Qumulo

Deploying Qumulo Clusters Using the AWS-SA-WAF-CLUSTER CloudFormation Template

Dack Busch

June 22, 2021

Table of Contents

Intended Audience

This document is intended for anyone using the AWS Qumulo Solution Architect (SA) Well Architected Framework (WAF) Cluster CloudFormation templates. These templates and associated files are referred to simply as the aws-sa-waf-cluster. This document is comprehensive and experienced AWS users may find it repetitive or obvious. Less experienced users will benefit from the detailed documentation. Leverage the Table of Contents to jump to the area of interest.

Overview

This guide provides instructions for deploying the aws-sa-waf-cluster set of templates in AWS to fully provision the infrastructure for a Qumulo cluster. Any subsequent configuration for the file data platform is outside the scope of this document. Refer to the Qumulo Knowledge Base for further information.

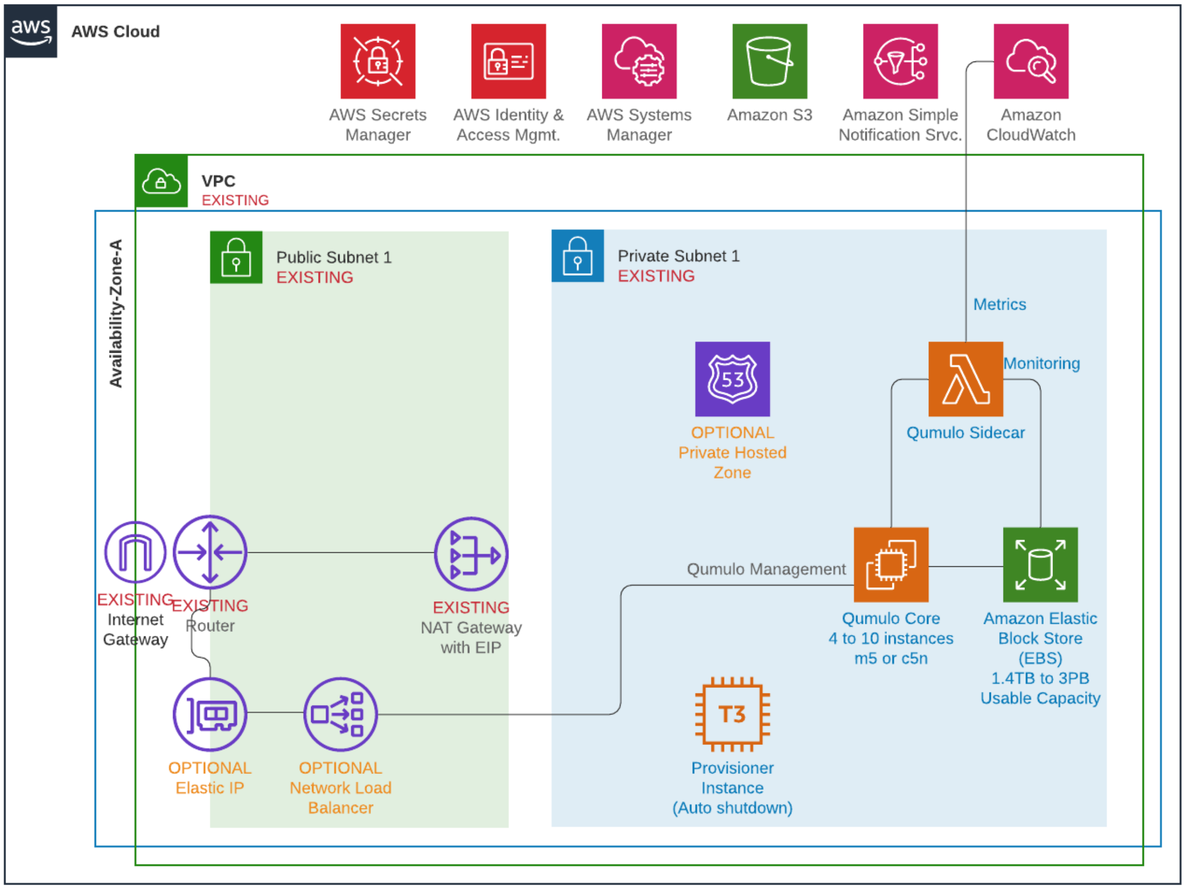
Software Licences

Prior to executing any of the aws-sa-waf-cluster templates a Qumulo AMI subscription must be accepted in the AWS Marketplace for a chosen AWS account. The templates documented here are much more comprehensive than those available by default in the AWS Marketplace, so don’t deploy from the AWS Marketplace. Simply accept the offer for the AMI of interest and close the AWS Marketplace session.

Architecture

Deploying the aws-sa-waf-cluster templates will instantiate the following infrastructure in AWS.

Qumulo WAF Deployment in an Existing VPC - Limited by Cloud Formation Template to 1TB-3PB of Capacity



As shown in Figure 1, the CloudFormation template expects the following:

- A VPC configured with a private subnet, public subnet, NAT gateway, and Internet Gateway
    - This basic infrastructure and the associated route tables are required to provide the automation infrastructure and cluster Internet connectivity.

As shown in Figure 1, the CloudFormation template sets up the following:

- A cluster of Qumulo EC2 instances
    - 4 to 10 nodes
    - 1TB to 3PB of usable capacity
- Multiple AWS Elastic Block Store (EBS) volumes connected to the Qumulo cluster
    - EBS Volume configurations (ie Disk Configs) vary depending on AMI ID
    - All flash (SSD) and Hybrid (SSD+HDD) Disk Configs are available
- The Qumulo Sidecar which consists of two Lambda functions
    - One Lambda function sends metrics for the cluster to Cloudwatch
    - The other Lambda function monitors the health of EBS volumes and automatically replaces any unhealthy volumes
- (Optional) AWS Route 53 private hosted zone
    - If R53 is resolving all DNS for the VPC then a R53 private hosted zone may be optionally provisioned to configure DNS A-records for the cluster.
- (Optional) Public IP Management
    - If desired a Network Load Balancer with an Elastic IP (public static) may also be configured
    - Note, this NLB listens only on port 443 and has some inherent DoS capabilities.
    - As a best practice the cluster should be managed long-term via a secure host in the public or private subnet.
    - This functionality is only intended for initial configuration inspection and validation in the event no other EC2 machines exist in the VPC to manage the cluster
- Provisioner
    - An EC2 instance configures multiple parameters on the Qumulo cluster and within the AWS infrastructure
    - This instance automatically shuts down after successful provisioning
    - It is also restarted during stack updates to provision modifications to the infrastructure

Planning the Deployment

Specialized Knowledge

Deploying this template requires only a moderate level of familiarity with AWS services. If you're new to AWS, see https://aws.amazon.com/getting-started/.

AWS Account

Deployment of this template requires an AWS account. If you don't have an account visit https://aws.amazon.com.

Technical Requirements

Before you launch the template, review the following information and requirements and ensure that your account and privileges are properly configured. Otherwise the deployment may fail.

Resource Quotas

Review current quota utilization and ensure that resources are available for the resources required for this deployment.

Resource	This Deployment Uses
Elastic IP (optional for Public Management)	1
Security Groups	2
AWS IAM roles	4
m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.16xlarge, c5n.9xlarge, or c5n.18xlarge	4 to 10 of the chosen instance type and associated vCPUs
Lambda functions	2
EBS TiB (gp2, st1, or sc1)	Chosen Disk Config TiB x # of EC2 instances

Supported Regions

Review current quota utilization and ensure that resources are available for the resources required for this deployment.

Americas

- us-east-1, US East (N. Virginia)
- us-east-2, US East (Ohio)
- us-west-1, US West (N. California)
- us-west-2, US West (Oregon)
- us-gov-west-1
- us-gov-east-1
- ca-central-1, Canada (Central)
- sa-east-1, South America (São Paulo)

Asia Pacific

- ap-northeast-1, Asia Pacific (Tokyo)
- ap-northeast-2, Asia Pacific (Seoul)
- ap-south-1, Asia Pacific (Mumbai)
- ap-southeast-1, Asia Pacific (Singapore)
- ap-southeast-2, Asia Pacific (Sydney)
- ap-east-1, Asia Pacific (Hong Kong)

Europe/Middle East/Africa

- eu-central-1, Europe (Frankfurt)
- eu-west-1, Europe (Ireland)
- eu-west-2, Europe (London)
- eu-west-3, Europe (Paris)
- eu-north-1, Europe (Stockholm)
- eu-south-1, Europe (Milan)
- me-south-1, Middle East (Bahrain)

IAM Permissions

Before launching the template, you must sign in to the AWS Management Console with IAM permissions for the resources that the template deploys and the services it leverages. The ***AdministratorAccess*** managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions. The following AWS services are required in a custom IAM role or IAM user to deploy this template:

application-autoscaling:*
applicationinsights:*
autoscaling:*
cloudformation:*
cloudtrail:*
cloudwatch:*
compute-optimizer:*
ec2:*
elasticloadbalancing:*
events:*
health:*
iam:*
kms:*
lambda:*
logs:*
resource-groups:*
route53:*
s3:*
secretsmanager:*
sns:*
ssm:*
sqs:*
tag:*

Deployment Options

This template deploys into an existing VPC. There are optional parameters which are denoted in the template with OPTIONAL:

1. AWS Local Zone deployment
2. Public IP Management
3. R53 Private Hosted Zone configuration
4. Customer Managed Key configuration
5. SNS Notifications
6. CloudWatch audit log configuration

Deployment Steps

Download the aws-sa-waf-cluster CloudFormation Folder

1. Go to https://github.com/Qumulo/aws-sa-waf-cluster and select the green **Code** button and then click on **Download Zip**.
2. Unzip the file on your local machine
3. Copy the top level folder and all contents, unmodified, to an AWS S3 bucket that your account has access to. Numerous tools exist to place this content in your S3 bucket like

the AWS S3 Console, AWS CLI commands, or custom S3 browser utilities. All that is critical is that all files are copied and the directory hierarchy is maintained.

Sign in to your AWS account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user role that has the necessary permissions. For details, see Planning the Deployment earlier in this document.
2. Make sure that your AWS account is configured correctly, as discussed in the Technical Requirements section earlier in this document.

Subscribe to the Qumulo Marketplace AMI

A subscription to the Qumulo AMI for the chosen configuration and deployment region is required.

1. Go to https://aws.amazon.com/marketplace and type **Qumulo** in the search bar. Select one of the available offerings with a designated usable capacity. NOTE: If you have a private offer you will receive an email with a link to accept the private offer. The **Customizable File Storage Node** configuration in the Marketplace requires a private offer.
2. Scroll down to **Usage Information** and note the type and number of EBS volumes per EC2 instance. If you've chosen a Hybrid Configuration (SSD+HDD), just note the type and number of st1 or sc1 EBS volumes per EC2 instance. As an example, the 1TB usable offering has 6x100GiB gp2 EBS volumes per EC2 instance. This would be referred to as a 600GiB All Flash EBS volume configuration later in the template. Had the 12TB usable hybrid configuration been chosen, 10x500GiB st1 EBS volumes per EC2 instance would be provisioned. This would be referenced as a 5TiB Hybrid-st1 EBS volume configuration later in the template. NOTE: If you have a private offer using the Customizable File Storage Node offering your Qumulo representative will let you know the appropriate disk configuration for your offering.
3. Click **Continue to Subscribe** in the upper right corner. The subscription will take a couple of minutes to process.
4. At this point the Marketplace process is complete when using the aws-sa-waf-cluster CloudFormation template.

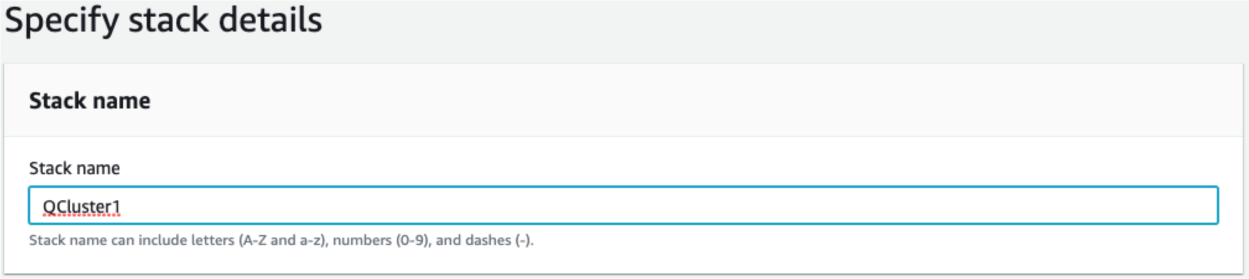
Launch the CloudFormation Template

1. Go to the **CloudFormation** view in the AWS Console
2. Select the AWS Region to deploy the Qumulo Cluster in from the upper-right corner of the AWS Console. NOTE: Later in the Template the AMI-ID will be required that matches the configuration for your selected region.
3. Duplicate the browser tab and switch to the **S3** view in the AWS Console
4. Navigate to the bucket you placed the aws-sa-waf-cluster folder in
5. Select the **aws-sa-waf-cluster** folder
6. Click on the template **qcluster-existingVPC.cft.yaml**
7. Copy the **Object URL** for the template (NOT the S3 URL)
8. Switch back to the CloudFormation browser tab
9. Click **Create Stack** and select **With new resources**
10. Keep the defaults and paste the template URL into the **Amazon S3 URL** field
11. Click **Next**
12. The template is now launched and you will see the list of parameters on the **Specify Stack Details** page

Entering Parameters in the Template

The template parameters are largely self documenting with intuitive names and detailed descriptions. However, this template does a lot of work, so some additional explanation is warranted. All sections of the template will be captured below and additional information provided for the parameters.

Stack Name Parameter



Specify stack details

Stack name

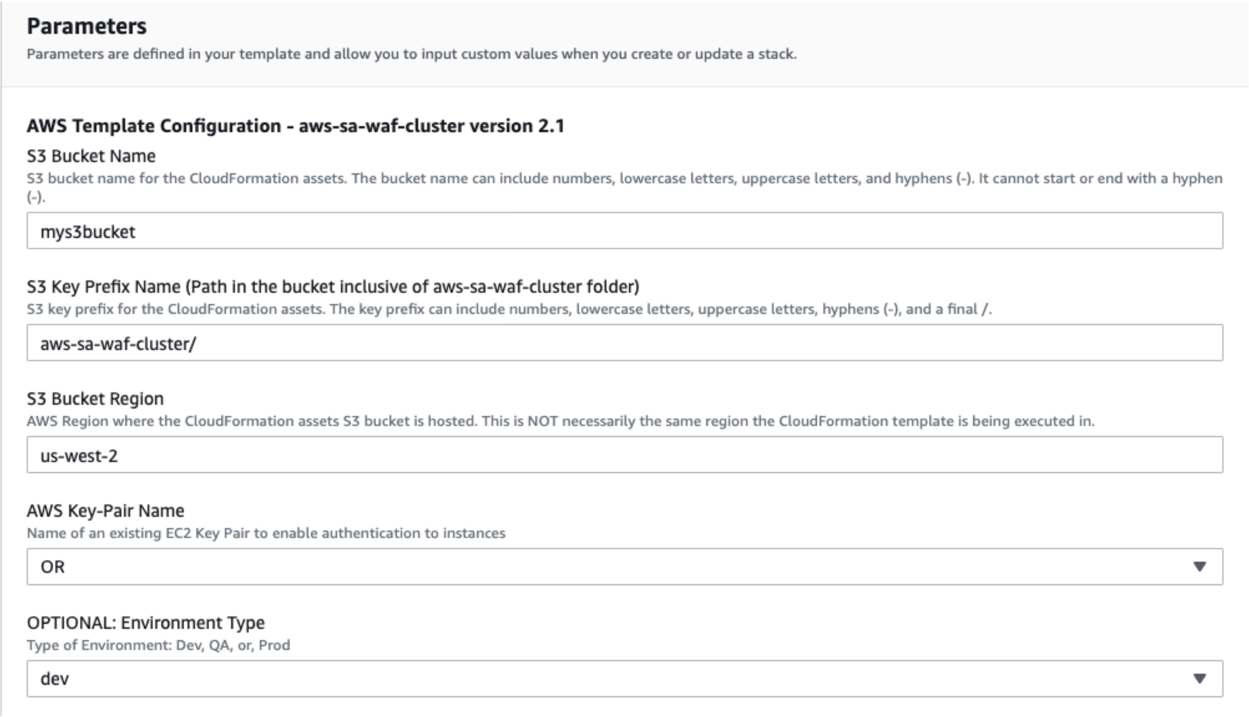
Stack name: QCluster1

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

While stack names can be fairly complex, this template extensively tags resources with the stack name, nested stack name, and unique stack numbers generated by AWS. Thus, less is more for the stack name. In this example **QCluster1** will suffice.

AWS Template Configuration Parameters

This section consists of basic AWS parameters. Since this is the beginning of the parameters for the template, the aws-sa-waf-cluster template version number is also referenced here.



Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

AWS Template Configuration - aws-sa-waf-cluster version 2.1

S3 Bucket Name

S3 bucket name for the CloudFormation assets. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).

mys3bucket

S3 Key Prefix Name (Path in the bucket inclusive of aws-sa-waf-cluster folder)

S3 key prefix for the CloudFormation assets. The key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and a final /.

aws-sa-waf-cluster/

S3 Bucket Region

AWS Region where the CloudFormation assets S3 bucket is hosted. This is NOT necessarily the same region the CloudFormation template is being executed in.

us-west-2

AWS Key-Pair Name

Name of an existing EC2 Key Pair to enable authentication to instances

OR ▼

OPTIONAL: Environment Type

Type of Environment: Dev, QA, or, Prod

dev ▼

S3 Bucket Name

This is simply the name of the S3 Bucket the aws-sa-waf-cluster folder was placed in. Note, the account you use to provision the cluster must have access to this bucket. Also, you may be wondering why does the template need to know the bucket and prefix for this template when it was just launched with the URL? This template uses nested stacks. The top-level stack uses the bucket and prefix supplied to generate URLs for the nested stacks.

S3 Key Prefix Name

For those new to AWS, this parameter is simply the path in the bucket inclusive of the aws-sa-waf-cluster folder. It must NOT start with a “/” and it MUST end with a “/”. This is the AWS S3 Key Prefix Name convention.

S3 Bucket Region

This is the region the S3 bucket is hosted in that contains the aws-sa-waf-cluster folder. In many cases this will NOT be the region the template is being executed in. S3 buckets are hosted in a region and available globally throughout AWS. To identify the region for your S3 bucket simply go to the AWS Console **S3** page, select **Buckets**, and the region will be listed just to the right of the bucket name.

AWS Key-Pair Name

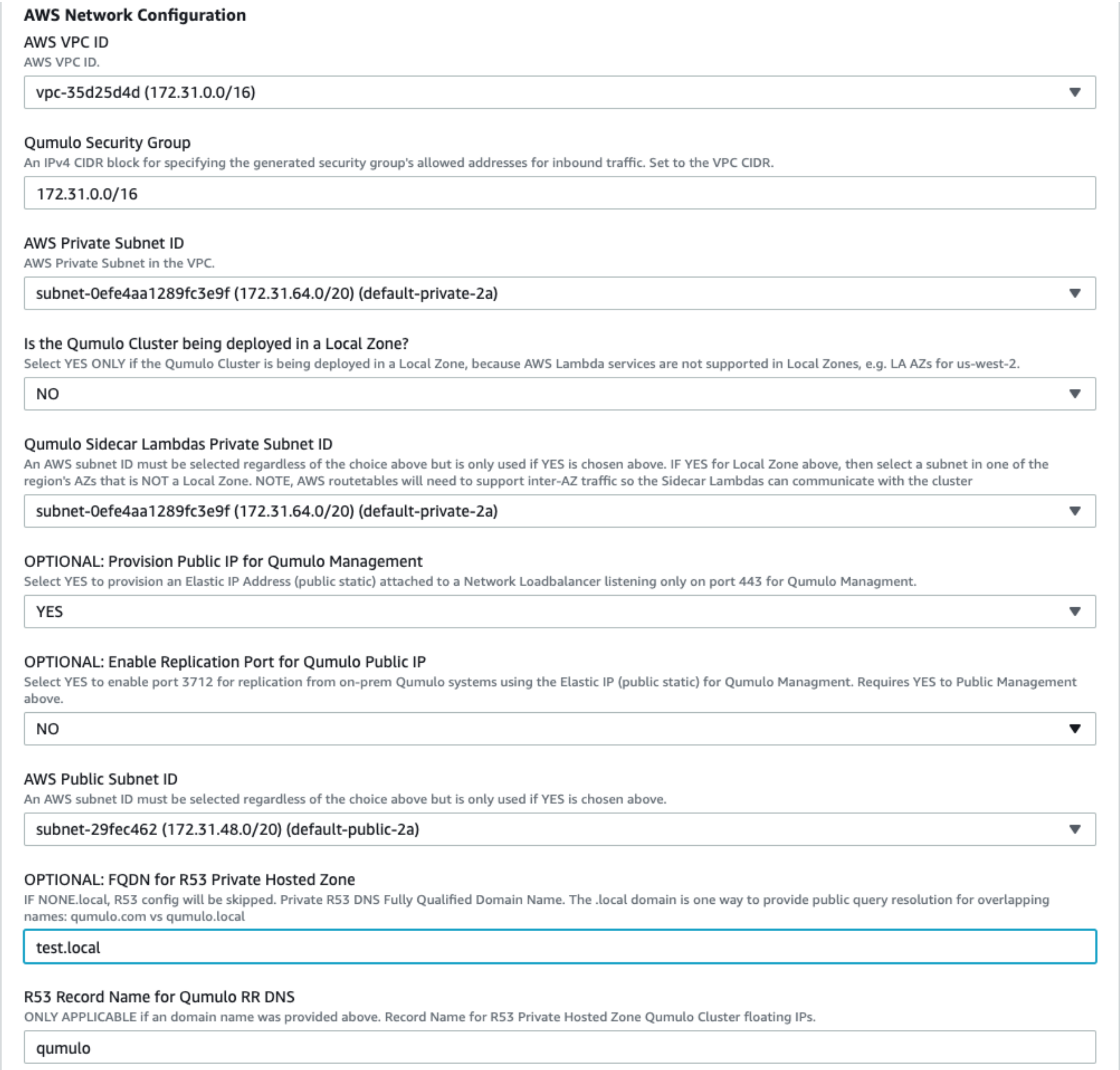
This field is a dynamic drop-down populated with all the key-pairs in the account for the region. Here a simple name of OR was chosen for the Oregon (us-west-2) region. Any parameter field with an arrow on the far right is dynamically populated with options to select. Further, these fields must all be populated with a selection or the template will fail upon execution.

OPTIONAL: Environment Type

This field is reserved for future use. It may be changed, but has no impact.

AWS Network Configuration Parameters

The next section consists of multiple parameters to configure the networking for the cluster and supporting elements.



AWS Network Configuration

AWS VPC ID

AWS VPC ID.

vpc-35d25d4d (172.31.0.0/16) ▼

Qumulo Security Group

An IPv4 CIDR block for specifying the generated security group's allowed addresses for inbound traffic. Set to the VPC CIDR.

172.31.0.0/16

AWS Private Subnet ID

AWS Private Subnet in the VPC.

subnet-0efe4aa1289fc3e9f (172.31.64.0/20) (default-private-2a) ▼

Is the Qumulo Cluster being deployed in a Local Zone?

Select YES ONLY if the Qumulo Cluster is being deployed in a Local Zone, because AWS Lambda services are not supported in Local Zones, e.g. LA AZs for us-west-2.

NO ▼

Qumulo Sidecar Lambdas Private Subnet ID

An AWS subnet ID must be selected regardless of the choice above but is only used if YES is chosen above. IF YES for Local Zone above, then select a subnet in one of the region's AZs that is NOT a Local Zone. NOTE, AWS routetables will need to support inter-AZ traffic so the Sidecar Lambdas can communicate with the cluster

subnet-0efe4aa1289fc3e9f (172.31.64.0/20) (default-private-2a) ▼

OPTIONAL: Provision Public IP for Qumulo Management

Select YES to provision an Elastic IP Address (public static) attached to a Network Loadbalancer listening only on port 443 for Qumulo Managment.

YES ▼

OPTIONAL: Enable Replication Port for Qumulo Public IP

Select YES to enable port 3712 for replication from on-prem Qumulo systems using the Elastic IP (public static) for Qumulo Managment. Requires YES to Public Management above.

NO ▼

AWS Public Subnet ID

An AWS subnet ID must be selected regardless of the choice above but is only used if YES is chosen above.

subnet-29fec462 (172.31.48.0/20) (default-public-2a) ▼

OPTIONAL: FQDN for R53 Private Hosted Zone

IF NONE.local, R53 config will be skipped. Private R53 DNS Fully Qualified Domain Name. The .local domain is one way to provide public query resolution for overlapping names: qumulo.com vs qumulo.local

test.local

R53 Record Name for Qumulo RR DNS

ONLY APPLICABLE if an domain name was provided above. Record Name for R53 Private Hosted Zone Qumulo Cluster floating IPs.

qumulo

AWS VPC ID

This field is a dynamic drop-down populated with all the VPCs in the account for the region. Choose the VPC to deploy in.

Qumulo Security Group

The Qumulo Security Group CIDR generally should match the VPC CIDR. This allows the cluster to communicate with any subnet within the VPC.

AWS Private Subnet ID

The cluster is deployed in a private subnet within the VPC. This field is a dynamic drop-down populated with all the subnets available within the Region. Select the subnet, and hence the Availability Zone (AZ), the cluster resides in. Make sure the subnet chosen is relevant for the VPC chosen. This can sometimes be confusing if the tags don't clarify the VPC the subnet resides in.

Is The Qumulo Cluster Being Deployed in a Local Zone?

Some AZs are AWS Local Zones. These AZs often have a subset of the functionality of the parent AZs in a given AWS Region. An example is the LA Local Zone that is part of the Oregon region with four parent AZs. Since AWS Lambda functions are not yet supported in Local Zones, change this field to **YES** if your cluster is being deployed in a Local Zone.

Qumulo Sidecar Lambda Private Subnet ID

In the event the cluster is being deployed in a Local Zone, choose a subnet to deploy the AWS Lambdas in that is in a parent AZ for the AWS region. Just like any other CloudFormation dynamic drop down, an option must be chosen. In this example the same private subnet ID was selected to make the parser happy. Note, if the Sidecar Lambdas are being deployed in a different private subnet than the cluster, the AWS route tables for the VPC must be configured to provide inter-AZ connectivity.

OPTIONAL: Provision Public IP for Qumulo Management

If this option is selected, an Elastic IP (public static IP) is assigned to an AWS Network Load Balancer that is connected to the cluster and listens only on port 443. This is not recommended for production clusters with sensitive data. To minimize the attack surface area, manage the cluster from an EC2 instance within your VPC. Note, AWS Local Zones do not support NLB target groups, so this option will be ignored if deploying the cluster in a Local Zone.

OPTIONAL: Enable Replication Port for Qumulo Public IP

The replication port can be enabled on the public interface for customers that want to replicate from one Qumulo cluster to another via the public Internet. This is fine for test purposes but should not be used on production clusters. Either a VPN or AWS direct connect should be used for production replication.

AWS Public Subnet ID

This parameter must be populated, even if the public management option is left at the default of **NO**. This is a basic template requirement for the CloudFormation parser even though the field is only used for provisioning in the event public management was selected.

OPTIONAL: FQDN for R53 Private Hosted Zone

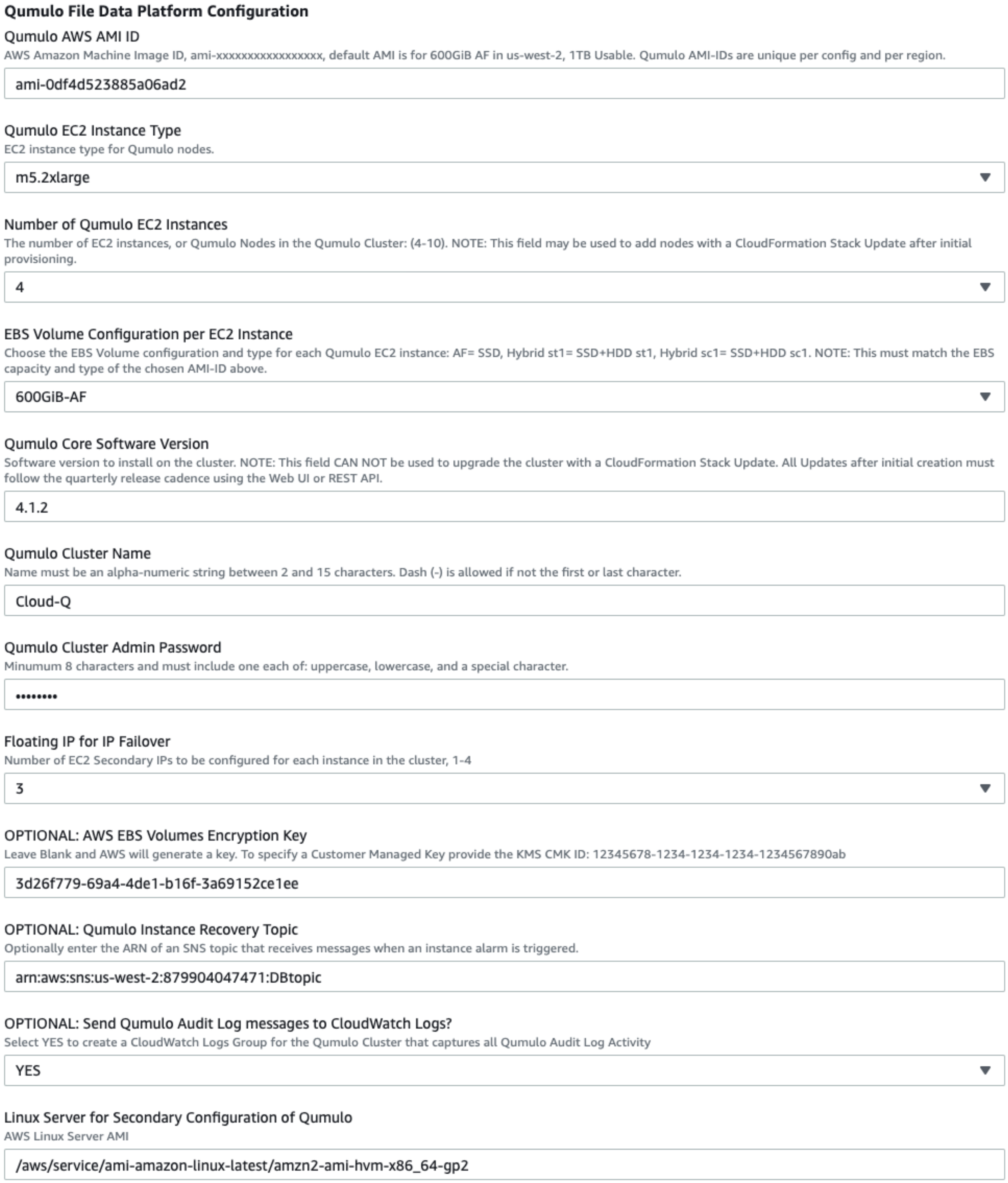
The template will optionally create a Route 53 Private Hosted Zone with equally weighted records, TTL=0, for the floating IPs on the cluster. If left at the default of **NONE.local** this option will be ignored. Here an FQDN of **test.local** was chosen since this VPC has no Active Directory server with DNS. (INSERT LINK TO SA KB on DNS IN AWS).

R53 Record Name for Qumulo RR DNS

This field is the DNS A-Record name for the Route 53 records that are created. This is only relevant if an FQDN was entered above other than **NONE.local**.

Qumulo File Data Platform Configuration Parameters

This section configures all the parameters that are specific to the Qumulo Cluster.



Qumulo File Data Platform Configuration

Qumulo AWS AMI ID
AWS Amazon Machine Image ID, ami-xxxxxxxxxxxxxxxxx, default AMI is for 600GiB AF in us-west-2, 1TB Usable. Qumulo AMI-IDs are unique per config and per region.

ami-0df4d523885a06ad2

Qumulo EC2 Instance Type
EC2 instance type for Qumulo nodes.

m5.2xlarge ▼

Number of Qumulo EC2 Instances
The number of EC2 instances, or Qumulo Nodes in the Qumulo Cluster: (4-10). NOTE: This field may be used to add nodes with a CloudFormation Stack Update after initial provisioning.

4 ▼

EBS Volume Configuration per EC2 Instance
Choose the EBS Volume configuration and type for each Qumulo EC2 instance: AF= SSD, Hybrid st1= SSD+HDD st1, Hybrid sc1= SSD+HDD sc1. NOTE: This must match the EBS capacity and type of the chosen AMI-ID above.

600GiB-AF ▼

Qumulo Core Software Version
Software version to install on the cluster. NOTE: This field CAN NOT be used to upgrade the cluster with a CloudFormation Stack Update. All Updates after initial creation must follow the quarterly release cadence using the Web UI or REST API.

4.1.2

Qumulo Cluster Name
Name must be an alpha-numeric string between 2 and 15 characters. Dash (-) is allowed if not the first or last character.

Cloud-Q

Qumulo Cluster Admin Password
Minumum 8 characters and must include one each of: uppercase, lowercase, and a special character.

••••••••

Floating IP for IP Failover
Number of EC2 Secondary IPs to be configured for each instance in the cluster, 1-4

3 ▼

OPTIONAL: AWS EBS Volumes Encryption Key
Leave Blank and AWS will generate a key. To specify a Customer Managed Key provide the KMS CMK ID: 12345678-1234-1234-1234-1234567890ab

3d26f779-69a4-4de1-b16f-3a69152ce1ee

OPTIONAL: Qumulo Instance Recovery Topic
Optionally enter the ARN of an SNS topic that receives messages when an instance alarm is triggered.

arn:aws:sns:us-west-2:879904047471:DBtopic

OPTIONAL: Send Qumulo Audit Log messages to CloudWatch Logs?
Select YES to create a CloudWatch Logs Group for the Qumulo Cluster that captures all Qumulo Audit Log Activity

YES ▼

Linux Server for Secondary Configuration of Qumulo
AWS Linux Server AMI

/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

Qumulo AWS AMI ID

The AMI ID is unique to the capacity configuration of the Qumulo node and the AWS region it is deployed in. Contact Qumulo for an AMI ID or accept the private offer emailed to you from Qumulo and we will provide the appropriate AMI ID.

Qumulo EC2 Instance Type

This field is a dynamic drop-down populated with the supported EC2 instance types. For low performance clusters an m5.2xlarge instance type may be selected. For very high performance clusters a c5n.18xlarge instance type may be used. If you don't know what instance type will support your workload contact Qumulo for recommendations.

Number of Qumulo EC2 Instances

This is another dynamic drop-down providing options from 4 to 10 instances. Capacity and performance scale with instance count. Most cloud based workloads can be facilitated with 10 or less nodes. If you need more than 10 nodes contact Qumulo. Note, this field can be used to increase the node count in a subsequent Stack Update.

EBS Volume Configuration per EC2 Instance

This is the disk configuration per EC2 Instance. All supported Qumulo disk configurations are available in this dynamic drop-down. However, only the disk configuration relevant for the AMI ID can be used. Recall in the Marketplace Subscription acceptance the type and number of EBS volumes was noted so you can easily select the correct configuration here. For private offers Qumulo will provide the disk configuration.

Qumulo Core Software Version

Qumulo releases AWS AMI IDs quarterly. Any AMI ID referenced above will have a specific version based on the quarter the subscription was accepted. As of the date of this document Qumulo Core 4.0.6 is the latest version. As Qumulo software continues to evolve you may enter any newer software version than that of the AMI ID when provisioning new clusters. The template will update all nodes to the desired software version before forming the first quorum for the cluster. Note, this field can't be used in a Stack Update to change the software version. Nor can it be used to install a version of software that is older than the version the AMI ID shipped with. For post deployment software upgrades refer to Qumulo KB Qumulo Core Upgrades via UI.

Qumulo Cluster Name

This parameter is simply the name given to the cluster. If you have multiple clusters in an AWS region, give them unique names.

Qumulo Cluster Admin Password

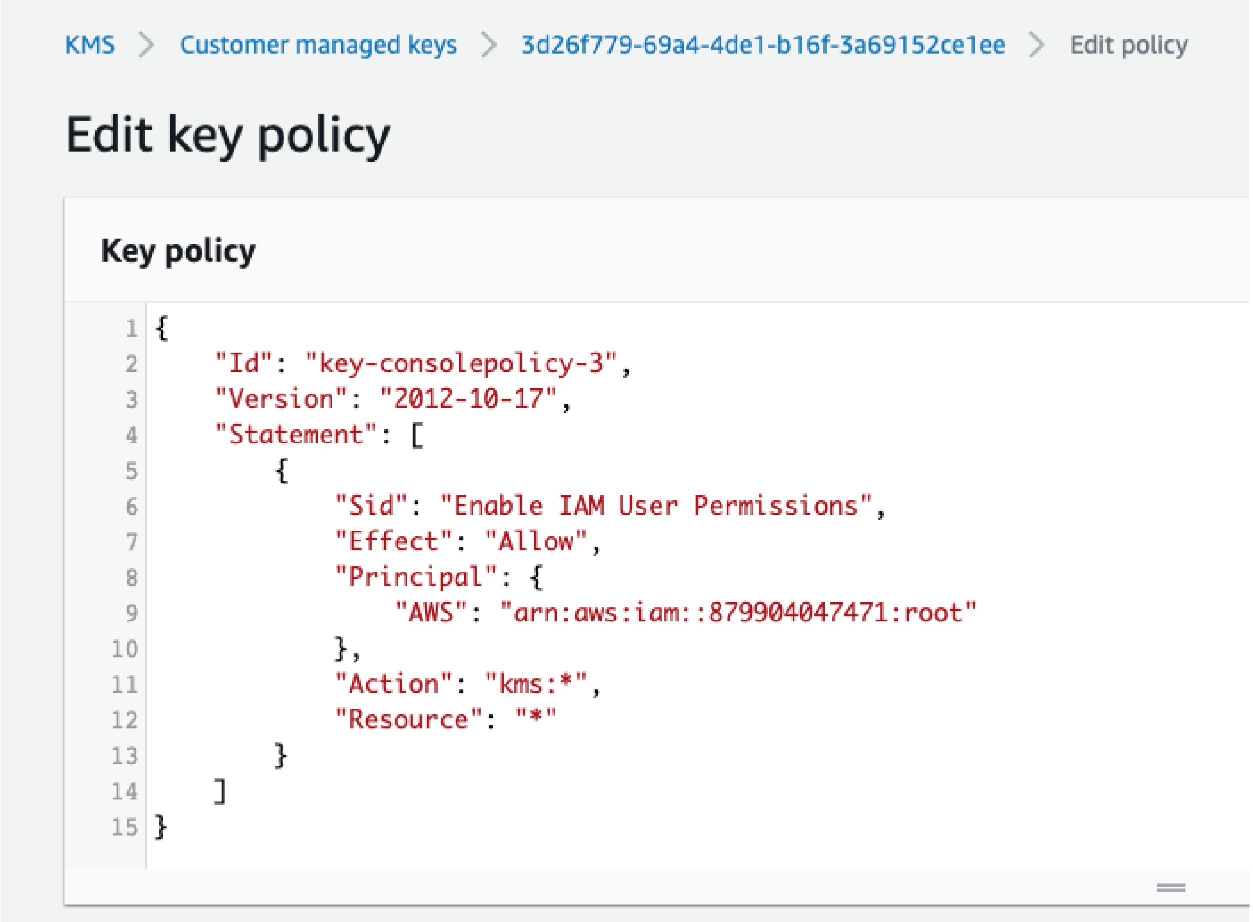
This parameter is the Admin Password assigned to the cluster. This password is also stored in AWS Secrets Manager for subsequent reference.

Floating IP for IP Failover

EC2 Instances running Qumulo Core support EC2 Secondary IP configuration. Within the Qumulo cluster these are referred to as Floating IPs. The cluster takes over ownership and management of these IPs to protect client connections in the event of an EC2 instance failure. By default three floating IPs per instance are recommended. Should any instance fail its load will be distributed to three adjacent instances in the cluster. Options for 1-4 floating IPs per instance are available. These IP addresses are configured in a Route 53 Private Hosted Zone if that option was selected in the previous section of the template. Otherwise, A-records must be set up in the chosen DNS server.

OPTIONAL: AWS EBS Volumes Encryption Key

All data at rest is encrypted. IF this field is left blank an AWS generated key is used. You may optionally specify a Customer Managed Key that has been setup in the AWS Key Management System as shown in the above example. Note, the Key Management System CMK policy for the key must not contain any leftover SIDs from previous provisioning. Assuming there are no other legitimate SIDs in the policy, a clean CMK policy should follow the following JSON structure below.



KMS > Customer managed keys > 3d26f779-69a4-4de1-b16f-3a69152ce1ee > Edit policy

Edit key policy

Key policy

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::879904047471:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

OPTIONAL: Qumulo Instance Recovery Topic

In the event of an EC2 Instance failure, Amazon Simple Notification Service (SNS) text or email messages will be sent via the configured SNS topic. Paste in your SNS topic ARN here.

OPTIONAL: Send Qumulo Audit Log Messages to CloudWatch Logs?

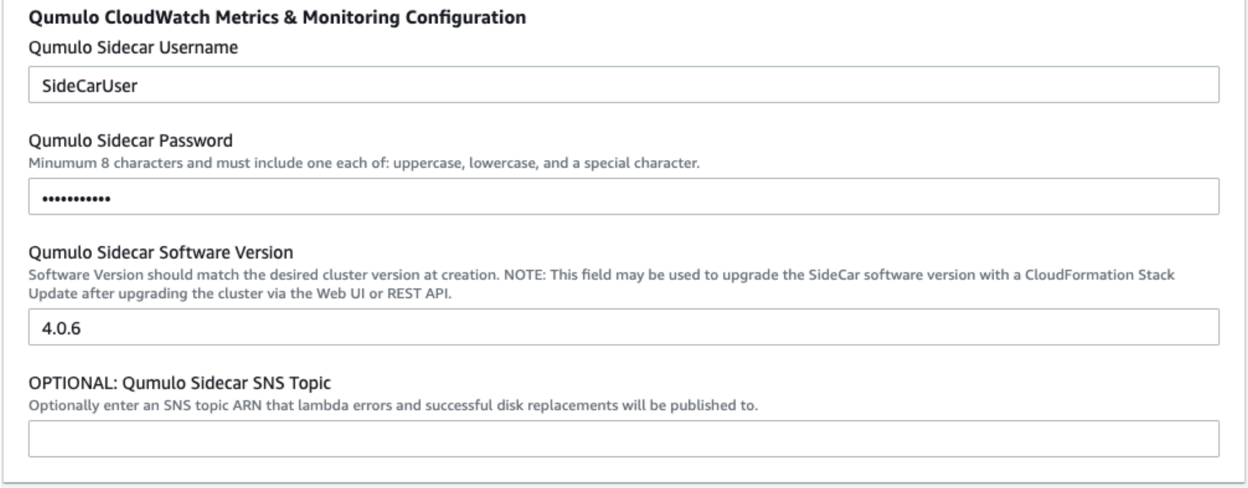
This parameter defaults to **NO**. To enable Qumulo Audit logs to be stored in a CloudWatch Log Group select **YES**.

Linux Server for Secondary Configuration of Qumulo

This parameter must be left as is. CloudFormation templates are able to parse this path to find the latest AWS Linux AMI ID for the provisioner node.

Qumulo CloudWatch Metrics & Monitoring Configuration Parameters

This section configures the Qumulo Sidecar.



Qumulo CloudWatch Metrics & Monitoring Configuration

Qumulo Sidecar Username

SideCarUser

Qumulo Sidecar Password

Minumum 8 characters and must include one each of: uppercase, lowercase, and a special character.

•••••••••••

Qumulo Sidecar Software Version

Software Version should match the desired cluster version at creation. NOTE: This field may be used to upgrade the SideCar software version with a CloudFormation Stack Update after upgrading the cluster via the Web UI or REST API.

4.0.6

OPTIONAL: Qumulo Sidecar SNS Topic

Optionally enter an SNS topic ARN that lambda errors and successful disk replacements will be published to.

Qumulo Sidecar Username

A username is configured on the cluster for Sidecar Lambda access. You may change this username if desired.

Qumulo Sidecar Password

Likewise, a password is created for the Sidecar username. Keep the default unless you want to change it. Regardless, these credentials are stored in Secrets Manager for subsequent reference.

Qumulo Sidecar Software Version

The Sidecar software version should match the cluster software version previously specified. Note, this field may be used with a Stack Update to install a newer version of the Sidecar Lambda software. This is especially helpful for production clusters that are upgraded post deployment via the Qumulo UI or API, so the Sidecar software version is synchronized with the cluster software version.

OPTIONAL: Qumulo Sidecar SNS Topic

In the event of an EBS Volume failure, Amazon Simple Notification Service (SNS) text or email messages will be sent via the configured SNS topic. Paste in your SNS topic ARN here.

Deploy the CloudFormation Stack

1. After completing all parameter entries choose **Next**.
2. On the **Configure stack options** page you can specify additional tags. When finished choose **Next**.
3. On the **Review** page confirm the template settings. Under **Capabilities**, at the bottom of the page, select the two check boxes to acknowledge that the template may create IAM resources and may require the ability to automatically expand macros. ***The template will fail if these check boxes are left unchecked.***
4. Choose **Create stack** to deploy the stack.

CloudFormation Nested Stack Deployment

The stack will take 15 to 20 minutes to deploy depending on the options chosen in the template. You can monitor the progress of the stack by choosing **Events** on the top-level stack named **QCluster1** in this example. Below is a description of each nested stack's function in the order they are deployed.

SECRETSSTACK Nested Stack

The first two stacks are launched in parallel. The SECRETS Stack stores usernames and passwords in Secrets Manager for the cluster, sidecar, and downloading software from Qumulo Trends. The purpose of leveraging Secrets Manager is to provide a secure reference for subsequent stacks and users who may forget the passwords assigned.

QIAMSTACK Nested Stack

The QIAM Stack creates an IAM profile for the Qumulo Cluster to enable the cluster to manage EC2 Secondary IP addresses (Floating IPs), decrypt data, send CloudWatch alarms, and send audit logs to CloudWatch Logs. Note, creating IAM roles in AWS takes some time so don't be alarmed if the QIAM stack takes 3 or 4 minutes.

QSTACK Nested Stack

The Q Stack spins up all the EC2 instances and EBS volumes for the cluster. It also creates a placement group for the cluster and tags all the EC2 instances with the appropriate stack name and node number. In addition, it creates CloudWatch alarms for EC2 instance failure and a security group for the cluster with the CIDR specified in the template.

MGMTNLBSTACK Nested Stack

If public management of the cluster was chosen in the template this nested stack is executed as long as the cluster is NOT being deployed in an AWS Local Zone. It spins up a Network Load Balancer with a public Elastic IP. The load balancer listens only on port 443 and optionally on port 3712 if the replication port was selected. This load balancer connects to the primary EC2 IP address on each node. These are known as the persistent IPs in the Qumulo UI.

QSIDECARSTACK Nested Stack

The SIDECAR stack launches in parallel with the MGMTNLB Stack. It creates two Lambda functions with the specified Sidecar software version. The first is the Metrics Lambda that sends Qumulo metrics to CloudWatch. The second is the Disk Recovery Lambda that monitors EBS volumes and automatically replaces any failed EBS volumes. IAM roles, permissions, and events are created for each Lambda function.

PROVISIONINGSTACK Nested Stack

This stack spins up an EC2 instance with custom user data. It configures the Qumulo Cluster and some AWS environment requirements.

Qumulo Configuration

- Software upgrades of QSTACK created nodes
- Forms the first quorum for the cluster
- Assigns Floating IP addresses to the cluster
- Configures Sidecar username, password, and custom RBAC role
- Configures Audit Logging for CloudWatch Logs
- Changes the admin password

AWS Configuration

- Checks for Public Internet reachability with a CURL test to google.com
- Assigns a QSTACK Policy to protect the cluster in subsequent Stack Updates
- Edits the Customer Managed Key Policy so Sidecar can create CMK encrypted volumes
- Tags EBS volumes with the stack name and volume type
- Tracks software versions, cluster IPs, instance IDs, & UUID in AWS Parameter Store
- Tracks the provisioning instance ‘last-run-status’ in Parameter Store

This instance automatically shuts down upon completion of its provisioning tasks.

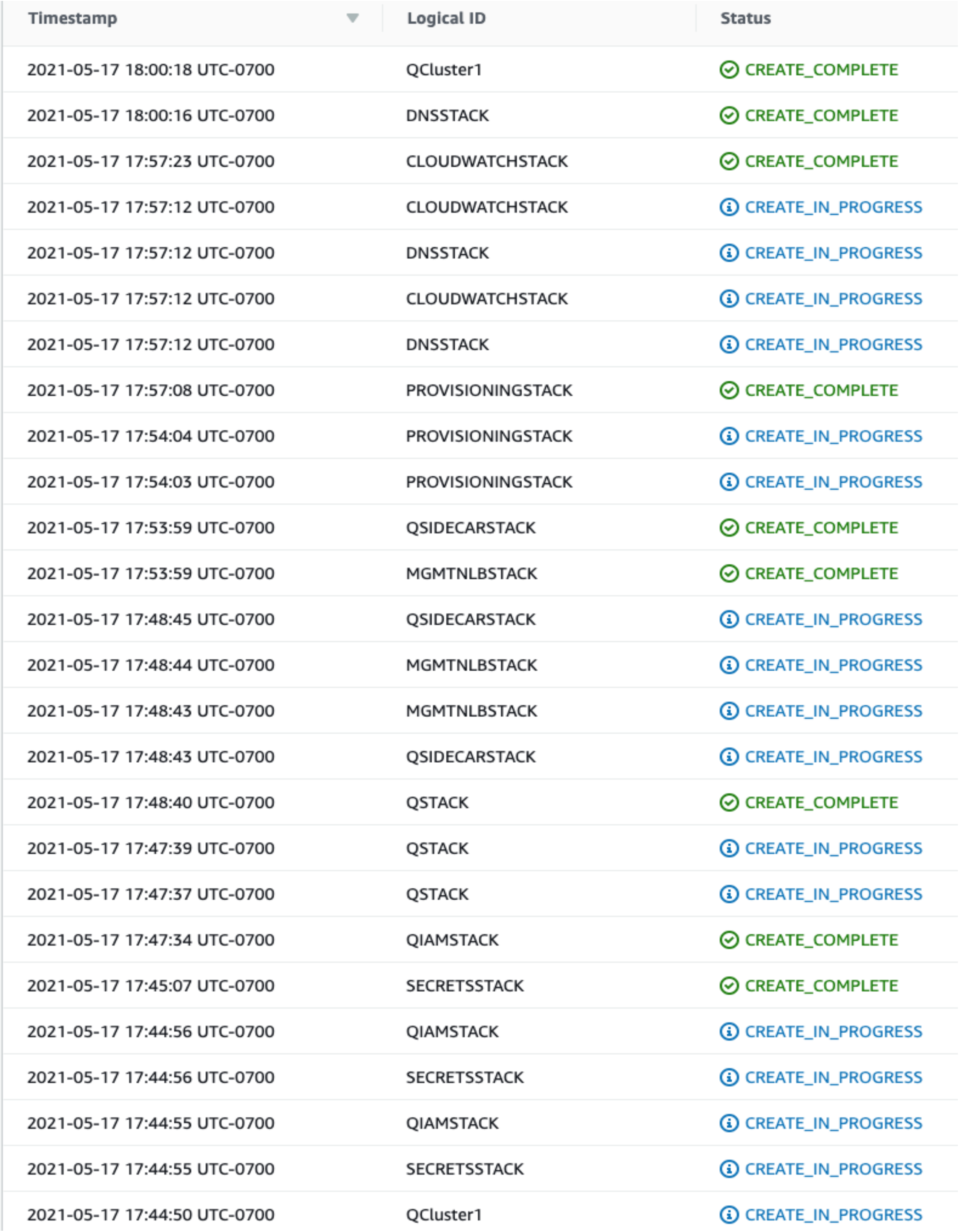
DNSSTACK Nested Stack

The final two stacks launch in parallel. If the Route 53 Private Hosted Zone FQDN was configured then the DNS stack is executed. It creates the private hosted zone and all the A-records with the name assigned in the template. All records are given a TTL=0. While round-robin behavior is the goal, Route 53 doesn't provide perfect round-robin. Instead the records are given an equal probability of resolution. Clients are well distributed, but not perfectly symmetric.

CLOUDWATCHSTACK Nested Stack

This stack creates resource groups, a CloudWatch dashboard, and a CloudWatch log group (optional) for the cluster. First, it creates a resource group for the EC2 instances and then it creates one or more resource groups for the EBS volumes. The resource groups created for the EBS volumes depend on the EBS volume configuration of the cluster. All Flash clusters will have just one resource group with the stack name and -SSD. Hybrid clusters will have two resource groups for EBS: one with -SSD and one with -HDD. The purpose of these resource groups is to provide a simple means to create a filtered view in CloudWatch for the EC2 and EBS metrics native to AWS.
A CloudWatch Dashboard is also created that presents key metrics sent by the Sidecar Metrics Lambda function. These are Qumulo specific metrics.
Finally, if Audit Logging was enabled a CloudWatch log group is created for the cluster. All administrative activity, Lambda access, and file/directory create/modify write activity is captured in this log.

Below is the event view for the top-level **QCluster1** stack. Note the timestamps to manage expectations on the duration for each nested stack.



Timestamp	Logical ID	Status
2021-05-17 18:00:18 UTC-0700	QCluster1	✓ CREATE_COMPLETE
2021-05-17 18:00:16 UTC-0700	DNSSTACK	✓ CREATE_COMPLETE
2021-05-17 17:57:23 UTC-0700	CLOUDWATCHSTACK	✓ CREATE_COMPLETE
2021-05-17 17:57:12 UTC-0700	CLOUDWATCHSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:57:12 UTC-0700	DNSSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:57:12 UTC-0700	CLOUDWATCHSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:57:12 UTC-0700	DNSSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:57:08 UTC-0700	PROVISIONINGSTACK	✓ CREATE_COMPLETE
2021-05-17 17:54:04 UTC-0700	PROVISIONINGSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:54:03 UTC-0700	PROVISIONINGSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:53:59 UTC-0700	QSIDECARSTACK	✓ CREATE_COMPLETE
2021-05-17 17:53:59 UTC-0700	MGMTNLBSTACK	✓ CREATE_COMPLETE
2021-05-17 17:48:45 UTC-0700	QSIDECARSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:48:44 UTC-0700	MGMTNLBSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:48:43 UTC-0700	MGMTNLBSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:48:43 UTC-0700	QSIDECARSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:48:40 UTC-0700	QSTACK	✓ CREATE_COMPLETE
2021-05-17 17:47:39 UTC-0700	QSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:47:37 UTC-0700	QSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:47:34 UTC-0700	QIAMSTACK	✓ CREATE_COMPLETE
2021-05-17 17:45:07 UTC-0700	SECRETSSTACK	✓ CREATE_COMPLETE
2021-05-17 17:44:56 UTC-0700	QIAMSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:44:56 UTC-0700	SECRETSSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:44:55 UTC-0700	QIAMSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:44:55 UTC-0700	SECRETSSTACK	ⓘ CREATE_IN_PROGRESS
2021-05-17 17:44:50 UTC-0700	QCluster1	ⓘ CREATE_IN_PROGRESS

Post Deployment Steps

Once the top-level stack event log shows **CREATE_COMPLETE,** CloudFormation has completed instantiation of all stack resources. Below are the steps to validate the deployment.

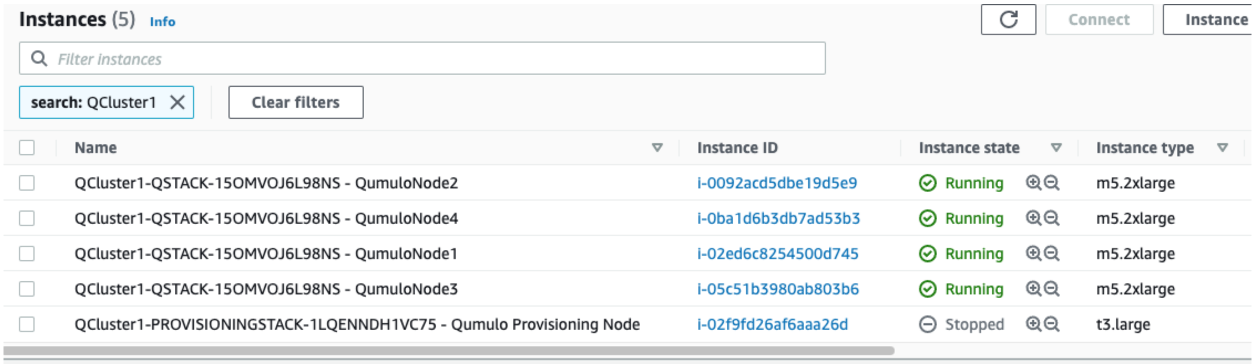
Review & Verify the AWS Infrastructure

Verify the Cluster Instances are Running

In the **AWS EC2 Console** filter on the stack name, clear the running instance filter, and verify the number of instances for the cluster is as expected. Four in this example.

Verify the Provisioning Instance has Stopped

CloudFormation has completed the instantiation of all resources, but this does not mean all resources are fully initialized and running. Specifically, the Provisioning instance will still be initializing. Given all the tasks the Provisioning instance has to accomplish it will require 6 to 10 minutes AFTER stack completion to finish all tasks. This variability is due to software upgrades of the instances. If it has to pull code and position it on S3 that takes some time as does the software upgrade. When it is finished it will automatically shutdown. If the provisioning instance has not stopped after 15 minutes, jump to the troubleshooting section.

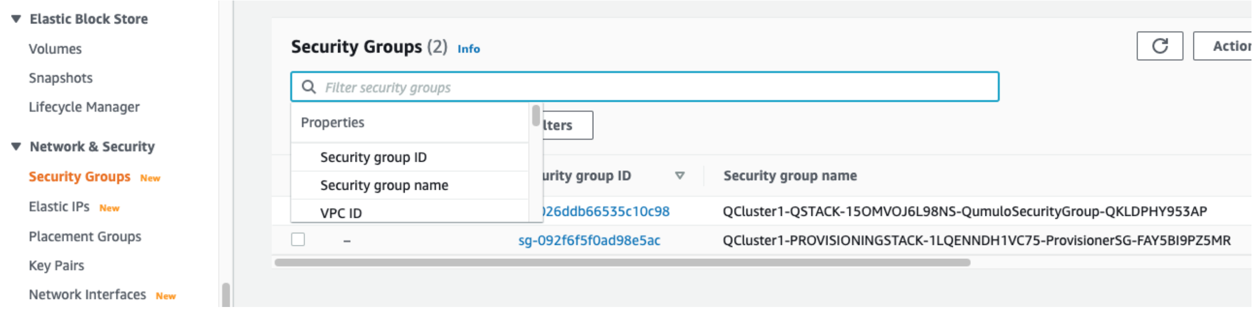


search: QCluster1

□	Name	Instance ID	Instance state	Instance type
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode2	i-0092acd5dbe19d5e9	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode4	i-0ba1d6b3db7ad53b3	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode1	i-02ed6c8254500d745	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode3	i-05c51b3980ab803b6	✓ Running	m5.2xlarge
□	QCluster1-PROVISIONINGSTACK-1LQENNDH1VC75 - Qumulo Provisioning Node	i-02f9fd26af6aaa26d	⊖ Stopped	t3.large

Verify the EC2 Security Groups

In the AWS Console go to the EC2 **Security Groups** page and filter on the top-level stack name. There will be two Security Groups that have been created. Select either to inspect the ports and CIDRs configured.

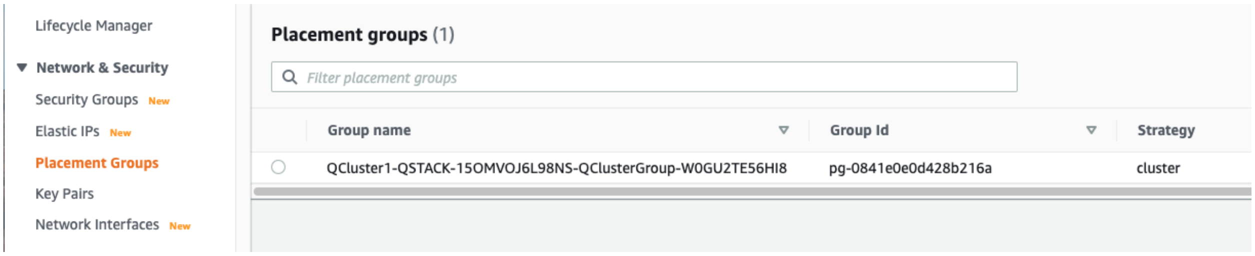


Security Groups (2) Info

		urity group ID	Security group name
		)26ddb66535c10c98	QCluster1-QSTACK-15OMVOJ6L98NS-QumuloSecurityGroup-QKLDPHY953AP
□	–	sg-092f6f5f0ad98e5ac	QCluster1-PROVISIONINGSTACK-1LQENNDH1VC75-ProvisionerSG-FAY5BI9PZ5MR

Verify the EC2 Placement Group for the Cluster

In the AWS Console go to **Placement Groups**. A placement group with the stack name has been created.

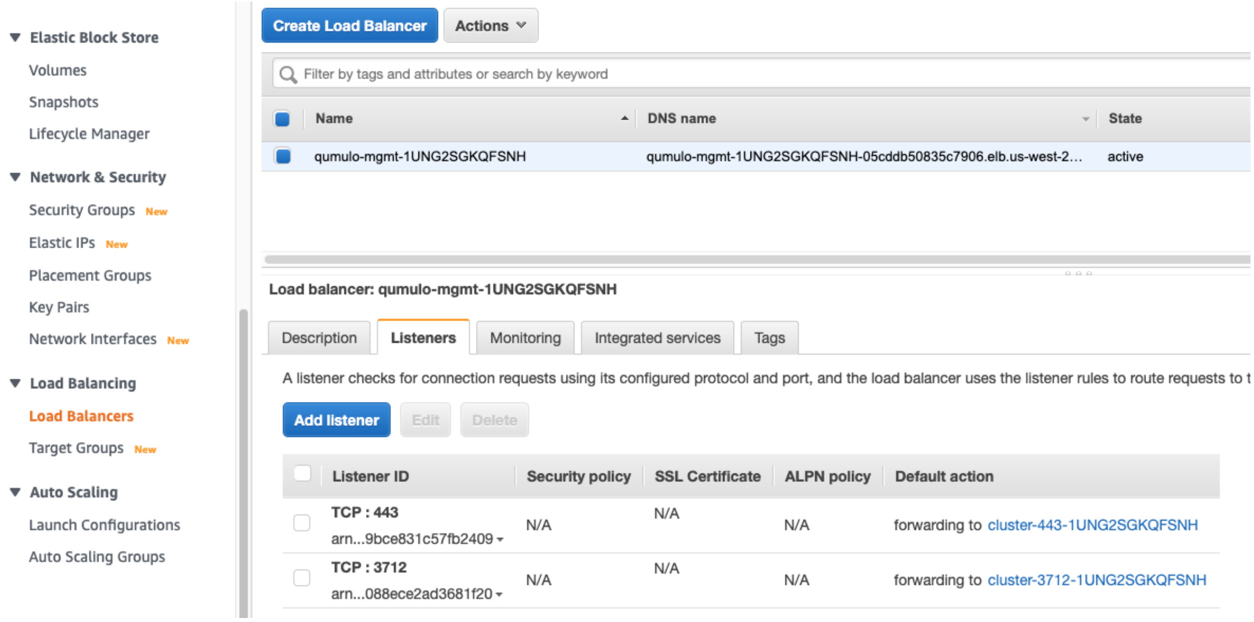


Placement groups (1)

	Group name	Group Id	Strategy
○	QCluster1-QSTACK-15OMVOJ6L98NS-QClusterGroup-W0GU2TE56HI8	pg-0841e0e0d428b216a	cluster

Verify the Load Balancer for Public Management (Optional)

In the AWS Console go to **Load Balancers**. If Public Management was selected in the template a load balancer has been created. It will be listening on 443, and if selected in the template, 3712 for replication.



	Name	DNS name	State
■	qumulo-mgmt-1UNG2SGKQFSNH	qumulo-mgmt-1UNG2SGKQFSNH-05cddb50835c7906.elb.us-west-2…	active

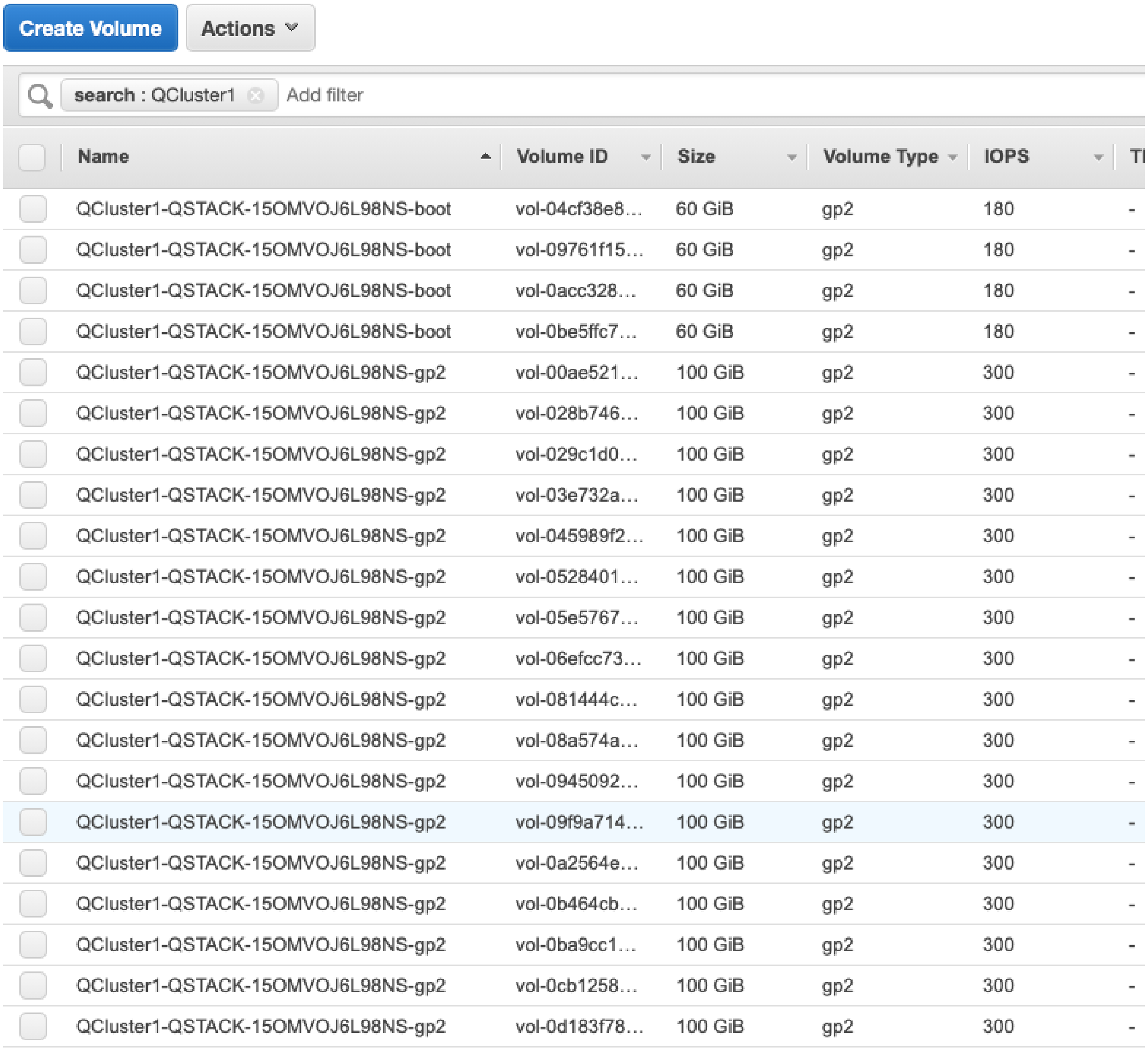
Load balancer: qumulo-mgmt-1UNG2SGKQFSNH

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to t

□	Listener ID	Security policy	SSL Certificate	ALPN policy	Default action
□	TCP : 443 arn...9bce831c57fb2409 ▾	N/A	N/A	N/A	forwarding to cluster-443-1UNG2SGKQFSNH
□	TCP : 3712 arn...088ece2ad3681f20 ▾	N/A	N/A	N/A	forwarding to cluster-3712-1UNG2SGKQFSNH

Verify EBS Volume Tags

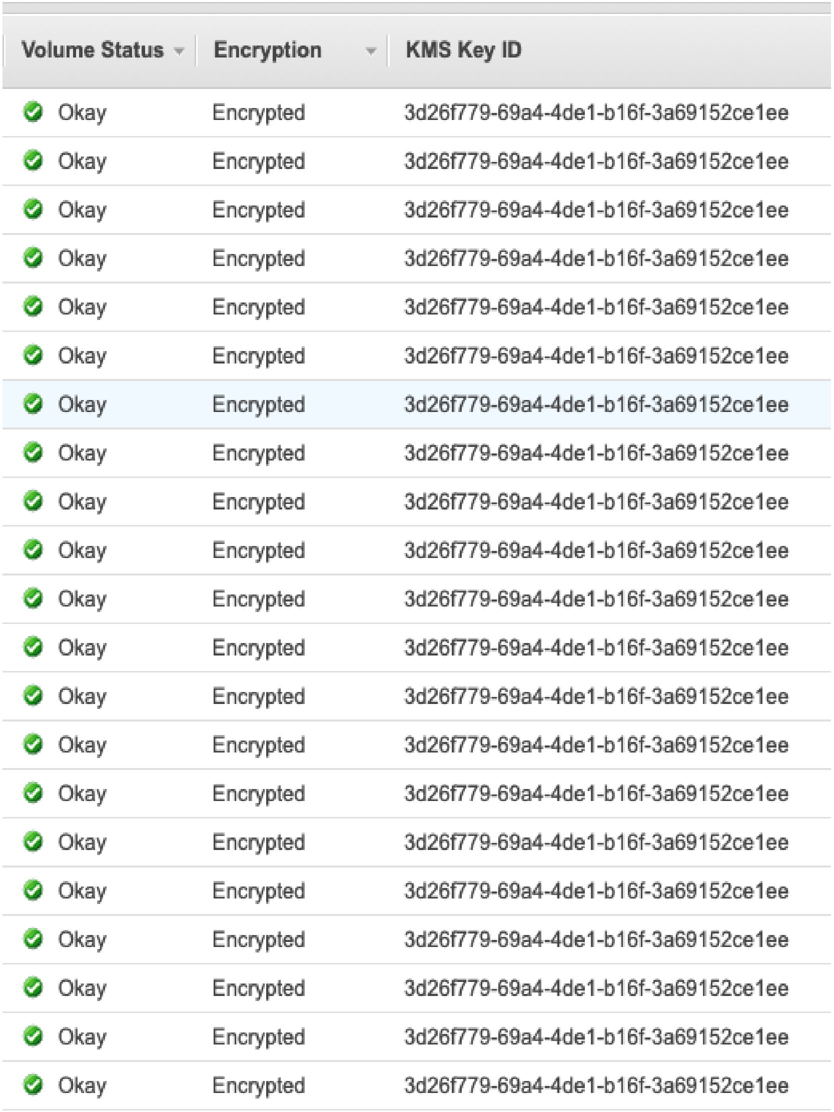
If the Provisioning instance has stopped the EBS volumes will be tagged accordingly for the cluster and EBS volume configuration. Go to the AWS Console **Elastic Block Store Volumes** page to verify. The type and number of EBS volumes will vary depending on EBS volume configuration chosen in the template and the number of EC2 instances.



□	Name	Volume ID	Size	Volume Type	IOPS	T
□	QCluster1-QSTACK-15OMVOJ6L98NS-boot	vol-04cf38e8…	60 GiB	gp2	180	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-boot	vol-09761f15…	60 GiB	gp2	180	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-boot	vol-0acc328…	60 GiB	gp2	180	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-boot	vol-0be5ffc7…	60 GiB	gp2	180	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-00ae521…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-028b746…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-029c1d0…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-03e732a…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-045989f2…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0528401…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-05e5767…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-06efcc73…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-081444c…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-08a574a…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0945092…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-09f9a714…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0a2564e…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0b464cb…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0ba9cc1…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0cb1258…	100 GiB	gp2	300	-
□	QCluster1-QSTACK-15OMVOJ6L98NS-gp2	vol-0d183f78…	100 GiB	gp2	300	-

Verify EBS Encryption with a CMK (Optional)

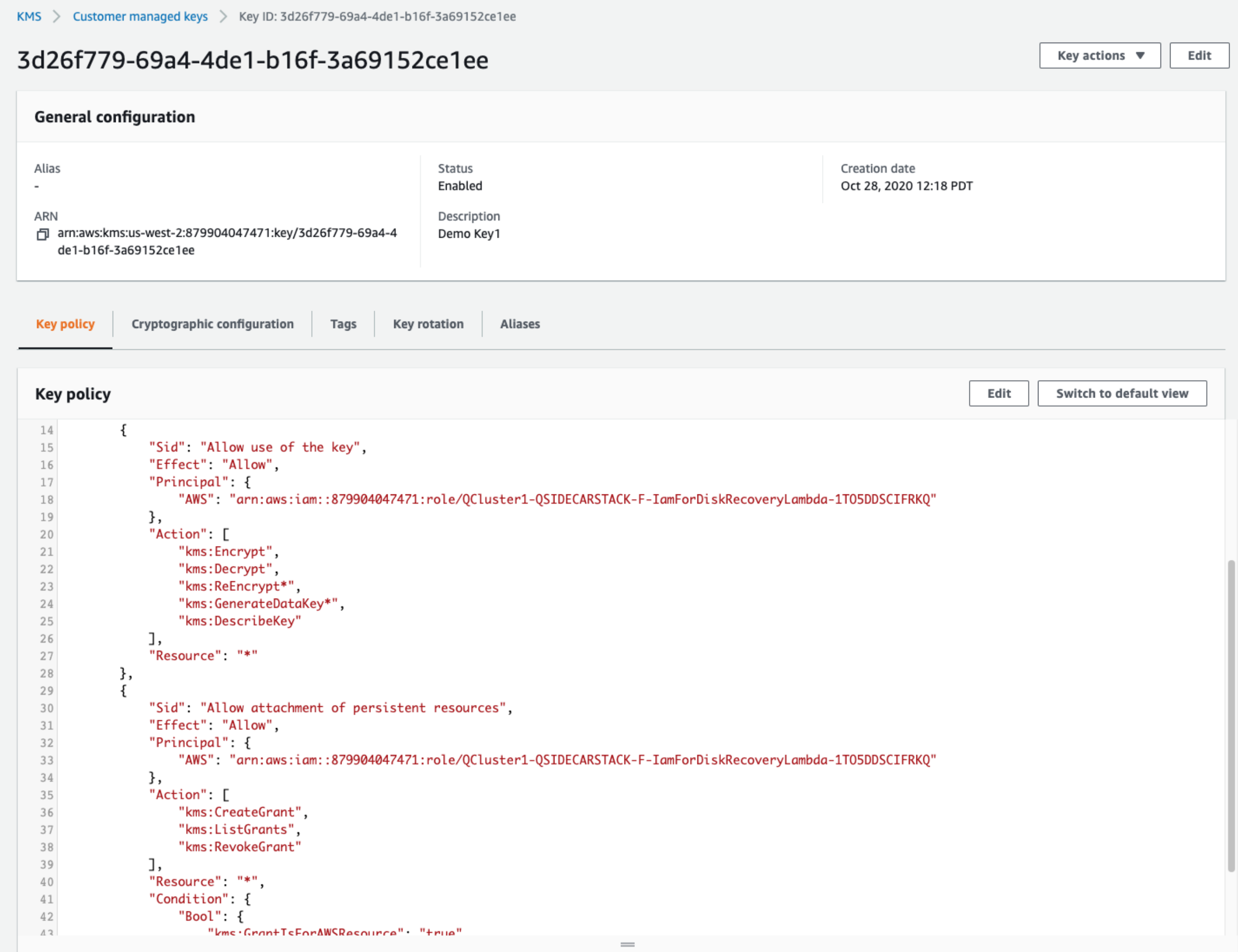
On the same page scroll to the right to verify that the volumes are encrypted with the Customer Managed Key assigned in the template. This is only relevant if a CMK was specified. If the field was left blank in the template, AWS will generate a key to encrypt the data at rest.



Volume Status	Encryption	KMS Key ID
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee
✓ Okay	Encrypted	3d26f779-69a4-4de1-b16f-3a69152ce1ee

Verify the KMS CMK Policy (Optional)

In the AWS Console go to the **Key Management Service** page and select the CMK that was chosen in the template. Verify that the policy has been updated with two SIDs, one for the Metrics Lambda and one for the Disk Recovery Lambda. If the policy is not updated it is likely the Provisioning node will not have shutdown because the policy was not cleaned up prior to launching the template. Without this policy modification in place the Sidecar will not be able to create a new EBS volume to replace a failed EBS volume.



Key ID: 3d26f779-69a4-4de1-b16f-3a69152ce1ee

3d26f779-69a4-4de1-b16f-3a69152ce1ee

General configuration

Alias
-

ARN
arn:aws:kms:us-west-2:879904047471:key/3d26f779-69a4-4de1-b16f-3a69152ce1ee

Status
Enabled

Description
Demo Key1

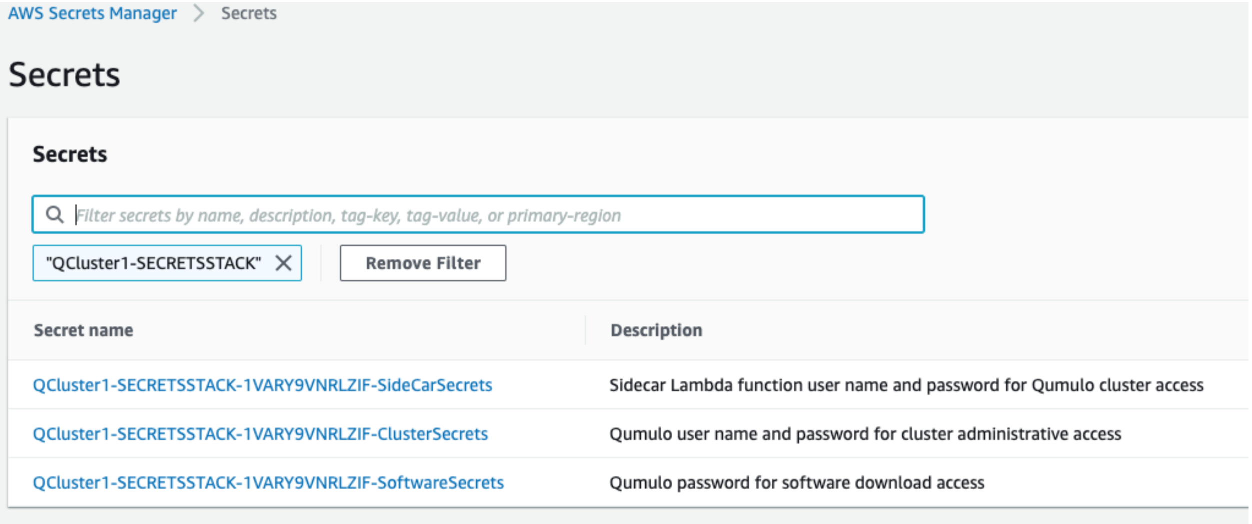
Creation date
Oct 28, 2020 12:18 PDT

Key policy

```
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::879904047471:role/QCluster1-QSIDECARSTACK-F-IamForDiskRecoveryLambda-1TO5DDSCIFRKQ"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::879904047471:role/QCluster1-QSIDECARSTACK-F-IamForDiskRecoveryLambda-1TO5DDSCIFRKQ"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
```

Verify Secrets Manager Secrets

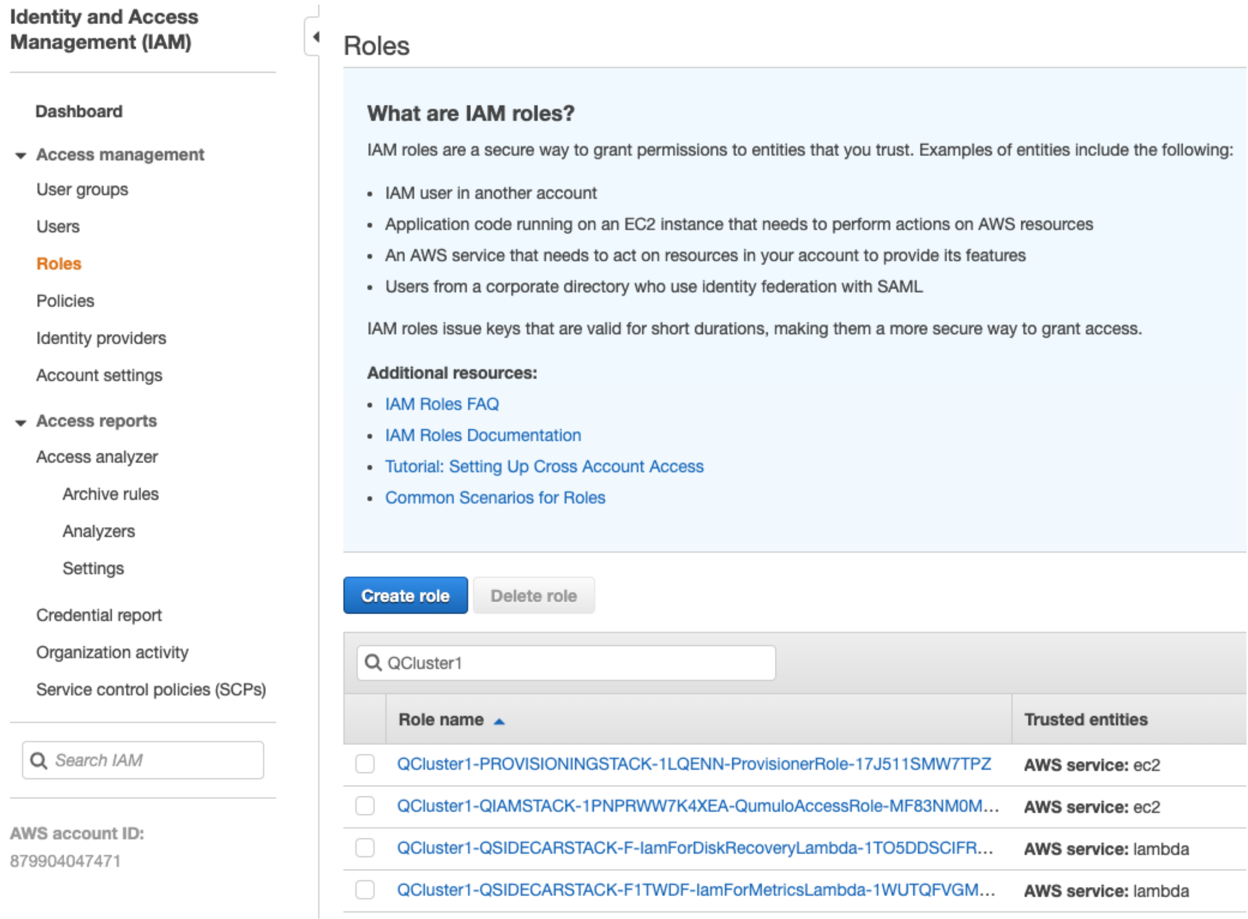
In the AWS Console go to the **Secrets Manager** page and filter on the top-level stack name. There will be three secrets that have been created to store username/password pairs. Select any of them to see the credentials.


AWS Secrets Manager > Secrets
Secrets
Secrets
Filter secrets by name, description, tag-key, tag-value, or primary-region
"QCluster1-SECRETSSTACK"
Remove Filter

Secret name	Description
QCluster1-SECRETSSTACK-1VARY9VNRLZIF-SideCarSecrets	Sidecar Lambda function user name and password for Qumulo cluster access
QCluster1-SECRETSSTACK-1VARY9VNRLZIF-ClusterSecrets	Qumulo user name and password for cluster administrative access
QCluster1-SECRETSSTACK-1VARY9VNRLZIF-SoftwareSecrets	Qumulo password for software download access

Verify the IAM Roles

In the AWS Console go to the IAM page and filter on the top-level stack name. There will be four IAM roles that have been created: two for the Sidecar, one for the cluster, and one for the provisioning instance.



AWS account ID: 879904047471

Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

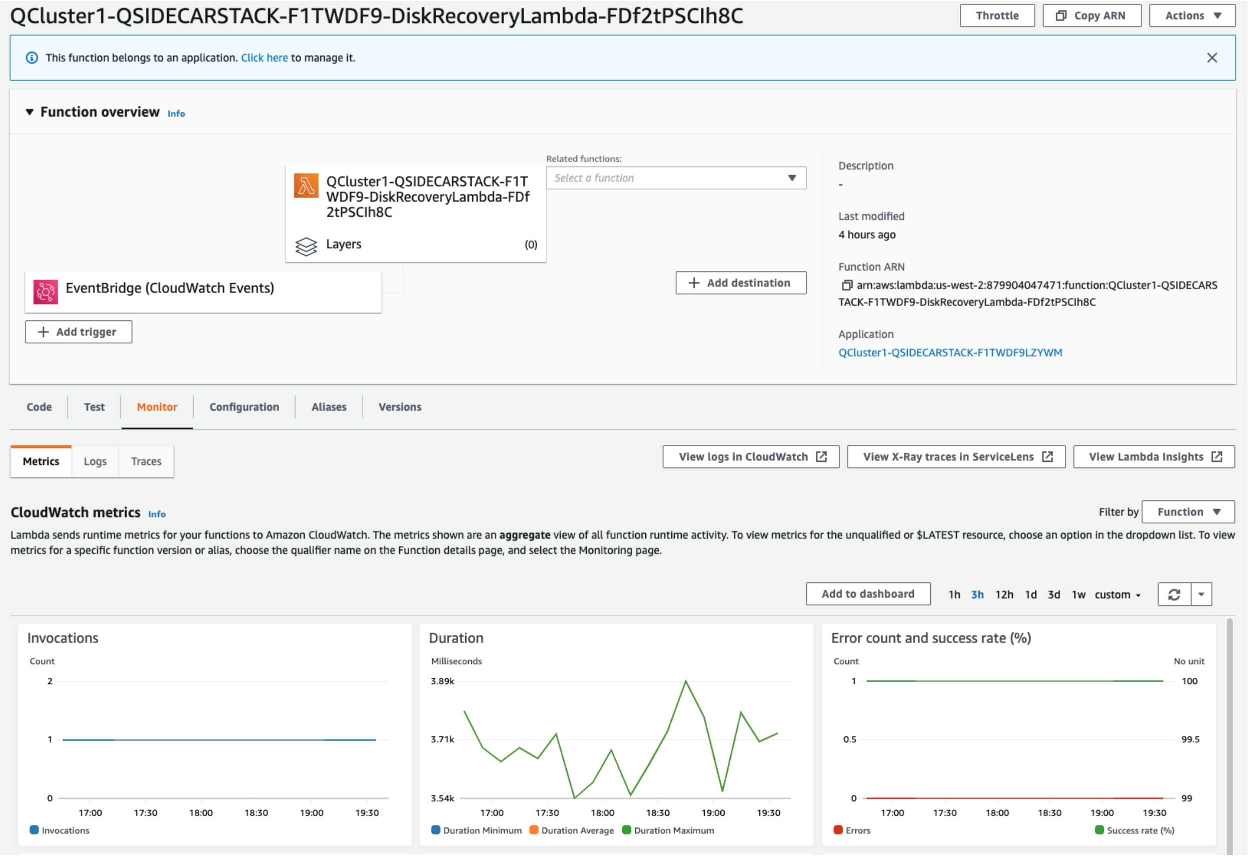
- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

QCluster1

	Role name ▲	Trusted entities
□	QCluster1-PROVISIONINGSTACK-1LQENN-ProvisionerRole-17J511SMW7TPZ	**AWS service:** ec2
□	QCluster1-QIAMSTACK-1PNPRWW7K4XEA-QumuloAccessRole-MF83NM0M…	**AWS service:** ec2
□	QCluster1-QSIDECARSTACK-F-IamForDiskRecoveryLambda-1TO5DDSCIFR…	**AWS service:** lambda
□	QCluster1-QSIDECARSTACK-F1TWDF-IamForMetricsLambda-1WUTQFVGM…	**AWS service:** lambda

Verify Sidecar Lambdas

In the AWS Console go to the **Lambda** page and filter on the top-level stack name. There will be two Lambda functions. Select the **Disk Recovery Lambda** and then choose **Monitor**. In the populated graphs check that the Error Count and Success Rate shows 100% green and 0% red. This confirms the Disk Recovery Lambda is communicating with the cluster. Review the Metrics Lambda in the same manner.



QCluster1-QSIDECARSTACK-F1TWDF9-DiskRecoveryLambda-FDf2tPSCIh8C

This function belongs to an application. Click here to manage it.

Description
-

Last modified
4 hours ago

Function ARN
arn:aws:lambda:us-west-2:879904047471:function:QCluster1-QSIDECARSTACK-F1TWDF9-DiskRecoveryLambda-FDf2tPSCIh8C

Application
QCluster1-QSIDECARSTACK-F1TWDF9LZYWM

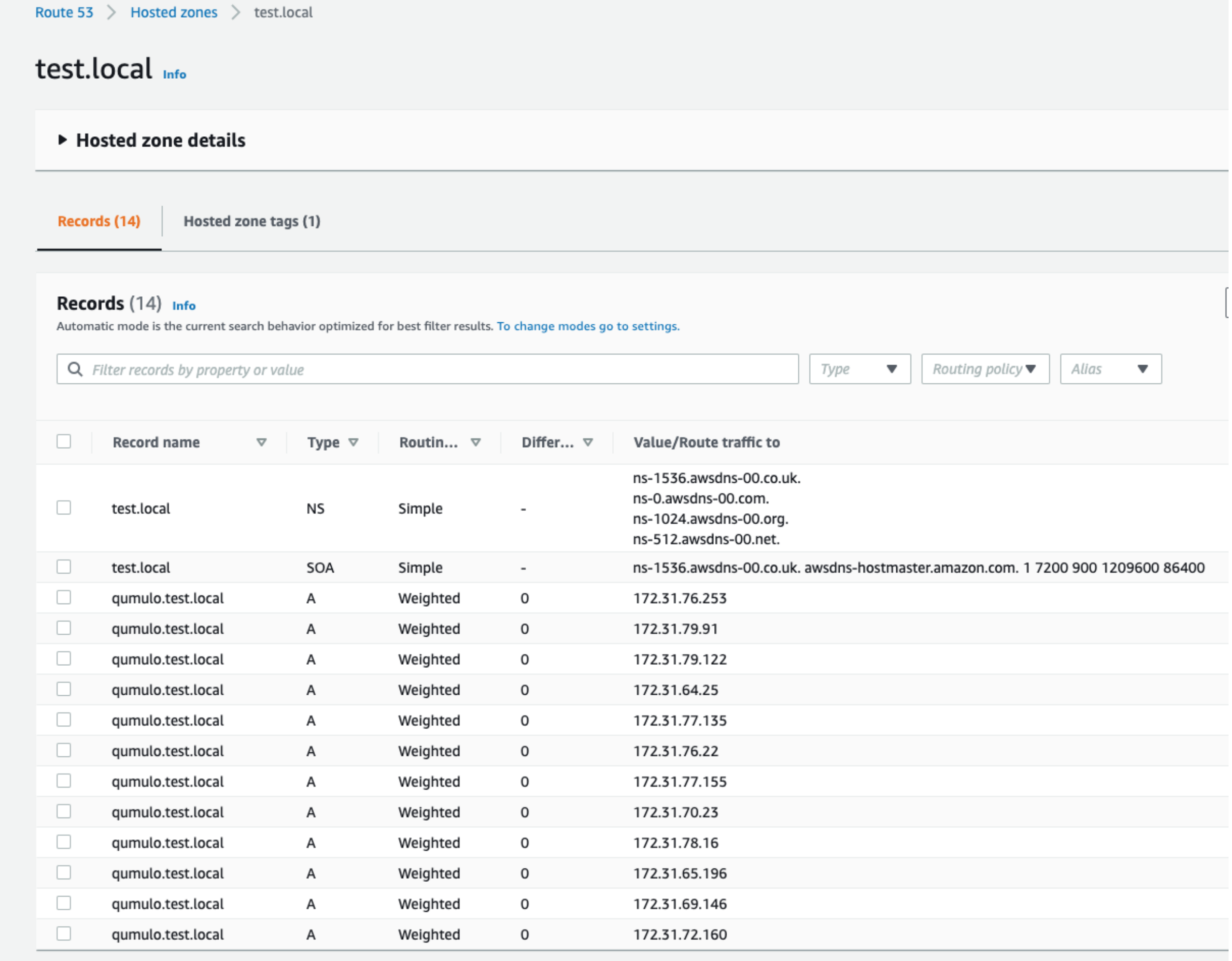
CloudWatch metrics

Lambda sends runtime metrics for your functions to Amazon CloudWatch. The metrics shown are an **aggregate** view of all function runtime activity. To view metrics for the unqualified or $LATEST resource, choose an option in the dropdown list. To view metrics for a specific function version or alias, choose the qualifier name on the Function details page, and select the Monitoring page.

Filter by: Function

Verify Route 53 Private Hosted Zone for DNS (Optional)

In the AWS Console go to **Route 53**. Select the Private Hosted Zone that was created. In this case it is **test.local**. Verify the A-records were created with the A-record name specified in the template. This is only relevant if an FQDN was specified, otherwise Route 53 configuration is skipped. Note, 12 A-records were created, one for each floating IP, since 4 EC2 instances with 3 floating IPs were chosen in the template.



Route 53 > Hosted zones > test.local

test.local Info

▸ Hosted zone details

Records (14) | Hosted zone tags (1)

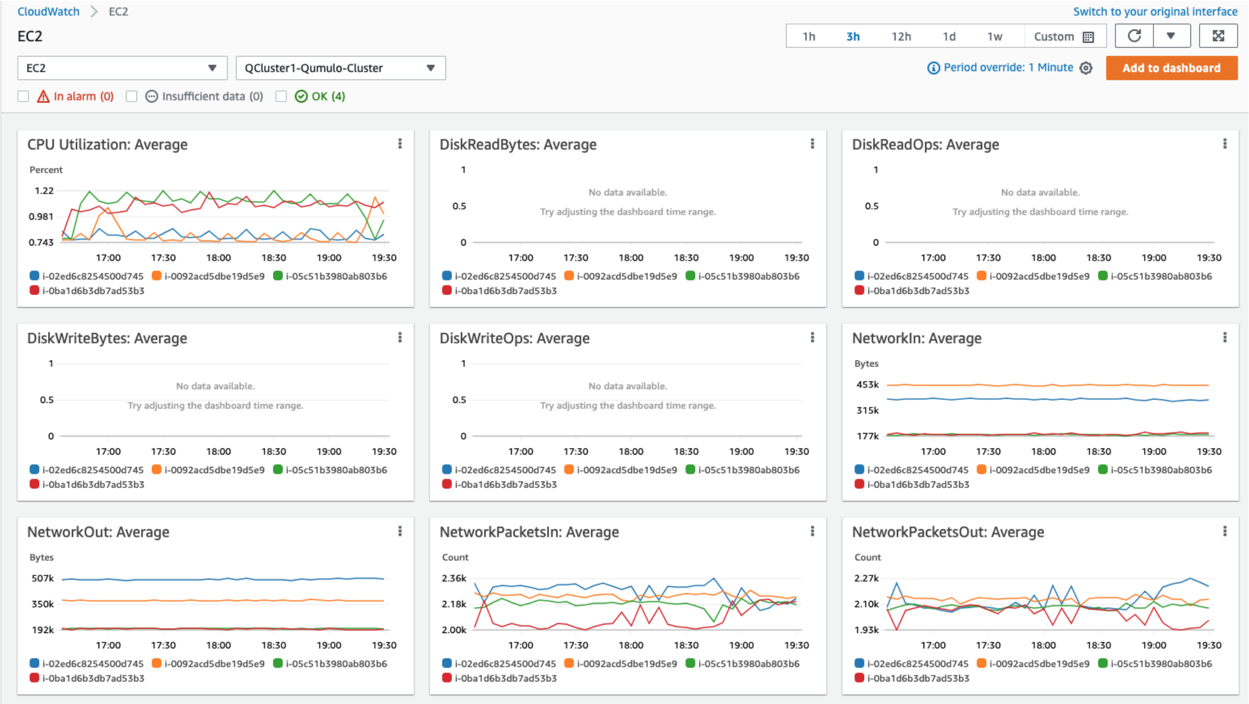
Records (14) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

□	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	test.local	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
□	test.local	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
□	qumulo.test.local	A	Weighted	0	172.31.76.253
□	qumulo.test.local	A	Weighted	0	172.31.79.91
□	qumulo.test.local	A	Weighted	0	172.31.79.122
□	qumulo.test.local	A	Weighted	0	172.31.64.25
□	qumulo.test.local	A	Weighted	0	172.31.77.135
□	qumulo.test.local	A	Weighted	0	172.31.76.22
□	qumulo.test.local	A	Weighted	0	172.31.77.155
□	qumulo.test.local	A	Weighted	0	172.31.70.23
□	qumulo.test.local	A	Weighted	0	172.31.78.16
□	qumulo.test.local	A	Weighted	0	172.31.65.196
□	qumulo.test.local	A	Weighted	0	172.31.69.146
□	qumulo.test.local	A	Weighted	0	172.31.72.160

Verify Resource Groups

In the AWS Console go to **CloudWatch**. In the first filter box choose **EC2** and then in the **Filter by resource group box** select the cluster with **Qumulo-Cluster-EC2-[Stack Name]**. This provides a CloudWatch filtered view of the EC2 instances for the cluster. CPU Utilization, network stats, boot volume stats, and alarm events are available.



CloudWatch > EC2

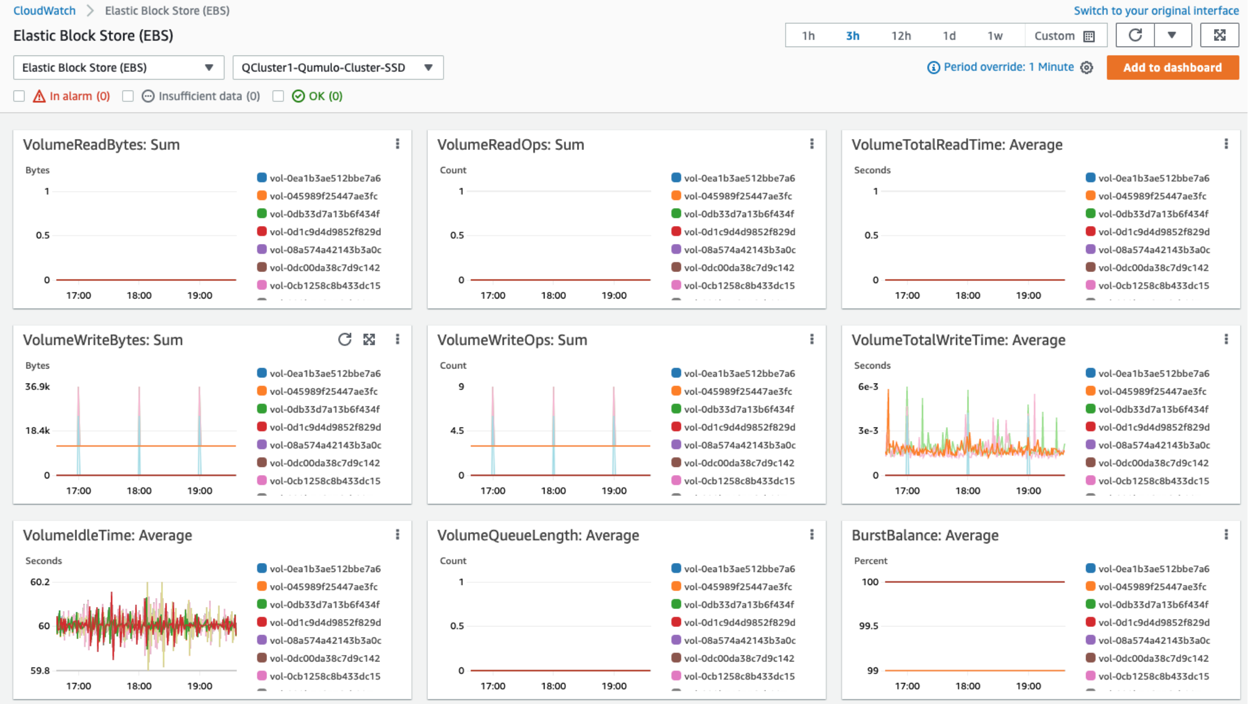
EC2

EC2 ▼ | QCluster1-Qumulo-Cluster ▼

□ In alarm (0) □ Insufficient data (0) □ OK (4)

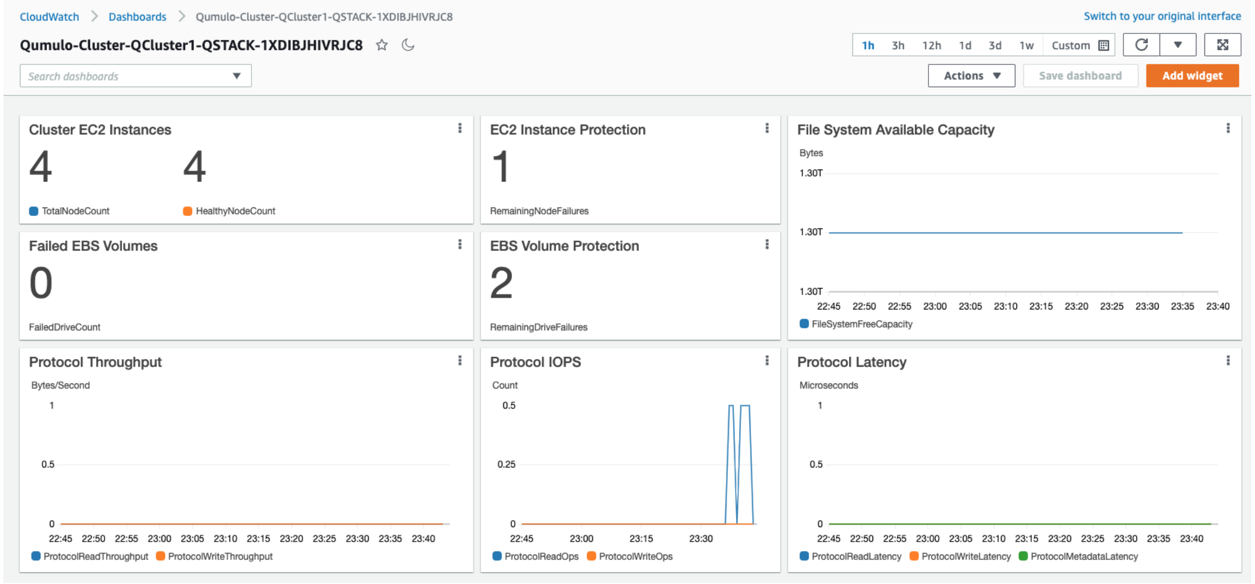
Period override: 1 Minute

Now clear the **Filter by resource group field** and select **EBS** in the first filter box. Now in the **Filter by resource group field** choose the cluster with **Qumulo-Cluster-[SSD or HDD]-[Stack Name]**. This is a CloudWatch view of the EBS volumes for the cluster. Note, boot volumes are not included in this view.



Verify CloudWatch Dashboard

In the AWS Console go to **CloudWatch > Dashboard > Qumulo-Cluster-[Stack Name]-QSTACK-[123456789ABCD]**. This is a dashboard that has been built to display the metrics sent by the Qumulo Sidecar Metrics Lambda function. Instance health, EBS health, Available Capacity, and Performance data are all available. This dashboard is very useful for historical data that is over 72 hours old. For real-time data visit the Qumulo cluster's UI. Note: If you are deploying multiple clusters in an AWS region give them unique Qumulo Cluster Names. Metrics are filtered based on the Qumulo Cluster Name.



CloudWatch > Dashboards > Qumulo-Cluster-QCluster1-QSTACK-1XDIBJHIVRJC8

Switch to your original interface

Qumulo-Cluster-QCluster1-QSTACK-1XDIBJHIVRJC8

Cluster EC2 Instances

4 TotalNodeCount

4 HealthyNodeCount

EC2 Instance Protection

1 RemainingNodeFailures

File System Available Capacity

Failed EBS Volumes

0 FailedDriveCount

EBS Volume Protection

2 RemainingDriveFailures

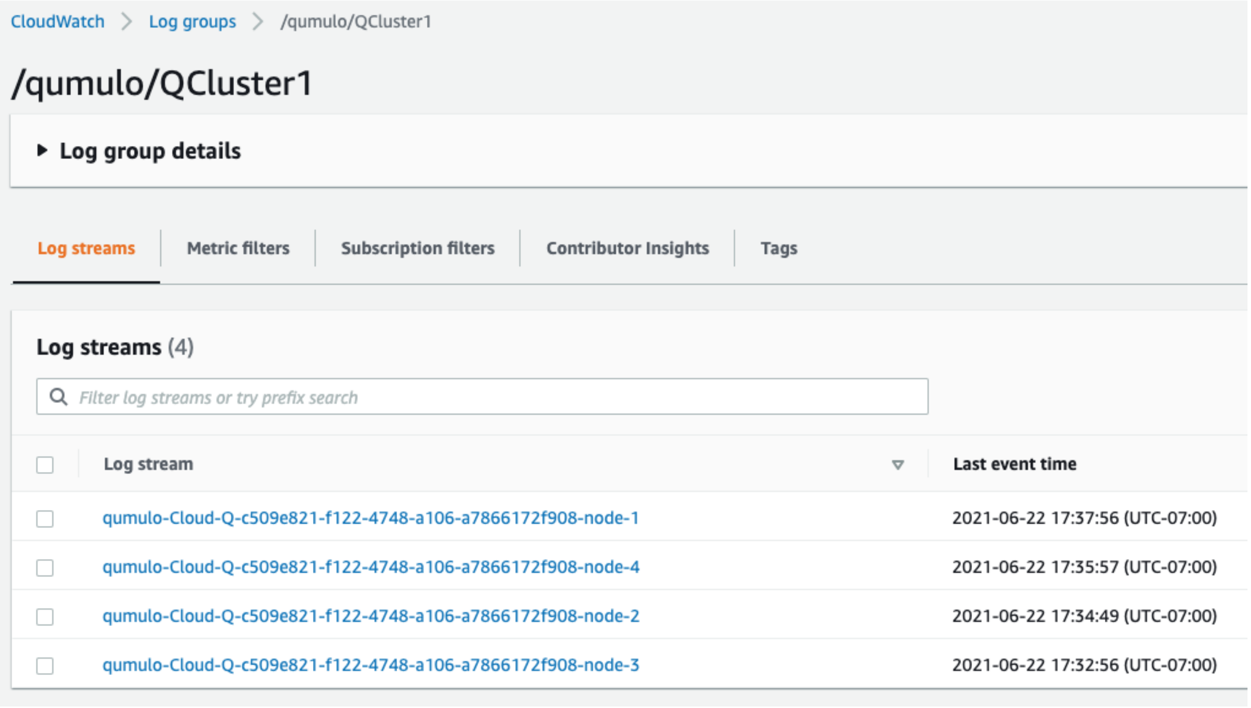
Protocol Throughput

Protocol IOPS

Protocol Latency

Verify CloudWatch Logs (Audit Logging)

In the AWS Console go to **CloudWatch > Log Groups > /qumulo/[Stack Name]**. This log group is configured if Audit Logging was enabled in the CloudFormation template. Log files will immediately be available for each instance in the cluster.



CloudWatch > Log groups > /qumulo/QCluster1

/qumulo/QCluster1

▶ Log group details

Log streams (4)

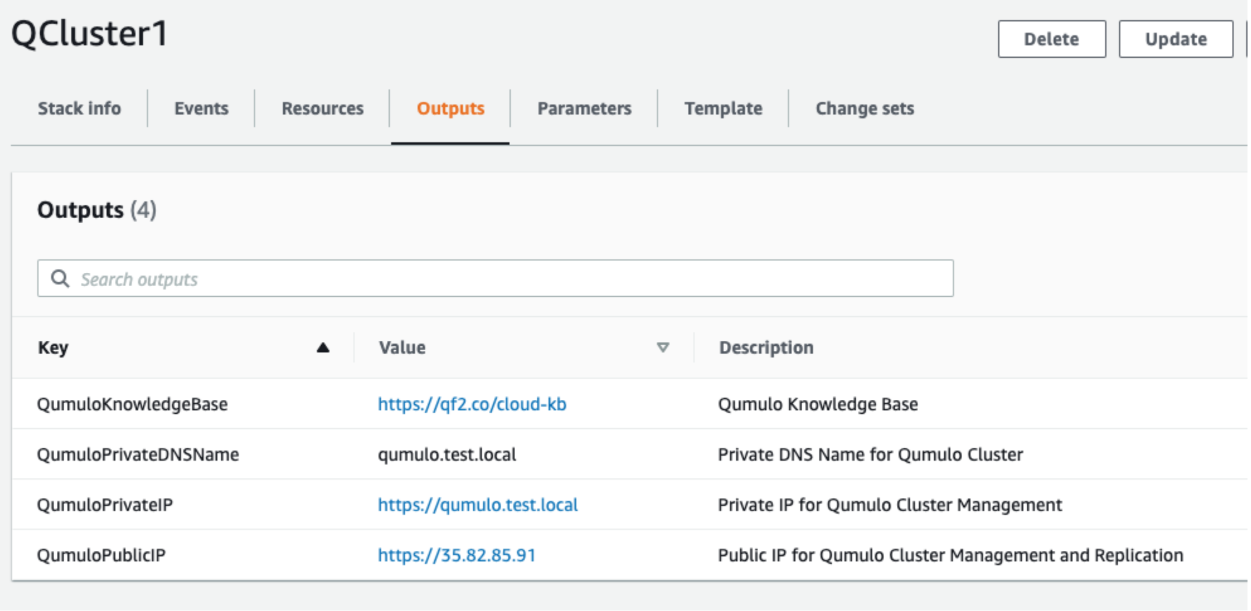
Filter log streams or try prefix search

□	Log stream	Last event time
□	qumulo-Cloud-Q-c509e821-f122-4748-a106-a7866172f908-node-1	2021-06-22 17:37:56 (UTC-07:00)
□	qumulo-Cloud-Q-c509e821-f122-4748-a106-a7866172f908-node-4	2021-06-22 17:35:57 (UTC-07:00)
□	qumulo-Cloud-Q-c509e821-f122-4748-a106-a7866172f908-node-2	2021-06-22 17:34:49 (UTC-07:00)
□	qumulo-Cloud-Q-c509e821-f122-4748-a106-a7866172f908-node-3	2021-06-22 17:32:56 (UTC-07:00)

Review & Verify the Qumulo Cluster Configuration

Review the Outputs of the CloudFormation Stack

Go to the **CloudFormation** page and select the top-level stack name, **Qcluster1**. Choose **Outputs**. If Route 53 was configured a URL to the private addresses, resolved by Route 53, will be shown. If Route 53 was skipped, a URL to the first node's primary IP address will be displayed. Likewise, if Public Management was chosen a URL to the Elastic IP (public static) address will be shown. If connecting via the public Internet, open a page from your local machine using the **QumuloPublicIP** URL. If connecting from within your VPC, paste the **QumuloPrivateIP** URL into the browser of an EC2 instance running Chrome.



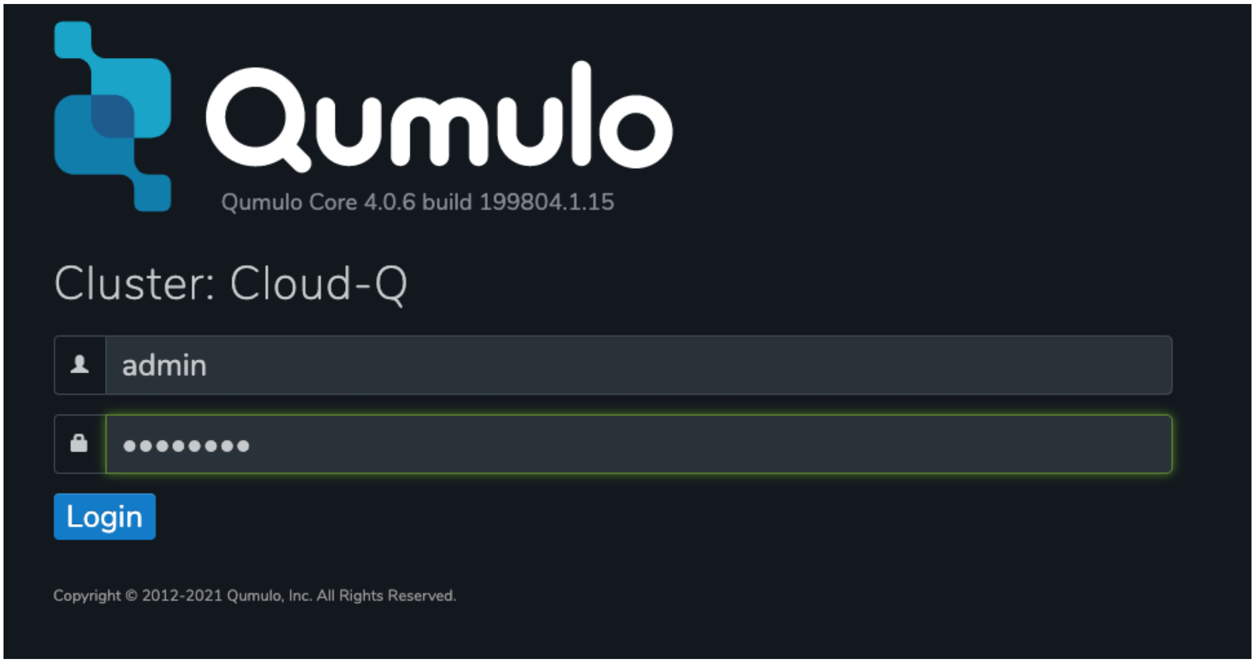
QCluster1

Outputs (4)

Key	Value	Description
QumuloKnowledgeBase	https://qf2.co/cloud-kb	Qumulo Knowledge Base
QumuloPrivateDNSName	qumulo.test.local	Private DNS Name for Qumulo Cluster
QumuloPrivateIP	https://qumulo.test.local	Private IP for Qumulo Cluster Management
QumuloPublicIP	https://35.82.85.91	Public IP for Qumulo Cluster Management and Replication

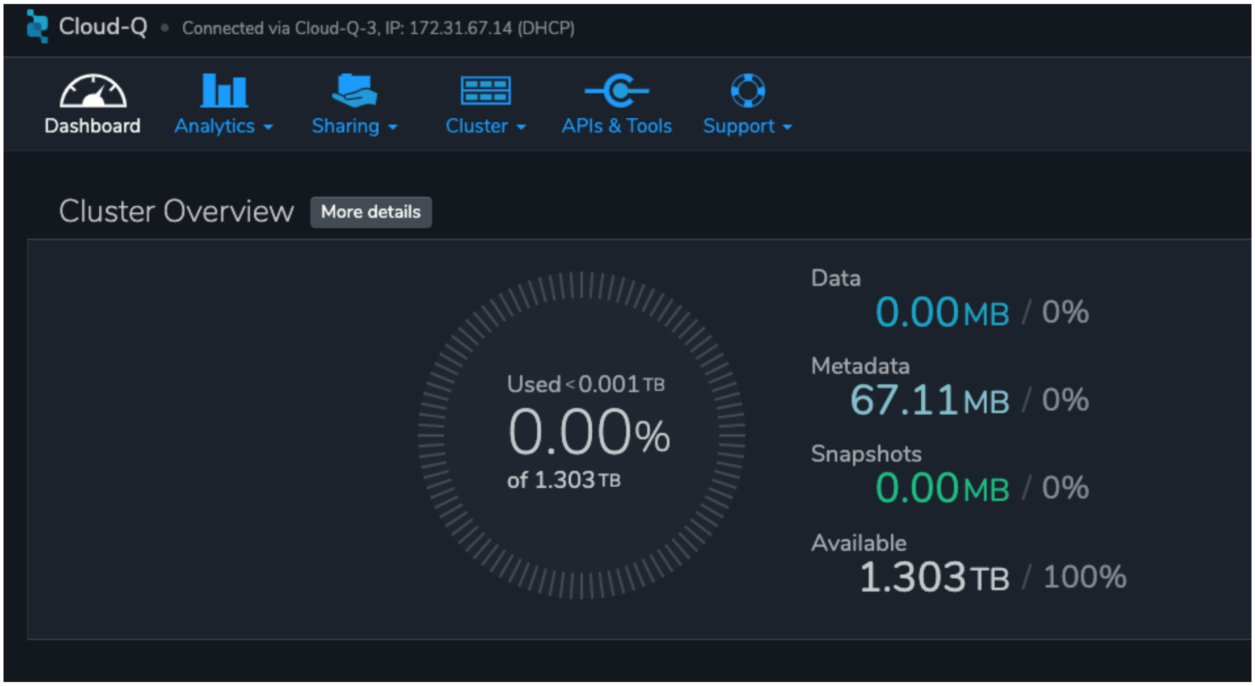
Verify Admin Password

The login page should authenticate with the credentials:
Username: **admin**
Password: '***your chosen Admin password***'
If you've forgotten the admin password entered in the template go to Secrets Manager and retrieve it.

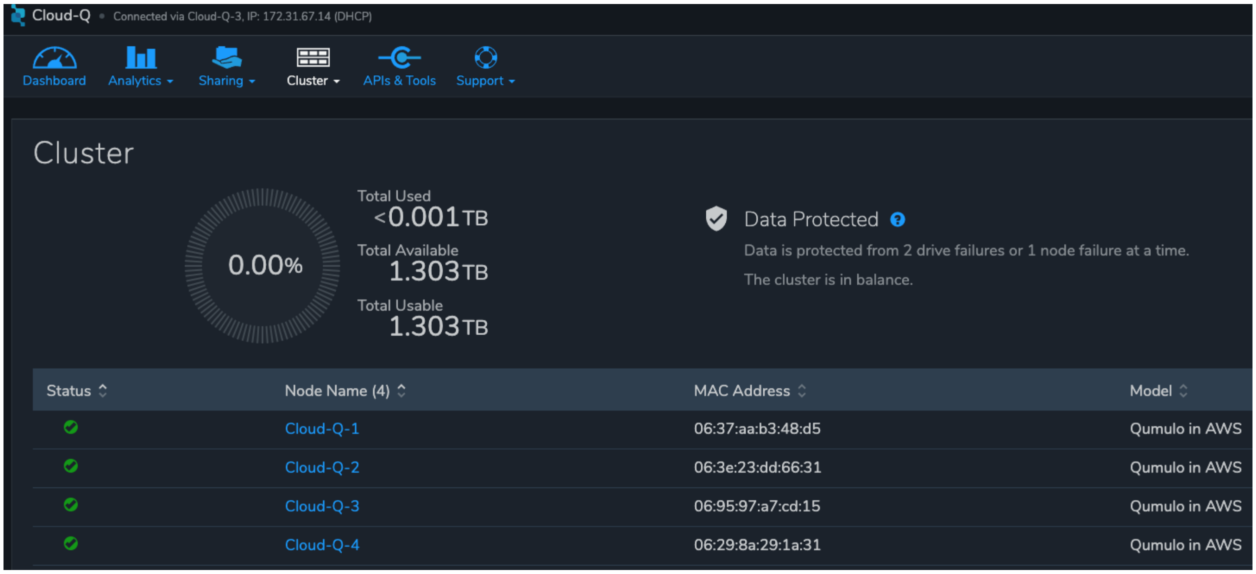

Qumulo
Qumulo Core 4.0.6 build 199804.1.15
Cluster: Cloud-Q
admin
••••••••
Login
Copyright © 2012-2021 Qumulo, Inc. All Rights Reserved.

Verify Quorum and Protection

After logging in, the cluster dashboard should be displayed. IF it isn't the cluster failed to form quorum. Jump to troubleshooting.



Choose **More details**. The number of nodes in the cluster should match what was provisioned in the template. Further, to the right is the protection status showing protection for 1 node failure or 2 disk failures.



Cluster

0.00%

Total Used <0.001 TB

Total Available 1.303 TB

Total Usable 1.303 TB

Data Protected

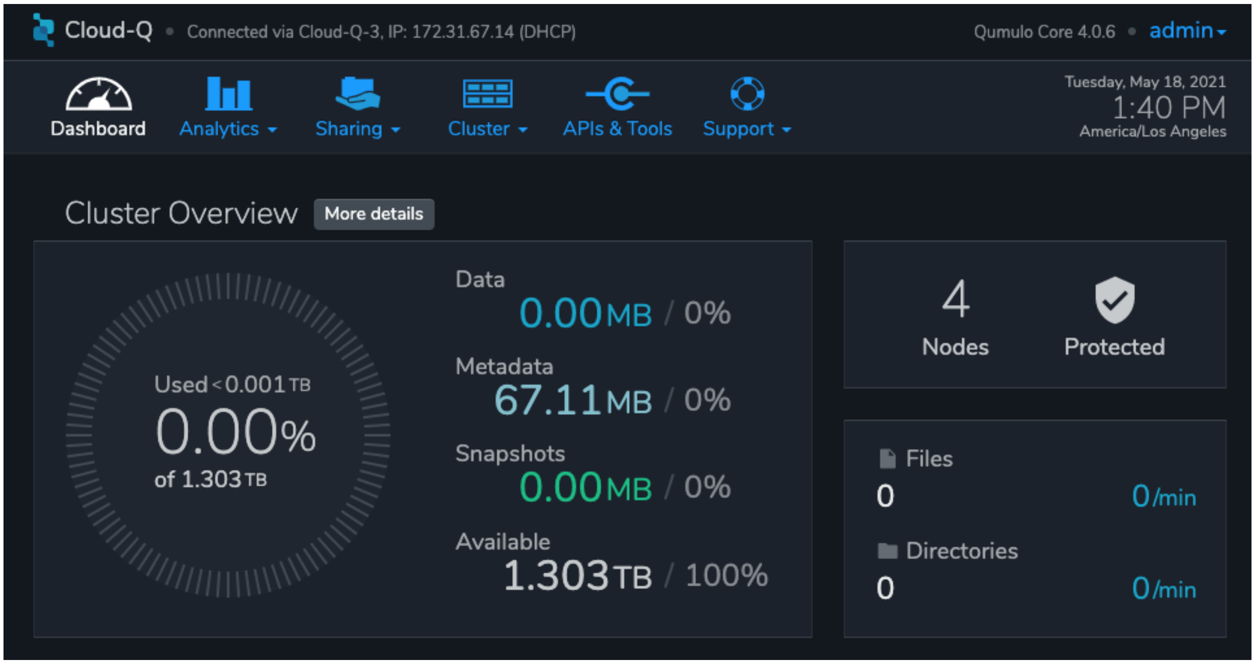
Data is protected from 2 drive failures or 1 node failure at a time.

The cluster is in balance.

Status	Node Name (4)	MAC Address	Model
✓	Cloud-Q-1	06:37:aa:b3:48:d5	Qumulo in AWS
✓	Cloud-Q-2	06:3e:23:dd:66:31	Qumulo in AWS
✓	Cloud-Q-3	06:95:97:a7:cd:15	Qumulo in AWS
✓	Cloud-Q-4	06:29:8a:29:1a:31	Qumulo in AWS

Verify Software Version

In the top right of the Qumulo UI the software version is displayed. This should match the software version requested when the template was filled in. Here it shows Qumulo Core version 4.0.6 as expected.



Cluster Overview

Used <0.001 TB

0.00%

of 1.303 TB

Data 0.00 MB / 0%

Metadata 67.11 MB / 0%

Snapshots 0.00 MB / 0%

Available 1.303 TB / 100%

4 Nodes

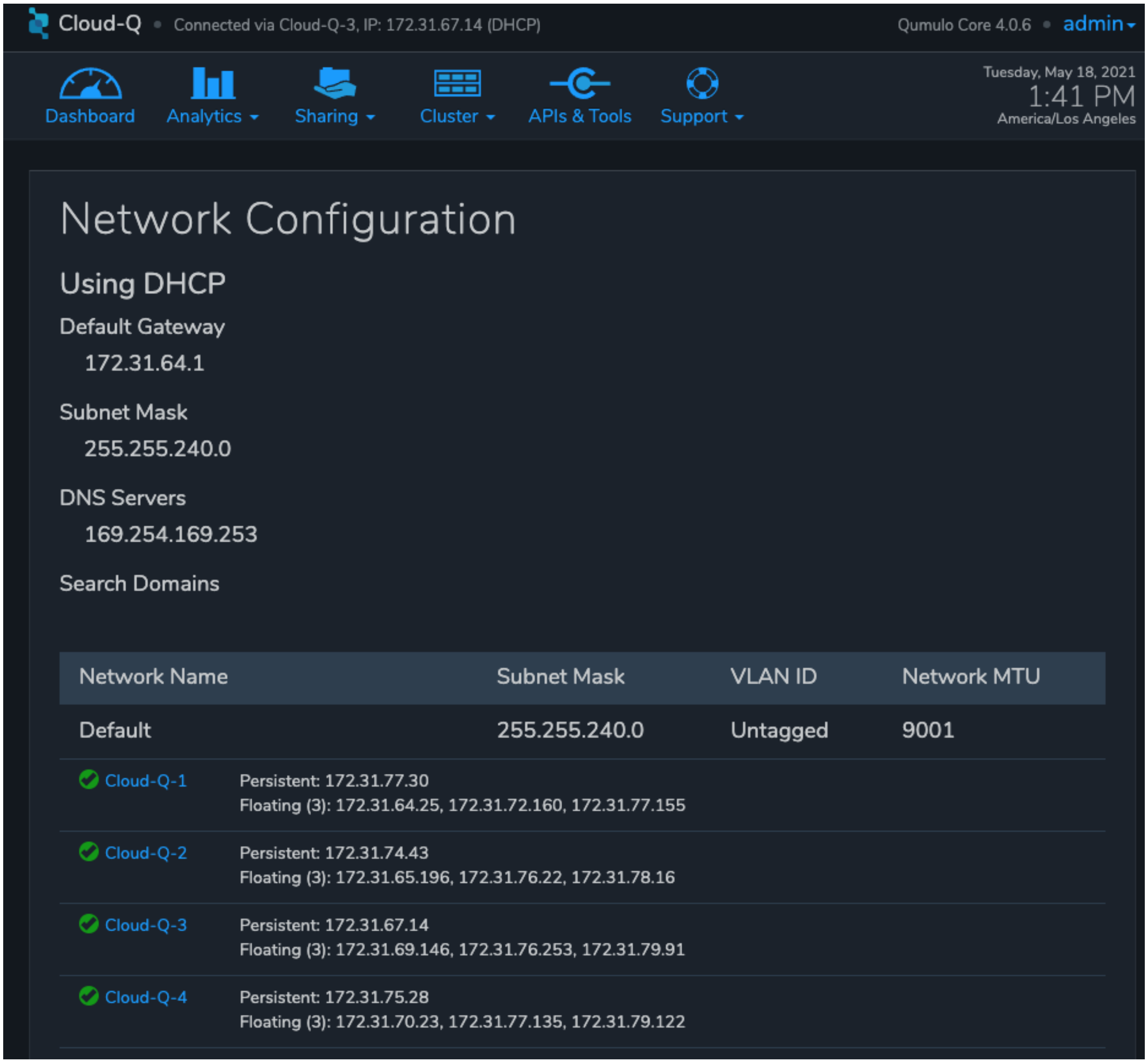
Protected

Files 0 0/min

Directories 0 0/min

Verify Floating IPs

Go to the **Cluster** tab and select **Network Configuration**. Each node will have a persistent IP. This is the EC2 primary IP address that is provided via DHCP at creation and subsequently never changes unless the instance is destroyed (i.e. terminated). Also, each node will have floating IPs associated with it. In this case the default of 3 floating IPs per instance was chosen. These IPs are EC2 secondary IPs that the cluster now manages as floating IPs. The AWS EC2 console will only display what EC2 secondary IPs were assigned to an instance at creation. For real-time status always refer to the Qumulo UI.



Network Configuration

Using DHCP

Default Gateway
172.31.64.1

Subnet Mask
255.255.240.0

DNS Servers
169.254.169.253

Search Domains

Network Name	Subnet Mask	VLAN ID	Network MTU
Default	255.255.240.0	Untagged	9001

✓ Cloud-Q-1	Persistent: 172.31.77.30 Floating (3): 172.31.64.25, 172.31.72.160, 172.31.77.155
✓ Cloud-Q-2	Persistent: 172.31.74.43 Floating (3): 172.31.65.196, 172.31.76.22, 172.31.78.16
✓ Cloud-Q-3	Persistent: 172.31.67.14 Floating (3): 172.31.69.146, 172.31.76.253, 172.31.79.91
✓ Cloud-Q-4	Persistent: 172.31.75.28 Floating (3): 172.31.70.23, 172.31.77.135, 172.31.79.122

Verify Sidecar User and Custom RBAC Configuration

Previously the Sidecar Lambda function connectivity to the cluster was verified. There's no need to review the Sidecar User and RBAC configuration. If you desire to review these they are under **Cluster** -> **Local Users & Groups** and **Cluster** -> **Role Management**, respectively.

Stack Update Options

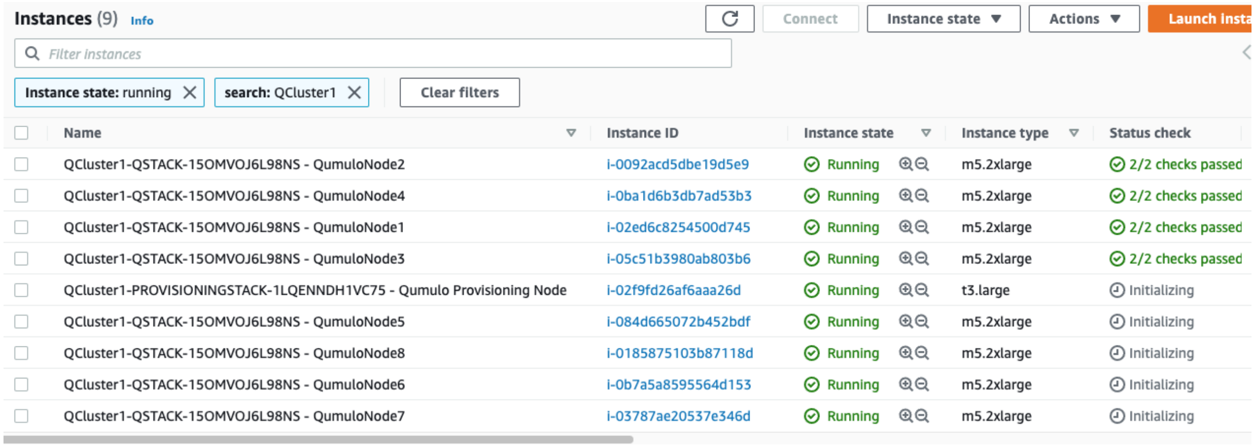
Adding Node(s) to the Cluster

A Qumulo cluster may be grown in both capacity and performance by adding additional nodes (EC2 instances) to the cluster. Each node added increases compute, networking, and storage capacity. To add nodes to a cluster follow the procedure below. Note, total instance count may only be increased, not decreased. If total instance count is decreased the stack update will fail and rollback.

IF you have upgraded the software on the cluster after initial deployment leave the software version for the cluster in the template as it was originally provisioned. The stack is unaware of this update and the software version field for the cluster can not be used for upgrades after initial deployment.

1. Go to the **CloudFormation** view in the AWS Console
2. Select the top-level stack name, **QCluster1** in this example
3. Select **Update** in the upper right corner
4. Keep the default **Use Current Template**
5. Select **Next**
6. The template as last populated will be displayed
7. Scroll down to the **Number of Qumulo EC2 Instances**
8. Increase the number of instances to the chosen value, **8** in this example
9. Select **Next**
10. Select **Next** again
11. **Check both boxes** acknowledging that CloudFormation may create IAM roles and that it may leverage CAPABILITY_AUTO_EXPAND.
12. Select **Update stack**

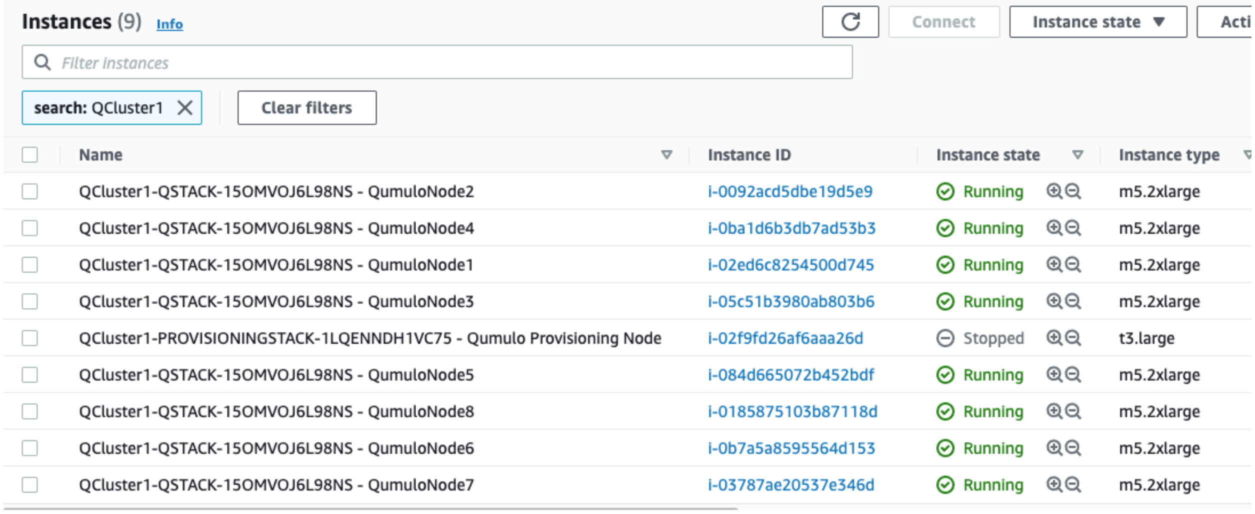
The stack will commence updating. In this case four nodes will be added to the cluster. This is not service impacting as the existing nodes are left untouched. There is a brief quorum bounce to add the four new nodes to the cluster. Below is a view of the AWS EC2 Console showing the new instances initializing.



□	Name	Instance ID	Instance state	Instance type	Status check
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode2	i-0092acd5dbe19d5e9	✓ Running	m5.2xlarge	✓ 2/2 checks passed
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode4	i-0ba1d6b3db7ad53b3	✓ Running	m5.2xlarge	✓ 2/2 checks passed
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode1	i-02ed6c8254500d745	✓ Running	m5.2xlarge	✓ 2/2 checks passed
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode3	i-05c51b3980ab803b6	✓ Running	m5.2xlarge	✓ 2/2 checks passed
□	QCluster1-PROVISIONINGSTACK-1LQENNDH1VC75 - Qumulo Provisioning Node	i-02f9fd26af6aaa26d	✓ Running	t3.large	Initializing
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode5	i-084d665072b452bdf	✓ Running	m5.2xlarge	Initializing
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode8	i-0185875103b87118d	✓ Running	m5.2xlarge	Initializing
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode6	i-0b7a5a8595564d153	✓ Running	m5.2xlarge	Initializing
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode7	i-03787ae20537e346d	✓ Running	m5.2xlarge	Initializing

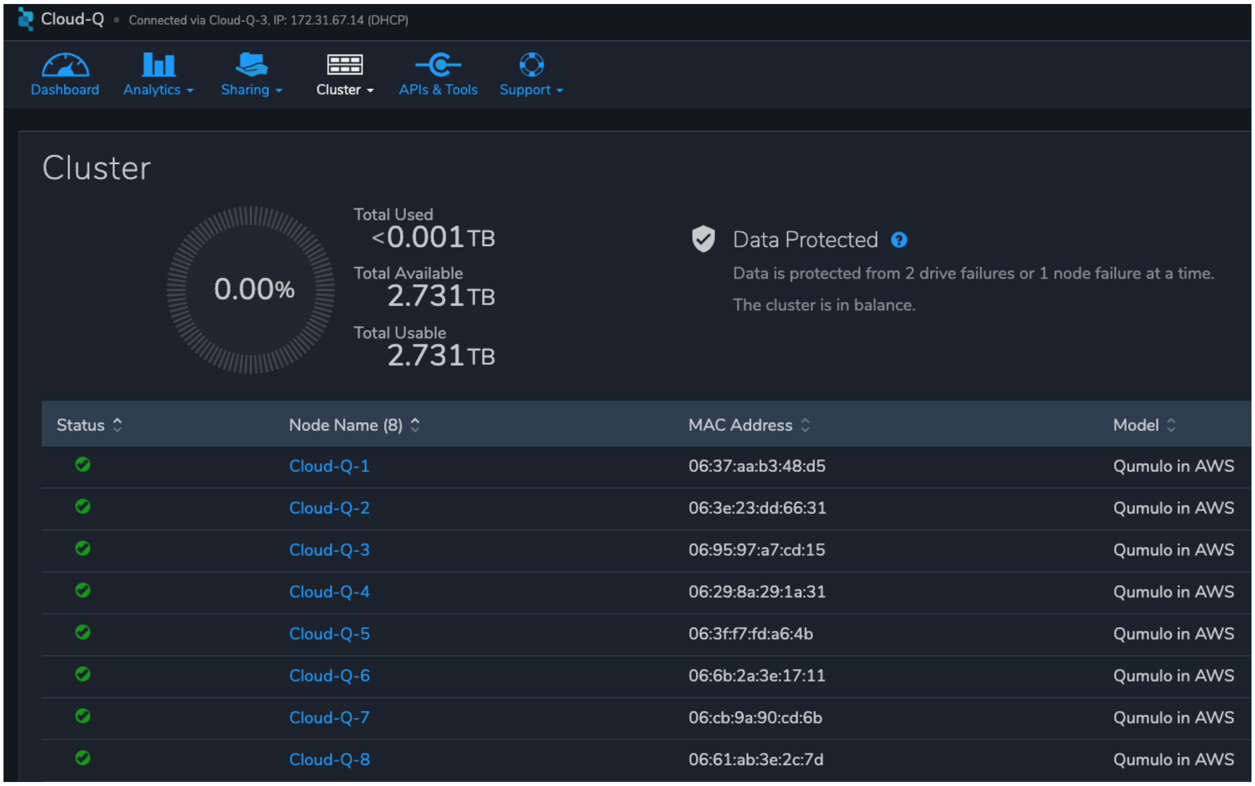
Notice that the Provisioning instance is also being restarted. This is by design. The Provisioner will query the latest version of software running on the cluster and upgrade all new nodes to this version of software before joining them to the cluster. Further, it tags all the new EBS volumes and updates the floating IPs.

This stack provisioned Public Management and Route 53 originally. With the addition of new nodes, IP addresses need to be added to the Load Balancer and the Route 53 Private Hosted Zone. The stack will automate these updates as well. You may review any nested stack to see what resources were modified or added in the stack **Events** tab. At the completion of node addition you may review any and all of the AWS infrastructure referencing the former section. As a final check make sure the Provisioning node shutdown which indicates success of all secondary provisioning.



□	Name	Instance ID	Instance state	Instance type
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode2	i-0092acd5dbe19d5e9	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode4	i-0ba1d6b3db7ad53b3	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode1	i-02ed6c8254500d745	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode3	i-05c51b3980ab803b6	✓ Running	m5.2xlarge
□	QCluster1-PROVISIONINGSTACK-1LQENNDH1VC75 - Qumulo Provisioning Node	i-02f9fd26af6aaa26d	⊖ Stopped	t3.large
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode5	i-084d665072b452bdf	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode8	i-0185875103b87118d	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode6	i-0b7a5a8595564d153	✓ Running	m5.2xlarge
□	QCluster1-QSTACK-15OMVOJ6L98NS - QumuloNode7	i-03787ae20537e346d	✓ Running	m5.2xlarge

Finally, login to the cluster and verify the node addition.



Cluster

0.00%

Total Used
<0.001TB
Total Available
2.731TB
Total Usable
2.731TB

Data Protected

Data is protected from 2 drive failures or 1 node failure at a time.

The cluster is in balance.

Status	Node Name (8)	MAC Address	Model
✓	Cloud-Q-1	06:37:aa:b3:48:d5	Qumulo in AWS
✓	Cloud-Q-2	06:3e:23:dd:66:31	Qumulo in AWS
✓	Cloud-Q-3	06:95:97:a7:cd:15	Qumulo in AWS
✓	Cloud-Q-4	06:29:8a:29:1a:31	Qumulo in AWS
✓	Cloud-Q-5	06:3f:f7:fd:a6:4b	Qumulo in AWS
✓	Cloud-Q-6	06:6b:2a:3e:17:11	Qumulo in AWS
✓	Cloud-Q-7	06:cb:9a:90:cd:6b	Qumulo in AWS
✓	Cloud-Q-8	06:61:ab:3e:2c:7d	Qumulo in AWS

Updating the Sidecar Software Version

A stack update may be used to update the Sidecar software version. Follow the same steps as a Node Addition, but change the Sidecar Software Version field to the desired version instead of changing the number of EC2 instances (steps 7 & 8 above). This is typically done after updating the cluster software via the Qumulo UI.

Removing or Adding Public Management

A stack update may be used to remove or add public management. Since this update is completely separate from the cluster there's no changes required to the cluster infrastructure or infrastructure touched by the Provisioning instance. Hence, it will not restart. Note, the MGMTNLBSTACK will be deleted when removing public management. This is expected. The stack will show as DELETE_FAILED for a period of time while CloudFormation retries the delete of the Elastic IP. Ultimately it will succeed.

Enabling or Disabling Audit Logging

A stack update may be used to enable or disable Qumulo audit logging. These logs are stored in a CloudWatch Logs log group. If a stack update is used to disable audit logging the log group will be deleted. Likewise, if audit logging is enabled in a stack update a log group will be created with the name **/qumulo/[Stack Name]**.

Other Stack Updates and the QSTACK Policy

The only restrictions placed on stack updates are for the Qumulo cluster. Specifically this is the QSTACK. The stack policy is applied by the Provisioning instance, and it forbids any modifications, deletions, or recreations of QSTACK EC2 and EBS infrastructure. This is to protect production environments from erroneous stack updates. In the event a stack update is attempted for an unsupported change the update will simply fail and rollback without harm. Many stack updates are possible and not all permutations have been tested. It is possible to change the R53 FQDN, but AWS requires the deletion of the current Private Hosted Zone and a new one will be rebuilt if the FQDN is modified in a stack update. In the stack update pages you can review the changes the update will make. The common examples are documented above that are most productive and well tested.

Changing Instance Types and EBS Volume Types

Qumulo does not support changing the cluster instance types with a stack update. This is prevented with the aforementioned stack policy. While it would be possible if allowed, it would stop all the instances, change the instance type, and restart them. This would be service impacting in a production environment. Instead Qumulo recommends shutting down an instance at a time so the cluster can leverage floating IPs and maintain the production workload.

Due to the permutations of EBS volume configurations the likelihood of user error is high attempting to change EBS volume types with a stack update. Rather than risk data loss this is blocked by the QSTACK policy.

For both instance type changes and EBS volume type changes Qumulo offers simple scripts that are production friendly.

Protecting Production Environments

In production deployments it is wise to enable Termination Protection for the entire stack. Multiple prompts are required to delete any infrastructure with Termination Protection enabled. To enable termination protection:

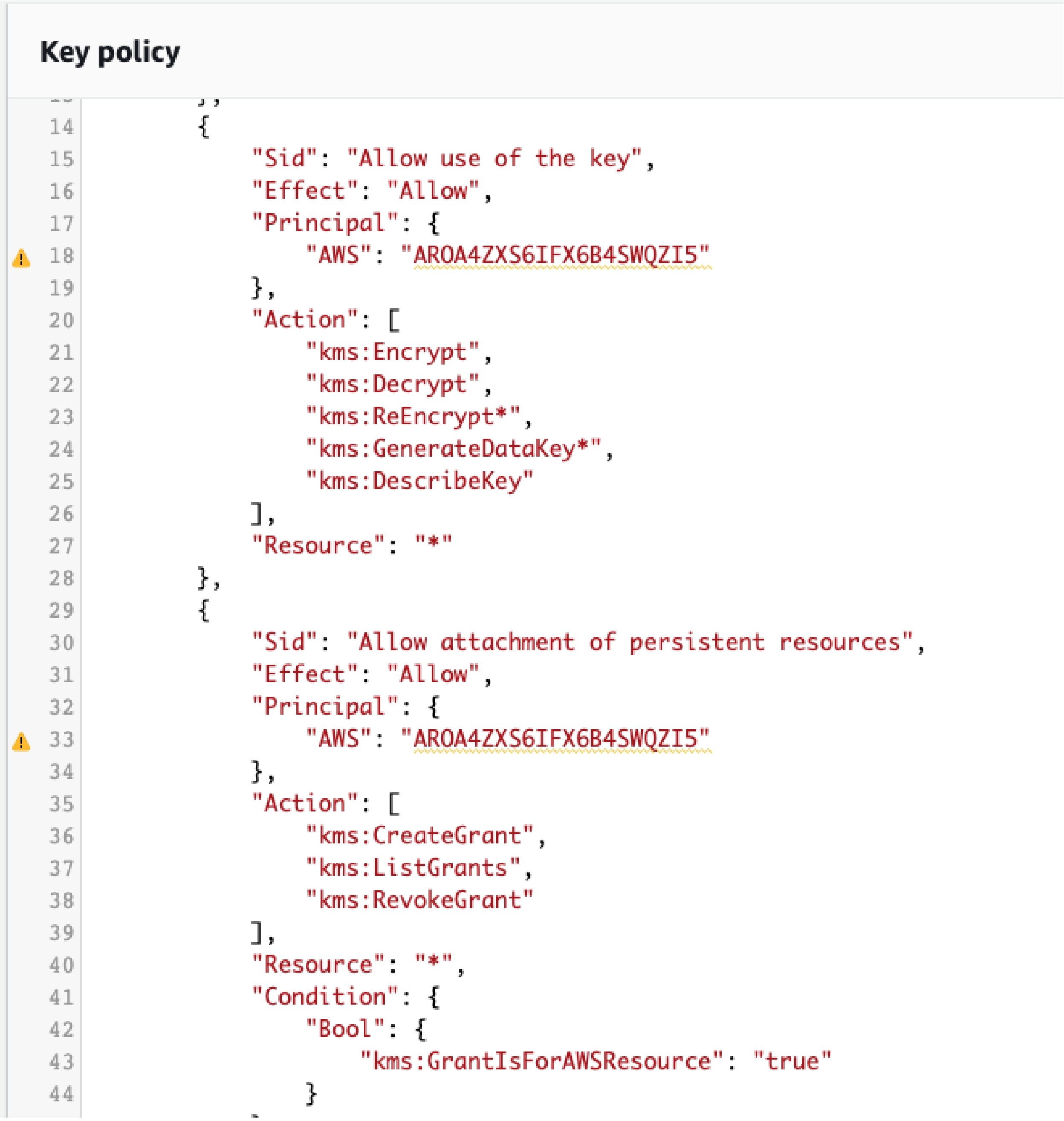
1. Go to the **CloudFormation** view in the AWS Console
2. Select the top-level stack name, **QCluster1** in this example
3. Select **Stack actions** in the upper right corner
4. Then select **Edit termination protection**
5. Select **Enabled**
6. Select **Save**

Deleting the Stack

When a cluster is no longer needed ensure all critical data has been removed from the cluster. Qumulo's SHIFT functionality may be used to natively copy data from the cluster to S3. Alternatively, Qumulo supports S3 Snapshots but rehydration will require a cluster with the same EBS volume configuration. Once the data has been archived with the chosen method simply select the **top-level stack** in CloudFormation and choose **Delete**. All resources will be deleted. Note, disable Termination Protection before deleting the stack if it was enabled.

If a Customer Managed Key was used for encryption at rest, the KMS CMK policy must be cleaned up. It's simplest to do this after the stack is completely deleted. AWS CloudFormation does not support CMK policy modifications so it is unable to track these changes that the Provisioning instance applied. Go to the **AWS Key Management Service** and select the **CMK** that was used. Then **Edit** the policy. **Delete** the two SIDs for the Sidecar and select **Save**. If the key policy had no other SIDs applied to it, aside from the Qumulo Sidecar SIDs, it will have the following JSON structure before and after being cleaned up.

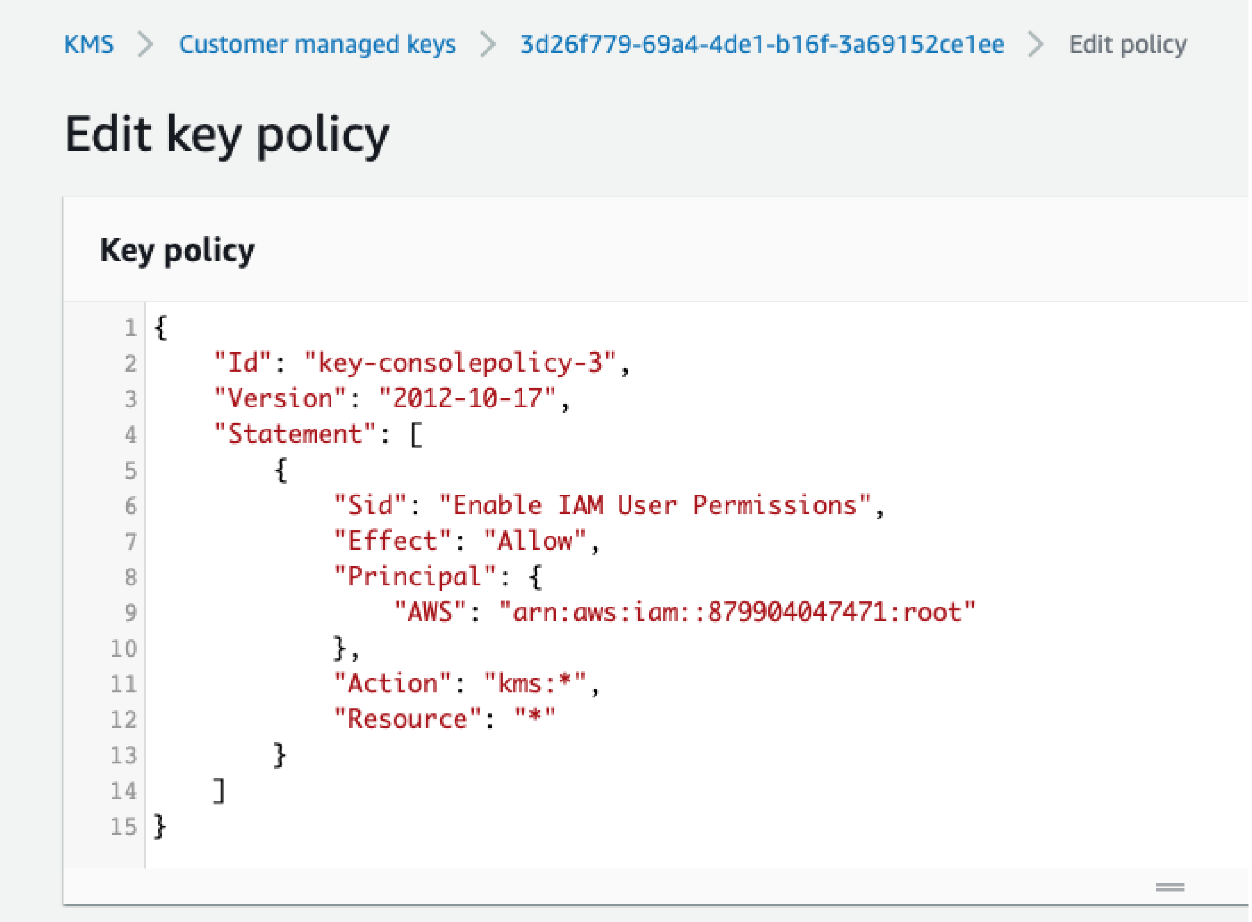
After Stack Deletion but before Cleanup



Key policy

```
        ],
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "AROA4ZXS6IFX6B4SWQZI5"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "AROA4ZXS6IFX6B4SWQZI5"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
```

After Cleanup



KMS > Customer managed keys > 3d26f779-69a4-4de1-b16f-3a69152ce1ee > Edit policy

Edit key policy

Key policy

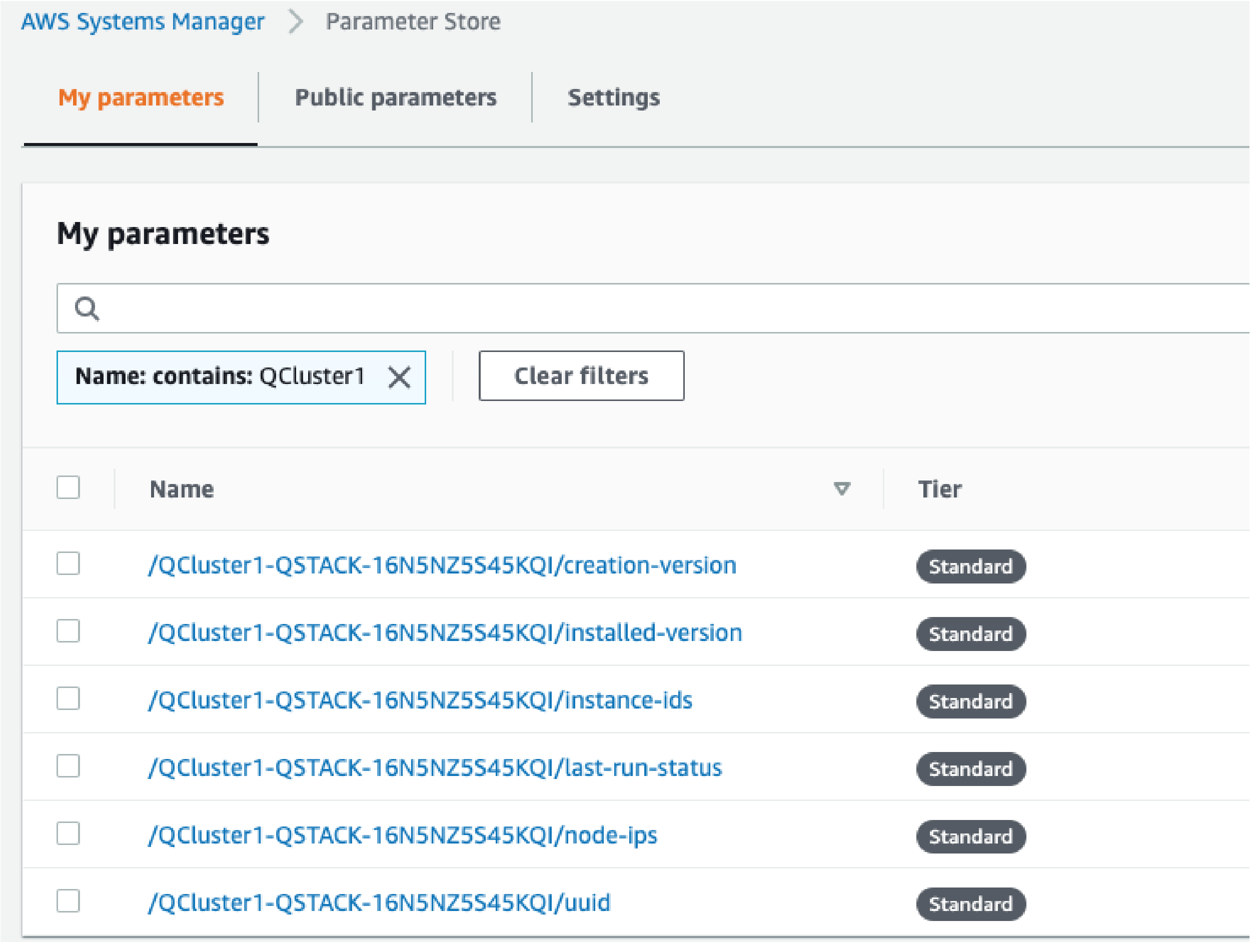
```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::879904047471:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

As of the date of this document AWS CloudFormation will fail to delete all of the MGMTNLB stack resources (If Public Management was provisioned). Simply let the deletion finish, reselect the MGMTNLB stack and delete it again, and then delete the top-level stack.

Troubleshooting

Where’s the UUID for the cluster?

The Provisioning instance grabs a copy of the UUID for the cluster after the first quorum is formed. Go to **Parameter Store** and filter on the top-level stack name. The following parameters are stored by the Provisioning instance. The UUID is last on the list. Select it to view the UUID.



My parameters

Name: contains: QCluster1

	Name	Tier
□	/QCluster1-QSTACK-16N5NZ5S45KQI/creation-version	Standard
□	/QCluster1-QSTACK-16N5NZ5S45KQI/installed-version	Standard
□	/QCluster1-QSTACK-16N5NZ5S45KQI/instance-ids	Standard
□	/QCluster1-QSTACK-16N5NZ5S45KQI/last-run-status	Standard
□	/QCluster1-QSTACK-16N5NZ5S45KQI/node-ips	Standard
□	/QCluster1-QSTACK-16N5NZ5S45KQI/uuid	Standard

The Stack failed on the first nested stack, SECRETSSTACK

The S3 Bucket, Key Name Prefix, or Object URL are not correct. Delete the stack and relaunch the template with the correct S3 parameters. Do NOT use the S3 URL. The stack will fail.

The Stack failed when provisioning the QSTACK

The four most common causes for this are:

1. An AWS Marketplace offer has not been accepted for the AMI ID that was chosen
2. The EBS volumes configuration doesn't match the AMI ID
3. The cluster failed to place in the placement group

Review the AMI ID and marketplace subscriptions. Double check the EBS volume config selected in the template. If the cluster failed to place, choose a different AZ to deploy the cluster in to find more available resources by selecting a different private subnet ID within the VPC. Delete the failed stack and relaunch the template after rectifying the problem.

The Stack Update failed and rolled back

No harm is done. No Qumulo Cluster parameters for the QSTACK, except the Number of EC2 Instances, can be changed. The number of instances can't be decreased.

The Cluster didn't form quorum

The four most common causes for this are:

1. The software version specified in the template doesn't exist
2. The software version specified in the template is older than the AMI software version
3. The S3 Bucket Region specified is incorrect
4. The VPC doesn't have public internet access, see **The Provisioning instance didn't shutdown**

Check for typos by reviewing the parameters entered in the template in the CloudFormation console. Review what version of Qumulo Core the AMI ID shipped with. This can be found in the Parameter Store under the top-level stack name/creation-version. This can also be found in the marketplace subscription. If an older version is needed use an older AMI ID. Finally, double check the S3 Bucket Region entered in the template.

The Provisioning instance didn't shutdown

Common Causes

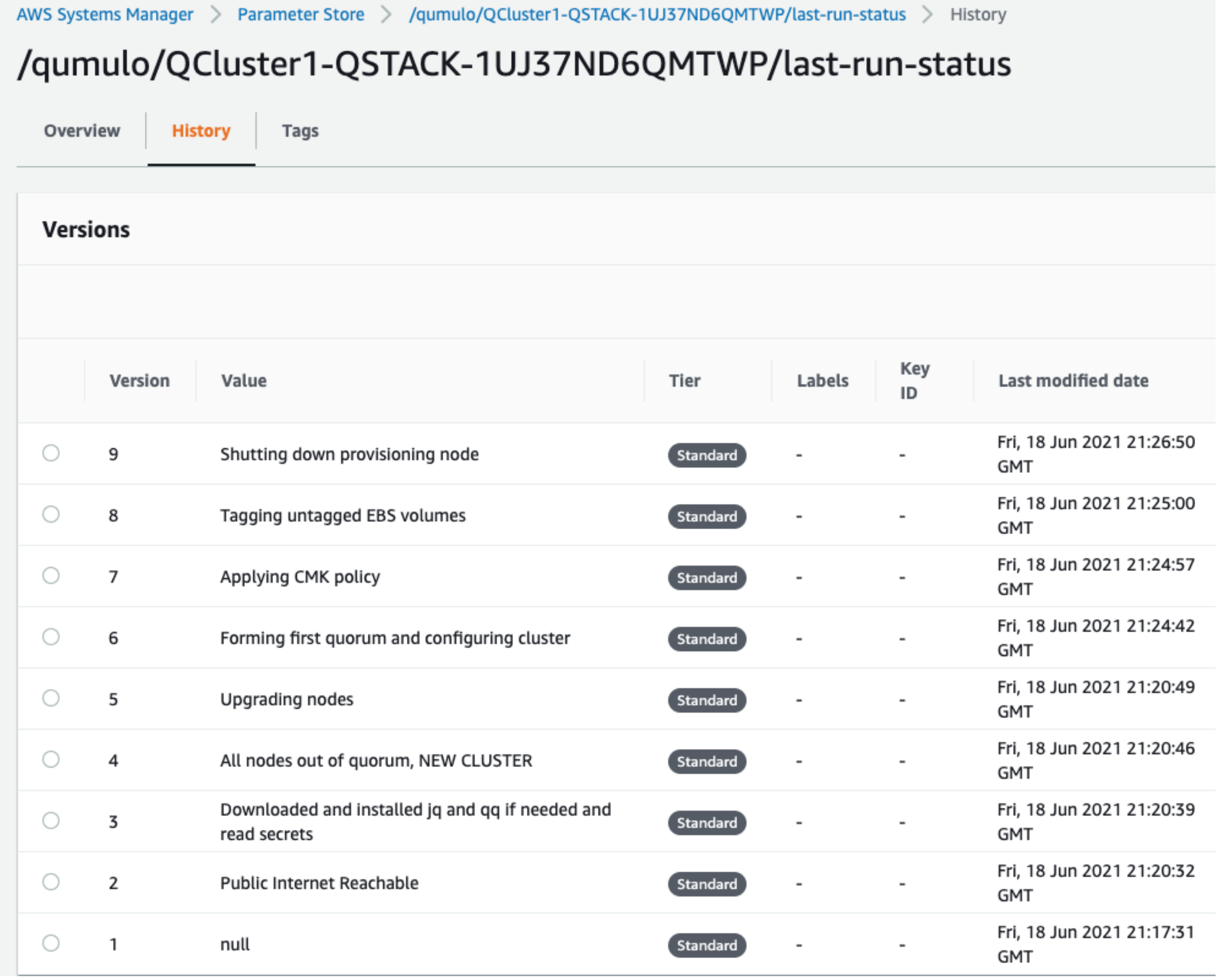
The two most common causes for this are:

1. The VPC doesn't have access to the public Internet or DNS resolution is not functioning. Without access to public infrastructure the Provisioning instance can't talk to AWS services like Secrets Manager, KMS, Parameter Store, or download the desired version of Qumulo Core software. Review the public and private subnets, their route tables, and the NAT Gateway. Review the AWS Parameter Store **last-run-status** to verify public internet connectivity (see the section below on last-run-status). Also double check that there are no Network ACLs blocking traffic.
2. A Customer Managed Key was provisioned and the policy was unable to be modified for the CMK because the policy didn't have valid SIDs before the template was launched.

Cleanup the CMK, correct the VPC infrastructure, delete the failed stack, and relaunch the template. See the section below 'Provisioning Instance Logic Diagram' for further troubleshooting details on the provisioning instance.

AWS Parameter Store last-run-status

If the Provisioning instance doesn't automatically shutdown, the AWS Systems Manager Parameter Store **last-run-status** parameter may be checked to see where it stopped. As shown below, the parameter history shows the major blocks in the code the provisioning instance executes. In this example QCluster1 was built for the first time as noted by the NEW CLUSTER update to the last-run-status parameter.



AWS Systems Manager > Parameter Store > /qumulo/QCluster1-QSTACK-1UJ37ND6QMTWP/last-run-status > History

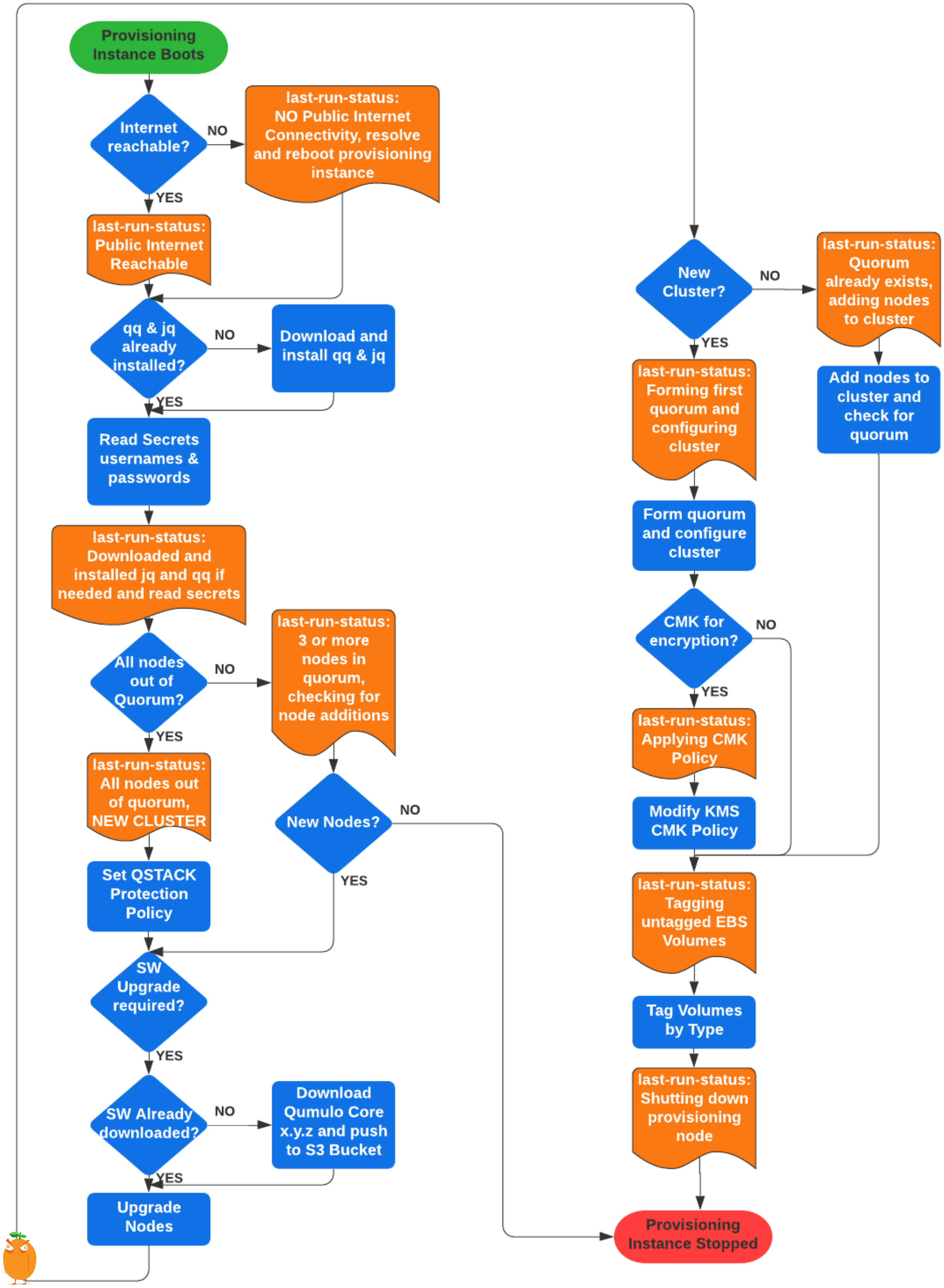
/qumulo/QCluster1-QSTACK-1UJ37ND6QMTWP/last-run-status

Versions

	Version	Value	Tier	Labels	Key ID	Last modified date
○	9	Shutting down provisioning node	Standard	-	-	Fri, 18 Jun 2021 21:26:50 GMT
○	8	Tagging untagged EBS volumes	Standard	-	-	Fri, 18 Jun 2021 21:25:00 GMT
○	7	Applying CMK policy	Standard	-	-	Fri, 18 Jun 2021 21:24:57 GMT
○	6	Forming first quorum and configuring cluster	Standard	-	-	Fri, 18 Jun 2021 21:24:42 GMT
○	5	Upgrading nodes	Standard	-	-	Fri, 18 Jun 2021 21:20:49 GMT
○	4	All nodes out of quorum, NEW CLUSTER	Standard	-	-	Fri, 18 Jun 2021 21:20:46 GMT
○	3	Downloaded and installed jq and qq if needed and read secrets	Standard	-	-	Fri, 18 Jun 2021 21:20:39 GMT
○	2	Public Internet Reachable	Standard	-	-	Fri, 18 Jun 2021 21:20:32 GMT
○	1	null	Standard	-	-	Fri, 18 Jun 2021 21:17:31 GMT

Provisioning instance flow chart

The provisioning instance executes the code in user data every boot cycle. The abbreviated logic diagram below shows the major branches and AWS SSM Parameter Store values for **last-run-status** throughout the execution of the code.


Provisioning Instance Boots
Internet reachable?
NO
last-run-status: NO Public Internet Connectivity, resolve and reboot provisioning instance
YES
last-run-status: Public Internet Reachable
qq & jq already installed?
NO
Download and install qq & jq
YES
Read Secrets usernames & passwords
last-run-status: Downloaded and installed jq and qq if needed and read secrets
All nodes out of Quorum?
NO
last-run-status: 3 or more nodes in quorum, checking for node additions
YES
last-run-status: All nodes out of quorum, NEW CLUSTER
New Nodes?
NO
YES
Set QSTACK Protection Policy
SW Upgrade required?
YES
SW Already downloaded?
NO
Download Qumulo Core x.y.z and push to S3 Bucket
YES
Upgrade Nodes
New Cluster?
NO
last-run-status: Quorum already exists, adding nodes to cluster
Add nodes to cluster and check for quorum
YES
last-run-status: Forming first quorum and configuring cluster
Form quorum and configure cluster
CMK for encryption?
NO
YES
last-run-status: Applying CMK Policy
Modify KMS CMK Policy
last-run-status: Tagging untagged EBS Volumes
Tag Volumes by Type
last-run-status: Shutting down provisioning node
Provisioning Instance Stopped

Download the Provisioning instance log

In the event none of the troubleshooting steps help to rectify the problems it’s likely the Provisioning instance log will be helpful. To retrieve the log follow these steps:

1. Go to the AWS Console **EC2 Instances** page
2. **Check the box** beside the Provisioning instance
3. Select **Actions** in the upper right corner
4. Select **Monitor & troubleshoot**
5. Select **Get system log**
6. Select Download in the upper right corner

Feel free to review the log right in the AWS console or download it to collaborate with Qumulo to resolve the problem. Often the log will show an obvious error pointing you to the resolution.