OpenShift Dedicated 4

プライベート接続の構成

OpenShift Dedicated のプライベート接続の設定

Last Updated: 2021-10-17

OpenShift Dedicated 4 プライベート接続の構成

OpenShift Dedicated のプライベート接続の設定

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

OpenShift Dedicated クラスターのプライベート接続

目次

第1章 AWS のプライベート接続の設定

1.1. AWS クラウドインフラストラクチャーのアクセスについて

Amazon Web Services (AWS) インフラストラクチャーへのアクセスにより、カスタマーポータルの組織管理者 およびクラスターの所有者は AWS の 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。AWS アクセスはカスタマー AWS ユーザーに付与でき、OpenShift Dedicated 環境のニーズに合わせてプライベートクラスターのアクセスを実装できます。

1. OpenShift Dedicated クラスターの AWS インフラストラクチャーアクセスの設定を開始します。AWS ユーザーおよび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。

2. 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の設定後に、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。

1.2. AWS インフラストラクチャーアクセスの設定

Amazon Web Services (AWS) インフラストラクチャーへのアクセスにより、カスタマーポータルの組織管理者 およびクラスターの所有者は AWS の 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、**Network Management** または **Read-only** アクセスのオプションを選択できます。

前提条件

- IAM パーミッションを持つ AWS アカウント。

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 アカウント内に **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. **Next:Tags** をクリックします。

e. オプション: タグを追加します。**Next:Review** をクリックします。

f. 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。

g. **Plans** セクションで、**Add plan** をクリックします。

h. 適切なユーザー名を指定します。

i. AWS アクセスタイプとして **AWS Management Console access** を選択します。

j. 組織に必要なパスワード要件を調整してから **Next:Permissions** をクリックします。

k. **Attach existing policies directly** オプションをクリックします。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** をクリックすると、成功ページが表示されます。

n. 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。**Close** をクリックします。

3. ブラウザーで OpenShift Cluster Manager (OCM) 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。

4. **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。

5. **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。

6. **AWS OSD console URL** をクリップボードにコピーします。

7. 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。

8. 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。

9. 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。

検証

- これで、**VPC** が **Recently visited services** の下に表示されます。

1.3. AWS VPC ピアリングの設定

Virtual Private Cloud (VPC) ピアリング接続は、2 つの VPC 間のネットワーク接続で、プライベート IPv4 アドレスまたは IPv6 アドレスを使用してこれらの間のトラフィックをルーティングできるようにします。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するように設定できます。

警告

クラスターがインストールされている VPC がピアリングされている場合、プライベートクラスターは OpenShift Cluster Manager (OCM) によって完全に削除することができません。

AWS は、中国を除く すべての商業地域でのリージョン間の VPC ピアリングをサポートします。

前提条件

- ピアリング要求を開始するために必要な Customer VPC に関する以下の情報を収集します。
  - Customer AWS アカウント番号
  - Customer VPC ID
  - Customer VPC リージョン
  - Customer VPC CIDR
- OpenShift Dedicated Cluster VPC で使用される CIDR ブロックを確認します。Customer VPC の CIDR ブロックとの重複や一致がある場合、これらの 2 つの VPC 間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 ピアリング設定 に関する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は、以下の手順を実行できます。

手順

1. VPC ピアリング要求を開始します。
2. VPC ピアリング要求を受け入れます。
3. VPC ピアリング接続の Route テーブルを更新します。

関連情報

- 詳細およびトラブルシューティングのヘルプは、『AWS VPC』ガイドを参照してください。

1.4. AWS VPN の設定

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仮想プライベートネットワーク (VPN) デバイスを使用するように設定できます。デフォルトで、AWS Virtual Private Cloud (VPC) に起動するインスタンスは、独自の (リモート) ネットワークと通信できません。AWS Site-to-Site VPN 接続を作成し、ルーティングを設定して接続経由でトラフィックを渡すことで、VPC からリモートネットワークへのアクセスを有効にできます。

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ません。詳細は、AWS Knowledge Center を参照してください。

プライベート接続を使用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。これには、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。

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: バージョン 8.3 を実行している Cisco ASA)。AWS ドキュメント 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な静的 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。

手順

1. VPN 接続を設定するために カスタマーゲートウェイを作成 します。
2. 仮想プライベートゲートウェイが目的の VPC に割り当てられていない場合は、仮想プライベートゲートウェイを 作成して割り当て ます。
3. ルーティングを設定し、VPN ルート伝播を有効にします。
4. セキュリティーグループを更新します。
5. サイト間 VPN 接続を確立します。

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。

関連情報

- 詳細およびトラブルシューティングのヘルプは、『AWS VPN』ガイドを参照してください。

1.5. AWS DIRECT CONNECT の設定

Amazon Web Services (AWS) Direct Connect 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、同じまたは別のアカウントでリモート Virtual Private Cloud (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 DXGateway 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、AWS アカウントに DXGateway 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は、プロセスに AWS アカウントが Association Proposal を DXGateway の所有者に送信します。DXGateway の所有者は、提案された CIDR が関連付けられているその他の VGW と競合しないようにする必要があります。

前提条件

- OpenShift Dedicated 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。
- 以下の情報を入力します。
  - Direct Connect Gateway ID。
  - 仮想インターフェースに関連付けられた AWS アカウント 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. VIF を作成する か、既存の VIF を表示 して、作成する必要のあるダイレクト接続の種別を判断します。
2. ゲートウェイを作成します。
   a. Direct Connect VIF タイプが **Private** の場合は、仮想プライベートゲートウェイを作成 します。
   b. Direct Connect VIF が **Public** の場合は、Direct Connect ゲートウェイを作成 します。
3. 使用する既存のゲートウェイがある場合は、関連付けの提案を作成 し、承認のために提案を DXGateway の所有者に送信します。

警告

既存の DXGateway に接続する場合は、コスト がかかります。

関連情報

- 詳細およびトラブルシューティングのヘルプは、「AWS Direct Connect」ガイドを参照してください。

第2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。

2.1. クラスター作成時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

- プライベートアクセスを許可するには、以下のプライベート接続を設定する必要があります。
  - VPC ピアリング
  - Cloud VPN
  - DirectConnect (AWS のみ)
  - TransitGateway (AWS のみ)
  - Cloud Interconnect (GCP のみ)

手順

1. OpenShift Cluster Manager (OCM) にログインします。
2. **Create cluster** → **OpenShift Dedicated** → **Create cluster** をクリックします。
3. クラスターの詳細を設定します。
4. 希望するネットワーク設定を選択する場合は、**Advanced** を選択します。
5. **Private** を選択します。

警告

Private に設定されている場合は、前提条件で説明されているように、クラウドプロバイダーにプライベート接続を設定しない限り、クラスターにアクセスできません。

6. **Create cluster** をクリックします。クラスター作成プロセスが開始され、完了するまでに 30 - 40 分かかります。

検証

- **Overview** タブの **Installing cluster** という見出しは、クラスターがインストール中であることを示し、この見出しからインストールログを確認できます。**Details** 見出しの **Status** インディケーターは、クラスターが使用できる **Ready** 状態であるかを示します。

2.2. 既存クラスターをプライベートにすることが可能

クラスターを作成したら、後でクラスターをプライベートにすることができます。

前提条件

- プライベートアクセスを許可するには、以下のプライベート接続を設定する必要があります。
  - VPC ピアリング
  - Cloud VPN
  - DirectConnect (AWS のみ)
  - TransitGateway (AWS のみ)
  - Cloud Interconnect (GCP のみ)

手順

1. OpenShift Cluster Manager (OCM) にログインします。
2. プライベートにするパブリッククラスターを選択します。
3. **Networking** タブの **Control Plane API endpoint**の下で、**Make API private** を選択します。

警告

Private に設定されている場合は、前提条件で説明されているように、クラウドプロバイダーにプライベート接続を設定しない限り、クラスターにアクセスできません。

4. **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場合があります。

2.3. 既存のプライベートクラスターをパブリックにすることが可能

プライベートクラスターを作成したら、後でクラスターをパブリックにすることができます。

手順

1. OpenShift Cluster Manager (OCM) にログインします。
2. パブリックにするプライベートクラスターを選択します。
3. **Networking** タブの **Control Plane API endpoint**の下で、 **Make API private** の選択を解除します。
4. **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場合があります。