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

Last Updated: 2022-11-28

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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

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

第1章 AWS でのクラスターの作成

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、または 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 でのクラスターの作成

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 クラスターを作成できます。

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。

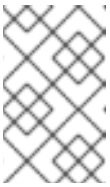
前提条件

- 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。
- 必要なクラスター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)**を参照してください。
- 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。
- クラスター全体のプロキシーを設定する場合は、クラスターがインストールされている VPC からプロキシーにアクセスできることを確認している。プロキシーは 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 Hybrid Cloud Console 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 のサブスクリプションオプションの詳細は、OpenShift Cluster Manager のドキュメントの OpenShift Dedicated クラスターサブスクリプションの管理 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。詳細については、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。

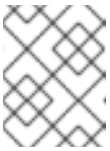
4. **Run on Amazon Web Services** を選択します。

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。

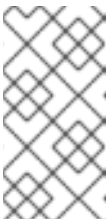
b. AWS IAM ユーザーアカウントの**AWS アクセスキー ID** および **AWS シークレットアクセスキー** を入力します。



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. **クラスター名** を追加します。

b. **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。

c. **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。

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

e. **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。

f. 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。

g. 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、クラスター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すが、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。

h. **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、クラスター内の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。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. 任意手順: **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。

11. **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。

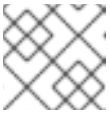
重要

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。

12. 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 プロキシー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. 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。

注記

クラスターをインストールするアベイラビリティーゾーンごとに、VPC がパブリックおよびプライベートサブネットで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。

15. 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。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。
      追加のプロキシー設定が必要ではなく、追加の認証局 (CA) を必要とする MITM の透過的なプロキシーネットワークを使用する場合には、MITM CA 証明書を指定する必要があります。

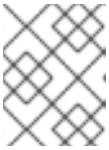
注記

HTTP または HTTPS プロキシー URL を指定せずに追加の信頼バンドルファイルをアップロードする場合、バンドルはクラスターに設定されますが、プロキシーで使用するように設定されていません。

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。

16. **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、または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。

17. **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 は、管理者の確認を受け取らずに、マイナーバージョンのスケジュールされた y-stream 更新を開始しません。
  管理者の確認については、OpenShift4.9 にアップグレードする際の管理者の確認 を参照してください。

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、Understanding Red Hat security ratings を参照してください。

18. 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。

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。

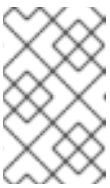
1.3. RED HAT クラウドアカウントを使用した AWS でのクラスターの作成

OpenShift Cluster Manager Hybrid Cloud Console 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 クラスターを作成できます。

手順

1. OpenShift Cluster Manager Hybrid Cloud Console 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 のサブスクリプションオプションの詳細は、OpenShift Cluster Manager のドキュメントの OpenShift Dedicated クラスターサブスクリプションの管理 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。詳細については、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 Open Shift 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、クラスターの名前を指定し、クラスターの詳細を指定します。

a. **クラスター名** を追加します。

b. **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。

c. **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。

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

e. 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。

f. 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。

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。

h. 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。

i. **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よって異なります。

7. 任意手順: **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、または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。

11. **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。

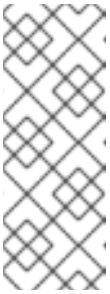
    b. クラスターの更新方法に基づいて管理者の承認を提供します。

    - 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 は、管理者の確認を受け取らずに、マイナーバージョンのスケジュールされた y-stream 更新を開始しません。
      管理者の確認については、OpenShift4.9 にアップグレードする際の管理者の確認 を参照してください。

    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、Understanding Red Hat security ratings 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。

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。
- 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 Storage 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についての詳細は、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。
- 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。

第2章 GCP でのクラスターの作成

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、または 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。

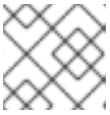
2.2. CCS を使用した GCP でのクラスターの作成

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 クラスターを作成できます。

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。
- 必要なクラスター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。
  - DNS 管理者
  - 組織ポリシービューアー
  - Owner
  - プロジェクト IAM 管理者
  - 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

- **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。

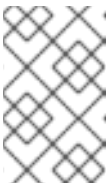
注記

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 Creating service account keys を参照してください。

- GCP の **Production 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。
- 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ーを設定する場合は、クラスターがインストールされている VPC からプロキシーにアクセスできることを確認している。プロキシーは 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 Hybrid Cloud Console 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 のサブスクリプションオプションの詳細は、OpenShift Cluster Manager のドキュメントの OpenShift Dedicated クラスターサブスクリプションの管理 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。詳細については、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、または **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. **クラスター名** を追加します。

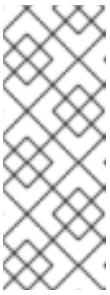
    b. **Version** ドロップダウンメニューからクラスターバージョンを選択します。

    c. **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。

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

    e. **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。

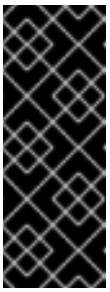
    f. オプション:etcd キー値の暗号化が必要な場合には、**Enable additional etcd encryption**を選択します。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。このオプションは、デフォルトで OpenShift Dedicated クラスターの etcd ボリュームを暗号化するコントロールプレーンのストレージ暗号化に追加されます。

    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。

    g. オプション:Google Cloud Key Management Service で独自の暗号化キーを提供する場合は、**Encrypt persistent volumes with customer keys**を選択します。このキーは、クラスター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。

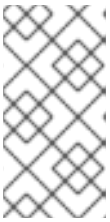
    重要

    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すが、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。

    h. **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、クラスター内の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。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. 任意手順: **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。

11. **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。

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 プロキシー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. 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。

15. 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。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。
      追加のプロキシー設定が必要ではなく、追加の認証局 (CA) を必要とする MITM の透過的なプロキシーネットワークを使用する場合には、MITM CA 証明書を指定する必要があります。

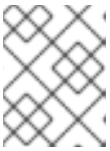
注記

HTTP または HTTPS プロキシー URL を指定せずに追加の信頼バンドルファイルをアップロードする場合、バンドルはクラスターに設定されますが、プロキシーで使用するように設定されていません。

    b. **Next** をクリックします。

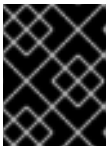
    OpenShift Dedicated でのプロキシーの設定に関する詳細は、**クラスター全体のプロキシーの設定** を参照してください。

16. **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、または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。

17. **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。

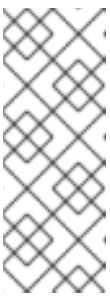
    b. クラスターの更新方法に基づいて管理者の承認を提供します。

    - 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 は、管理者の確認を受け取らずに、マイナーバージョンのスケジュールされた y-stream 更新を開始しません。
      管理者の確認については、OpenShift4.9 にアップグレードする際の管理者の確認 を参照してください。

    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、Understanding Red Hat security ratings を参照してください。

18. 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。

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。

2.3. 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 Hybrid Cloud Console 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 Hybrid Cloud Console 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 のサブスクリプションオプションの詳細は、OpenShift Cluster Manager のドキュメントの OpenShift Dedicated クラスターサブスクリプションの管理 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。詳細については、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 Open Shift 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、クラスターの名前を指定し、クラスターの詳細を指定します。
   a. **クラスター名** を追加します。
   b. **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。
   c. **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。
   d. **Single zone** または **Multi-zone** 設定を選択し ます。

e. 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。

f. 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。

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。

h. 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。

i. **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

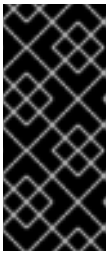
クラスターの作成後に、コンピュートノード数を変更できますが、マシンプールのコンピュートノードインスタンスのタイプを変更することはできません。CCS モデルを使用するクラスターの場合、インストール後に別のインスタンスタイプを使用するマシンプールを追加できます。利用可能なノード数および種類は、OpenShift Dedicated のサブスクリプションによって異なります。

7. 任意手順: **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、または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。

11. **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。

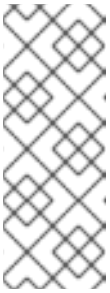
    b. クラスターの更新方法に基づいて管理者の承認を提供します。

    - 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 は、管理者の確認を受け取らずに、マイナーバージョンのスケジュールされた y-stream 更新を開始しません。
      管理者の確認については、OpenShift4.9 にアップグレードする際の管理者の確認 を参照してください。

    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、Understanding Red Hat security ratings 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。

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. 関連情報

- 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 の永続ストレージについての詳細は、OpenShift Dedicated サービス定義の Storage セクションを参照してください。
- OpenShift Dedicated のロードバランサーについての詳細は、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。
- 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。

第3章 アイデンティティープロバイダーの設定

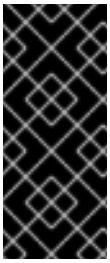
OpenShift Dedicated クラスターの作成後に、アイデンティティープロバイダーを設定して、ユーザーがクラスターにアクセスする方法を決定する必要があります。

3.1. アイデンティティー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ープロバイダーを指定するように設定できます。アイデンティティー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ープロバイダー

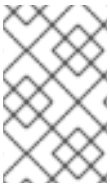
以下の種類のアイデンティティープロバイダーを設定できます。

アイデンティティープロバイダー	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 アイデンティティープロバイダーを設定します。
GitLab	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ープロバイダーとして使用するように GitLab アイデンティティープロバイダーを設定します。
Google	Google の OpenID Connect 統合機能を使用して Google アイデンティティー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 アイデンティティープロバイダーを設定します。
OpenID Connect	Authorization Code Flow を使用して OpenID Connect アイデンティティープロバイダーと統合するように OpenID Connect (OIDC) アイデンティティー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 アイデンティティー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 アイデンティティープロバイダーのオプションは、静的な管理者ユーザーを 1 つ作成するのを可能にするために含まれています。Htpasswd は、OpenShift Dedicated の一般使用向けのアイデンティティー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、**HTPasswd 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。

3.1.2. アイデンティティー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ー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
name	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、アイデンティティー名が作成されます。
mappingMethod	新規アイデンティティー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。 **claim** デフォルトの値です。アイデンティティー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ーにマッピングされている場合は失敗します。 **lookup** 既存のアイデンティティー、ユーザーアイデンティティーマッピング、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ー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ー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。 **generate** アイデンティティー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既存のアイデンティティーにマッピングされている場合は、一意のユーザー名が生成されます。例: **myuser2**この方法は、OpenShift Dedicated のユーザー名とアイデンティティープロバイダーのユーザー名との正確な一致を必要とする外部プロセス (LDAP グループ同期など) と組み合わせて使用することはできません。 **add** アイデンティティー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、アイデンティティー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ー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ープロバイダーが複数設定されている場合に必要です。



注記

mappingMethod パラメーターを **add** に設定すると、アイデンティティー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ーを既存ユーザーにマッピングできます。

3.2. GITHUB アイデンティティープロバイダーの設定

GitHub アイデンティティープロバイダーを、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ために、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

- OAuth アプリケーションを、GitHub 組織管理者によって GitHub 組織設定 内に直接作成している。
- 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 Hybrid Cloud Console から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあ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、アイデンティティー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. アイデンティティー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** は提供される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. 任意手順: 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ー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ープロバイダーが **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 アイデンティティー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ープロバイダーとして使用するように GitLab アイデンティティー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 Hybrid Cloud Console から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあ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、アイデンティティー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. アイデンティティー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** は提供される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ー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ープロバイダーが **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 アイデンティティー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 アイデンティティープロバイダーを設定します。

警告

Google をアイデンティティー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 Hybrid Cloud Console から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあ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、アイデンティティー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. アイデンティティー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** は提供される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 アイデンティティー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ープロバイダーが **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 アイデンティティー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 アイデンティティープロバイダーを設定します。

前提条件

- LDAP アイデンティティー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
ldap	通常の LDAP の場合は、文字列 **ldap** を使用します。セキュアな LDAP (LDAPS) の場合は、代わりに **ldaps** を使用します。
host:port	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 **localhost:389**、LDAPS の場合は **localhost:636** です。
basedn	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になければなりませんが、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。
attribute	検索対象の属性です。RFC 2255 はコンマ区切りの属性の一覧を許可しますが、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 **uid** 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トリー間で一意の属性を選択することを推奨します。
scope	検索の範囲です。**one** または **sub** 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 **sub** が使用されます。
filter	有効な LDAP 検索フィルターです。指定しない場合、デフォルトは **(objectClass=*)** 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

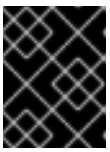
1. OpenShift Cluster Manager Hybrid Cloud Console から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

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、アイデンティティー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. アイデンティティー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ー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 アイデンティティー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ー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 **で Insecure** オプションを確認する必要があります。

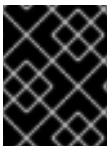
12. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **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 アイデンティティープロバイダーの設定

OpenID アイデンティティープロバイダーを、Authorization Code Flow を使用して OpenID Connect アイデンティティー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 アイデンティティープロバイダーが OpenID Connect Discovery 仕様を実装する必要があります。

要求は、OpenID アイデンティティー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 Issuer 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ー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す。標準の要求は以下の通りです。

要求	説明
preferred_username	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。**janedoe** 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。
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 Hybrid Cloud Console から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあ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、アイデンティティー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. アイデンティティー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** は提供される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. Authorization Code Flow を使用して承認リクエストを作成します。

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 アイデンティティー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ープロバイダーが **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 アイデンティティー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 アイデンティティー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。

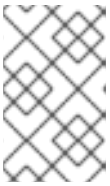
重要

HTPasswd アイデンティティープロバイダーのオプションは、静的な管理者ユーザーを 1 つ作成するのを可能にするために含まれています。Htpasswd は、OpenShift Dedicated の一般使用向けのアイデンティティー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 Hybrid Cloud Console から、クラスターページに移動し、**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. アイデンティティープロバイダーの **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、アイデンティティー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 アイデンティティー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。

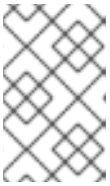
   - Customer Cloud Subscription (CCS) インフラストラクチャータイプを使用して OpenShift Dedicated をインストールする場合は、**dedicated-admins** グループまたは **cluster-admins** グループのいずれかを選択します。**dedicated-admin** グループのユーザーには、OpenShift Dedicated の標準の管理者権限があります。**cluster-admins** グループのユーザーには、クラスターへの完全な管理アクセス権限があります。

   - 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 アイデンティティープロバイダーは、**Access control → Identity providers** ページに表示されます。



注記

アイデンティティー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 アイデンティティー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。

3.8. クラスターへのアクセス

アイデンティティー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 Hybrid Cloud Console 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ー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ー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 Hybrid Cloud Console から、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. アイデンティティー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. アイデンティティー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承認要求を完了します。

第4章 OPENSHIFT 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

本セクションの手順に従って、ユーザーから **dedicated-admin** 権限を取り除くことができます。

前提条件

- OpenShift Cluster Manager Hybrid Cloud Console 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 アイデンティティープロバイダーを設定し、アイデンティティー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 Hybrid Cloud Console 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

- 特権の取り消し後に、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

アイデンティティープロバイダーを設定済みのアイデンティティープロバイダーから削除して、アイデンティティープロバイダーからクラスターへのアクセス権限を取り除くことができます。

OpenShift Dedicated クラスターに異なるタイプのアイデンティティー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ー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への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 アイデンティティープロバイダーを設定し、アイデンティティープロバイダーユーザーを追加している。

手順

1. 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。
   - アイデンティティープロバイダー設定で GitHub 組織が使用される場合は、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。
   - アイデンティティー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

- アイデンティティープロバイダーからユーザーを削除した後に、ユーザーはクラスターに対して認証できません。

第5章 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。

- OpenShift Cluster Manager Hybrid Cloud Console 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 Hybrid Cloud Console から、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。