OpenShift Dedicated 4

Configuring private connections

Configuring private connections for OpenShift Dedicated

Last Updated: 2021-10-14

OpenShift Dedicated 4 Configuring private connections

Configuring private connections for OpenShift Dedicated

Legal Notice

Abstract

Private connections on your OpenShift Dedicated cluster

Table of Contents

CHAPTER 1. CONFIGURING PRIVATE CONNECTIONS FOR AWS

1.1. UNDERSTANDING AWS CLOUD INFRASTRUCTURE ACCESS

NOTE

AWS cloud infrastructure access does not apply to the Customer Cloud Subscription (CCS) infrastructure type that is chosen when you create a cluster because CCS clusters are deployed onto your account.

Amazon Web Services (AWS) infrastructure access permits Customer Portal Organization Administrators and cluster owners to enable AWS Identity and Access Management (IAM) users to have federated access to the AWS Management Console for their OpenShift Dedicated cluster. AWS access can be granted for customer AWS users, and private cluster access can be implemented to suit the needs of your OpenShift Dedicated environment.

1. Get started with configuring AWS infrastructure access for your OpenShift Dedicated cluster. By creating an AWS user and account and providing that user with access to the OpenShift Dedicated AWS account.

2. After you have access to the OpenShift Dedicated AWS account, use one or more of the following methods to establish a private connection to your cluster:

   - Configuring AWS VPC peering: Enable VPC peering to route network traffic between two private IP addresses.

   - Configuring AWS VPN: Establish a Virtual Private Network to securely connect your private network to your Amazon Virtual Private Cloud.

   - Configuring AWS Direct Connect: Configure AWS Direct Connect to establish a dedicated network connection between your private network and an AWS Direct Connect location.

After configuring your cloud infrastructure access, learn more about Configuring a private cluster.

1.2. CONFIGURING AWS INFRASTRUCTURE ACCESS

Amazon Web Services (AWS) infrastructure access allows Customer Portal Organization Administrators and cluster owners to enable AWS Identity and Access Management (IAM) users to have federated access to the AWS Management Console for their OpenShift Dedicated cluster. Administrators can select between **Network Management** or **Read-only** access options.

Prerequisites

- An AWS account with IAM permissions.

Procedure

1. Log in to your AWS account. If necessary, you can create a new AWS account by following the AWS documentation.

2. Create an IAM user with **STS:AllowAssumeRole** permissions within the AWS account.

a. Open the IAM dashboard of the AWS Management Console.

b. In the **Policies** section, click **Create Policy**.

c. Select the **JSON** tab and replace the existing text with the following:

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

d. Click **Next:Tags**.

e. Optional: Add tags. Click **Next:Review**

f. Provide an appropriate name and description, then click **Create Policy**.

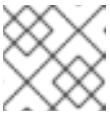
g. In the **Users** section, click **Add user**.

h. Provide an appropriate user name.

i. Select **AWS Management Console access** as the AWS access type.

j. Adjust the password requirements as necessary for your organization, then click **Next:Permissions**.

k. Click the **Attach existing policies directly** option. Search for and check the policy created in previous steps.



NOTE

It is not recommended to set a permissions boundary.

l. Click **Next: Tags**, then click **Next: Review**. Confirm the configuration is correct.

m. Click **Create user**, a success page appears.

n. Gather the IAM user's Amazon Resource Name (ARN). The ARN will have the following format: **arn:aws:iam::000111222333:user/username**. Click **Close**.

3. Open the OpenShift Cluster Manager (OCM) in your browser and select the cluster you want to allow AWS infrastructure access.

4. Select the **Access control** tab, and scroll to the **AWS Infrastructure Access** section.

5. Paste the **AWS IAM ARN** and select **Network Management** or **Read-only** permissions, then click **Grant role**.

6. Copy the **AWS OSD console URL** to your clipboard.

7. Sign in to your AWS account with your Account ID or alias, IAM user name, and password.
8. In a new browser tab, paste the AWS OSD Console URL that will be used to route to the AWS Switch Role page.
9. Your account number and role will be filled in already. Choose a display name if necessary, then click **Switch Role**.

Verification

- You now see **VPC** under **Recently visited services**.

1.3. CONFIGURING AWS VPC PEERING

A Virtual Private Cloud (VPC) peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. You can configure an Amazon Web Services (AWS) VPC containing an OpenShift Dedicated cluster to peer with another AWS VPC network.

WARNING

Private clusters cannot be fully deleted by the OpenShift Cluster Manager (OCM) if the VPC the cluster is installed in is peered.

AWS supports inter-region VPC peering between all commercial regions excluding China.

Prerequisites

- Gather the following information about the Customer VPC that is required to initiate the peering request:
  - Customer AWS account number
  - Customer VPC ID
  - Customer VPC Region
  - Customer VPC CIDR
- Check the CIDR block used by the OpenShift Dedicated Cluster VPC. If it overlaps or matches the CIDR block for the Customer VPC, then peering between these two VPCs is not possible; see the Amazon VPC Unsupported VPC peering configurations documentation for details. If the CIDR blocks do not overlap, you can proceed with the procedure.

Procedure

1. Initiate the VPC peering request.
2. Accept the VPC peering request.

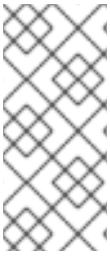
3. Update your Route tables for the VPC peering connection .

Additional resources

- For more information and troubleshooting help, see the AWS VPC guide.

1.4. CONFIGURING AN AWS VPN

You can configure an Amazon Web Services (AWS) OpenShift Dedicated cluster to use a customer's on-site hardware Virtual Private Network (VPN) device. By default, instances that you launch into an AWS Virtual Private Cloud (VPC) cannot communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN connection, and configuring routing to pass traffic through the connection.



NOTE

AWS VPN does not currently provide a managed option to apply NAT to VPN traffic. See the AWS Knowledge Center for more details.

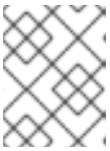
Routing all traffic, for example **0.0.0.0/0**, through a private connection is not supported. This requires deleting the internet gateway, which disables SRE management traffic.

Prerequisites

- Hardware VPN gateway device model and software version, for example Cisco ASA running version 8.3. See the AWS documentation to confirm whether your gateway device is supported by AWS.
- Public, static IP address for the VPN gateway device.
- BGP or static routing: if BGP, the ASN is required. If static routing, you must configure at least one static route.
- Optional: IP and port/protocol of a reachable service to test the VPN connection.

Procedure

1. Create a customer gateway to configure the VPN connection.
2. If you do not already have a Virtual Private Gateway attached to the intended VPC, create and attach a Virtual Private Gateway.
3. Configure routing and enable VPN route propagation .
4. Update your security group .
5. Establish the Site-to-Site VPN connection .



NOTE

Note the VPC subnet information, which you must add to your configuration as the remote network.

Additional resources

- For more information and troubleshooting help, see the AWS VPN guide.

1.5. CONFIGURING AWS DIRECT CONNECT

Amazon Web Services (AWS) Direct Connect requires a hosted Virtual Interface (VIF) connected to a Direct Connect Gateway (DXGateway), which is in turn associated to a Virtual Gateway (VGW) or a Transit Gateway in order to access a remote Virtual Private Cloud (VPC) in the same or another account.

If you do not have an existing DXGateway, the typical process involves creating the hosted VIF, with the DXGateway and VGW being created in your AWS account.

If you have an existing DXGateway connected to one or more existing VGWs, the process involves your AWS account sending an Association Proposal to the DXGateway owner. The DXGateway owner must ensure that the proposed CIDR will not conflict with any other VGWs they have associated.

Prerequisites

- Confirm the CIDR range of the OpenShift Dedicated VPC will not conflict with any other VGWs you have associated.
- Gather the following information:
  - The Direct Connect Gateway ID.
  - The AWS Account ID associated with the virtual interface.
  - The BGP ASN assigned for the DXGateway. Optional: the Amazon default ASN may also be used.

Procedure

1. Create a VIF or view your existing VIFs to determine the type of direct connection you need to create.
2. Create your gateway.
   a. If the Direct Connect VIF type is **Private**, create a virtual private gateway.
   b. If the Direct Connect VIF is **Public**, create a Direct Connect gateway.
3. If you have an existing gateway you want to use, create an association proposal and send the proposal to the DXGateway owner for approval.

WARNING

When connecting to an existing DXGateway, you are responsible for the costs.

Additional resources

- For more information and troubleshooting help, see the AWS Direct Connect guide.

CHAPTER 2. CONFIGURING A PRIVATE CLUSTER

An OpenShift Dedicated cluster can be made private so that internal applications can be hosted inside a corporate network. In addition, private clusters can be configured to have only internal API endpoints for increased security.

OpenShift Dedicated administrators can choose between public and private cluster configuration from within the **OpenShift Cluster Manager** (OCM). Privacy settings can be configured during cluster creation or after a cluster is established.

2.1. ENABLING A PRIVATE CLUSTER DURING CLUSTER CREATION

You can enable private cluster settings when creating a new cluster.

Prerequisites

- The following private connections must be configured to allow private access:
  - VPC Peering
  - Cloud VPN
  - DirectConnect (AWS only)
  - TransitGateway (AWS only)
  - Cloud Interconnect (GCP only)

Procedure

1. Log in to OpenShift Cluster Manager (OCM).
2. Click **Create cluster → OpenShift Dedicated → Create cluster**.
3. Configure your cluster details.
4. When selecting your preferred network configuration, select **Advanced**.
5. Select **Private**.

WARNING

When set to **Private**, you cannot access your cluster unless you have configured the private connections in your cloud provider as outlined in the prerequisites.

6. Click **Create cluster**. The cluster creation process begins and takes about 30-40 minutes to complete.

Verification

- The **Installing cluster** heading, under the **Overview** tab, indicates that the cluster is installing and you can view the installation logs from this heading. The **Status** indicator under the **Details** heading indicates when your cluster is **Ready** for use.

2.2. ENABLING AN EXISTING CLUSTER TO BE PRIVATE

After a cluster has been created, you can later enable the cluster to be private.

Prerequisites

- The following private connections must be configured to allow private access:
  - VPC Peering
  - Cloud VPN
  - DirectConnect (AWS only)
  - TransitGateway (AWS only)
  - Cloud Interconnect (GCP only)

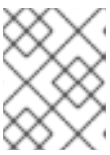
Procedure

1. Log in to OpenShift Cluster Manager (OCM).
2. Select the public cluster you would like to make private.
3. On the **Networking** tab, select **Make API private** under **Control Plane API endpoint**

WARNING

When set to **Private**, you cannot access your cluster unless you have configured the private connections in your cloud provider as outlined in the prerequisites.

4. Click **Change settings**.



NOTE

Transitioning your cluster between private and public can take several minutes to complete.

2.3. ENABLING AN EXISTING PRIVATE CLUSTER TO BE PUBLIC

After a private cluster has been created, you can later enable the cluster to be public.

Procedure

1. Log in to OpenShift Cluster Manager (OCM).
2. Select the private cluster you would like to make public.
3. On the **Networking** tab, deselect **Make API private** under **Control Plane API endpoint**
4. Click **Change settings**.

NOTE

Transitioning your cluster between private and public can take several minutes to complete.