Enabling MFA Delete for AWS S3 Buckets

Introduction

When working with S3 Versioning in Amazon S3 buckets, you can optionally add another layer of security by configuring a bucket to enable MFA (multi-factor authentication) delete. When you do this, the bucket owner must include two forms of authentication in any request to delete a version or change the versioning state of the bucket.

- from AWS documentation

Details

- Only the **root account** for the AWS account can enable MFA delete for an S3 bucket.
- For most Cornell AWS accounts, the CIT Cloud Team manages the root credentials. If you would like to have MFA delete enabled for a bucket and the Cloud Team manages the root credentials, please submit a ticket to cloud-support@cornell.edu including the following information:
  - AWS account ID or moniker for the account
  - name of the target bucket – please create the bucket prior to making the request

CLI Command for Enabling MFA Delete

Beyond needing root credentials to enable MFA delete, there are additional requirements:

- MFA delete can be enabled only via the AWS CLI or SDK. It cannot be enabled via the AWS S3 web console.
- Since the root user in Cornell AWS accounts is generally not allowed to have AWS access keys configured, the root user must *temporarily* create access keys to use with the CLI/SDK.
  - One might think that a work-around for the access keys requirement would be to use the AWS CloudShell, which automatically creates temporary access keys for CLI commands. However, those temporary access keys won't work for enabling MFA delete. The access keys must be standard access keys for the root user (but with such keys configured in CloudShell you can issue the CLI command from there).
  - ⚠️ Be sure that any root user access keys created for enabling MFA delete are deleted immediately after use.

```
# Virtual MFA token
aws s3api put-bucket-versioning \
    --bucket BUCKET_NAME \
    --versioning-configuration Status=Enabled,MFADelete=Enabled \
    --mfa "arn:aws:iam::123456789012:mfa/root-account-mfa-device MFA_CODE"

# -OR-
# Physical MFA token
aws s3api put-bucket-versioning \
    --bucket BUCKET_NAME \
    --versioning-configuration Status=Enabled,MFADelete=Enabled \
    --mfa "MFA_SERIAL_NUMBER MFA_CODE"
```

- BUCKET_NAME is the name (not ARN) of the bucket for which you wish to enable MFA delete. E.g., "my-important-bucket".
- The argument to the "mfa" parameter is a string made up of the ARN (virtual), or serial number (physical), of the MFA device, followed by a space, followed by the 6-digit code from the MFA device.
- This command also enables versioning for the bucket; versioning is a prerequisite for enabling MFA delete.

References

- Cornell documentation
  - Standard AWS Account Configurations
- AWS documentation
  - Configuring MFA delete
  - Creating access keys for the root user