Terraform - Cloud Q on AWS

Deploying in a VPC on AWS with no Internet Access

Dack Busch/Gokul Kuppuraj, Feb 20th, 2022

Overview

The Terraform provided expects a NAT Gateway in the existing VPC chosen. However, it is possible to deploy without internet access.

To support deployments without public internet connectivity the VPC must be configured with:

- VPC Interface Endpoints to support AWS services
- A security group applied to each VPC Interface Endpoint
- A Gateway VPC Endpoint for S3 access
- If software upgrades are to be performed by the provisioning instance, then Qumulo Core software images must be placed in the /upgrade folder within the Terraform project in the Qumulo Trends file naming convention.

VPC Interface Endpoints

It is recommended to leave the policy for each endpoint as Full Access. The following VPC Interface Endpoints must be configured when deploying without internet Access:

Endpoint Interface Service	Required for Production	Deployment/Stack Update
cloudformation		✅
ec2	✅	✅
events	✅	✅
kms	✅	✅
lambda	✅	✅
logs	✅	✅
monitoring	✅	✅
profile	✅	✅
S3 (gateway endpoint)	✅	✅
secretsmanager		✅
Sns (if using notifications)	✅	✅
ssm		✅
sts	✅	✅

VPC Interface Endpoints Security Group rules

To allow traffic from the provisioning node and the Qumulo cluster the security group applied to the VPC interface endpoints must have the following Security Groups added as Inbound Rule Sources:

- [deployment_unique_name]-**provisioner-security-group**
- [deployment_unique_name]-**qumulo-security-group**

Automated Qumulo Core upgrades during deployment

If you enter a newer software version than the Qumulo Core AMI was released with, the provisioning instance will expect to find the code via the internet, or in this case from the S3 bucket and prefix specified in .tfvars. All quarterly released images between the AMI ID release version to, and including, the requested version must be present in the bucket. For example, if the AMI was released with 4.0.6 and the desired version is 4.2.3, then 4.1.0.1, 4.2.0, and 4.2.3 versions must be in the bucket. To see the quarterly release cadence just cat the file:

<project path>/modules/qprovisioner/functions/upgrade-order.txt.

The image(s) must be in the Qumulo Trends format: **qumulo_upgrade_cloud_x.y.z.qimg**. If you have downloaded Qumulo Cloud .img files from Box.com just rename them to the Qumulo Trends format. Place the image(s) in the Terraform project at:

<project path>/modules/qprovisioner/upgrade/

Terraform will copy these files to the bucket/prefix specified in .tfvars on the next apply.

If the software images are not present in the S3 bucket the Provisioning instance will not shutdown, nor will it progress with provisioning activities. Once the images are available the provisioning instance will pick up where it left off on a subsequent Terraform apply.