



## OpenShift Dedicated 4

# OpenShift Dedicated クラスターのインストール、アクセス、および削除

OpenShift Dedicated クラスターのインストール、アクセス、および削除



## OpenShift Dedicated 4 OpenShift Dedicated クラスターのインストール、アクセス、および削除

---

OpenShift Dedicated クラスターのインストール、アクセス、および削除

## 法律上の通知

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

このドキュメントでは、OpenShift Dedicated クラスターをインストールする方法を説明します。このドキュメントには、ID プロバイダーの設定方法の詳細も記載されています。

---

## 目次

<b>第1章 AWS でのクラスターの作成</b> .....	<b>3</b>
1.1. 前提条件	3
1.2. CCS を使用した AWS でのクラスターの作成	3
1.3. RED HAT クラウドアカウントを使用した AWS でのクラスターの作成	9
1.4. 関連情報	12
<b>第2章 GCP でのクラスターの作成</b> .....	<b>13</b>
2.1. 前提条件	13
2.2. CCS を使用した GCP でのクラスターの作成	13
2.3. GOOGLE CLOUD MARKETPLACE を使用して GCP 上にクラスターを作成する	19
2.4. RED HAT クラウドアカウントを使用した GCP でのクラスターの作成	24
2.5. RED HAT MARKETPLACE を使用した GCP でのクラスターの作成	28
2.6. 関連情報	33
<b>第3章 アイデンティティプロバイダーの設定</b> .....	<b>34</b>
3.1. アイデンティティプロバイダーについて	34
3.2. GITHUB アイデンティティプロバイダーの設定	35
3.3. GITLAB アイデンティティプロバイダーの設定	37
3.4. GOOGLE アイデンティティプロバイダーの設定	38
3.5. LDAP アイデンティティプロバイダーの設定	39
3.6. OPENID アイデンティティプロバイダーの設定	41
3.7. HTTPASSWD アイデンティティプロバイダーの設定	43
3.8. クラスターへのアクセス	44
<b>第4章 OPENSIFT DEDICATED クラスターへのアクセスおよび権限の取り消し</b> .....	<b>46</b>
4.1. ユーザーからの管理者権限の削除	46
4.2. クラスターへのユーザーアクセスの取り消し	46
<b>第5章 OPENSIFT DEDICATED クラスターの削除</b> .....	<b>48</b>
5.1. クラスターの削除	48



# 第1章 AWS でのクラスタの作成

Customer Cloud Subscription (CCS) モデルを通じて独自の AWS アカウントを使用するか、Red Hat が所有する AWS インフラストラクチャーアカウントを使用して、Amazon Web Services (AWS) に OpenShift Dedicated をインストールできます。

## 1.1. 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。

## 1.2. CCS を使用した AWS でのクラスタの作成

Customer Cloud Subscription (CCS) 請求モデルを使用すると、所有している既存の Amazon Web Services (AWS) アカウントに OpenShift Dedicated クラスタを作成できます。

CCS モデルを使用して OpenShift Dedicated を AWS アカウントにデプロイし、管理する場合には、いくつかの前提条件を満たす必要があります。

### 前提条件

- OpenShift Dedicated で使用する AWS アカウントを設定している。
- AWS アカウントにサービスをデプロイしていない。
- 必要なクラスタサイズをサポートするために必要な AWS アカウントのクォータおよび制限を設定している。
- **AdministratorAccess** ポリシーが割り当てられた **osdCcsAdmin** AWS Identity and Access Management (IAM) ユーザーがある。
- AWS 組織にサービスコントロールポリシー (SCP) を設定している。詳細は、**Minimum required service control policy (SCP)** を参照。
- AWS の **Business Support** またはそれ以上のサービスを用意することを検討してください。
- クラスタ全体のプロキシを設定する場合は、クラスタがインストールされている VPC からプロキシにアクセスできることを確認している。プロキシは VPC のプライベートサブネットからもアクセスできる必要があります。

### 手順

1. [OpenShift Cluster Manager](#) にログインし、**Create cluster** をクリックします。
2. **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については、OpenShift Cluster Manager ドキュメントの [クラスタ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よって異なります。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 Amazon Web Services** を選択します。
  5. クラウドプロバイダーを選択したら、表示されている **前提条件** を確認して完了します。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。
  6. AWS アカウントの詳細を指定します。
    - a. **AWS アカウント ID** を入力します。
    - b. AWS IAM ユーザーアカウントの **AWS アクセスキー ID** および **AWS シークレットアクセスキー** を入力します。



### 注記

AWS でこれらの認証情報を取り消すと、これらの認証情報を使用して作成されたクラスターへのアクセスが失われます。

- c. オプション: **Bypass AWS Service Control Policy (SCP) checks** を選択して、SCP チェックを無効にすることができます。



### 注記

AWS SCP によっては、必要なパーミッションがある場合でもインストールに失敗することがあります。SCP チェックを無効にすると、インストールを続行できます。チェックがバイパスされた場合でも SCP が有効になります。

7. **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。
8. **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、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。



- d. **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。
- e. **Single zone** または **Multi-zone** 設定を選択します。
- f. **Enable user workloads 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ック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。
- g. オプション:etcd キー値の暗号化が必要な場合には、**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。

- h. オプション: 独自の AWS Key Management Service (KMS) キーの Amazon Resource Name (ARN) を提供する場合は、**Encrypt persistent volumes with customer keys** を選択します。このキーは、クラスタ内のすべてのコントロールプレーン、インフラストラクチャー、ワーカーノードのルートボリューム、および永続ボリュームを暗号化するために使用されます。



### 重要

デフォルトのストレージクラスから作成された永続ボリューム (PV) のみが、この特定のキーで暗号化されます。

他のストレージクラスを使用して作成された PV は引き続き暗号化されませんが、ストレージクラスがこのキーを使用するように特別に設定されていない限り、PV はこのキーで暗号化されません。

- i. **Next** をクリックします。
9. **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ゾーンを使用している場合、コンピュータノード数はゾーンごとに設定されます。



### 注記

クラスタの作成後に、クラスタ内のコンピュータノード数を変更できますが、マシンプールのコンピュータ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。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よって異なります。

10. Instance Metadata Service (IMDS) タイプを設定します。IMDSv1 と IMDSv2 の両方のタイプを使用するか、EC2 インスタンスで IMDSv2 のみを使用するように要求します。実行中のインスタンスからインスタンスメタデータにアクセスするには、以下の 2 つの方法があります。

- Instance Metadata Service バージョン 1 (IMDSv1) - リクエスト/レスポンスメソッド
- Instance Metadata Service バージョン 2 (IMDSv2) - セッション指向のメソッド



### 重要

クラスターの作成後に Instance Metadata Service の設定を変更することはできません。



### 注記

IMDSv2 はセッション指向のリクエストを使用します。セッション指向のリクエストでは、セッション期間を定義するセッショントークンを作成します。セッション期間は最小 1 秒、最大 6 時間です。指定された期間中は、後続のリクエストに同じセッショントークンを使用できます。指定された期間が経過した後は、今後のリクエストに使用する新しいセッショントークンを作成する必要があります。

IMDS の詳細は、AWS ドキュメントの [Instance metadata and user data](#) を参照してください。

11. 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。
12. **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。



### 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、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はアクセスできません。

13. オプション: クラスターを既存の AWS Virtual Private Cloud (VPC) にインストールするには、以下を実行します。
  - a. **Install to an existing VPC** を選択します。
  - b. 既存の VPC にインストールし、プライベート API エンドポイントを使用することを選択した場合は、 **Use a PrivateLink** を選択します。このオプションを選択した場合に、AWS PrivateLink エンドポイントのみを使用した Red Hat Site Reliability Engineering (SRE) によるクラスターへの接続が可能になります。

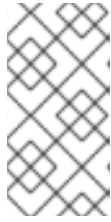


### 注記

**Use a PrivateLink** オプションは、クラスターの作成後に変更できません。

- c. 既存の VPC にインストールし、クラスターの HTTP または HTTPS プロキシを有効にする場合は、 **Configure a cluster-wide proxy** を参照してください。
14. **Next** をクリックします。
  15. クラスターを既存の AWS 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。クラウドネットワークアドレス変換 (NAT) とク

ラウトルーターを作成しておく必要があります。Cloud NAT と Google VPC については、関連情報のセクションを参照してください。



### 注記

クラスタをインストールするアベイラビリティゾーンごとに、VPC がパブリックおよびプライベートサブネットを設定されるようにする必要があります。PrivateLink を使用する場合には、プライベートサブネットのみが必要になります。

- a. オプション: **追加のセキュリティーグループ** を展開し、デフォルトで作成されるマシンプール内のノードに適用する追加のカスタムセキュリティーグループを選択します。すでにセキュリティーグループを作成し、このクラスタ用に選択した VPC にそのグループを関連付けている必要があります。クラスタを作成した後は、デフォルトのマシンプールにセキュリティーグループを追加または編集することはできません。デフォルトでは、指定したセキュリティーグループはすべてのノードタイプに追加されます。ノードタイプごとに異なるセキュリティーグループを適用するには、**Apply the same security groups to all node types** チェックボックスをオフにします。

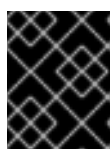
詳細は、**関連情報** の **セキュリティーグループ** の要件を参照してください。

16. クラスタ全体のプロキシ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 検査プロキシを使用する場合は、プロキシのアイデンティティ証明書が 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、プロキシが透過的であるか、**http-proxy** 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 でのプロキシの設定に関する詳細は、**クラスタ全体のプロキシの設定** を参照してください。
17. **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、**Machine CIDR** 範囲は VPC サブネットに一致する必要があります。



### 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。

## 18. 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: クラスターアップグレード時の **ノードのドレイン (解放)** 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または安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

19. 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。
20. 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、クラスタは準備が完了した状態になります。

### 1.3. RED HAT クラウドアカウントを使用した AWS でのクラスタの作成

[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 Amazon Web Services (AWS) に OpenShift Dedicated クラスタを作成できます。

#### 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については、OpenShift Cluster Manager ドキュメントの [クラスタ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 Amazon Web Services** を選択し、**Next** をクリックします。
  5. **Cluster details** ページで、クラスタの名前を指定し、クラスタの詳細を指定します。
    - a. **Cluster name** を追加します。
    - b. オプション: クラスタを作成すると、**openshiftapps.com** にプロビジョニングされたクラスタのサブドメインとしてドメイン接頭辞が生成されます。クラスタ名が 15 文字以下の場合、その名前がドメイン接頭辞に使用されます。クラスタ名が 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バージョンを選択します。
    - d. **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。
    - e. **Single zone** または **Multi-zone** 設定を選択します。

- f. 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。
- g. 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。
- h. **Enable user workloads 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ック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。
- i. オプション: etcd キー値の暗号化が必要な場合には、**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。

- j. **Next** をクリックします。

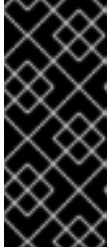
6. **Default machine pool** ページで、**Compute node instance type** および **Compute node count** を選択します。利用可能なノードの数およびタイプは、OpenShift Dedicated のサブスクリプションによって異なります。複数のアベイラビリティゾーンを使用している場合、コンピュートノード数はゾーンごとに設定されます。



### 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よって異なります。

7. 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。
8. **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。
9. **Next** をクリックします。
10. **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にアクセスできません。

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

a. クラスタ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: クラスタアップグレード時の **ノードのドレイン (解放)** 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

クラスタのセキュリティまたは安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

12. 選択の概要を確認し、**Create cluster** をクリックしてクラスタ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。

13. 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。

## 1.4. 関連情報

- OpenShift Dedicated でのプロキシの設定に関する詳細は、[クラスター全体のプロキシの設定](#) を参照してください。
- CCS デプロイメントに必要な AWS サービスコントロールポリシーの詳細は、[最低限必要な Service Control Policy \(SCP\)](#) を参照してください。
- OpenShift Dedicated の永続ストレージについての詳細は、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。
- カスタムの追加セキュリティーグループの要件は、[追加のカスタムセキュリティーグループ](#) を参照してください。



## 第2章 GCP でのクラスタの作成

Customer Cloud Subscription (CCS) モデルを通じて独自の GCP アカウントを使用するか、Red Hat が所有する GCP インフラストラクチャーアカウントを使用して、Google Cloud Platform (GCP) に OpenShift Dedicated をインストールできます。

### 2.1. 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。

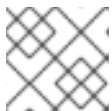
### 2.2. CCS を使用した GCP でのクラスタの作成

Customer Cloud Subscription (CCS) 請求モデルを使用すると、所有している既存の Google Cloud Platform (GCP) アカウントに OpenShift Dedicated クラスタを作成できます。

CCS モデルを使用して OpenShift Dedicated を GCP アカウントにデプロイし、管理する場合には、いくつかの前提条件を満たす必要があります。

#### 前提条件

- OpenShift Dedicated で使用する GCP アカウントを設定している。
- 必要なクラスタサイズをサポートするために必要な GCP アカウントのクォータおよび制限を設定している。
- GCP プロジェクトを作成している。



#### 注記

プロジェクト名は 10 文字以下である必要があります。

- GCP プロジェクトで Google Cloud Resource Manager API を有効にしている。プロジェクトの API の有効化に関する詳細は、[Google Cloud のドキュメント](#) を参照してください。
- **osd-ccs-admin** という名前の GCP の IAM サービスアカウントに以下のロールが割り当てられている。
  - Compute 管理者
  - DNS 管理者
  - セキュリティー管理者
  - Service Account Admin
  - サービスアカウントキー管理者
  - Service Account User
  - 組織ポリシービューアー
  - サービス管理管理者

- サービス使用状況の管理
- ストレージ管理者
- ロードバランサー計算の管理者
- ロール閲覧者
- ロール管理者
- **osd-ccs-admin** GCP サービスアカウントのキーを作成し、それを **osServiceAccount.json** という名前のファイルにエクスポートしている。



### 注記

GCP サービスアカウントのキーを作成し、それを JSON ファイルにインポートする方法は、Google Cloud のドキュメントの [サービスアカウントキーの作成](#) を参照。

- GCP の [サポートを強化](#) するか、またはそれ以上の機能を用意することを検討してください。
- 潜在的な競合を防ぐためには、OpenShift Dedicated をインストールする前にプロジェクトで他のリソースがプロビジョニングされないようにすることを検討してください。
- クラスター全体のプロキシを設定する場合は、クラスターがインストールされている VPC からプロキシにアクセスできることを確認している。

## 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については、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よって異なります。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 Platform** を選択します。

5. クラウドプロバイダーを選択したら、表示されている **前提条件** を確認して完了します。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。
6. JSON 形式で GCP サービスアカウントの秘密鍵を指定します。 **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。
7. **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。
8. **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、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。
  - d. **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。
  - e. **Single zone** または **Multi-zone** 設定を選択します。
  - f. オプション: クラスターのインストール時にシールドされた VM を使用するには、 **Enable Secure Boot for Shielded VMs** を選択します。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。GCP 組織ポリシーの制約の詳細は、 [組織ポリシーの制約](#) を参照してください。

- g. **Enable user workloads 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ック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。
9. 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。

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。
- b. オプション: etcd キー値の暗号化が必要な場合には、**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. 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。
  - d. **Next** をクリックします。
10. **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ゾーンを使用している場合、コンピュータ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、クラスター内のコンピュータノード数を変更できますが、マシンプールのコンピュータ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。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よって異なります。

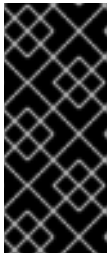
11. オプション: **Edit node labels** を展開してラベルをノードに追加します。**Add label** をクリックしてさらにノードラベルを追加し、**Next** を選択します。
12. **Network configuration** ページで **Public** または **Private** を選択し、クラスターのパブリックまたはプライベート API エンドポイントおよびアプリケーションルートを使用します。



### 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、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はアクセスできません。

13. オプション: クラスタを既存の GCP Virtual Private Cloud (VPC) にインストールするには、以下を実行します。
  - a. **Install to an existing VPC** を選択します。
  - b. 既存の VPC にインストールし、クラスタの HTTP または HTTPS プロキシを有効にする場合は、**Configure a cluster-wide proxy** を参照してください。
14. **Next** をクリックします。
15. オプション: クラスタを GCP の共有 VPC にインストールする場合は、以下を実行します。



### 重要

クラスタを共有 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 GCP 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、クラスタの作成が失敗します。



### 重要

クラスタ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、**Computer Network Administrator**、**Compute Security Administrator**、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。

16. クラスタを既存の GCP 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。クラウドネットワークアドレス変換 (NAT) とクラウドルーターを作成しておく必要があります。Cloud NAT と Google VPC については、[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。

17. クラスタ全体のプロキシ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 検査プロキシを使用する場合は、プロキシのアイデンティティ証明書が 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、プロキシが透過的であるか、**http-proxy** 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。

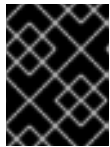
OpenShift Dedicated でのプロキシの設定に関する詳細は、**クラスター全体のプロキシの設定** を参照してください。

18. **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、**Machine CIDR** 範囲は VPC サブネットに一致する必要があります。



### 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。

19. **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: クラスタアップグレード時の **ノードのドレイン (解放)** 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

クラスタのセキュリティまたは安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

20. 選択の概要を確認し、**Create cluster** をクリックしてクラスタ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。
21. 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

GCP 共有 VPC にインストールされたクラスタを削除する場合は、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、クラスタは準備が完了した状態になります。

## 2.3. GOOGLE CLOUD MARKETPLACE を使用して GCP 上にクラスタを作成する

OpenShift Cluster Manager Hybrid Cloud Console 経由で Google Cloud 上に OpenShift Dedicated (OSD) クラスタを作成する場合、お客様は優先的に使用する請求モデルとして Google Cloud Marketplace を選択できます。この請求モデルにより、Red Hat のお客様は、Google Cloud Marketplace を通じて購入した OpenShift Dedicated に対して [Google Committed Use Discounts \(CUD\)](#) を利用できるようになります。OSD の価格は従量制で、お客様は Google Cloud アカウントを通じて直接請求されます。

## 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. **On-Demand** サブスクリプションタイプを選択します。

- b. ドロップダウンメニューから **Google Cloud Marketplace** を選択します。
  - c. **Customer Cloud Subscription** インフラストラクチャタイプを選択します。
  - d. **Next** をクリックします。
4. **Cloud provider** ページで、指定されている前提条件と Google の利用規約を確認します。サービスアカウントキーを追加します。
- a. **Review Google Terms and Agreements** リンクをクリックします。
  - b. クラスターの作成を続行するには、Google の利用規約に同意することを示すチェックボックスをクリックします。
  - c. サービスアカウントキーを追加します。



### 注記

サービスアカウントキーの詳細は、**Service account key**の横にある情報アイコンをクリックすると確認できます。

- d. **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。
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、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ます。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. **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。
  - e. **Single zone** または **Multi-zone** 設定を選択します。
  - f. オプション: クラスターのインストール時にシールドされた VM を使用するには、**Enable Secure Boot for Shielded VMs** を選択します。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。GCP 組織ポリシーの制約の詳細は、[組織ポリシーの制約](#) を参照してください。



- g. **Enable user workloads 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ック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. 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。

**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。
- b. オプション: etcd キー値の暗号化が必要な場合には、**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。

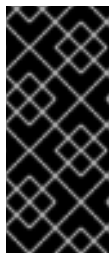
- c. オプション: クラスタで FIPS 検証を必須にする場合は、**Enable FIPS cryptography** を選択します。
7. **Next** をクリックします。
8. **Machine pool** ページで、**Compute node instance type** および **Compute node count** を選択します。利用可能なノードの数およびタイプは、OpenShift Dedicated のサブスクリプションによって異なります。複数のアベイラビリティゾーンを使用している場合、コンピュートノード数はゾーンごとに設定されます。



## 注記

クラスターの作成後に、コンピュータノード数を変更できますが、作成したマシンプールのコンピュータ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。インストール後に、カスタマイズされた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よって異なります。

9. 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。
10. **Next** をクリックします。
11. **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。
12. オプション: クラスターを既存の GCP Virtual Private Cloud (VPC) にインストールするには、以下を実行します。
  - a. **Install to an existing VPC** を選択します。
  - b. 既存の VPC にインストールし、クラスターの HTTP または HTTPS プロキシを有効にする場合は、**Configure a cluster-wide proxy** を参照してください。
13. **Next** をクリックします。
14. オプション: クラスターを GCP の共有 VPC にインストールする場合は、以下を実行します。



## 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 GCP 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、**Computer Network Administrator**、**Compute Security Administrator**、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。

15. クラスターを既存の GCP 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。クラウドネットワークアドレス変換 (NAT) とク

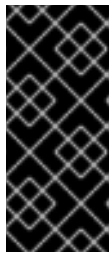
ラウトルーターを作成しておく必要があります。Cloud NAT と Google VPC については、関連情報のセクションを参照してください。



### 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。

16. **Next** をクリックします。
17. クラスタ全体のプロキシ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 検査プロキシを使用する場合は、プロキシのアイデンティティ証明書が 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、プロキシが透過的であるか、**http-proxy** 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 でのプロキシの設定に関する詳細は、**クラスタ全体のプロキシの設定** を参照してください。
18. **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にアクセスできません。

19. **Cluster update strategy** ページで、更新設定を行います。
  - a. クラスタ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: クラスターアップグレード時の **ノードのドレイン (解放)** 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または安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

20. 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。
21. 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。

## 2.4. RED HAT クラウドアカウントを使用した GCP でのクラスターの作成

[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 Platform (GCP) 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せん。  
OpenShift Dedicated サブスクリプションオプションについては、OpenShift Cluster Manager ドキュメントの [クラスタ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 Platform** を選択し、**Next** をクリックします。
5. **Cluster details** ページで、クラスタの名前を指定し、クラスタの詳細を指定します。
  - a. **Cluster name** を追加します。
  - b. オプション: クラスタを作成すると、**openshiftapps.com** にプロビジョニングされたクラスタのサブドメインとしてドメイン接頭辞が生成されます。クラスタ名が 15 文字以下の場合、その名前がドメイン接頭辞に使用されます。クラスタ名が 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バージョンを選択します。
  - d. **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。
  - e. **Single zone** または **Multi-zone** 設定を選択します。
  - f. オプション: クラスタのインストール時にシールドされた VM を使用するには、**Enable Secure Boot for Shielded VMs** を選択します。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。GCP 組織ポリシーの制約の詳細は、[組織ポリシーの制約](#) を参照してください。

- 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. **Enable user workloads 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ック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。
- j. オプション:etcd キー値の暗号化が必要な場合には、**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。

- k. **Next** をクリックします。

6. **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ゾーンを使用している場合、コンピューター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、コンピューターノード数を変更できますが、マシンプールのコンピューター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よって異なります。

7. 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。
8. **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。
9. **Next** をクリックします。
10. **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にアクセスできません。

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

a. クラスタ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: クラスタアップグレード時の **ノードのドレイン (解放)** 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

クラスタのセキュリティまたは安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

12. 選択の概要を確認し、**Create cluster** をクリックしてクラスタ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。

13. 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。

## 2.5. RED HAT MARKETPLACE を使用した GCP でのクラスターの作成

OpenShift Cluster Manager Hybrid Cloud Console 経由で Google Cloud 上に OpenShift Dedicated (OSD) クラスターを作成する場合、お客様は優先的に使用する請求モデルとして Red Hat Marketplace を選択できます。OSD の価格は従量制で、お客様は Red Hat Marketplace アカウントを通じて直接請求されます。

### 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. **On-Demand** サブスクリプションタイプを選択します。
  - b. ドロップダウンメニューから **Red Hat Marketplace** を選択します。
  - c. **Next** をクリックします。
4. **Cloud provider** ページで以下を行います。
  - a. **Google Cloud** をクラウドプロバイダーとして選択します。
  - b. クラスターの作成継続に必要なすべての前提条件を読み、完了していることを示すチェックボックスをクリックします。
  - c. サービスアカウントキーを追加します。



### 注記

サービスアカウントキーの詳細は、**Service account key** の横にある情報アイコンをクリックすると確認できます。

- d. **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。
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、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バージョンを選択します。
- d. **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。
- e. **Single zone** または **Multi-zone** 設定を選択します。
- f. オプション: クラスタのインストール時にシールドされた VM を使用するには、**Enable Secure Boot for Shielded VMs** を選択します。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。GCP 組織ポリシーの制約の詳細は、[組織ポリシーの制約](#) を参照してください。

- g. **Enable user workloads 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ック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. 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。

**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。
- b. オプション: etcd キー値の暗号化が必要な場合には、**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. 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。

7. **Next** をクリックします。

- 8. **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ゾーンを使用している場合、コンピュータ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、コンピュータノード数を変更できますが、作成したマシンプールのコンピュータ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。インストール後に、カスタマイズされた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よって異なります。

- 9. 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。

10. **Next** をクリックします。

- 11. **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。

- 12. オプション: クラスターを既存の GCP Virtual Private Cloud (VPC) にインストールするには、以下を実行します。

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

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

13. **Next** をクリックします。

- 14. オプション: クラスターを GCP の共有 VPC にインストールする場合は、以下を実行します。



### 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 GCP 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、**Computer Network Administrator**、**Compute Security Administrator**、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。

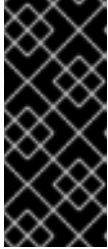
15. クラスターを既存の GCP VPC にインストールする場合、**Virtual Private Cloud (VPC) サブネット設定** を指定して、**Next** を選択します。クラウドネットワークアドレス変換 (NAT) とクラウドルーターを作成しておく必要があります。Cloud NAT と Google VPC については、関連情報のセクションを参照してください。



### 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。

16. **Next** をクリックします。
17. クラスター全体のプロキシ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 検査プロキシを使用する場合は、プロキシのアイデンティティ証明書が 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、プロキシが透過的であるか、**http-proxy** 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 でのプロキシの設定に関する詳細は、**クラスター全体のプロキシの設定** を参照してください。
18. **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。

19. **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: クラスターアップグレード時の **ノードのドレイン (解放)** 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または安定性に大きく影響する重大なセキュリティ問題がある場合、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評価の説明は、[Red Hat セキュリティ評価について](#) を参照してください。

20. 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。

21. 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、クラスタは準備が完了した状態になります。

## 2.6. 関連情報

- OpenShift Dedicated でのプロキシの設定に関する詳細は、[クラスタ全体のプロキシの設定](#) を参照してください。
- OpenShift Dedicated の永続ストレージについての詳細は、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。
- クラスタ全体のプロキシに必要なクラウドネットワークアドレス変換 (NAT) の一般情報は、Google ドキュメントの [Cloud NAT 概要](#) を参照してください。
- クラスタ全体のプロキシに必要な Cloud Router の一般情報は、Google ドキュメントの [Cloud Router 概要](#) 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 [VPC ネットワークの作成と管理](#) を参照してください。

## 第3章 アイデンティティプロバイダーの設定

OpenShift Dedicated クラスターの作成後に、アイデンティティプロバイダーを設定して、ユーザーがクラスターにアクセスする方法を決定する必要があります。

### 3.1. アイデンティティプロバイダーについて

OpenShift Dedicated には、ビルトイン OAuth サーバーが含まれます。開発者および管理者は OAuth アクセストークンを取得して、API に対して認証します。管理者は、クラスターのインストール後に、OAuth をアイデンティティプロバイダーを指定するように設定できます。アイデンティティプロバイダーを設定すると、ユーザーはログインし、クラスターにアクセスできます。

#### 3.1.1. サポートされるアイデンティティプロバイダー

以下の種類のアイデンティティプロバイダーを設定できます。

アイデンティティプロバイダー	説明
GitHub または GitHub Enterprise	GitHub または GitHub Enterprise の OAuth 認証サーバーに対して、ユーザー名とパスワードを検証するように GitHub アイデンティティプロバイダーを設定します。
GitLab	<a href="https://gitlab.com">GitLab.com</a> またはその他の GitLab インスタンスをアイデンティティプロバイダーとして使用するように GitLab アイデンティティプロバイダーを設定します。
Google	<a href="#">Google の OpenID Connect 統合機能</a> を使用して Google アイデンティティプロバイダーを設定します。
LDAP	単純なバインド認証を使用して、LDAPv3 サーバーに対してユーザー名とパスワードを検証するように LDAP アイデンティティプロバイダーを設定します。
OpenID Connect	<a href="#">Authorization Code Flow</a> を使用して OpenID Connect アイデンティティプロバイダーと統合するように OpenID Connect (OIDC) アイデンティティプロバイダーを設定します。
htpasswd	単一の静的管理ユーザー用に htpasswd アイデンティティプロバイダーを設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。
	<div style="display: flex; align-items: flex-start;"> <div style="width: 40px; height: 40px; background: repeating-linear-gradient(45deg, transparent, transparent 2px, black 2px, black 4px); margin-right: 10px;"></div> <div> <p><b>重要</b></p> <p>htpasswd ID プロバイダーオプションは、単一の静的管理ユーザーを作成できるようにするためだけに含まれています。htpasswd は、OpenShift Dedicated の汎用 ID プロバイダーとしてはサポートされていません。単一ユーザーを設定する手順は、<a href="#">htpasswd アイデンティティプロバイダーの設定</a> を参照してください。</p> </div> </div>

#### 3.1.2. アイデンティティプロバイダーパラメーター



以下のパラメーターは、すべてのアイデンティティプロバイダーに共通するパラメーターです。

パラメーター	説明
<b>name</b>	プロバイダー名は、プロバイダーのユーザー名に接頭辞として付加され、アイデンティティ名が作成されます。
<b>mappingMethod</b>	<p>新規アイデンティティがログイン時にユーザーにマップされる方法を定義します。以下の値のいずれかを入力します。</p> <p><b>claim</b> デフォルトの値です。アイデンティティの推奨ユーザー名を持つユーザーをプロビジョニングします。そのユーザー名を持つユーザーがすでに別のアイデンティティにマッピングされている場合は失敗します。</p> <p><b>lookup</b> 既存のアイデンティティ、ユーザーアイデンティティマッピング、およびユーザーを検索しますが、ユーザーまたはアイデンティティの自動プロビジョニングは行いません。これにより、クラスター管理者は手動で、または外部のプロセスを使用してアイデンティティとユーザーを設定できます。この方法を使用する場合は、ユーザーを手動でプロビジョニングする必要があります。</p> <p><b>add</b> アイデンティティの推奨ユーザー名を持つユーザーをプロビジョニングします。推奨ユーザー名を持つユーザーがすでに存在する場合、アイデンティティは既存のユーザーにマッピングされ、そのユーザーの既存のアイデンティティマッピングに追加されます。これは、同じユーザーセットを識別して同じユーザー名にマッピングするアイデンティティプロバイダーが複数設定されている場合に必要です。</p>



### 注記

**mappingMethod** パラメーターを **add** に設定すると、アイデンティティプロバイダーの追加または変更時に新規プロバイダーのアイデンティティを既存ユーザーにマッピングできます。

## 3.2. GITHUB アイデンティティプロバイダーの設定

GitHub アイデンティティプロバイダーを、GitHub または GitHub Enterprise の OAuth 認証サーバーに対してユーザー名とパスワードを検証し、OpenShift Dedicated クラスターにアクセスするように設定します。OAuth は OpenShift Dedicated と GitHub または GitHub Enterprise 間のトークン交換フローを容易にします。



### 警告

GitHub 認証を設定することによって、ユーザーは GitHub 認証情報を使用して OpenShift Dedicated にログインできます。GitHub ユーザー ID を持つすべてのユーザーが OpenShift Dedicated クラスターにログインできないようにするには、アクセスを特定の GitHub 組織またはチームのユーザーに制限する必要があります。

## 前提条件

- GitHub 組織管理者が、GitHub [組織設定](#) 内に OAuth アプリケーションを直接作成している。
- [GitHub 組織またはチーム](#) が GitHub アカウントに設定されている。

## 手順

1. [OpenShift Cluster Manager](#) から、**Clusters** ページに移動し、アイデンティティプロバイダーを設定するクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



### 注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティプロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitHub** を選択します。
5. アイデンティティプロバイダーの一意の名前を入力します。この名前は後で変更することができません。
  - **OAuth callback URL** が指定のフィールドに自動的に生成されます。これを使用して GitHub アプリケーションを登録します。

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下に例を示します。

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
```

6. [アプリケーションを GitHub に登録](#) します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. GitHub から提供される **Client ID** および **Client secret** を入力します。
9. **hostname** を入力します。GitHub Enterprise のホステッドインスタンスを使用する場合は、ホスト名を入力する必要があります。
10. オプション: 認証局 (CA) ファイルを使用して、設定された GitHub Enterprise URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティプロバイダーに割り当てます。
11. **Use organizations** または **Use teams** を選択し、アクセスを特定の GitHub 組織または GitHub チームに制限します。
12. アクセスを制限する組織またはチームの名前を入力します。**Add more** をクリックして、ユーザーが所属できる複数の組織またはチームを指定します。



13. **Confirm** をクリックします。

#### 検証

- 設定されたアイデンティティプロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

### 3.3. GITLAB アイデンティティプロバイダーの設定

GitLab.com またはその他の GitLab インスタンスをアイデンティティプロバイダーとして使用するよう GitLab アイデンティティプロバイダーを設定します。

#### 前提条件

- GitLab バージョン 7.7.0 から 11.0 を使用する場合は、**OAuth 統合** を使用して接続します。GitLab バージョン 11.1 以降の場合は、OAuth ではなく **OpenID Connect (OIDC)** を使用して接続します。

#### 手順

1. **OpenShift Cluster Manager** から、**Clusters** ページに移動し、アイデンティティプロバイダーを設定するクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



#### 注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティプロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitLab** を選択します。
5. アイデンティティプロバイダーの一意的名前を入力します。この名前は後で変更することができません。
  - **OAuth callback URL** が指定のフィールドに自動的に生成されます。この URL を GitLab に指定します。

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下に例を示します。

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
```

6. **GitLab に新規アプリケーションを追加**します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. GitLab から提供される **Client ID** および **Client secret** を入力します。

9. GitLab プロバイダーの **URL** を入力します。
10. オプション: 認証局 (CA) ファイルを使用して、設定された GitLab URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティプロバイダーに割り当てます。
11. **Confirm** をクリックします。

## 検証

- 設定されたアイデンティティプロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 3.4. GOOGLE アイデンティティプロバイダーの設定

ユーザーが Google 認証情報で認証できるように Google アイデンティティプロバイダーを設定します。



### 警告

Google をアイデンティティプロバイダーとして使用することで、Google ユーザーはサーバーに対して認証されます。**hostedDomain** 設定属性を使用して、特定のホストドメインのメンバーに認証を限定することができます。

## 手順

1. [OpenShift Cluster Manager](#) から、**Clusters** ページに移動し、アイデンティティプロバイダーを設定するクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



### 注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティプロバイダーを設定することもできます。

4. ドロップダウンメニューから **Google** を選択します。
5. アイデンティティプロバイダーの一意の名前を入力します。この名前は後で変更することができません。
  - **OAuth callback URL** が指定のフィールドに自動的に生成されます。この URL を Google に指定します。

```
https://oauth-openshift.apps.<cluster_name>.<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下に例を示します。

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
```

6. [Google の OpenID Connect 統合機能](#) を使用して Google アイデンティティプロバイダーを設定します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. 登録済みの Google プロジェクトの **Client ID** と、Google が発行する **Client secret** を入力します。
9. ホストされたドメインを入力して、ユーザーを Google Apps ドメインに制限します。
10. **Confirm** をクリックします。

### 検証

- 設定されたアイデンティティプロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 3.5. LDAP アイデンティティプロバイダーの設定

単純なバインド認証を使用して LDAPv3 サーバーに対してユーザー名とパスワードを検証するように LDAP アイデンティティプロバイダーを設定します。

### 前提条件

- LDAP アイデンティティプロバイダーを設定する場合は、設定済みの **LDAP URL** を入力する必要があります。設定される URL は、LDAP ホストと使用する検索パラメーターを指定する RFC 2255 URL です。URL の構文は以下のようになります。

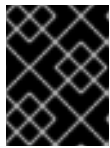
```
ldap://host:port/basedn?attribute?scope?filter
```

URL コンポーネント	説明
<b>ldap</b>	通常の LDAP の場合は、文字列 <b>ldap</b> を使用します。セキュアな LDAP (LDAPS) の場合は、代わりに <b>ldaps</b> を使用します。
<b>host:port</b>	LDAP サーバーの名前とポートです。デフォルトは、ldap の場合は <b>localhost:389</b> 、LDAPS の場合は <b>localhost:636</b> です。
<b>basedn</b>	すべての検索が開始されるディレクトリーのブランチの DN です。これは少なくともディレクトリーツリーの最上位である必要がありますが、ディレクトリーのサブツリーを指定することもできます。
<b>attribute</b>	検索対象の属性です。RFC 2255 はコンマ区切りの属性のリストを許可しますが、属性をどれだけ指定しても最初の属性のみが使用されます。属性を指定しない場合は、デフォルトで <b>uid</b> が使用されます。使用しているサブツリーのすべてのエンタリー間で一意の属性を選択することを推奨します。

URL コンポーネント	説明
<b>scope</b>	検索の範囲です。 <b>one</b> または <b>sub</b> のいずれかを指定できます。範囲を指定しない場合は、デフォルトの範囲として <b>sub</b> が使用されます。
<b>filter</b>	有効な LDAP 検索フィルターです。指定しない場合のデフォルトは <b>(objectClass=*)</b> です。

検索の実行時に属性、フィルター、指定したユーザー名が組み合わされて以下のような検索フィルターが作成されます。

```
(<filter>(<attribute>=<username>))
```



### 重要

LDAP ディレクトリーの検索に認証が必要な場合は、エントリー検索の実行に使用する **bindDN** と **bindPassword** を指定します。

## 手順

1. [OpenShift Cluster Manager](#) から、**Clusters** ページに移動し、アイデンティティプロバイダーを設定するクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

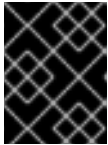


### 注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティプロバイダーを設定することもできます。

4. ドロップダウンメニューから **LDAP** を選択します。
5. アイデンティティプロバイダーの一意の名前を入力します。この名前は後で変更することができません。
6. ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
7. **LDAP URL** を入力して、使用する LDAP 検索パラメーターを指定します。
8. オプション: **Bind DN** および **Bind password** を入力します。
9. LDAP 属性をアイデンティティにマップする属性を入力します。
  - 値をユーザー ID として使用する ID 属性を入力します。**Add more** をクリックして、複数の ID 属性を追加します。

- オプション: 表示名の値として使用する **Preferred username** 属性を入力します。 **Add more** をクリックして、優先する複数のユーザー名属性を追加します。
  - オプション: メールアドレスの値として使用する **Email** 属性を入力します。 **Add more** をクリックして、複数のメール属性を追加します。
10. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを LDAP アイデンティティプロバイダーに追加し、設定された URL のサーバー証明書を検証します。 **Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティプロバイダーに割り当てます。
  11. オプション: 高度なオプションで、LDAP プロバイダーを **非セキュア** にするよう選択できます。このオプションを選択すると、CA ファイルは使用できません。



### 重要

非セキュアな LDAP 接続 (ldap:// またはポート 389) を使用している場合は、設定ウィザードで **Insecure** オプションを確認する必要があります。

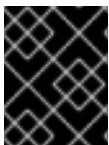
12. **Confirm** をクリックします。

### 検証

- 設定されたアイデンティティプロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 3.6. OPENID アイデンティティプロバイダーの設定

[Authorization Code Flow](#) を使用して、OpenID アイデンティティプロバイダーを OpenID Connect アイデンティティプロバイダーと統合するように設定します。



### 重要

OpenShift Dedicated の認証 Operator では、設定済みの OpenID Connect アイデンティティプロバイダーが [OpenID Connect Discovery](#) 仕様を実装する必要があります。

要求は、OpenID アイデンティティプロバイダーから返される JWT **id\_token** から読み取られ、指定される場合は発行者 URL によって返される JSON から読み取られます。

1つ以上の要求をユーザーのアイデンティティを使用するように設定される必要があります。

また、どの要求をユーザーの推奨ユーザー名、表示名およびメールアドレスとして使用するか指定することができます。複数の要求が指定されている場合は、値が入力されている最初の要求が使用されません。標準の要求は以下の通りです。

要求	説明
<code>preferred_username</code>	ユーザーのプロビジョニング時に優先されるユーザー名です。 <b>janedoe</b> などのユーザーを参照する際に使用する省略形の名前です。通常は、ユーザー名またはメールなどの、認証システムのユーザーのログインまたはユーザー名に対応する値です。

要求	説明
email	メールアドレス。
name	表示名。

詳細は、[OpenID claim のドキュメント](#) を参照してください。

### 前提条件

- OpenID Connect を設定する前に、OpenShift Dedicated クラスターで使用する Red Hat 製品またはサービスのインストール前提条件を確認してください。

### 手順

1. [OpenShift Cluster Manager](#) から、**Clusters** ページに移動し、アイデンティティプロバイダーを設定するクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



#### 注記

クラスターの作成後に表示される警告メッセージの **Add OAuth configuration** リンクをクリックして、アイデンティティプロバイダーを設定することもできます。

4. ドロップダウンメニューから **OpenID** を選択します。
5. アイデンティティプロバイダーの一意的名前を入力します。この名前は後で変更することができません。
  - **OAuth callback URL** が指定のフィールドに自動的に生成されます。

```
https://oauth-openshift.apps.<cluster_name>.<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下に例を示します。

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid
```

6. [認可リクエストを作成する](#) 手順に従って、新しい OpenID Connect クライアントを OpenID ID プロバイダーに登録します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. OpenID から提供される **Client ID** および **Client secret** を入力します。

9. **Issuer URL** を入力します。これは、OpenID プロバイダーが発行者 ID としてアサートする URL です。URL クエリーパラメーターまたはフラグメントのない https スキームを使用する必要があります。
10. メールアドレスの値として使用する **Email** 属性を入力します。 **Add more** をクリックして、複数のメール属性を追加します。
11. 優先するユーザー名の値として使用する **Name** 属性を入力します。 **Add more** をクリックして、優先する複数のユーザー名を追加します。
12. 表示名の値として使用する **Preferred username** 属性を入力します。 **Add more** をクリックして、複数の表示名を追加します。
13. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを OpenID アイデンティティプロバイダーに追加します。
14. オプション: 高度なオプションから、**追加のスコープ** を追加できます。デフォルトでは、**OpenID** の範囲が要求されます。
15. **Confirm** をクリックします。

## 検証

- 設定されたアイデンティティプロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 3.7. HTPASSWD アイデンティティプロバイダーの設定

クラスター管理者権限で単一の静的ユーザーを作成するように `htpasswd` アイデンティティプロバイダーを設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。



### 重要

`htpasswd` ID プロバイダーオプションは、単一の静的管理ユーザーを作成できるようにするためだけに含まれています。`htpasswd` は、OpenShift Dedicated の汎用 ID プロバイダーとしてはサポートされていません。

## 手順

1. [OpenShift Cluster Manager](#) から、**Clusters** ページに移動し、クラスターを選択します。
2. **Access control** → **Identity providers** の順に選択します。
3. **Add identity provider** をクリックします。
4. **Identity Provider** ドロップダウンメニューから **HTPasswd** を選択します。
5. アイデンティティプロバイダーの **Name** フィールドに一意の名前を追加します。
6. 静的ユーザーに推奨されるユーザー名およびパスワードを使用するか、独自のユーザー名およびパスワードを作成します。





## 注記

この手順で定義した認証情報は、以下の手順で **Add** を選択した後に表示されません。認証情報を失った場合は、アイデンティティプロバイダーを再作成し、認証情報を再度定義する必要があります。

7. **Add** を選択して `htpasswd` アイデンティティプロバイダーおよび単一の静的ユーザーを作成します。
8. クラスターを管理する静的ユーザーにパーミッションを付与します。
  - a. **Access control** → **Cluster Roles and Access** で、**Add user** を選択します。
  - b. 前のステップで作成した静的ユーザーの **User ID** を入力します。
  - c. **グループ** を選択します。
    - Customer Cloud Subscription (CCS) インフラストラクチャータイプを使用して OpenShift Dedicated をインストールする場合は、**dedicated-admins** グループまたは **cluster-admins** グループのいずれかを選択します。**dedicated-admin** グループのユーザーには、OpenShift Dedicated の標準の管理者権限があります。**cluster-admins** グループのユーザーには、クラスターへの完全な管理アクセス権限があります。
    - Red Hat クラウドアカウントインフラストラクチャータイプを使用して OpenShift Dedicated をインストールする場合は、**dedicated-admins** グループが自動的に選択されます。
  - d. **Add user** を選択して、管理者権限をユーザーに付与します。

## 検証

- 設定された `htpasswd` アイデンティティプロバイダーは、**Access control** → **Identity providers** ページに表示されます。



## 注記

アイデンティティプロバイダーの作成後に、同期は通常 2 分以内に完了します。`htpasswd` アイデンティティプロバイダーが利用可能になると、ユーザーとしてクラスターにログインできます。

- 管理ユーザーは、**Access control** → **Cluster Roles and Access** ページで確認できます。ユーザーの管理グループメンバーシップも表示されます。

## 関連情報

- [お客様管理者ユーザー](#)

## 3.8. クラスターへのアクセス

アイデンティティプロバイダーを設定したら、ユーザーは Red Hat OpenShift Cluster Manager からクラスターにアクセスできます。

## 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。
- クラスターにアイデンティティプロバイダーを設定している。
- 設定したアイデンティティプロバイダーにユーザーアカウントを追加している。

## 手順

1. [OpenShift Cluster Manager](#) で、アクセスするクラスターをクリックします。
2. **Open Console** をクリックします。
3. アイデンティティプロバイダーをクリックし、クラスターにログインするためのクレデンシャルを指定します。
4. **Open console** をクリックし、クラスターの Web コンソールを開きます。
5. アイデンティティプロバイダーをクリックし、クラスターにログインするためのクレデンシャルを指定します。プロバイダーによって提示される認可要求を完了します。

## 第4章 OPENSIFT DEDICATED クラスターへのアクセスおよび権限の取り消し

クラスターの所有者は、管理者権限および OpenShift Dedicated クラスターへのユーザーアクセスを取り消すことができます。


### 4.1. ユーザーからの管理者権限の削除

このセクションの手順に従って、ユーザーの **dedicated-admin** 権限を取り消すことができます。

#### 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。
- クラスターに GitHub アイデンティティプロバイダーを設定し、アイデンティティプロバイダーユーザーを追加している。
- ユーザーに **dedicated-admin** 権限が付与されている。

#### 手順

1. [OpenShift Cluster Manager](#) に移動し、クラスターを選択します。
2. **Access control** タブをクリックします。
3. **Cluster Roles and Access** タブで、ユーザーの横にある  を選択し、**Delete** をクリックします。

#### 検証

- 権限を取り消すと、ユーザーは、クラスターの OpenShift Cluster Manager ページの **Access control** → **Cluster Roles** および **Access** に **dedicated-admins** グループの一部として一覧表示されなくなります。

### 4.2. クラスターへのユーザーアクセスの取り消し

アイデンティティプロバイダーを設定済みのアイデンティティプロバイダーから削除して、アイデンティティプロバイダーユーザーのクラスターアクセス権を取り消すことができます。

OpenShift Dedicated クラスターに異なるタイプのアイデンティティプロバイダーを設定できます。以下の手順例では、クラスターへのアイデンティティプロビジョニング用に設定された GitHub 組織またはチームのメンバーのクラスターアクセス権を取り消すことができます。

#### 前提条件

- OpenShift Dedicated クラスターがある。
- GitHub ユーザーアカウントがある。

- クラスターに GitHub アイデンティティプロバイダーを設定し、アイデンティティプロバイダーユーザーを追加している。

## 手順

1. [github.com](https://github.com) に移動し、GitHub アカウントにログインします。
2. GitHub 組織またはチームからユーザーを削除します。
  - アイデンティティプロバイダー設定で GitHub 組織を使用する場合は、GitHub ドキュメントの [組織からのメンバーの削除](#) の手順に従います。
  - アイデンティティプロバイダー設定が GitHub 組織のチームを使用する場合は、GitHub ドキュメントの [チームからの組織メンバーの削除](#) の手順に従います。

## 検証

- アイデンティティプロバイダーからユーザーを削除すると、そのユーザーはクラスターで認証されません。

## 第5章 OPENSIFT 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。

- [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

GCP 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。