manager が、管理者承認なしでマイナーバージョンのスケジュールされた y-stream 更新を開始することはありません。

c. 繰り返し更新を選択した場合は、ドロップダウンメニューから希望の曜日およびアップグレード開始時刻 (UTC) を選択します。

d. オプション: クラスターのアップグレード時における **ノード drain (Pod の退避)** の猶予期間を設定できます。デフォルトで **1時間** の猶予期間が設定されています。

e. **Next** をクリックします。

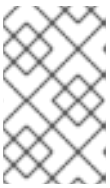


注記

クラスターのセキュリティーまたは安定性に大きく影響する重大なセキュリティー問題がある場合、Red Hat サイト信頼性エンジニアリング (SRE) は、影響を受けない最新の z ストリームバージョンへの自動更新をスケジュールする場合があります。更新は、お客様に通知された後、48 時間以内に適用されます。重大な影響を及ぼすセキュリティー評価の説明は、Red Hat セキュリティー評価について を参照してください。

25. 選択の概要を確認し、**Create cluster** をクリックしてクラスターのインストールを開始します。インストールが完了するまで約 30 - 40 分かかります。

26. オプション: **Overview** タブで、**Delete Protection: Disabled** のすぐ下にある **Enable** を選択して、削除保護機能を有効にできます。これにより、クラスターが削除されなくなります。削除保護を無効にするには、**Disable** を選択します。デフォルトでは、クラスターは削除保護機能が無効になった状態で作成されます。



注記

Google Cloud 共有 VPC にインストールされたクラスターを削除する場合は、ホストプロジェクトの VPC オーナーに、クラスター作成時に言及したサービスアカウントに付与された IAM ポリシーロールを削除するように通知します。

検証

- クラスターの **Overview** ページで、インストールの進捗をモニターできます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。

重要

インストール中にクラスターのデプロイメントが失敗すると、インストールプロセス中に作成された特定のリソースが Google Cloud アカウントから自動的に削除されません。Google Cloud アカウントからこれらのリソースを削除するには、障害が発生したクラスターを削除する必要があります。

3.4. 関連情報

- Workload Identity Federation の詳細は、Workload Identity Federation 認証を使用した Google Cloud 上でのクラスターの作成 を参照してください。
- Private Service Connect (PSC) の詳細は、Private Service Connect の概要 を参照してください。
- OpenShift Dedicated でのプロキシーの設定に関する詳細は、クラスター全体のプロキシーの設定 を参照してください。
- OpenShift Dedicated の永続ストレージの詳細は、OpenShift Dedicated サービス定義の ストレージ セクションを参照してください。
- OpenShift Dedicated のロードバランサーの詳細は、OpenShift Dedicated サービス定義の ロードバランサー セクションを参照してください。
- etcd 暗号化の詳細は、etcd 暗号化サービスの定義 を参照してください。
- OpenShift Dedicated バージョンのライフサイクル期間の詳細は、OpenShift Dedicated の更新ライフサイクル を参照してください。
- クラスター全体のプロキシーに必要な Cloud ネットワークアドレス変換 (NAT) の一般的な情報は、Google ドキュメントの Cloud NAT overview を参照してください。
- クラスター全体のプロキシーに必要な Cloud Router に関する一般的な情報は、Google ドキュメントの Cloud Router overview を参照してください。
- Google Cloud Provider アカウント内で VPC を作成する方法は、Google ドキュメントの Create and manage VPC networks を参照してください。
- アイデンティティープロバイダーの設定は、アイデンティティープロバイダーの設定 を参照してください。
- クラスター権限の取り消しは、OpenShift Dedicated クラスターへのアクセスおよび権限の取り消し を参照してください。

第4章 RED HAT クラウドアカウントを使用して GOOGLE CLOUD 上にクラスターを作成する

OpenShift Cluster Manager を使用して、Red Hat が所有する標準のクラウドプロバイダーアカウントを使用して Google Cloud に OpenShift Dedicated クラスターを作成できます。

4.1. 前提条件

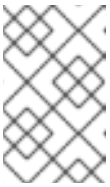
- OpenShift Dedicated の概要 と、アーキテクチャーの概念 に関するドキュメントを確認している。
- OpenShift Dedicated クラウドデプロイメントオプション を確認している。

4.2. OPENSHIFT CLUSTER MANAGER を使用して、RED HAT クラウドアカウントで GOOGLE CLOUD 上にクラスターを作成する

OpenShift Cluster Manager を使用して、Red Hat が所有する標準のクラウドプロバイダーアカウントを使用して Google Cloud に OpenShift Dedicated クラスターを作成できます。

手順

1. OpenShift Cluster Manager にログインし、**Create cluster** をクリックします。
2. **Cloud** タブで、**Red Hat OpenShift Dedicated** 行の **Create cluster** をクリックします。
3. **Billing model** セクションで、サブスクリプションのタイプおよびインフラストラクチャーのタイプを設定します。
   a. **Annual** サブスクリプションタイプを選択します。Red Hat クラウドアカウントを使用してクラスターをデプロイする場合は、**Annual** サブスクリプションタイプのみを使用できます。
   OpenShift Dedicated サブスクリプションオプションは、OpenShift Cluster Manager ドキュメントの クラスターのサブスクリプションと登録 を参照してください。

   注記

   Annual サブスクリプションタイプに必要なリソースクォータが利用可能でなければなりません。詳細は、営業担当者または Red Hat サポートにお問い合わせください。

   b. **Red Hat cloud account** インフラストラクチャータイプを選択して、Red Hat が所有するクラウドプロバイダーアカウントに OpenShift Dedicated をデプロイします。
   c. **Next** をクリックします。
4. **Run on Google Cloud** を選択し、**Next** をクリックします。
5. **Cluster details** ページで、クラスターの名前を指定し、クラスターの詳細を指定します。
   a. **Cluster name** を追加します。
   b. オプション: クラスターを作成すると、**openshiftapps.com** にプロビジョニングされたクラスターのサブドメインとしてドメイン接頭辞が生成されます。クラスター名が 15 文字以

下の場合は、その名前がドメイン接頭辞に使用されます。クラスター名が 15 文字を超える場合、ドメイン接頭辞は 15 文字の文字列としてランダムに生成されます。
サブドメインをカスタマイズするには、**Create custom domain prefix**チェックボックスをオンにし、**Domain prefix** フィールドにドメイン接頭辞名を入力します。ドメイン接頭辞は 15 文字を超えてはならず、組織内で一意である必要があり、クラスターの作成後に変更できません。

c. **Version** ドロップダウンメニューからクラスターバージョンを選択します。

d. **Channel group** ドロップダウンメニューからチャネルグループを選択します。

注記

チャネルグループオプションには、**Stable** (デフォルトオプション) と **EUS** が含まれます。Stable および EUS チャネルグループオプションの詳細は、更新チャネルとリリースについて を参照してください。

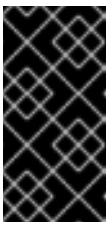
e. **Region** ドロップダウンメニューからクラウドプロバイダーのリージョンを選択します。

f. **Single zone** または **Multi-zone** 設定を選択します。

g. クラスターの **Persistent storage** 容量を選択します。詳細は、OpenShift Dedicated サービス定義の **Storage** セクションを参照してください。

h. クラスターに必要な **Load balancers** の数を指定します。詳細は、OpenShift Dedicated サービス定義の **Load balancers** セクションを参照してください。

i. オプション: クラスターのインストール時に Shielded VM を使用するには、**Enable Secure Boot support for Shielded VMs** を選択します。クラスターを作成すると、**Enable Secure Boot support for Shielded VMs** 設定を変更できなくなります。詳細は、Shielded VMs を参照してください。



重要

組織でポリシー制約 **constraints/compute.requireShieldedVm** が有効になっている場合、クラスターを正常に作成するには、**Enable Secure Boot support for Shielded VMs** を選択する必要があります。Google Cloud 組織ポリシーの制約に関する詳細は、組織ポリシーの制約 を参照してください。

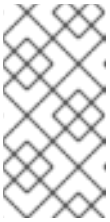
重要

ベアメタルインスタンスタイプを使用して作成された Google Cloud 上の OpenShift Dedicated クラスターでは、**Enable Secure Boot support for Shielded VMs** はサポートされていません。詳細は、Google Cloud ドキュメントの Limitations を参照してください。

j. **Enable user workload monitoring** を選択したままにして、Red Hat サイト信頼性エンジニアリング (SRE) プラットフォームメトリクスから切り離して独自のプロジェクトをモニターします。このオプションはデフォルトで有効になっています。

6. オプション: **Advanced Encryption** を展開して、暗号化設定を変更します。

a. オプション: クラスターで FIPS 検証を必須にする場合は、**Enable FIPS cryptography** を選択します。



注記

Enable FIPS cryptography を選択すると、**Enable additional etcd encryption** がデフォルトで有効になり、無効にできなくなります。**Enable FIPS cryptography** を選択しなくても、**Enable additional etcd encryption** は選択できます。

b. オプション: etcd キー値の暗号化が必要な場合は、**Enable additional etcd encryption** を選択します。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。このオプションは、デフォルトで OpenShift Dedicated クラスターの etcd ボリュームを暗号化するコントロールプレーンのストレージ暗号化に追加されます。

注記

etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。お客様のユースケースで特に etcd 暗号化が必要な場合にのみ、暗号化を有効にすることを検討してください。

c. **Next** をクリックします。

7. **Default machine pool** ページで、**Compute node instance type** および **Compute node count** を選択します。利用可能なノードの数およびタイプは、OpenShift Dedicated のサブスクリプションによって異なります。複数のアベイラビリティーゾーンを使用している場合、コンピュートノード数はゾーンごとに設定されます。

注記

クラスターの作成後に、コンピュートノード数を変更できますが、マシンプールのコンピュートノードインスタンスのタイプを変更することはできません。CCS モデルを使用するクラスターの場合、インストール後に別のインスタンスタイプを使用するマシンプールを追加できます。利用可能なノード数および種類は、OpenShift Dedicated のサブスクリプションに応じて異なります。

8. オプション: **Edit node labels** を展開してラベルをノードに追加します。**Add label** をクリックしてさらにノードラベルを追加し、**Next** を選択します。

9. **Cluster privacy** ダイアログボックスで、**Public** または **Private** を選択し、クラスターのパブリックまたはプライベート API エンドポイントおよびアプリケーションルートを使用します。

10. **Next** をクリックします。

11. **CIDR ranges** ダイアログで、カスタムの Classless Inter-Domain Routing (CIDR) 範囲を設定するか、提供されるデフォルトを使用します。

重要

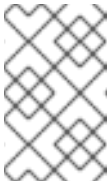
CIDR 設定は後で変更することはできません。続行する前に、ネットワーク管理者と選択内容を確認してください。

クラスターのプライバシーが **Private** に設定されている場合は、クラウドプロバイダーでプライベート接続を設定するまでクラスターにアクセスできません。

12. **Cluster update strategy** ページで、更新設定を行います。

    a. クラスターの更新方法を選択します。

    - 各更新を個別にスケジュールする場合は、**Individual updates** を選択します。以下はデフォルトのオプションになります。
    - **Recurring updates** を選択して、更新が利用可能な場合に、希望の曜日と開始時刻にクラスターを更新します。



注記

OpenShift Dedicated の更新ライフサイクルのドキュメントでライフサイクルの終了日を確認できます。詳細は、OpenShift Dedicated 更新ライフサイクル を参照してください。

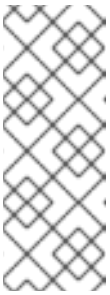
    b. クラスターの更新方法に基づいて管理者の承認を提供します。

    - 個別の更新: 承認が必要な更新バージョンを選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。
    - 定期的な更新: クラスターの定期的な更新を選択した場合は、管理者の確認を提供し、**Approve and continue** をクリックします。OpenShift Cluster Manager が、管理者承認なしでマイナーバージョンのスケジュールされた y-stream 更新を開始することはありません。

    c. 繰り返し更新を選択した場合は、ドロップダウンメニューから希望の曜日およびアップグレード開始時刻 (UTC) を選択します。

    d. オプション: クラスターのアップグレード時における **ノード drain (Pod の退避)** の猶予期間を設定できます。デフォルトで **1 時間** の猶予期間が設定されています。

    e. **Next** をクリックします。



注記

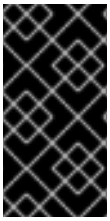
クラスターのセキュリティーまたは安定性に大きく影響する重大なセキュリティー問題がある場合、Red Hat サイト信頼性エンジニアリング (SRE) は、影響を受けない最新の z ストリームバージョンへの自動更新をスケジュールする場合があります。更新は、お客様に通知された後、48 時間以内に適用されます。重大な影響を及ぼすセキュリティー評価の説明は、Red Hat セキュリティー評価について を参照してください。

13. 選択の概要を確認し、**Create cluster** をクリックしてクラスターのインストールを開始します。インストールが完了するまで約 30 - 40 分かかります。

14. オプション: **Overview** タブで、**Delete Protection: Disabled** のすぐ下にある **Enable** を選択して、削除保護機能を有効にできます。これにより、クラスターが削除されなくなります。削除保護を無効にするには、**Disable** を選択します。デフォルトでは、クラスターは削除保護機能が無効になった状態で作成されます。

検証

- クラスターの **Overview** ページで、インストールの進捗をモニターできます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。



重要

インストール中にクラスターのデプロイメントが失敗すると、インストールプロセス中に作成された特定のリソースが Google Cloud アカウントから自動的に削除されません。Google Cloud アカウントからこれらのリソースを削除するには、障害が発生したクラスターを削除する必要があります。

4.3. 次のステップ

- クラスターのアイデンティティープロバイダーの設定は、アイデンティティープロバイダーの設定 を参照してください。
- クラスターのユーザーに管理者権限を付与する方法は、ユーザーへの管理者権限の付与 を参照してください。

第5章 GOOGLE CLOUD 上の OPENSHIFT DEDICATED クラスターの削除

クラスターの所有者は、OpenShift Dedicated クラスターを削除できます。

5.1. クラスターの削除

Red Hat OpenShift Cluster Manager で OpenShift Dedicated クラスターを削除できます。

前提条件

- OpenShift Cluster Manager にログインしている。
- OpenShift Dedicated クラスターを作成している。

手順

1. OpenShift Cluster Manager で、削除するクラスターをクリックします。
2. **Actions** ドロップダウンメニューから **Delete cluster** を選択します。
3. 太字で強調表示されているクラスターの名前を入力してから **Delete** をクリックします。クラスターの削除は自動的に実行されます。

注記

Google Cloud 共有 VPC にインストールされたクラスターを削除する場合は、ホストプロジェクトの VPC オーナーに、クラスター作成時に言及したサービスアカウントに付与された IAM ポリシーロールを削除するように通知します。