Cloud Q Quick Start
Deleting the CloudFormation Stack
Dack Busch, Dec 10th, 2021

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 Once the data has been archived with the chosen method then use CloudFormation to update the stack to **Disable Termination Protection**. Finally, select the **top-level stack** in CloudFormation and choose **Delete**. All resources will be deleted.

Cleanup Customer Managed Key policy in KMS

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.

Before manual cleanup but after stack deletion:

```
Key policy

14        },
         {
15             "Sid": "Allow use of the key",
16             "Effect": "Allow",
17             "Principal": {
⚠ 18               "AWS": "AROA4ZXS6IFX6B4SWQZI5"
19             },
20             "Action": [
21                 "kms:Encrypt",
22                 "kms:Decrypt",
23                 "kms:ReEncrypt*",
24                 "kms:GenerateDataKey*",
25                 "kms:DescribeKey"
26             ],
27             "Resource": "*"
28        },
29         {
30             "Sid": "Allow attachment of persistent resources",
31             "Effect": "Allow",
32             "Principal": {
⚠ 33               "AWS": "AROA4ZXS6IFX6B4SWQZI5"
34             },
35             "Action": [
36                 "kms:CreateGrant",
37                 "kms:ListGrants",
38                 "kms:RevokeGrant"
39             ],
40             "Resource": "*",
41             "Condition": {
42                 "Bool": {
43                     "kms:GrantIsForAWSResource": "true"
44                 }
```

After manual cleanup:

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

Edit key policy

Key policy

```
1  {
2      "Id": "key-consolepolicy-3",
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6              "Sid": "Enable IAM User Permissions",
7              "Effect": "Allow",
8              "Principal": {
9                  "AWS": "arn:aws:iam::879904047471:root"
10             },
11             "Action": "kms:*",
12             "Resource": "*"
13         }
14     ]
15 }
```