Michael Nguyen
12/15/2024
MET CS690 E2-IND
Professor Zhang

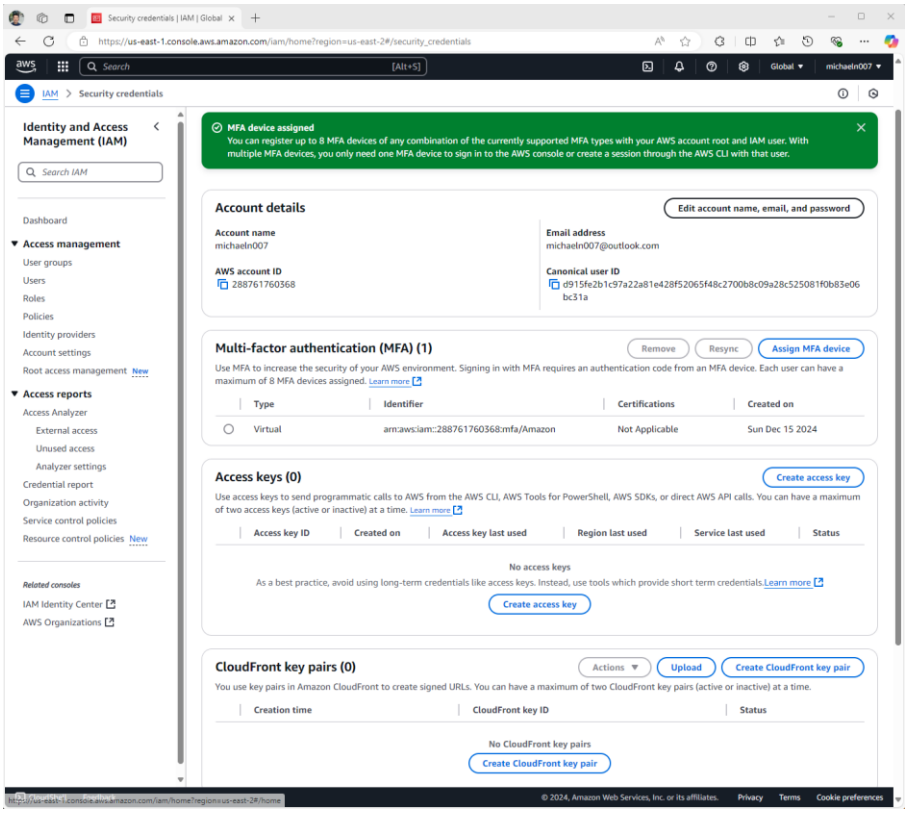
Lab 4 Brief Instruction

In this lab, we will follow Amazon Security Workshop to perform several IAM tasks. You want to follow the instructions given in the workshop and screenshot the outputs for each step.

The link to the workshop: https://catalog.workshops.aws/well-architected-security/en-US
We do not need to do all the tasks for this lab, but only the following (it is your discretion to continue other tasks if you are interested):

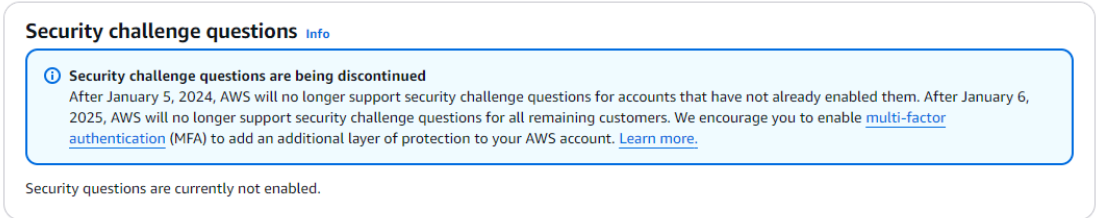
1. Security Foundations
    a. AWS Account Setup and Root User

1.1-1.2 – Enable a Virtual MFA Device for Your AWS Account Root User



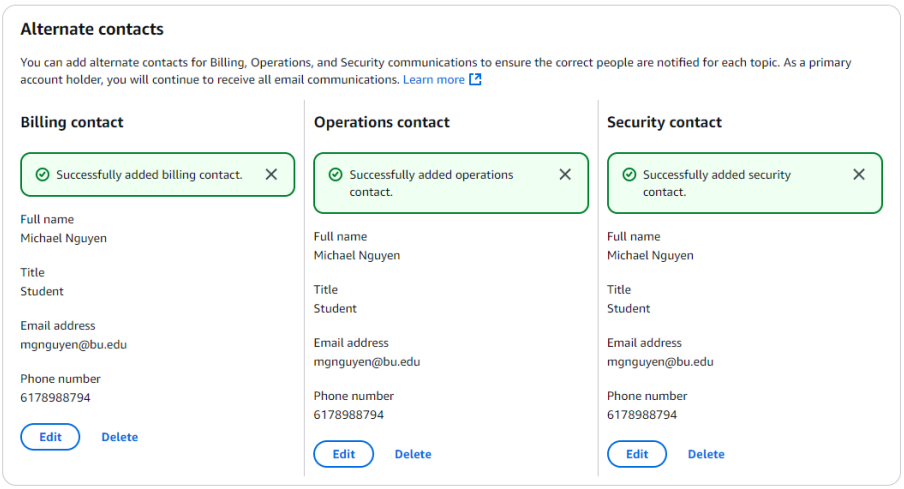
Creating an AWS Account and adding an MFA.

1.3 Configure Account Security Challenge Questions



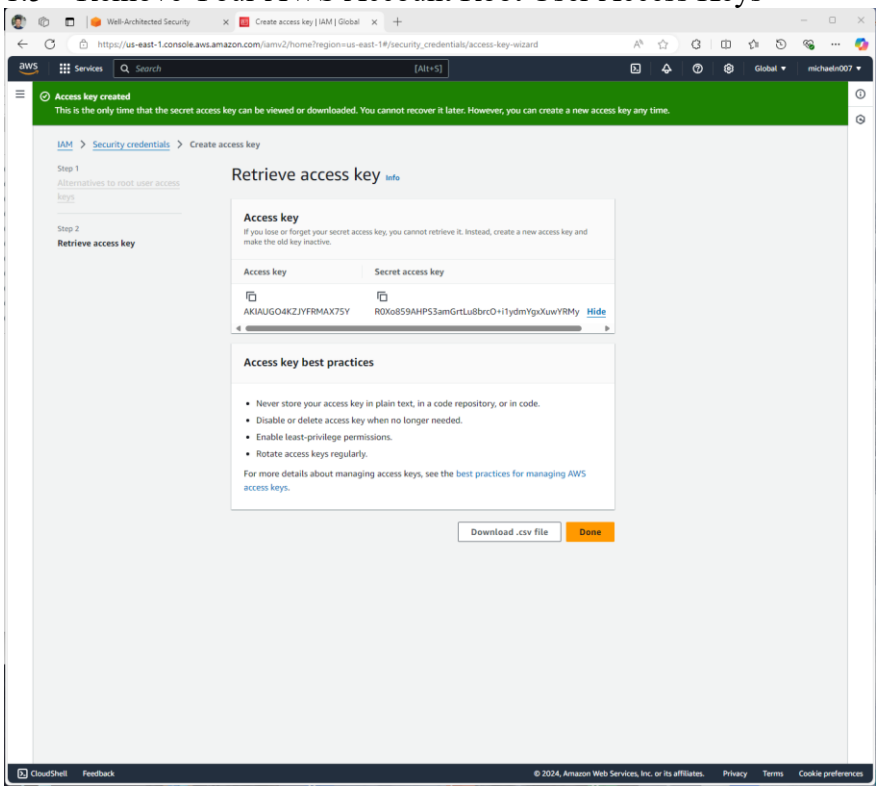
Configure Account Security Challenge Questions, however, it is discontinued after January 5th of 2024.

1.4 - Configure Account Alternate Contacts



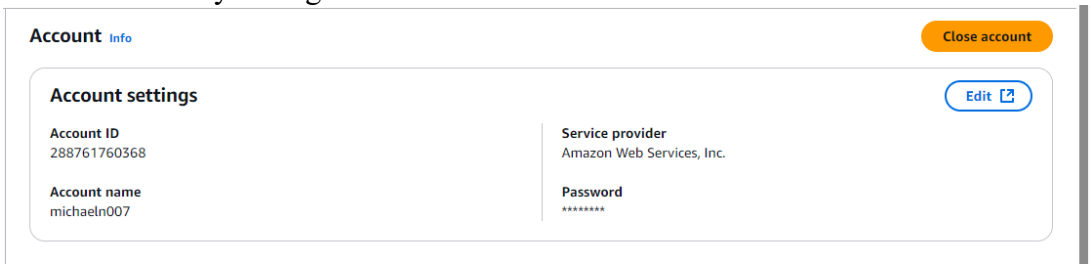
Configuring the Account Alternate Contacts

1.5 – Remove Your AWS Account Root User Access Keys



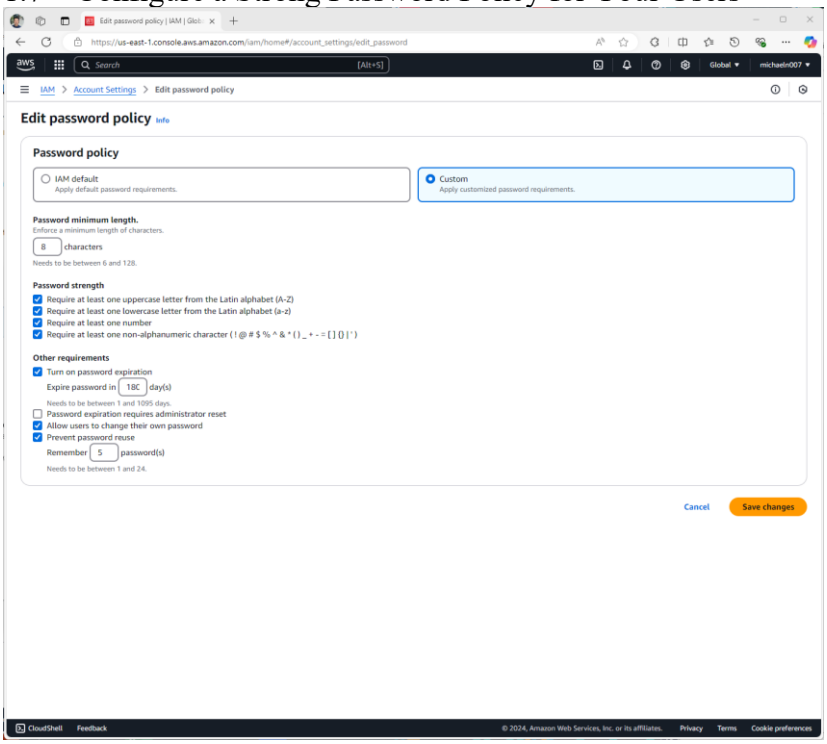
Creating an AWS Account Root User Access Key.

1.6 – Periodically Change the AWS Account Root User Password



*Setting an account password policy for IAM user, however the policy does not apply to your AWS account root user (a minimum of 8 characters and a maximum of 128 characters. - Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * () <> [] {} | _ + - = symbols. - Not be identical to your AWS account name or email address).*

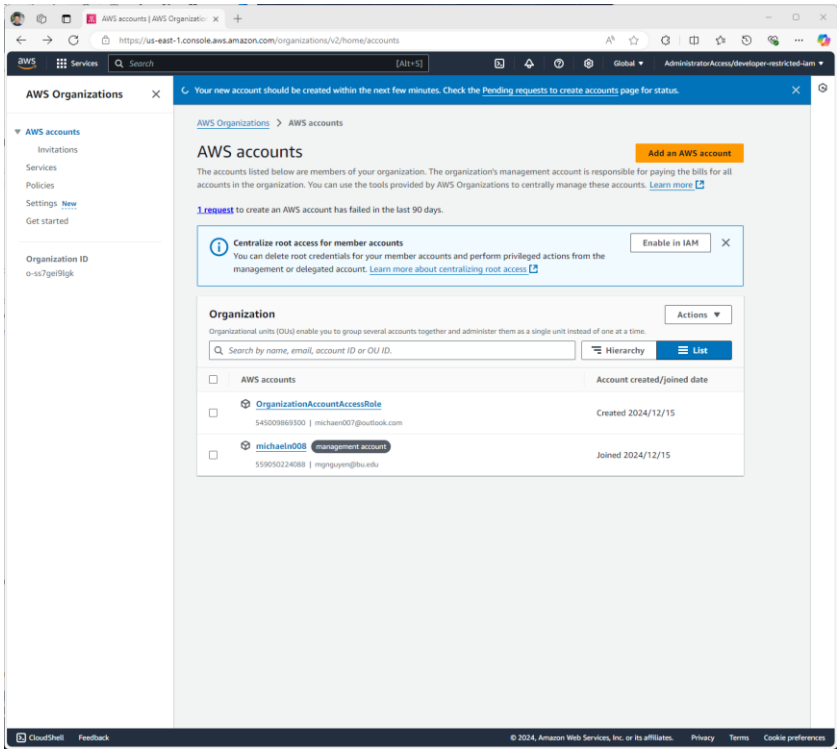
1.7 – Configure a Strong Password Policy for Your Users



Configuring a Custom Password Policy for Users

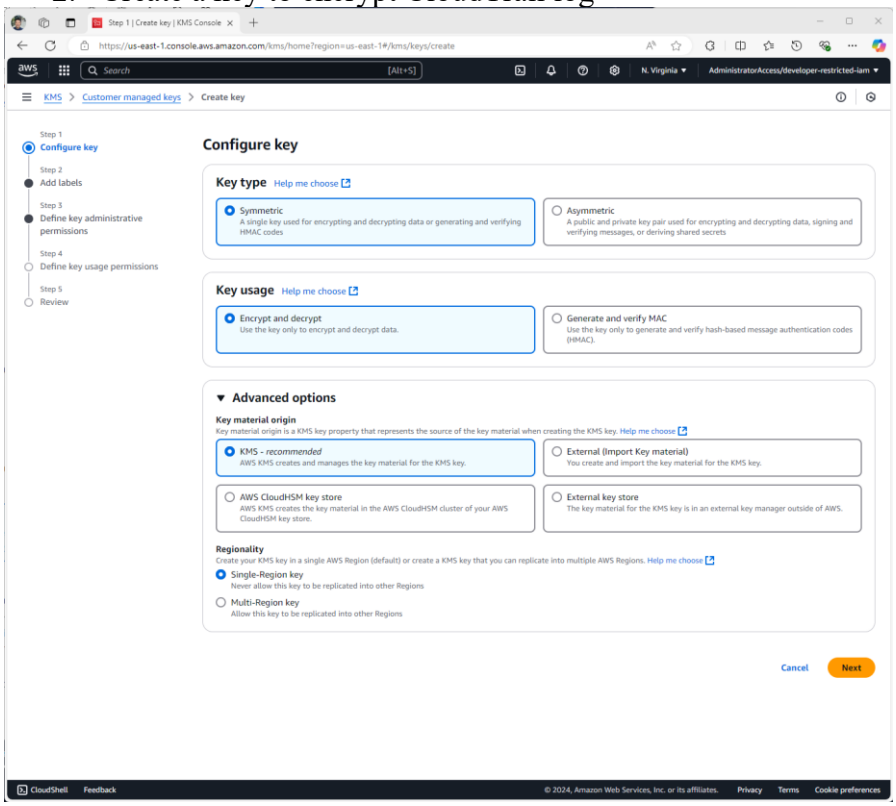
b. Creating data bunker account in console

1. Create a logging account from the organizations management account

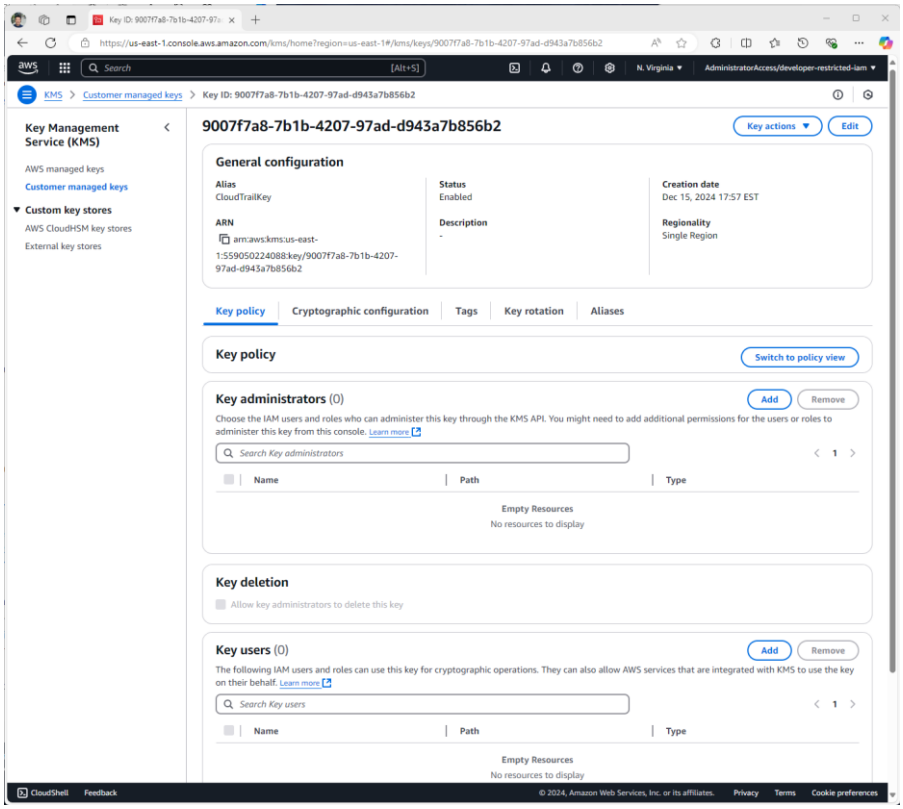


Created an OrganizationAccountAccessRole

2. Create a key to encrypt CloudTrail log

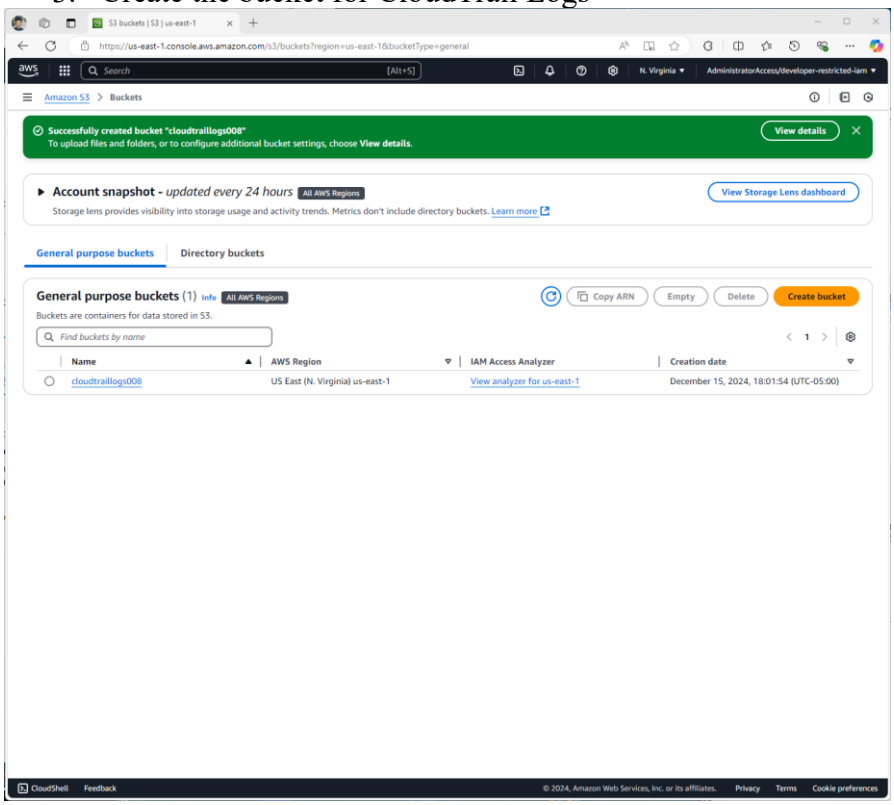


Configuring CloudTrailKey

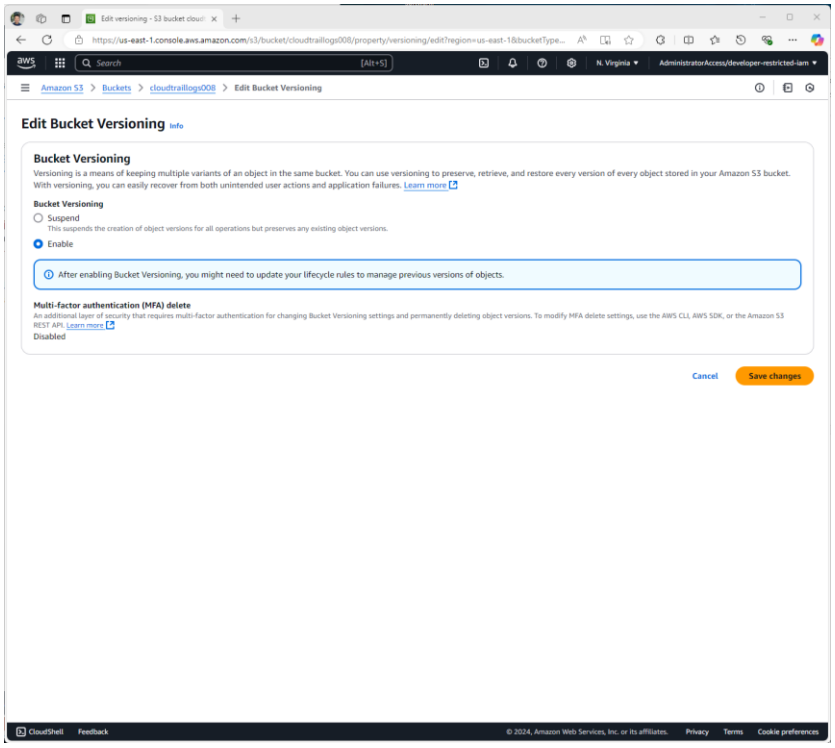


CloudTrailKey information

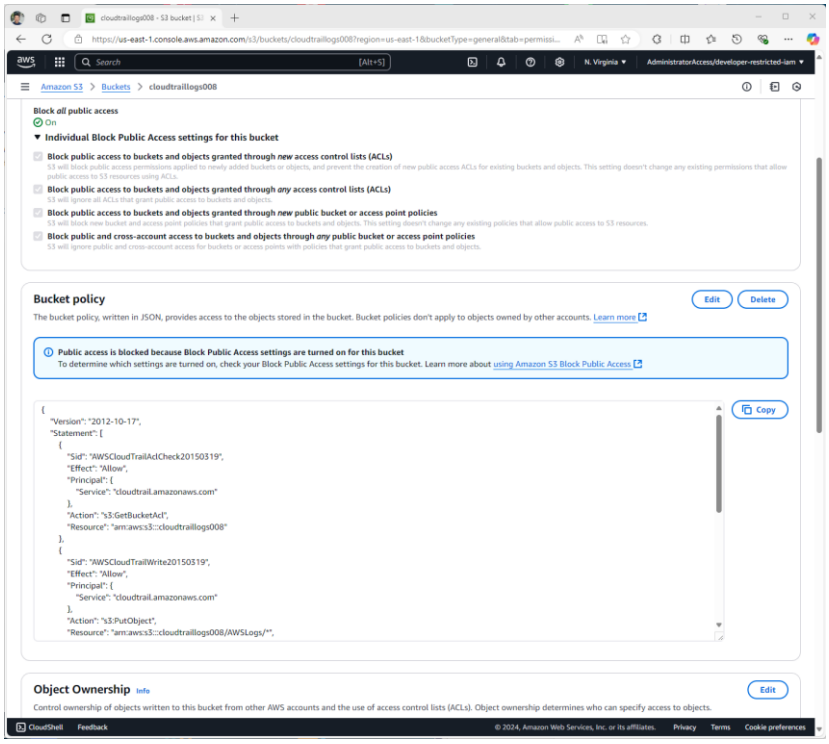
3. Create the bucket for CloudTrail Logs



Creating a bucket for Cloud Trail Logs

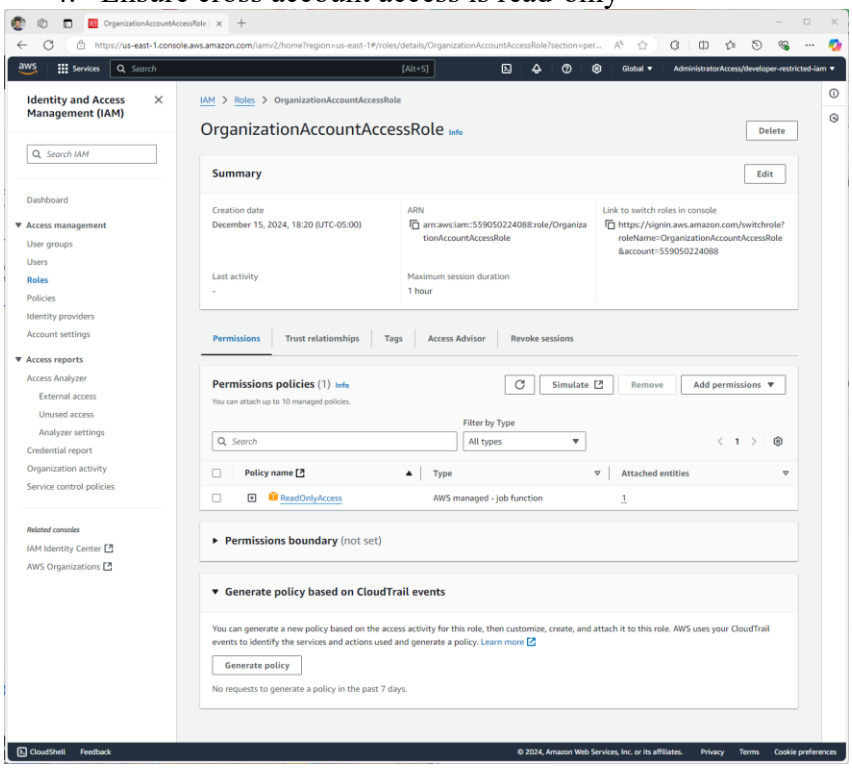


Enable bucket visioning

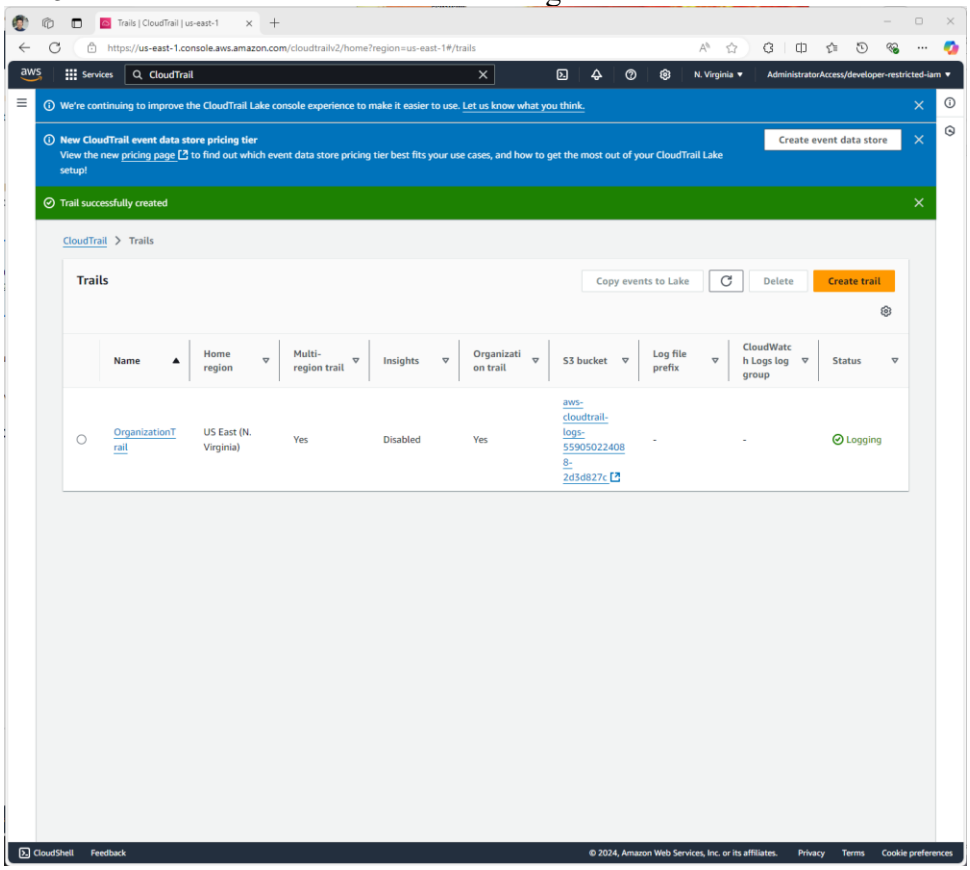


Creating a bucket policy in the Permissions tab

4. Ensure cross account access is read-only



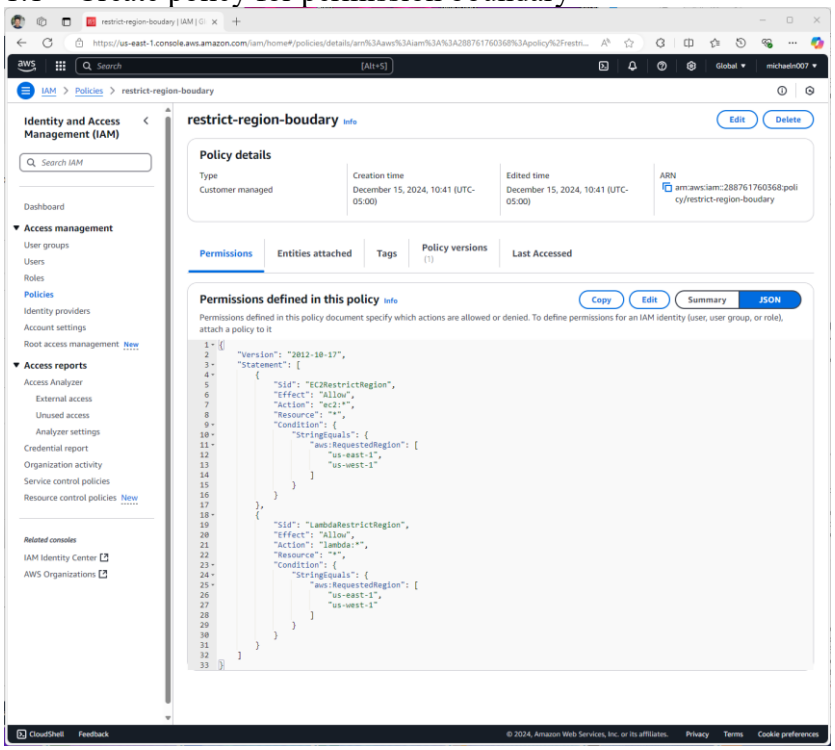
5. Turn on CloudTrail from the management account



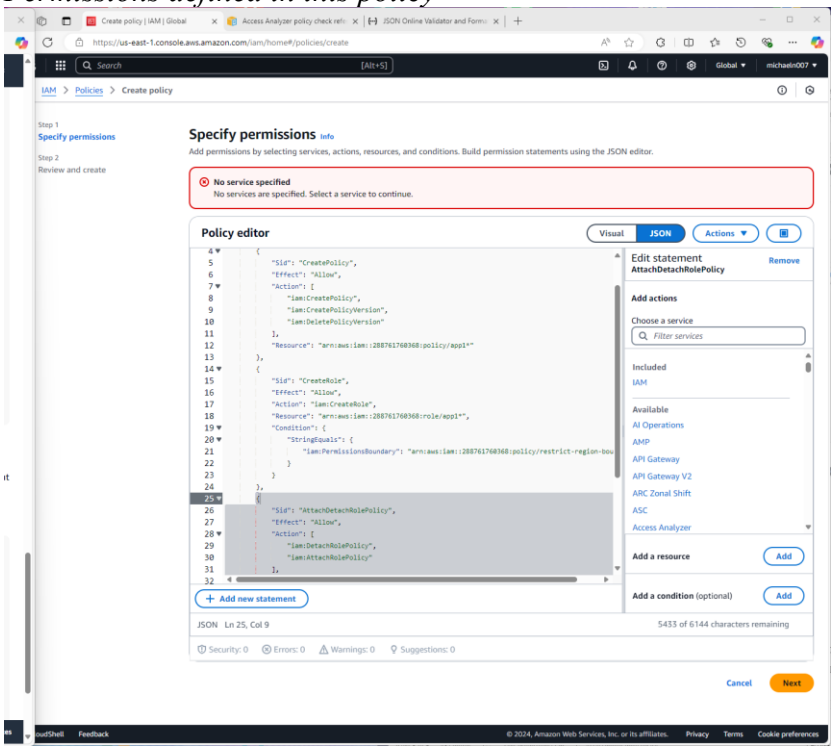
Creating a Cloud Trail Logs account

2. Identity and Access Management
    a. IAM Permission Boundaries Delegating Role Creation

1.1 – Create policy for permission boundary

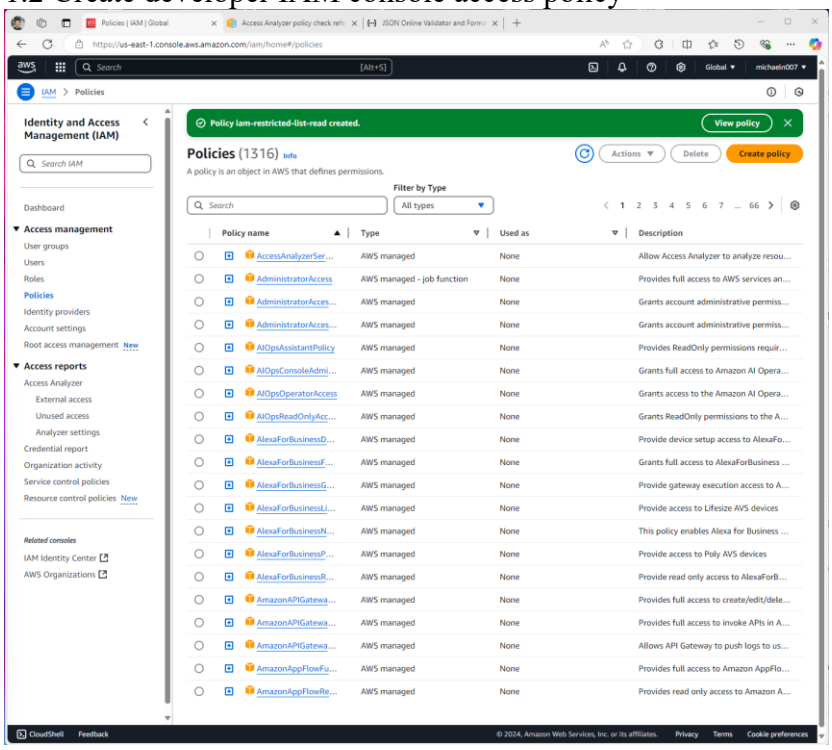


Permissions defined in this policy



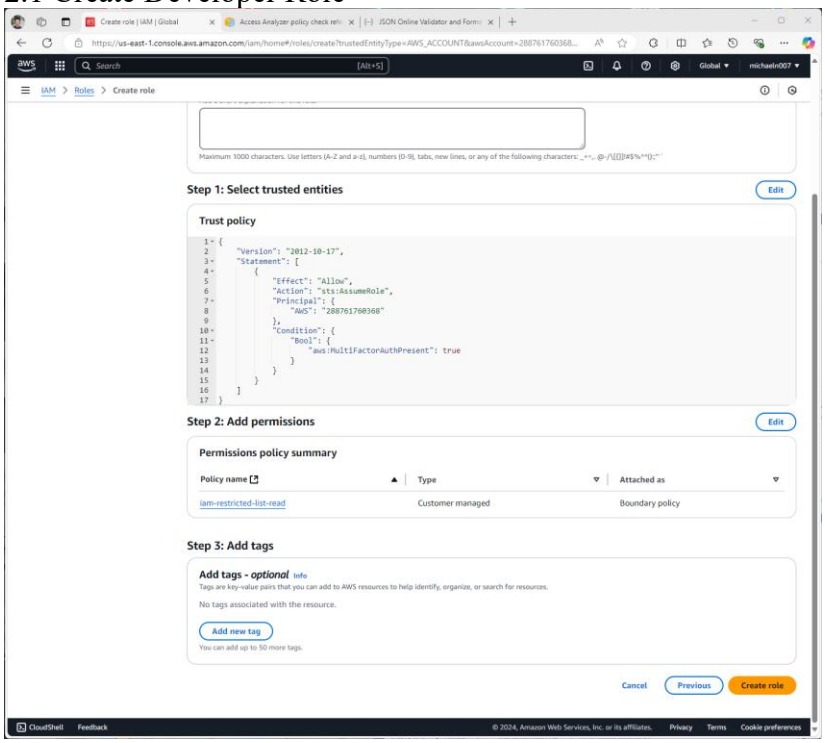
Creating a createrole-restrict-region-boundary with account id placeholders

1.2 Create developer IAM console access policy



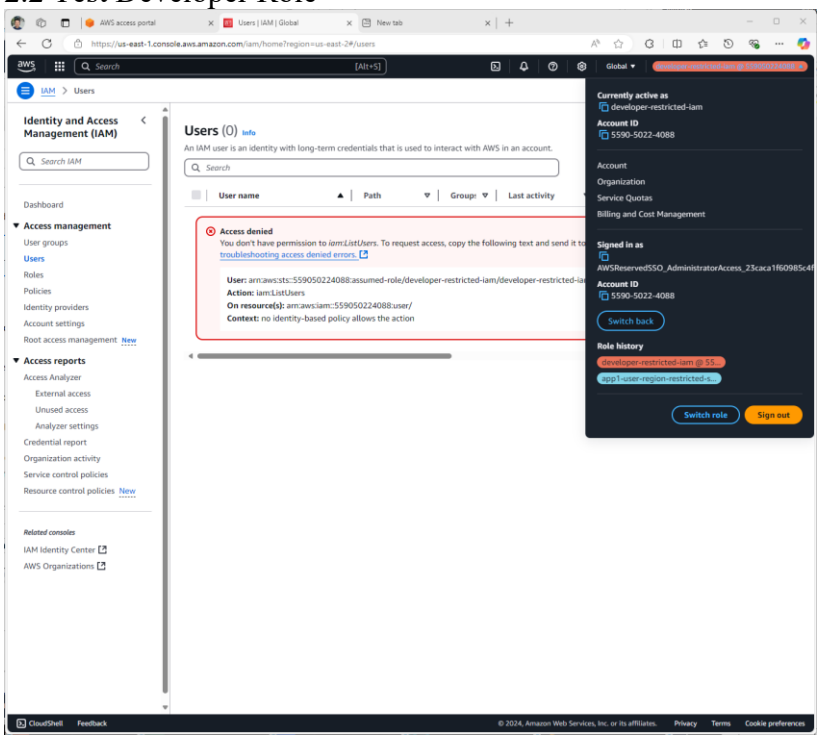
Creating an iam-restricted-list-read policy

2.1 Create Developer Role



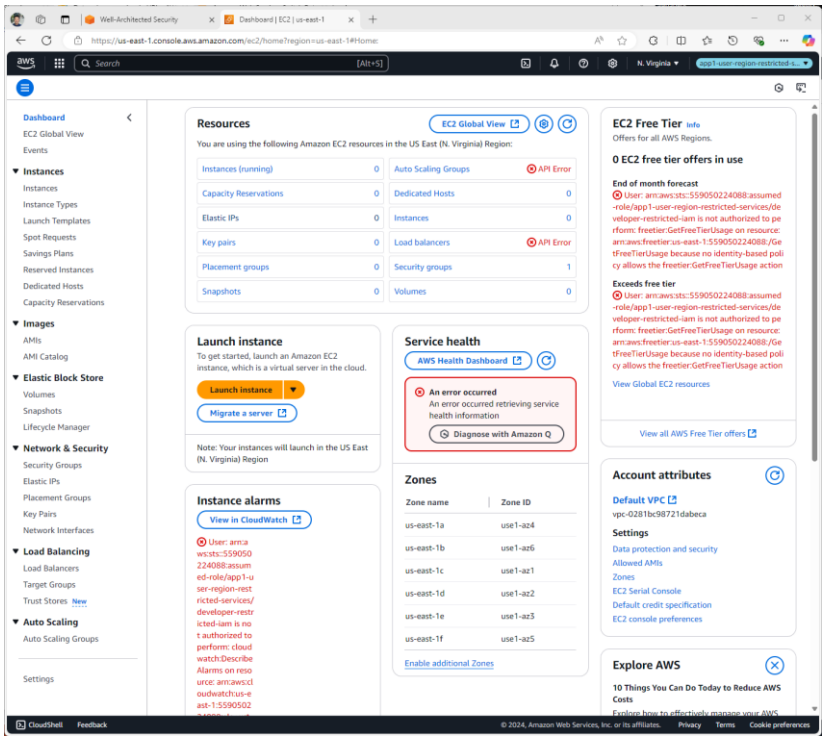
Creating a developer-restricted-iam role

2.2 Test Developer Role



Switching roles to developer-restricted-iam
(I had to create an administrator user for IAM role for this to work, since I don't have one)

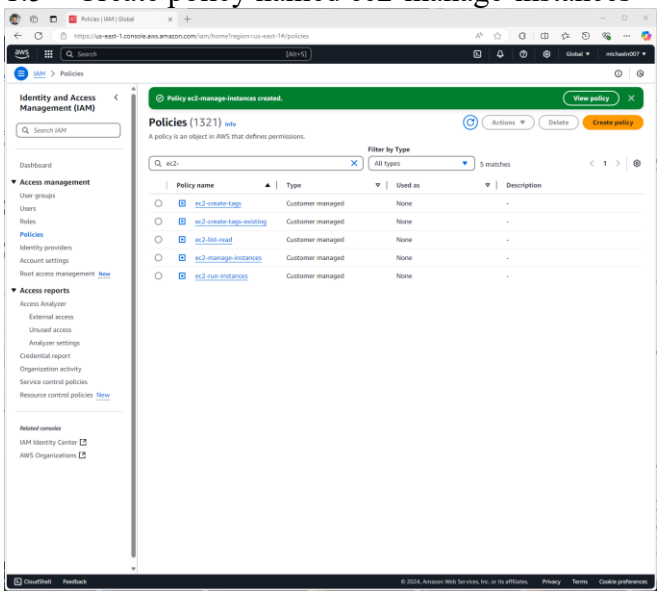
3.1-3.2 Create User Role and Test User Role



The second User role for app1-user-region-restricted-services

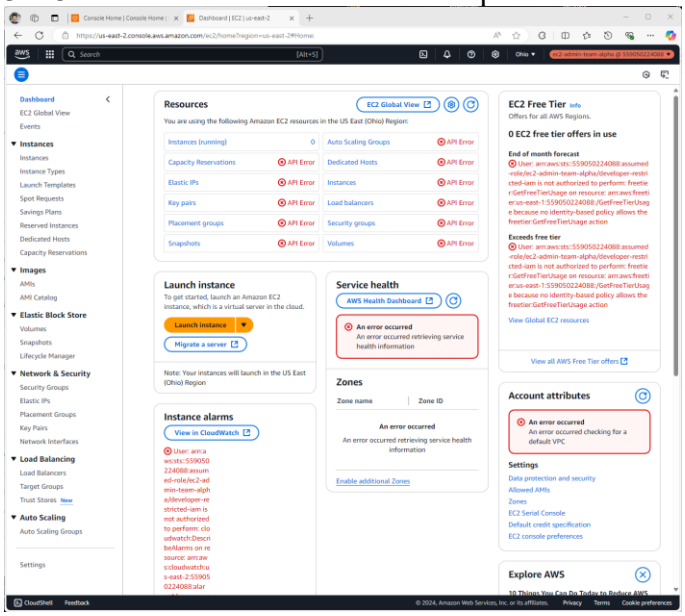
b. IAM Tag Based Access Control for EC2

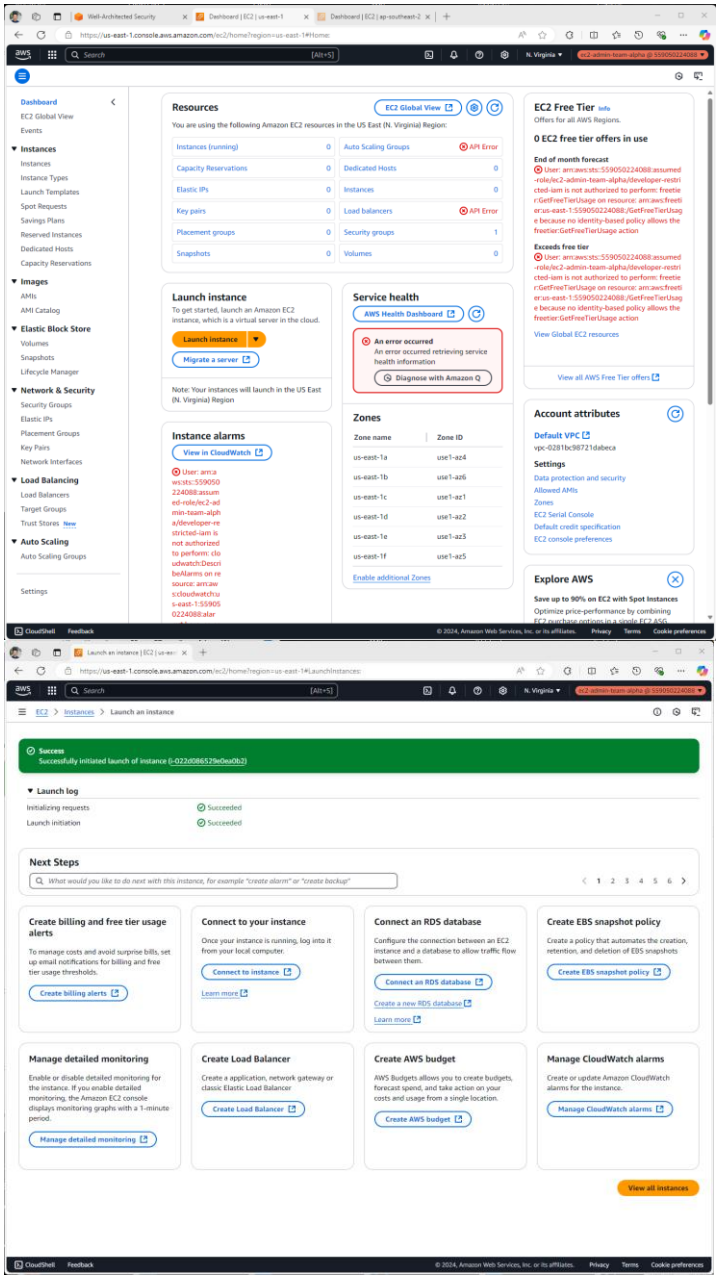
1.1 – Create policy named ec2-list-read
1.2 – Create policy named ec2-create-tags
1.3 – Create policy named ec2-create-tags-existing
1.4 – Create policy named ec2-run-instances
1.5 – Create policy named ec2-manage-instances



Created 1.1-1.5 policies named ec2-list-read, ec2-create-tags, ec2-create-tags-existing, ec2-run-instances, and ec2-manage-instances

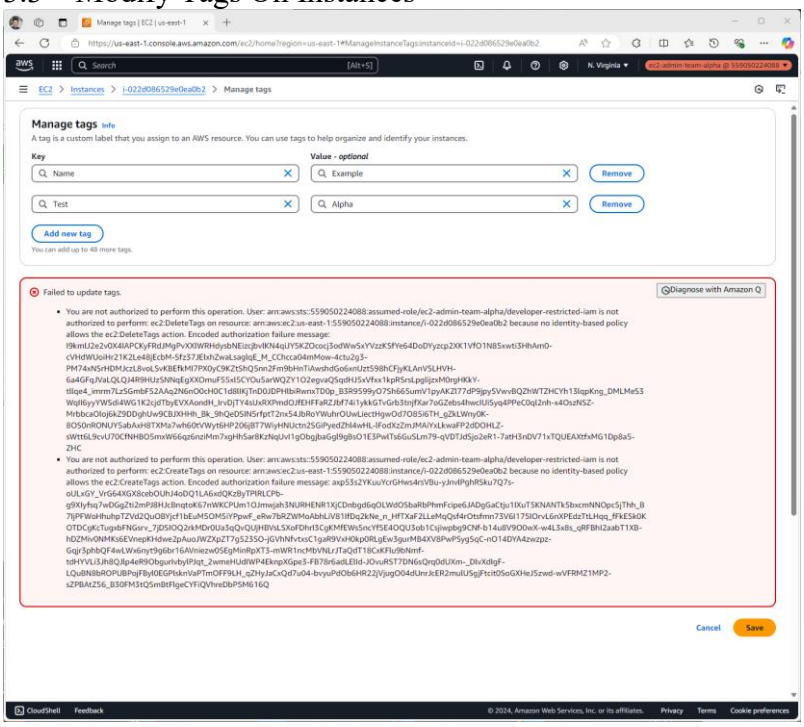
3.1-3.2 – Assume ec2-admin-team-alpha Role and Launch Instance With & Without Tags



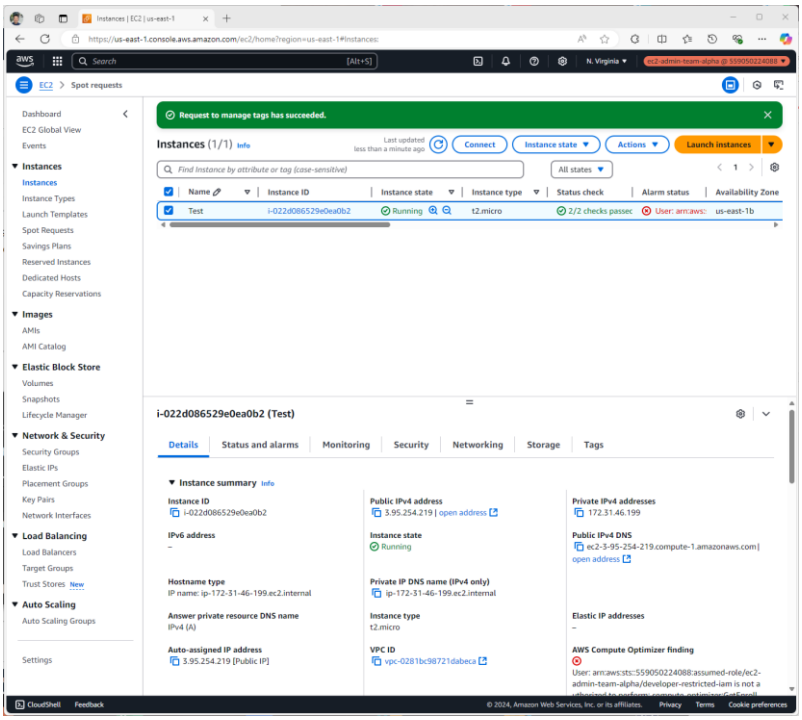


Successfully initiated launch of instance

3.3 – Modify Tags On Instances



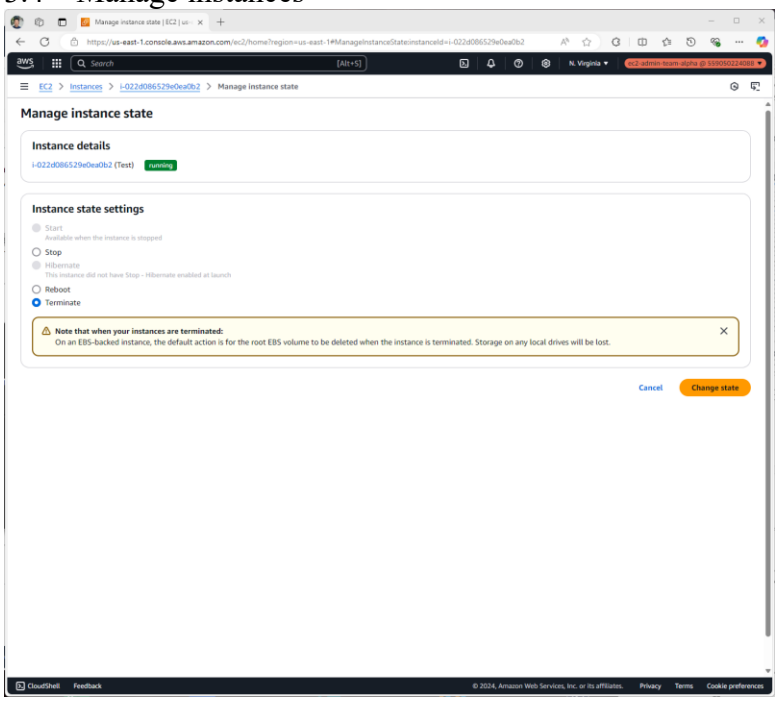
Managing tags of team key to test



Choose *Manage Tags*, try changing the *Team* key to a value of **Test** then choose *Save*. An error message should appear

Change the *Team* key back to Alpha, and edit the *Name* key to a value of **Test** and choose *Save*. The request should succeed

3.4 – Manage instances

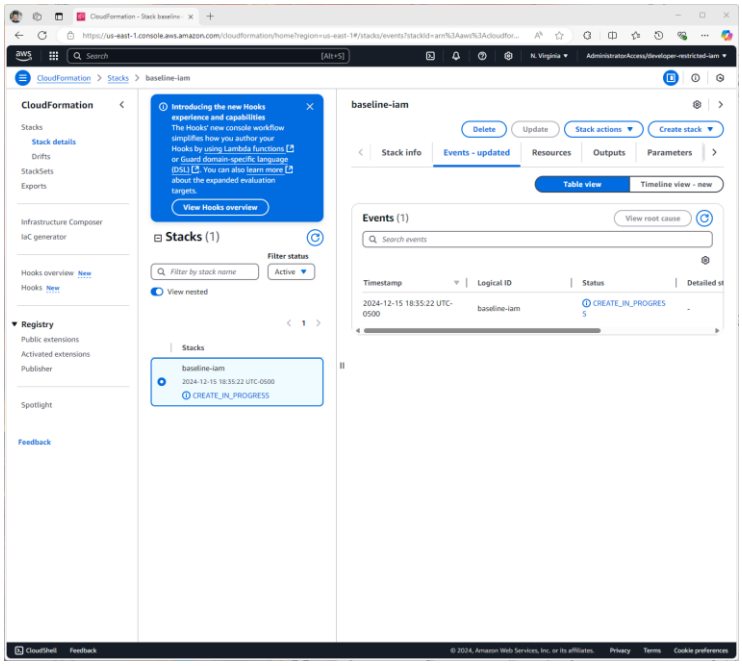


Terminating the instance of Test

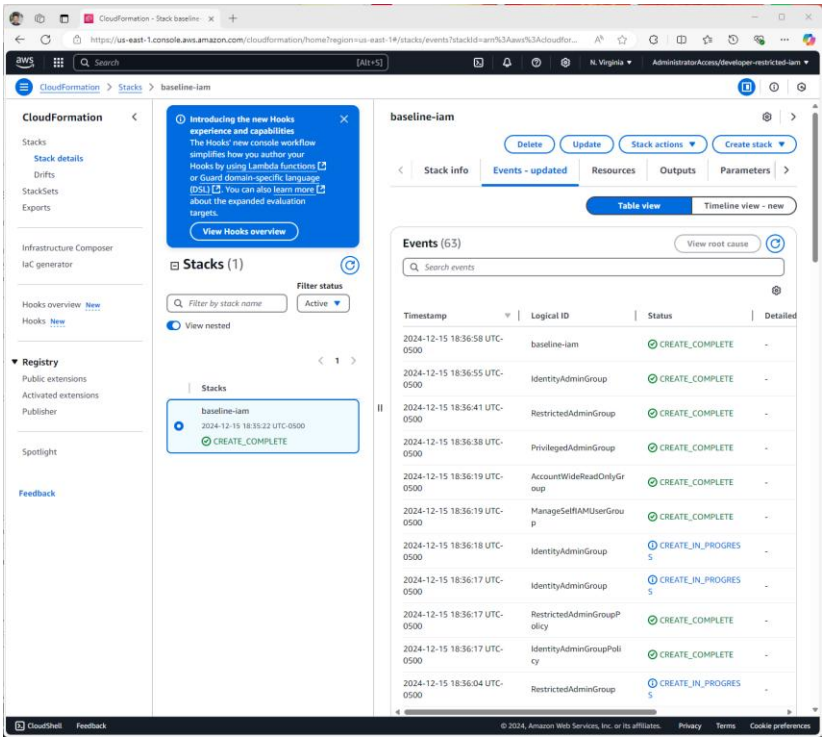
Professor Zhang, there was some mistakes along the way, so I created a new AWS account using the mgnguyen@bu.edu email address instead of my personal email address. So, therefore, some of the screenshots shows the other User Account ID instead.

c. Automated Deployment of IAM Groups and Roles

1.1 – Create AWS CloudFormation Stack

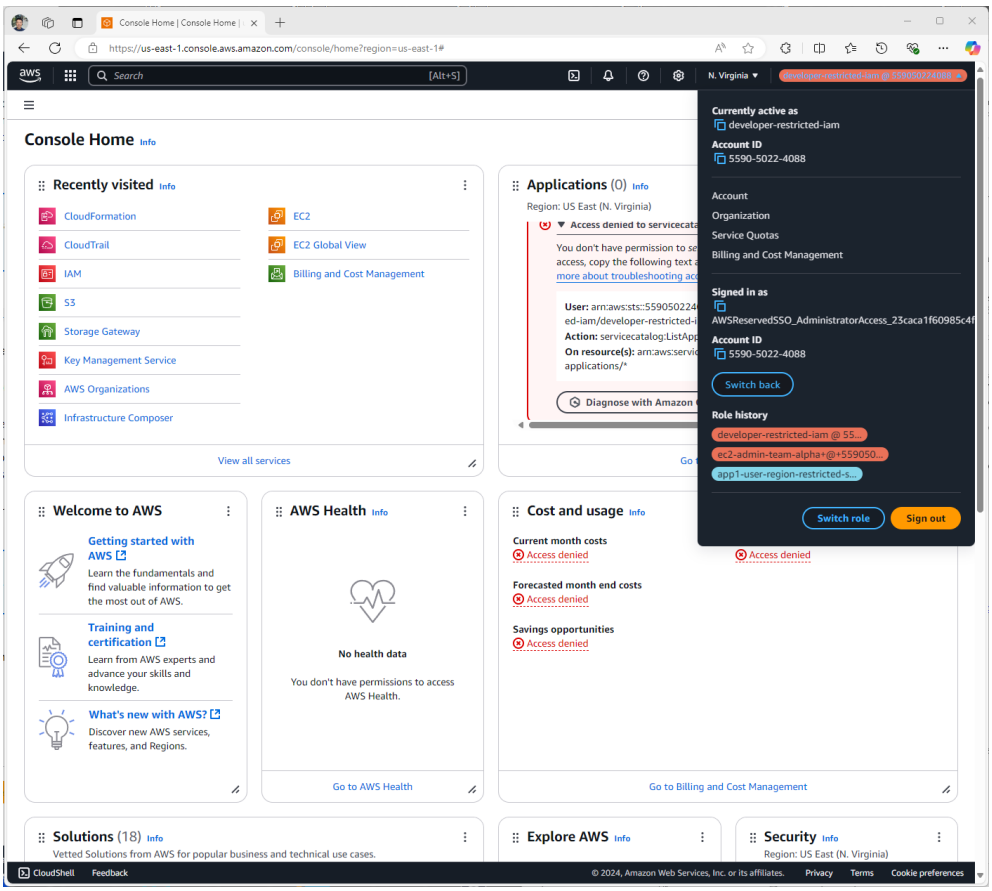


AWS CloudFormation Stack CREATE_IN_PROGRESS



CREATE_COMPLETE for AWS CloudFormation Stack

2.1 Use Restricted Administrator Role in Web Console



Granted Administrator Roles in Switch Role

Professor Zhang, I did the additional work of "Create a Data Bunker Account" and "Automated Deployment of IAM Groups and Roles. Thank you so much!

Several notes as below:

A. In Security Foundations-> AWS Account Setup and Root User->Account Setting & Root User Security:

   1.3 no need to do
   1.6 no need to do
   1.7 Choose Custom, make some changes to the password policy and explain the reasons of your changes.
   NOTE: To continue the next step, here you need to create an IAM user, provide user access to the AWS Management Console, choose a password you can remember, attach Administrator Access policy to the user, and configure MFA for the user.

B. In Identity and Access Management-> IAM Permission Boundaries Delegating Role Creation->create IAM policies:

   NOTE: in Step 1 of 1.1: "Sign in to the AWS Management Console as an IAM user with MFA enabled that can assume roles in your AWS account". You will not log in as root user anymore. You need to login as the IAM user you created in the previous step: Security Foundations.
   1.3 There is an error in the policy of **createrole-restrict-region-boundary**. You need to fix it on your own

Deliverables: You need to submit a document with all the screenshots and a summary of what you learned from this lab.