# OpenShift Dedicated 4

## クラウドインフラストラクチャーアクセス

OpenShift Dedicated 4 でのクラウドインフラストラクチャーアクセス

Last Updated: 2020-05-28

# OpenShift Dedicated 4 クラウドインフラストラクチャーアクセス

OpenShift Dedicated 4 でのクラウドインフラストラクチャーアクセス

## 法律上の通知



## 概要

OpenShift Dedicated 4 でのクラウドインフラストラクチャー

# 目次

# 第1章 クラウドインフラストラクチャーアクセスについて

Amazon Web Services (AWS) インフラストラクチャーアクセスにより、Customer Portal Organization Administrator およびクラスターの所有者は AWS Identity and Access Management (IAM) ユーザーに OpenShift Dedicated クラスターの AWS 管理コンソールへのフェデレーションアクセスを持たせることができます。

## 1.1. AWS アクセスの有効化

AWS アクセスはカスタマー AWS ユーザーに付与でき、OpenShift Dedicated 環境の各種ニーズに合わせてプライベートのクラスターアクセスを実装できます。

OpenShift Dedicated クラスターの AWS インフラストラクチャーへのアクセスを開始します。AWS ユーザーとアカウントを作成し、そのユーザーに OpenShift Dedicated AWS アカウントへのアクセスを提供します。

OpenShift Dedicated AWS アカウントへのアクセスを取得した後に、以下の方法のいずれかを使用してクラスターへのプライベート接続を確立します。

- AWS VPC ピアリングの設定: VPC ピアリングを有効にして、2 つのプライベート IP アドレス間のネットワークトラフィックをルーティングします。
- AWS VPN の設定: プライベートネットワークを Amazon Virtual Private Cloud にセキュアに接続するために、仮想プライベートネットワークを確立します。
- AWS Direct Connect の設定: プライベートネットワークと AWS Direct Connect の場所との間に専用のネットワーク接続を確立するように AWS Direct Connect を設定します。

クラウドインフラストラクチャーアクセスを設定した後に、プライベートクラスターの設定について確認してください。

# 第2章 AWS インフラストラクチャーへのアクセス

Amazon Web Services (AWS) インフラストラクチャーアクセスにより、Customer Portal Organization Administrator およびクラスターの所有者は AWS Identity and Access Management (IAM) ユーザーに OpenShift Dedicated クラスターの AWS 管理コンソールへのフェデレーションアクセスを持たせることができます。管理者は、ネットワーク管理または読み取り専用アクセスのオプションを選択できます。

## 2.1. AWS インフラストラクチャーアクセスの設定

**前提条件**

- IAM パーミッションを持つ AWS アカウント。

### 2.1.1. IAM パーミッションを持つ AWS アカウントの作成

AWS インフラストラクチャーへのアクセスを設定する前に、AWS アカウントで IAM パーミッションを設定する必要があります。

**手順**

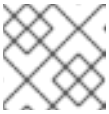
1. AWS アカウントにログインします。必要な場合は、AWS ドキュメントに従って新規 AWS アカウントを作成できます。
2. AWS アカウントで **STS:AllowAssumeRole** パーミッションを持つ IAM ユーザーを作成します。
   a. AWS 管理コンソールの IAM ダッシュボードを開きます。
   b. **Policies** セクションで、 **Create Policy** をクリックします。
   c. **JSON** タブを選択し、既存のテキストを以下に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
     {
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "*"
     }
  ]
}
```

   d. **Review Policy** をクリックします。
   e. 適切な名前および説明を指定してから **Create Policy** をクリックします。
   f. **Users** セクションで、**Add plan** をクリックします。
   g. 適切なユーザー名を指定します。
   h. 必要に応じて **AWS 管理コンソールアクセス** および他のロールを選択します。
   i. 組織に必要なパスワード要件を調整してから **Next: Policy** をクリックします。

j. **Attach existing policies directly** オプションをクリックします。

k. 直前の手順で作成したポリシーを検索し、確認します。



**注記**

パーミッションの境界を設定することは推奨されていません。

l. **Next: Tags** をクリックしてから **Next: Review** をクリックします。設定が正しいことを確認します。

m. **Create user** をクリックしてから、成功したことを示すページで **Close** をクリックします。

3. IAM ユーザーの Amazon Resource Name (ARN) を収集します。ARN の形式は **arn:aws:iam::000111222333:user/username** のようになります。

### 2.1.2. OpenShift Cluster Manager からの IAM ロールの付与

**手順**

1. ブラウザーで OpenShift Dedicated Cluster Manager を開き、AWS インフラストラクチャーアクセスを許可するクラスターを選択します。

2. **Access control** タブを選択し、 **AWS Infrastructure Access** セクションにスクロールします。

3. AWS IAM ARN を貼り付け、**Network Management** または **Read-only** パーミッションを選択してから **Grant role** をクリックします。

4. AWS OSD Console の URL をクリップボードにコピーします。

5. アカウント ID またはエイリアス、IAM ユーザー名、およびパスワードを使用して AWS アカウントにサインインします。

6. 新規のブラウザータブで、AWS Switch Role ページにルート指定するために使用される AWS OSD Console URL を貼り付けます。

7. アカウント番号とロールはすでに入力されています。必要な場合は表示名を選択してから **Switch Role** をクリックします。これで、**VPC** が **Recently visited services** の下に表示されます。

# 第3章 AWS VPC ピアリングの設定

このサンプルプロセスでは、OpenShift Dedicated クラスターを含む Amazon Web Services (AWS) VPC を別の AWS VPC ネットワークとピア接続できるように設定します。AWS VPC ピアリング接続の作成、または他の使用可能な設定についての詳細は、AWS VPC ピアリングについてのガイドを参照してください。

## 3.1. VPC ピアリングの用語

2 つの別個の AWS アカウントで 2 つの VPC 間に VPC ピアリング接続を設定する場合は、以下の用語が使用されます。

| | |
|---|---|
| OSD AWS アカウント | OpenShift Dedicated クラスターを含む AWS アカウント。 |
| OSD クラスター VPC | OpenShift Dedicated クラスターを含む VPC。 |
| カスタマー AWS アカウント | ピア接続に使用する OSD 以外の AWS アカウント。 |
| カスタマー VPC | ピア接続に使用する AWS アカウントの VPC。 |
| カスタマー VPC リージョン | カスタマー VPC が置かれているリージョン。 |

**注記**

2018 年 7 月時点で、AWS は中国を除くすべての商業地域の間でのリージョン間の VPC ピアリングをサポートします。

## 3.2. VPC ピア要求の開始

VPC ピアリング接続要求は OSD AWS アカウントからカスタマー AWS アカウントに送信できます。

**前提条件**

- ピアリング要求を開始するのに必要なカスタマー VPC に関する以下の情報を収集します。
  - カスタマー AWS アカウント番号
  - カスタマー VPC ID
  - カスタマー VPC リージョン
  - カスタマー VPC CIDR
- OpenShift Dedicated Cluster VPC で使用される CIDR ブロックを確認します。カスタマー VPC の CIDR ブロックとの重複があるか、またはこのブロックとの不一致がある場合、これらの 2

つの VPC 間でのピアリングは実行できません。詳細は、Amazon VPC の「サポートされていない VPC ピア接続設定」ドキュメントを参照してください。CIDR ブロックが重複しない場合、以下の手順を実行できます。

**手順**

1. OSD AWS アカウントの Web コンソールにログインし、クラスターがホストされているリージョンの **VPC Dashboard** に移動します。
2. **Peering Connections** ページに移動し、**Create Peering Connection** ボタンをクリックします。
3. ログインしているアカウントの詳細と、接続しているアカウントおよび VPC の詳細を確認します。
   a. **Peering connection name tag** VPC ピアリング接続の説明的な名前を設定します。
   b. **VPC (Requester)**: ドロップダウン *リストから OpenShift Dedicated Cluster VPC ID を選択します。
   c. **Account**: **Another account** を選択し、カスタマー AWS アカウント番号 *(ダッシュなし) を指定します。
   d. **Region**: カスタマー VPC リージョンが現在のリージョンとは異なる場合、**Another Region** を選択し、ドロップダウンリストからカスタマー VPC リージョンを選択します。
   e. **VPC (Accepter)**: カスタマー VPC ID を設定します。
4. **Create Peering Connection** をクリックします。
5. 要求が **Pending** 状態になることを確認します。ステータスが **Failed** の場合、詳細を確認して、このプロセスを繰り返します。

**追加リソース**

- OSD AWS アカウント用の Web コンソールへのログイン

## 3.3. VPC ピア要求の受け入れ

VPC ピアリング接続の作成後に、カスタマー AWS アカウントで要求を受け入れる必要があります。

**前提条件**

- VPC ピア要求を開始します。

**手順**

1. AWS Web Console にログインします。
2. **VPC Service** に移動します。
3. **Peering Connections** に移動します。
4. **Pending peering connection** をクリックします。

5. 要求の送信元である AWS アカウントおよび VPC ID を確認します。これは、OSD AWS アカウントおよび OpenShift Dedicated Cluster VPC からのものである必要があります。

6. **Accept Request** をクリックします。

## 3.4. ルーティングテーブルの設定

VPC ピアリング要求を受け入れた後に、両方の VPC はそれらのルートをピアリング接続全体で通信できるように設定する必要があります。

**前提条件**

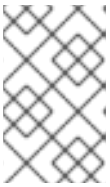
- VPC ピア要求を開始し、受け入れます。

**手順**

1. OSD AWS アカウントで AWS Web Console にログインします。

2. **VPC Service** に移動してから、 **Route Tables** に移動します。

3. OpenShift Dedicated クラスター VPC のルートテーブルを選択します。



**注記**

クラスターによっては、特定の VPC に複数のルートテーブルがある場合があります。明示的に関連付けられたサブネットが多数あるプライベートのルートテーブルを選択します。

4. **Routes** タブを選択してから **Edit** を選択します。

5. **Destination** テキストボックスにカスタマー VPC CIDR ブロックを入力します。

6. **Target** テキストボックスに Peering Connection ID を入力します。

7. **Save** をクリックします。

8. 他の VPC の CIDR ブロックについて同じプロセスを実行する必要があります。

    a. カスタマー AWS Web Console にログインし、→ **VPC Service** → **Route Tables** に移動します。

    b. VPC のルートテーブルを選択します。

    c. **Routes** タブを選択してから **Edit** を選択します。

    d. **Destination** テキストボックスに OpenShift Dedicated Cluster VPC CIDR ブロックを入力します。

    e. **Target** テキストボックスに Peering Connection ID を入力します。

    f. **Save** をクリックします。

VPC ピアリング接続が完了しました。検証手順に従って、ピアリング接続全体での接続が機能していることを確認します。

## 3.5. VPC ピアリングの検証およびトラブルシューティング

VPC ピアリング接続を設定したら、これが正しく設定され、機能していることを確認することが推奨されます。

**前提条件**

- VPC ピア要求を開始し、受け入れます。
- ルーティングテーブルの設定

**手順**

- AWS コンソールで、ピアリングされたクラスター VPC のルートテーブルを確認します。ルーティングテーブルを設定する手順に従い、VPC CIDR 範囲の宛先をピアリング接続ターゲットにポイントするルートテーブルエントリーがあることを確認します。
  正しいルートが OpenShift Dedicated Cluster VPC ルートテーブルおよびカスタマー VPC ルートテーブルの両方で使用されることが予想される場合、接続を以下の **netcat** メソッドを使用してテストする必要があります。テスト呼び出しに成功する場合、VPC ピアリングは適切に機能していることになります。
- エンドポイントデバイスへのネットワーク接続をテストするには、**nc** (または **netcat**) が便利なトラブルシューティングツールです。これはデフォルトのイメージに含まれ、接続を確立できる場合に迅速かつ明確に出力を提供します。

  a. **busybox** イメージを使用して一時的な Pod を作成します。これは後で自らをクリーンアップします。

  ```
  $ oc run netcat-test \
      --image=busybox -i -t \
      --restart=Never --rm \
      -- /bin/sh
  ```

  b. **nc** を使用して接続を確認します。

  - 接続の成功した結果の例:

  ```
  / nc -zvv 192.168.1.1 8080
  10.181.3.180 (10.181.3.180:8080) open
  sent 0, rcvd 0
  ```

  - 接続の失敗した結果の例:

  ```
  / nc -zvv 192.168.1.2 8080
  nc: 10.181.3.180 (10.181.3.180:8081): Connection refused
  sent 0, rcvd 0
  ```

  c. コンテナーを終了します。これにより Pod が自動的に削除されます。

  ```
  / exit
  ```

# 第4章 AWS VPN の設定

このサンプルプロセスでは、Amazon Web Services (AWS) OpenShift Dedicated クラスターを、お客様のオンサイトのハードウェア VPN デバイスを使用するように設定します。

**注記**

AWS VPN は現在、NAT を VPN トラフィックに適用するための管理オプションを提供していません。詳細は、AWS ナレッジセンターを参照してください。

**注記**

プライベート接続を経由したすべてのトラフィックのルーティング (**0.0.0.0/0**など) はサポートされていません。この場合、SRE 管理トラフィックを無効にするインターネットゲートウェイを削除する必要があります。

ハードウェア VPN デバイスを使用して AWS VPC をリモートネットワークに接続する方法については、Amazon VPC の「VPN 接続」ドキュメントを参照してください。

## 4.1. VPN 接続の作成

以下の手順に従って、Amazon Web Services (AWS) OpenShift Dedicated クラスターを、お客様のオンサイトのハードウェア VPN デバイスを使用できるように設定できます。

**前提条件**

- ハードウェア VPN ゲートウェイデバイスモデルおよびソフトウェアバージョン (例: Cisco ASA バージョン 8.3 を実行)。Amazon VPC のネットワーク管理者ガイドを参照して、お使いのゲートウェイデバイスが AWS でサポートされているかどうかを確認します。
- VPN ゲートウェイデバイスのパブリック静的 IP アドレス。
- BGP または静的ルーティング: BGP の場合は、ASN が必要です。静的ルーティングの場合は、1 つ以上の静的ルートを設定する必要があります。
- オプション: VPN 接続をテストするための到達可能なサービスの IP およびポート/プロトコル。

### 4.1.1. VPN 接続の設定

**手順**

1. OSD AWS Account Dashboard にログインし、VPC Dashboard に移動します。
2. **Your VPCs** をクリックし、 OpenShift Dedicated クラスターが含まれる VPC の名前および VPC ID を特定します。
3. VPC Dashboard から **Customer Gateway** をクリックします。
4. **Create Customer Gateway** をクリックし、これに分かりやすい名前を付けます。
5. ルーティング方法 (**Dynamic** または **Static**) を選択します。
6. Dynamic の場合は、表示されるフィールドに BGP ASN を入力します。

7. VPN ゲートウェイエンドポイント IP アドレスに貼り付けます。
8. **Create** をクリックします。
9. 仮想プライベートゲートウェイが意図されている VPC に割り当てられていない場合は、以下を実行します。
    a. VPC Dashboard で **Virtual Private Gateway** をクリックします。
    b. **Create Virtual Private Gateway**をクリックし、これに分かりやすい名前を付け、**Create** をクリックします。
    c. デフォルトの Amazon デフォルト ASN のままにします。
    d. 新たに作成したゲートウェイを選択し、**Attach to VPC** をクリックし、これを以前に指定したクラスター VPC に割り当てます。

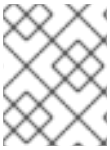
### 4.1.2. VPN 接続の確立

**手順**

1. VPC ダッシュボードから、**Site-to-Site VPN Connections** をクリックします。
2. **Create VPN Connection** をクリックします。
    a. これに分かりやすい名前タグを指定します。
    b. 以前に作成した仮想プライベートゲートウェイを選択します。
    c. Customer Gateway で、**Existing**を選択します。
    d. 名前でカスタマーゲートウェイデバイスを選択します。
    e. VPN が BGP を使用する場合は **Dynamic** を選択し、それ以外の場合は **Static** を選択します。静的 IP CIDR を入力します。複数の CIDR がある場合は、各 CIDR を **Another Rule** として追加します。
    f. **Create** をクリックします。
    g. VPN のステータスが **Available** に変更するまで待機します (約 5 分から 10 分)。
3. 作成したばかりの VPN を選択し、**Download Configuration** をクリックします。
    a. ドロップダウンリストから、カスタマーゲートウェイデバイスのベンダー、プラットフォーム、およびバージョンを選択し、**Download** をクリックします。
    b. **Generic** ベンダー設定は、プレーンテキスト形式で情報を取得する場合にも利用できます。

**注記**

VPN 接続が確立されたら、Route Propagation をセットアップしてください。セットアップしない場合、VPN が予想通りに機能しない可能性があります。



**注記**

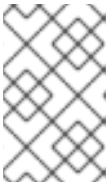
VPC サブネット情報をメモします。これは、リモートネットワークとして設定に追加する必要があります。

### 4.1.3. VPN ルート伝播の有効化

VPN 接続を設定したら、必要なルートが VPC のルートテーブルに追加されるように、ルートの伝播が有効にされていることを確認する必要があります。

**手順**

1. VPC Dashboard で、**Route Tables** をクリックします。
2. OpenShift Dedicated クラスターが含まれる VPC に関連付けられたプライベートルートテーブルを選択します。



**注記**

クラスターによっては、特定の VPC に複数のルートテーブルがある場合があります。明示的に関連付けられたサブネットが多数あるプライベートのルートテーブルを選択します。

3. **Route Propagation** タブをクリックします。
4. 表示されるテーブルに、以前に作成した仮想プライベートゲートウェイが表示されます。**Propagate column** の値を確認します。
    a. Propagate が **No**に設定されている場合には、**Edit route propagation** をクリックして、仮想プライベートゲートウェイの名前の横にある Propagate チェックボックスにチェックを入れ、**Save** をクリックします。

VPN トンネルを設定し、AWS がこれを **Up** として検出すると、静的ルートまたは BGP ルートは自動的にルートテーブルに追加されます。

## 4.2. VPN 接続の確認

ご使用の側から VPN トンネルを設定した後に、そのトンネルが AWS コンソールで稼働していること、およびトンネル全体で接続が機能していることを確認します。

**前提条件**

- VPN 接続が作成されている。

**手順**

1. **トンネルが AWS で稼働していることを確認します。**
    a. VPC Dashboard で、**VPN Connections** をクリックします。
    b. 以前に作成した VPN 接続を選択し、**Tunnel Details** タブをクリックします。
    c. 1 つ以上の VPN トンネルが **Up** になっていることを確認できます。
2. **接続を確認します。**

エンドポイントデバイスへのネットワーク接続をテストするには、**nc** (または **netcat**) が便利なトラブルシューティングツールになります。これはデフォルトのイメージに含まれ、接続を確立できる場合に迅速かつ明確に出力を提供します。

a. **busybox** イメージを使用して一時的な Pod を作成します。これは後で自らをクリーンアップします。

```
$ oc run netcat-test \
    --image=busybox -i -t \
    --restart=Never --rm \
    -- /bin/sh
```

b. **nc** を使用して接続を確認します。

- 接続の成功した結果の例:

```
/ nc -zvv 192.168.1.1 8080
10.181.3.180 (10.181.3.180:8080) open
sent 0, rcvd 0
```

- 接続の失敗した結果の例:

```
/ nc -zvv 192.168.1.2 8080
nc: 10.181.3.180 (10.181.3.180:8081): Connection refused
sent 0, rcvd 0
```

c. コンテナーを終了します。これにより Pod が自動的に削除されます。

```
/ exit
```

## 4.3. VPN 接続のトラブルシューティング

**トンネルが接続しない**
トンネル接続が依然として **Down** の場合は、以下の点を確認できます。

- AWS トンネルは VPN 接続を開始しません。接続の試行は Customer Gateway から開始する必要があります。
- ソーストラフィックが、設定されたカスタマーゲートウェイと同じ IP から送信されることを確認します。AWS は、ソース IP アドレスが一致しないゲートウェイへのすべてのトラフィックを通知なしでドロップします。
- 設定が AWS でサポートされる値と一致することを確認します。これには、IKE バージョン、DH グループ、IKE ライフタイムなどが含まれます。
- VPC のルートテーブルを再確認します。伝播が有効にされており、ターゲットとして先に作成した仮想プライベートゲートウェイを持つエントリーがルートテーブルにあることを確認します。
- 中断を生じさせる可能性のあるファイアウォールルールがないことを確認します。
- ポリシーベースの VPN を使用しているかどうかを確認します。これを使用している場合、その設定によっては複雑な状態が生じる可能性があります。

- トラブルシューティングの手順についての詳細は、AWS ナレッジセンターを参照してください。

**トンネルが接続状態にならない**
トンネル接続を一貫して **Up** の状態にすることができない場合は、すべての AWS トンネル接続がゲートウェイから開始される必要があることに注意してください。AWS トンネルはトンネリングを開始しません。

Red Hat は、ご使用の側から SLA モニター (Cisco ASA) または一部のデバイスをセットアップすることを推奨しています。これにより、VPC CIDR 範囲内で設定されるすべての IP アドレスで、**ping**、**nc**、**telnet** などの対象 (interesting) トラフィックが絶えず送信されます。接続が成功したかどうかにかかわらず、トラフィックがトンネルにダイレクトされます。

**Down 状態のセカンダリートンネル**
VPN トンネルが作成されると、AWS は追加のフェイルオーバートンネルを作成します。ゲートウェイデバイスによっては、セカンダリートンネルが **Down** 状態として表示される場合があります。

AWS 通知は以下のようになります。

> You have new non-redundant VPN connections
>
> One or more of your vpn connections are not using both tunnels. This mode of operation is not highly available and we strongly recommend you configure your second tunnel. View your non-redundant VPN connections.

# 第5章 AWS DIRECT CONNECT の設定

このプロセスでは、OpenShift Dedicated で AWS Direct Connect 仮想インターフェースを許可する方法について説明します。AWS Direct Connect の種類および設定についての詳細は、「AWS Direct Connect コンポーネント」ドキュメントを参照してください。

## 5.1. AWS DIRECT CONNECT メソッド

Direct Connect 接続では、ホストされた Virtual Interface (VIF) が Direct Connect Gateway (DXGateway) に接続されている必要があります。これは次に、同じまたは別のアカウントでリモート VPC にアクセスするために Virtual Gateway (VGW) または Transit Gateway に関連付けられます。

既存の DXValidation がない場合、通常のプロセスではホストされた VIF を作成し、OSD AWS アカウントに DXValidation および VGW が作成されます。

既存の DXGateway が 1 つ以上の既存の VGW に接続されている場合、このプロセスでは、OSD AWS Account が Association Proposal (関連付けの提案) を DXGateway の所有者に送信します。DXGateway の所有者は、提案される CIDR が関連付けのあるその他の VGW と競合しないことを確認する必要があります。

詳細は、以下の AWS ドキュメントを参照してください。

- 仮想インターフェイス
- Direct Connect ゲートウェイ
- アカウント間で仮想プライベートゲートウェイを関連付ける

**重要**

既存の DXValidation に接続する場合は、料金がかかります。

選択可能な 2 つの設定オプションは、以下のとおりです。

| | |
|---|---|
| 方法 1 | ホストされた VIF を作成してから、DXGateway および VGW を作成します。 |
| 方法 2 | 所有している既存の Direct Connect Gateway 経由で接続を要求します。 |

## 5.2. ホストされた仮想インターフェースの作成

**前提条件**

- OSD AWS Account ID を収集します。

### 5.2.1. Direct Connect 接続のタイプの判別

Direct Connect Virtual Interface の詳細を表示して、接続のタイプを判別します。

**手順**

1. OSD AWS Account Dashboard にログインし、適切なリージョンを選択します。

2. **Services** メニューから **Direct Connect** を選択します。
3. 受け入れを待機している 1 つ以上の仮想インターフェースがあります。いずれかの仮想インターフェースを選択して **Summary** を表示します。
4. 仮想インターフェースタイプ (private または public) を表示します。
5. **Amazon side ASN** の値を記録します。

Direct Connect Virtual Interface タイプが Private の場合は、Virtual Private Gateway が作成されます。Direct Connect Virtual Interface が Public の場合は、Direct Connect Gateway が作成されます。

### 5.2.2. Private Direct Connect の作成

Direct Connect Virtual Interface タイプが Private の場合は、Private Direct Connect が作成されます。

**手順**

1. OSD AWS Account Dashboard にログインし、適切なリージョンを選択します。
2. AWS リージョンから、**Services** メニューで **VPC** を選択します。
3. **VPN Connections** から **Virtual Private Gateways** を選択します。
4. **Create Virtual Private Gateway** をクリックします。
5. 仮想プライベートゲートウェイに適切な名前を付けます。
6. **Custom ASN** を選択し、以前に収集した **Amazon side ASN** 値を入力します。
7. 仮想プライベートゲートウェイを作成します。
8. 新たに作成した Virtual Private Gateway をクリックし、**Actions** タブから **Attach to VPC** を選択します。
9. 一覧から **OSD Cluster VPC** を選択し、仮想プライベートゲートウェイを VPC に割り当てます。
10. **Services** メニューから **Direct Connect** をクリックします。一覧から、Direct Connect 仮想インターフェースのいずれかを選択します。
11. **I understand that Direct Connect port charges apply once I click Accept Connection** メッセージを確認した後に、**Accept Connection** を選択します。
12. 仮想プライベートゲートウェイ接続に対して **Accept** を選択し、直前の手順で作成した仮想プライベートゲートウェイを選択します。
13. **Accept** を選択し、接続を受け入れます。
14. 複数の仮想インターフェースがある場合は、直前の手順を繰り返します。

### 5.2.3. Public Direct Connect の作成

Direct Connect Virtual Interface タイプが Public の場合は、Public Direct Connect が作成されます。

**手順**

1. OSD AWS Account Dashboard にログインし、適切なリージョンを選択します。
2. OSD AWS Account リージョンから、**Services** メニューで **Direct Connect** を選択します。
3. **Direct Connect Gateways** および **Create Direct Connect Gateway** を選択します。
4. Direct Connect Gateway に適切な名前を付けます。
5. **Amazon side ASN** で、以前に収集した Amazon side ASN 値を入力します。
6. Direct Connect Gateway を作成します。
7. **Services** メニューから **Direct Connect** を選択します。
8. 一覧から、Direct Connect Virtual Interface のいずれかを選択します。
9. **I understand that Direct Connect port charges apply once I click Accept Connection**メッセージを確認した後に、**Accept Connection** を選択します。
10. Direct Connect Gateway Connection に対して **Accept** を選択し、直前の手順で作成した Direct Connect Gateway を選択します。
11. **Accept** をクリックして接続を受け入れます。
12. 複数の仮想インターフェースがある場合は、直前の手順を繰り返します。

### 5.2.4. 仮想インターフェースの検証

Direct Connect 仮想インターフェースが許可されたら、短い時間待機し、インターフェースの状態を確認します。

**手順**

1. OSD AWS Account Dashboard にログインし、適切なリージョンを選択します。
2. OSD AWS Account リージョンから、**Services** メニューで **Direct Connect** を選択します。
3. 一覧から、Direct Connect Virtual Interface のいずれかを選択します。
4. インターフェースの状態が **Available** になったことを確認します。
5. インターフェース BGP のステータスが **Up** になったことを確認します。
6. 残りの Direct Connect インターフェースに対してこの検証を繰り返します。

Direct Connect 仮想インターフェースが利用可能になった後に、OSD AWS Account Dashboard にログインし、ご使用の側からの設定に使用する Direct Connect 設定ファイルをダウンロードできます。

## 5.3. 既存の DIRECT CONNECT GATEWAY への接続

**前提条件**

- OSD VPC の CIDR 範囲が、関連付けのあるその他の VGW と競合しないことを確認します。
- 以下の情報を収集します。

- Direct Connect Gateway ID。
- 仮想インターフェースに関連付けられた AWS Account ID。
- DXGateway に割り当てられた BGP ASN。オプション: Amazon のデフォルト ASN も使用できます。

**手順**

1. OSD AWS Account Dashboard にログインし、適切なリージョンを選択します。
2. OSD AWS Account リージョンから、**Services** メニューで **VPC** を選択します。
3. **VPN Connections** から、 **Virtual Private Gateways** を選択します。
4. **Create Virtual Private Gateway** を選択します。
5. 仮想プライベートゲートウェイに適切な名前を付けます。
6. **Custom ASN** をクリックし、以前に使用された **Amazon side ASN** 値を入力するか、または Amazon で提供される ASN を使用します。
7. 仮想プライベートゲートウェイを作成します。
8. OSD AWS Account Dashboard の **Navigation** ペインで、**Virtual private gateways** を選択し、仮想プライベートゲートウェイを選択します。**View details** を選択します。
9. **Direct Connect gateway associations** を選択し、**Associate Direct Connect gateway** をクリックします。
10. **Association account type** で、 Account の所有者について **Another account** を選択します。
11. **Direct Connect gateway owner** について、Direct Connect ゲートウェイを所有する AWS アカウントの ID を入力します。
12. **Association settings** で、 Direct Connect ゲートウェイ ID について、Direct Connect ゲートウェイの ID を入力します。
13. **Association settings** で、仮想インターフェースの所有者について、関連付けのために仮想インターフェースを所有する AWS アカウントの ID を入力します。
14. オプション: プレフィックスを Allowed のプレフィックスに追加し、それらをコンマで区切ります。
15. **Associate Direct Connect gateway** を選択します。
16. Association Proposal (関連付けの提案) が送信された後は、受け入れを待機します。実行する必要のある最終手順については、AWS ドキュメンテーションを参照してください。

## 5.4. DIRECT CONNECT のトラブルシューティング

詳細なトラブルシューティングについては、「AWS Direct Connect のトラブルシューティング」ドキュメントを参照してください。

# 第6章 プライベートクラスターの設定

OpenShift Dedicated クラスターをプライベートにし、内部アプリケーションを企業ネットワーク内でホストできるようにします。さらに、プライベートクラスターは、セキュリティーを強化するために内部 API エンドポイントのみを持つように設定できます。

OpenShift Dedicated 管理者は、**OpenShift Cluster Manager** (OCM) 内からパブリックおよびプライベートのクラスター設定のいずれかを選択できます。プライバシー設定は、クラスターの作成時またはクラスターの設定後に設定できます。

## 6.1. 新規クラスターでのプライベートクラスターの有効化

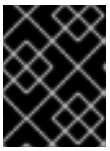
新規クラスターの作成時にプライベートクラスター設定を有効にできます。

**前提条件**

- AWS VPC ピアリング、VPN、DirectConnect、または TransitGateway はプライベートアクセスを許可するように設定されています。

**手順**

1. OpenShift Cluster Manager で、**Create cluster** をクリックし、**OpenShift Dedicated** を選択します。
2. クラスターの詳細を設定し、Networking セクションで **Advanced** を選択します。
3. ネットワークの CIDR 要件を判別し、必要なフィールドに入力します。



**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。

4. **Cluster Privacy**で **Private** を選択します。

## 6.2. 既存クラスターでのプライベートクラスターの有効化

クラスターの作成後にプライベートクラスターを有効にできます。

**前提条件**

- AWS VPC ピアリング、VPN、DirectConnect、または TransitGateway はプライベートアクセスを許可するように設定されています。

**手順**

1. OpenShift Cluster Manager でクラスターにアクセスします。
2. **Networking** タブに移動します。
3. **Master API endpoint**で **Make API private** を選択し、 **Change settings** をクリックします。

**注記**

クラスターをプライベートとパブリックの間で移行するには、完了までに数分の時間がかかることがあります。

## 6.3. プライベートクラスターでのパブリッククラスターの有効化

プライベートクラスターをパブリック向けに設定できます。

**手順**

1. OpenShift Cluster Manager でクラスターにアクセスします。
2. **Networking** タブに移動します。
3. **Master API endpoint** で **Make API private** の選択を解除し、**Change settings** をクリックします。

**注記**

クラスターをプライベートとパブリックの間で移行するには、完了までに数分の時間がかかることがあります。

**注記**

Red Hat Service Reliability Engineering (SRE) は、**cloud-ingress-operator** および既存の ElasticSearch Load Balancer または Amazon S3 フレームワークを介してパブリックまたはプライベートクラスターにアクセスできます。SRE はセキュアなエンドポイントを介してクラスターにアクセスし、メンテナンスおよびサービスタスクを実行できます。