

Create a VPC

This module describes how to create a Virtual Private Cloud (VPC).

- Create a VPC, on page 1

Create a VPC

As an XRd-specific requirement, the data traffic flowing through the XRd instance must be separated from the cluster control-plane traffic. The separation is achieved by using different Virtual Private Cloud (VPC) subnets for the control-plane and data-plane traffic.

Amazon provides a simple CloudFormation template to create a VPC that has two public subnets and two private subnets. An internet gateway is used to give the public subnets full access to the internet, and the private subnets are shielded through a NAT gateway.

Note This template brings up a VPC with access to the internet. If you want to shield the VPC from the internet, you can create a VPC without an internet gateway. In that case, ensure that all the additional requirements described in the AWS documentation on Private Clusters is met.

If you want to diverge from this example configuration, refer to the AWS documentation and ensure that your VPC is correctly set up for an EKS cluster.

You can create a VPC by running the following CLI commands:

```
aws cloudformation create-stack \
  --stack-name xrd-eks-vpc-stack \
  --template-url
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml
 \
  --parameters \
    ParameterKey=VpcBlock,ParameterValue=10.0.0.0/16 \
    ParameterKey=PublicSubnet01Block,ParameterValue=10.0.50.0/24 \
    ParameterKey=PublicSubnet02Block,ParameterValue=10.0.51.0/24 \
    ParameterKey=PrivateSubnet01Block,ParameterValue=10.0.0.0/24 \
    ParameterKey=PrivateSubnet02Block,ParameterValue=10.0.1.0/24
```

This command returns quickly, but the process continues in the background. If you want to wait until the completion of VPC creation, use the following command:

```
aws cloudformation wait stack-create-complete \
  --stack-name xrd-eks-vpc-stack
```

VPC is created with a VPC block (`10.0.0.0/16`), two public subnets (`10.0.50.0/24, 10.0.51.0/24`), and two private subnets (`10.0.0.0/24, 10.0.1.0/24`).

Once the VPC creation is completed, you can run the following command to get the output details.

```
aws cloudformation describe-stacks \
  --stack-name xrd-eks-vpc-stack \
  --query "Stacks[0].Outputs"
```

Make a note of the VPC ID `<vpc-id>` and private subnet IDs `<private-subnet-1>, <private-subnet-2>`, as you may require them when you create cluster and nodes.

Create a Security Group

You must create a security group in the VPC for EKS Control Plane traffic.

To create a security group that allows communication between the worker nodes and the cluster, use the following command:

```
aws ec2 create-security-group --group-name "xrd-eks-cp-comms" \
  --description "Control plane communication for the XRd EKS Cluster" \
  --vpc-id <vpc-id>
```

Make a note of the output group ID `<sg_id>`.

When a security group is created, Amazon EC2 creates a default egress rule that allows egress traffic. Since ingress rules aren't added by default, all incoming traffic is dropped. So, you must add an ingress rule to allow all traffic within the security group. For example,

```
aws ec2 authorize-security-group-ingress \
  --group-id <sg-id> \
  --source-group <sg-id> \
  --protocol all
```