

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.

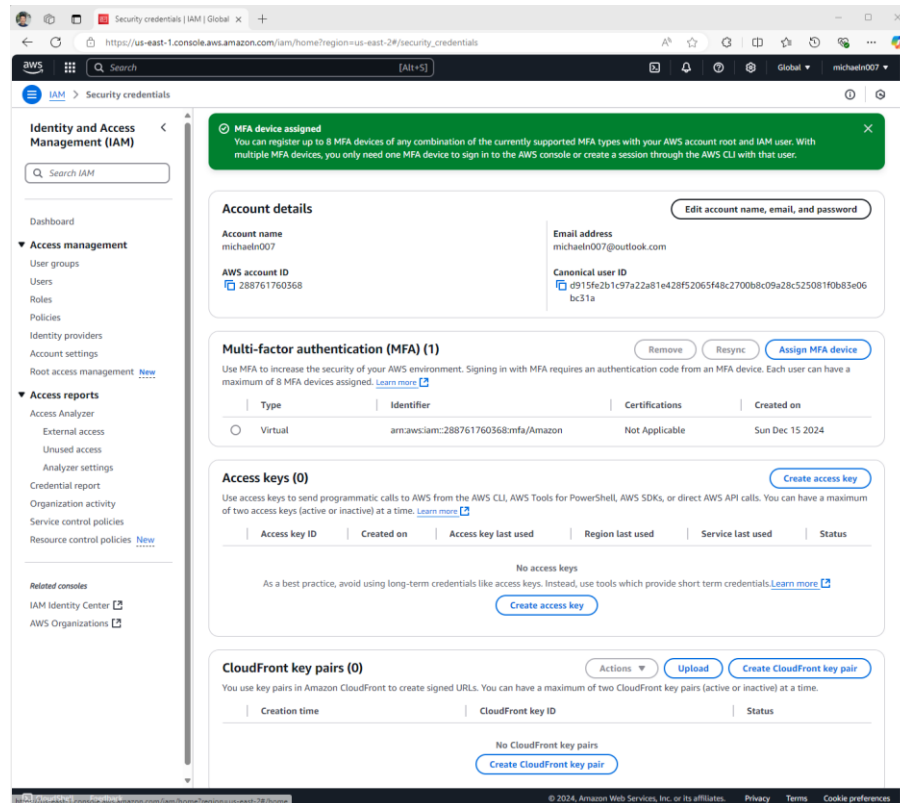
The link to the workshop: <https://catalog.workshops.aws/well-architected-security/en-US>

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

Security challenge questions [Info](#)

Security challenge questions are being discontinued
After January 5, 2024, AWS will no longer support security challenge questions for accounts that have not already enabled them. After January 6, 2025, AWS will no longer support security challenge questions for all remaining customers. We encourage you to enable [multi-factor authentication \(MFA\)](#) to add an additional layer of protection to your AWS account. [Learn more.](#)

Security questions are currently not enabled.

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

1.4 - Configure Account Alternate Contacts

Alternate contacts

You can add alternate contacts for Billing, Operations, and Security communications to ensure the correct people are notified for each topic. As a primary account holder, you will continue to receive all email communications. [Learn more](#)

Billing contact	Operations contact	Security contact
Successfully added billing contact.	Successfully added operations contact.	Successfully added security contact.
Full name Michael Nguyen	Full name Michael Nguyen	Full name Michael Nguyen
Title Student	Title Student	Title Student
Email address mnguyen@bu.edu	Email address mnguyen@bu.edu	Email address mnguyen@bu.edu
Phone number 6178988794	Phone number 6178988794	Phone number 6178988794
Edit Delete	Edit Delete	Edit Delete

Configuring the Account Alternate Contacts

1.5 – Remove Your AWS Account Root User Access Keys

Retrieve access key

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAUJGO4KZJYFRMAX7SY	RDXoBS9AHPS3amGrLul8brCD+11ydmYgoXuwYRM

Access key best practices

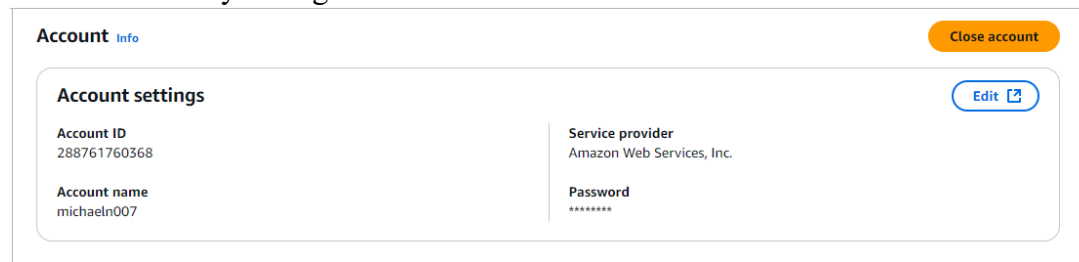
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#) [Done](#)

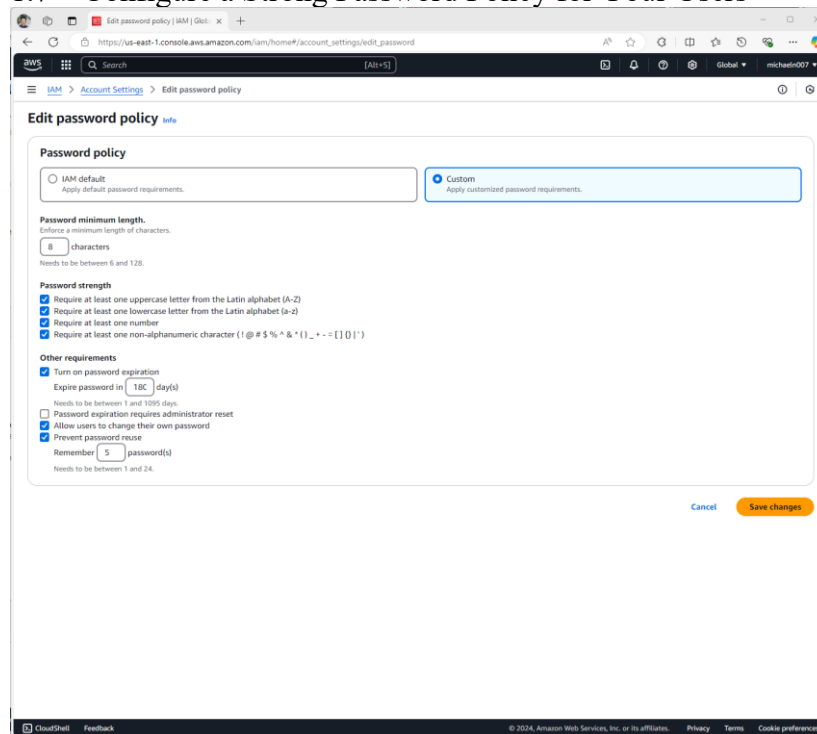
Creating an AWS Account Root User Access Key.

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).*

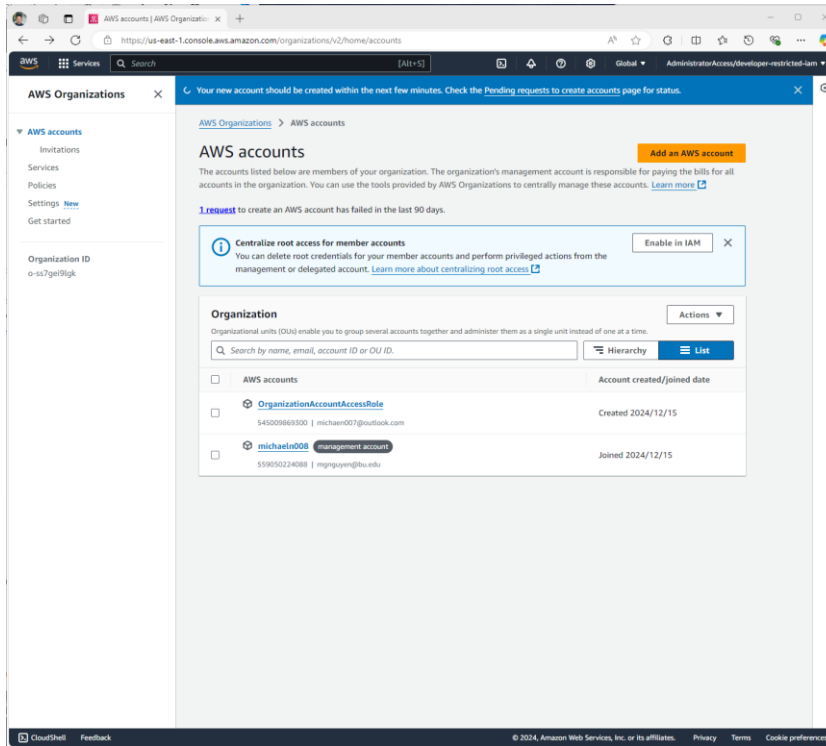
1.7 – Configure a Strong Password Policy for Your Users



Configuring a Custom Password Policy for Users

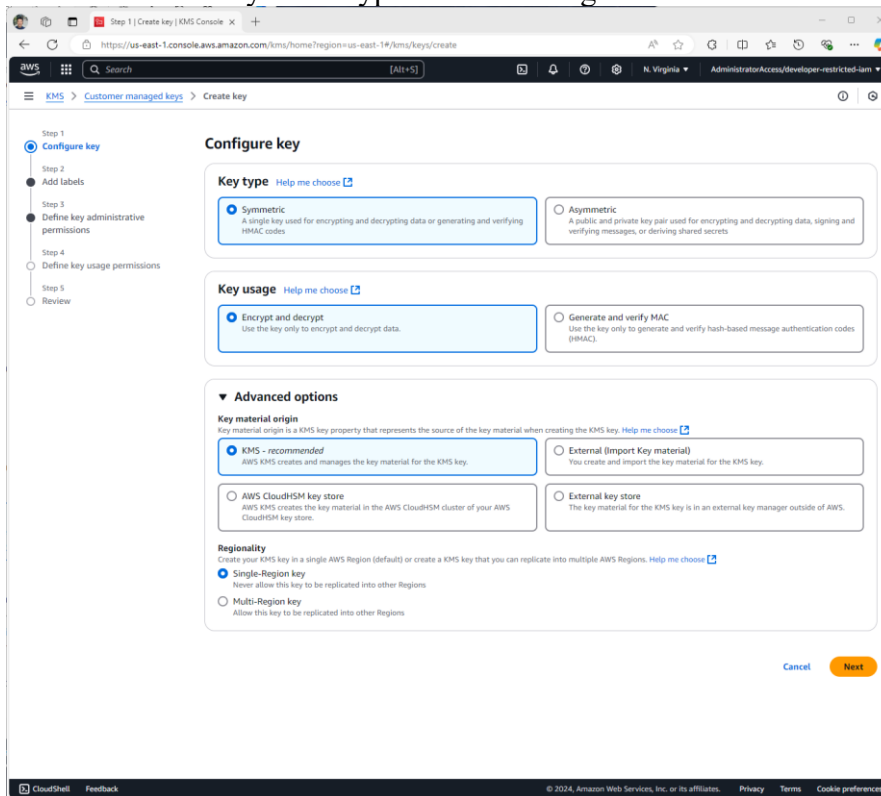
b. Creating data bunker account in console

1. Create a logging account from the organizations management account

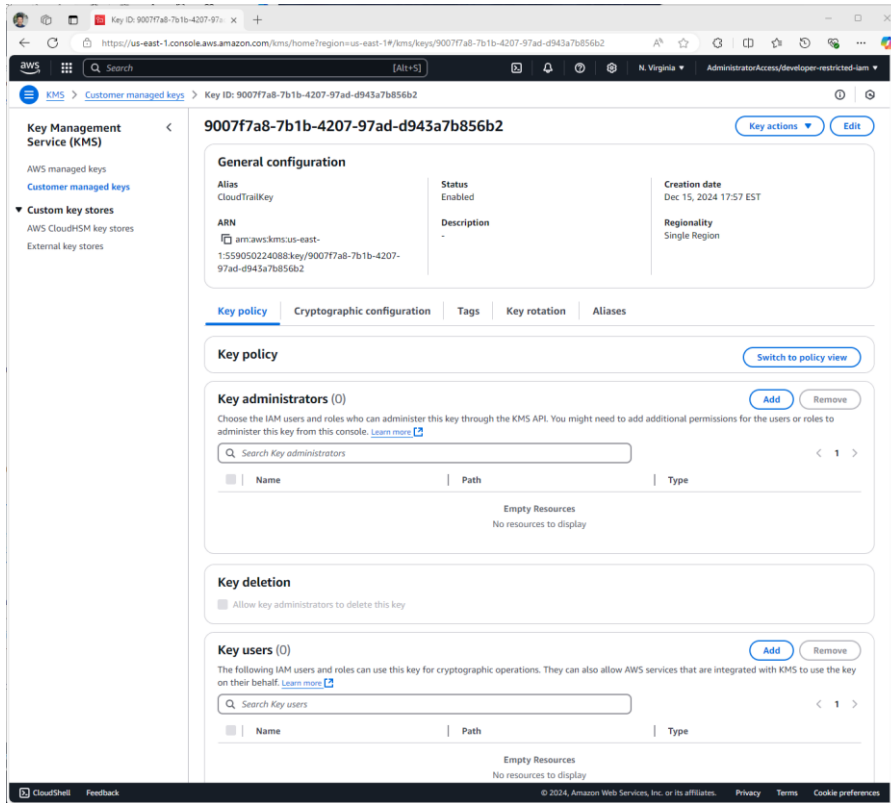


Created an OrganizationAccountAccessRole

2. Create a key to encrypt CloudTrail log

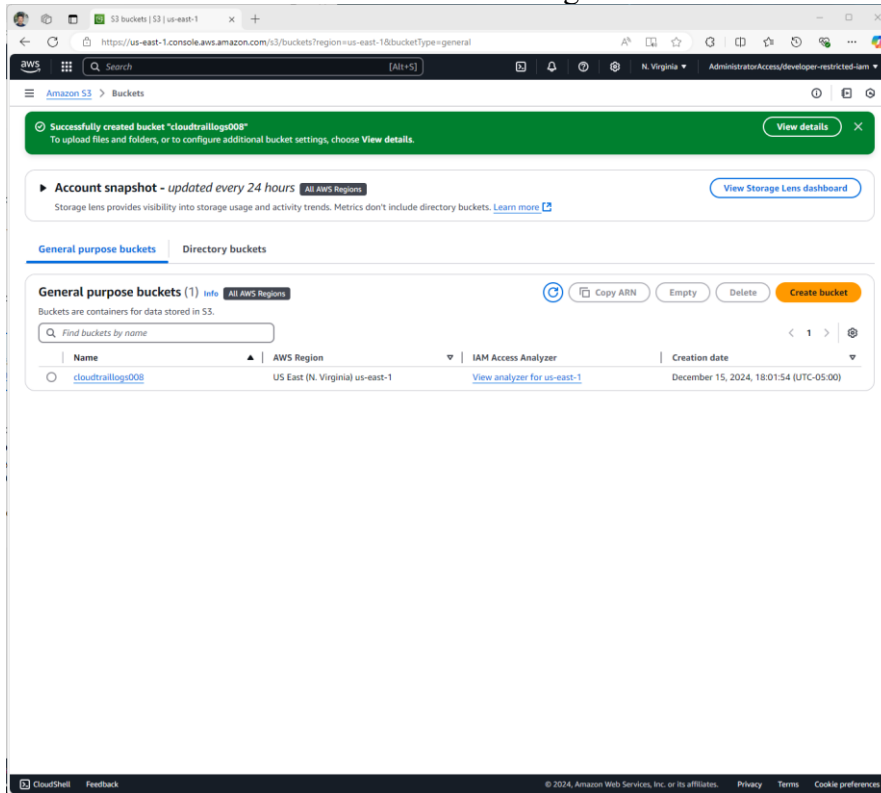


Configuring CloudTrailKey

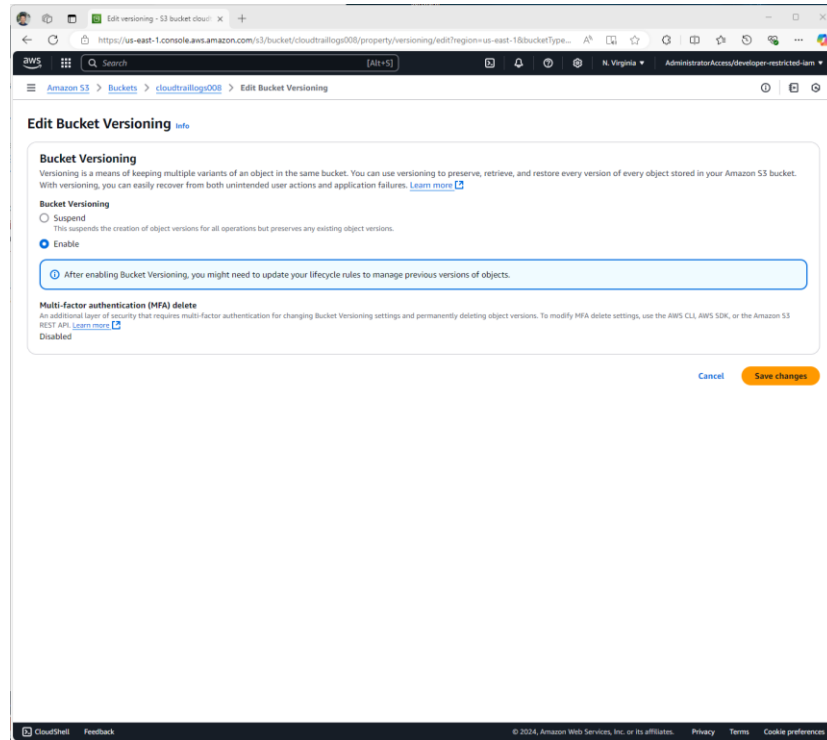


CloudTrailKey information

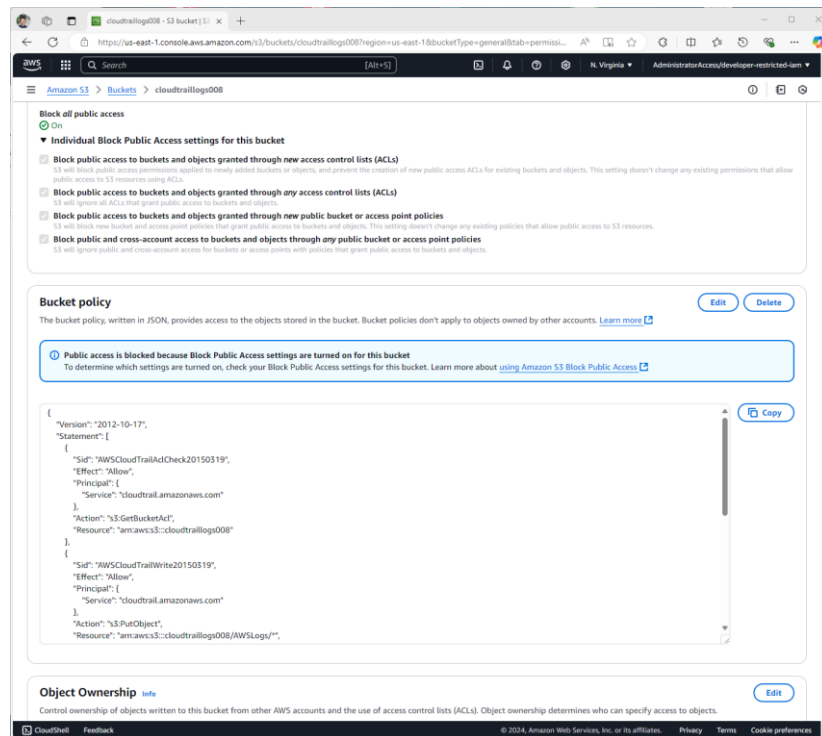
3. Create the bucket for CloudTrail Logs



Creating a bucket for Cloud Trail Logs

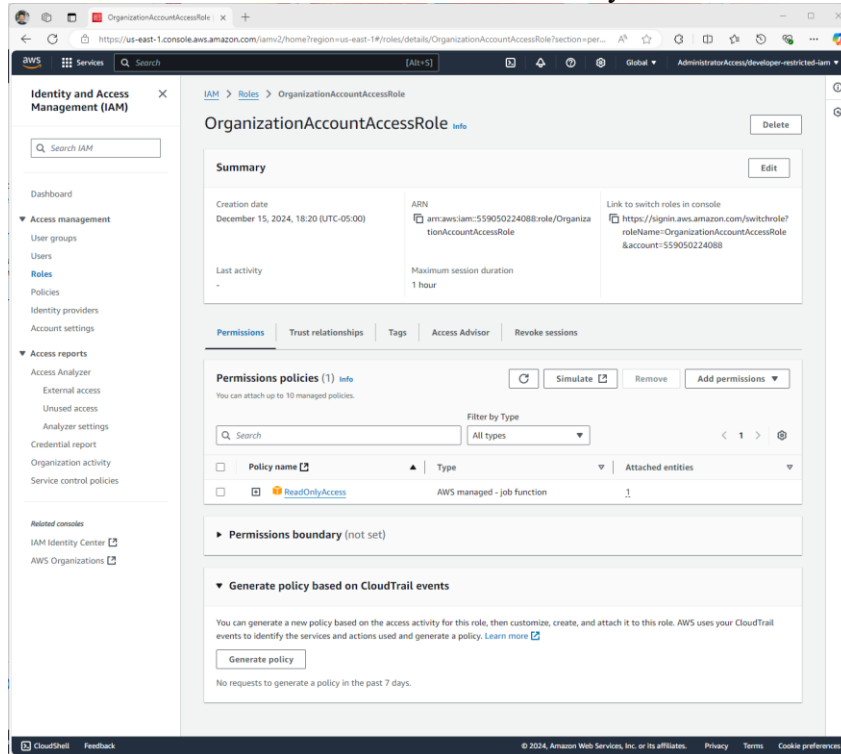


Enable bucket visioning

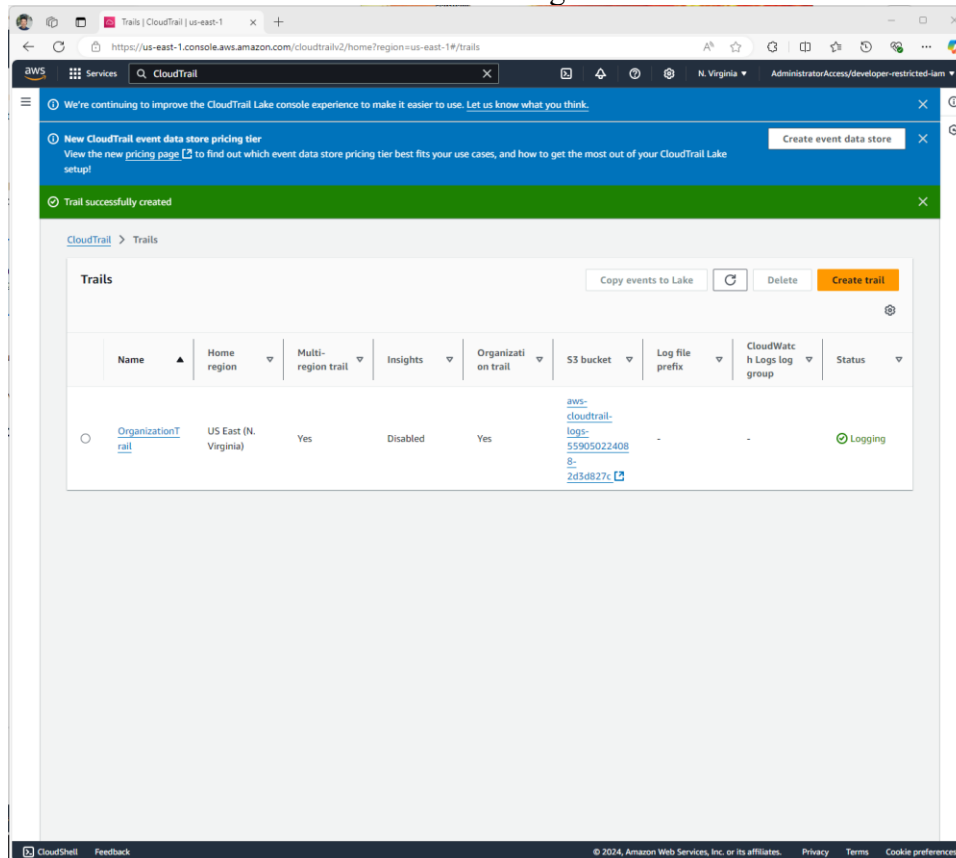


Creating a bucket policy in the Permissions tab

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

The screenshot shows the AWS IAM console page for a policy named 'restrict-region-boundary'. The page is divided into several sections:

- Policy details:** Shows the policy type as 'Customer managed', creation and edited times as 'December 15, 2024, 10:41 (UTC-05:00)', and the ARN as 'arn:aws:iam:288761760368:policy/restrict-region-boundary'.
- Permissions defined in this policy:** A JSON editor showing the policy document. The document defines two statements: 'EC2RestrictRegion' and 'LambdaRestrictRegion'. Both statements allow actions on resources in specific regions ('us-east-1' and 'us-west-1').

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "EC2RestrictRegion",
6-       "Effect": "allow",
7-       "Action": "ec2:*",
8-       "Resource": "*",
9-       "Condition": {
10-        "StringEquals": {
11-          "aws:RequestedRegion": [
12-            "us-east-1",
13-            "us-west-1"
14-          ]
15-        }
16-      }
17-     },
18-     {
19-       "Sid": "LambdaRestrictRegion",
20-       "Effect": "allow",
21-       "Action": "lambda:*",
22-       "Resource": "*",
23-       "Condition": {
24-        "StringEquals": {
25-          "aws:RequestedRegion": [
26-            "us-east-1",
27-            "us-west-1"
28-          ]
29-        }
30-      }
31-     }
32-   ]
33- }
```

Permissions defined in this policy

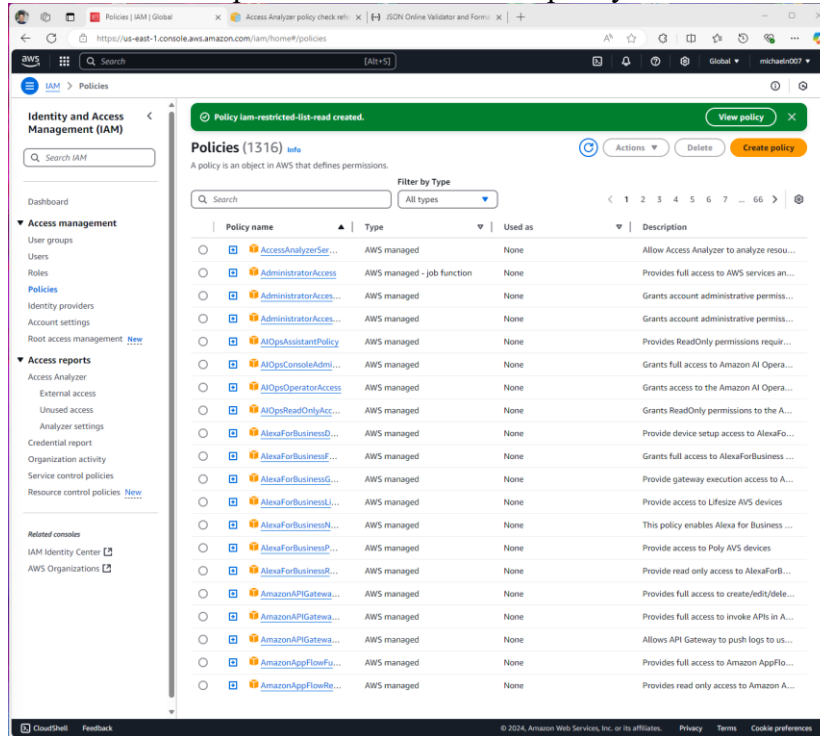
The screenshot shows the 'Create policy' wizard in the AWS IAM console, specifically Step 1: 'Specify permissions'. The page includes a 'Policy editor' with a JSON editor and a 'Visual' view. The JSON editor shows the following policy document:

```
4 * {
5   "Sid": "CreatePolicy",
6   "Effect": "allow",
7   "Action": [
8     "iam:CreatePolicy",
9     "iam:DeletePolicyVersion",
10    "iam:DeletePolicyVersion"
11  ],
12   "Resource": "arn:aws:iam:288761760368:policy/role*",
13 },
14 {
15   "Sid": "CreateRole",
16   "Effect": "allow",
17   "Action": "iam:CreateRole",
18   "Resource": "arn:aws:iam:288761760368:role/appl*",
19   "Condition": {
20     "StringEquals": {
21       "iam:PermissionsBoundary": "arn:aws:iam:288761760368:policy/restrict-region-boundary"
22     }
23   }
24 },
25 {
26   "Sid": "AttachDetachRolePolicy",
27   "Effect": "allow",
28   "Action": [
29     "iam:DetachRolePolicy",
30     "iam:AttachRolePolicy"
31   ],
32 }
```

The 'Visual' view shows a list of services and actions. The 'IAM' service is selected, and the 'iam:CreatePolicy', 'iam:DeletePolicyVersion', and 'iam:AttachRolePolicy' actions are visible. The 'iam:CreateRole' action is also visible, but it is not selected. The 'iam:DetachRolePolicy' action is also visible, but it is not selected. The 'iam:AttachRolePolicy' action is also visible, but it is not selected.

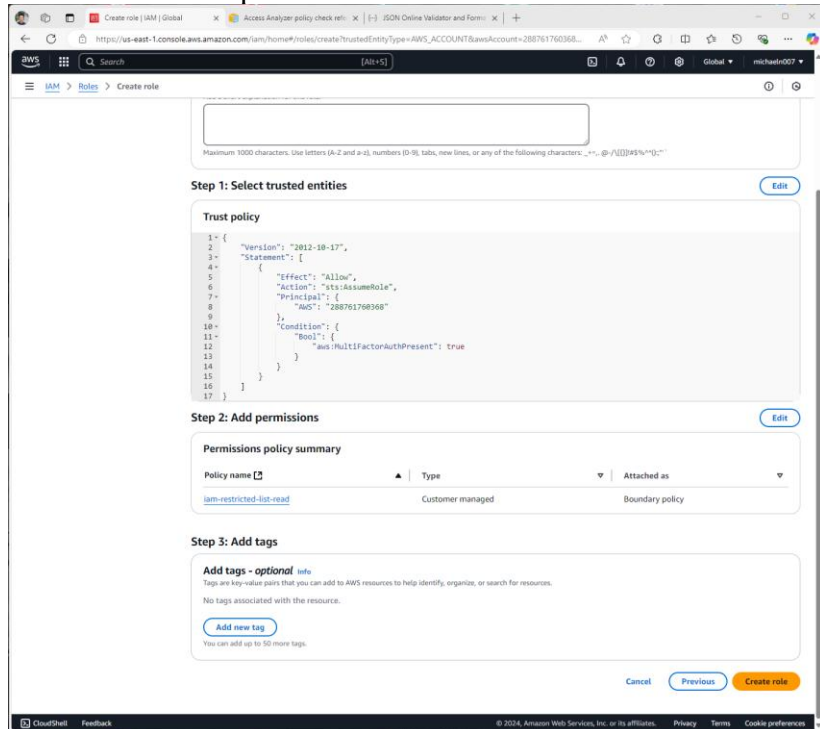
Creating a createrole-restrict-region-boundary with account id placeholders

1.2 Create developer IAM console access policy



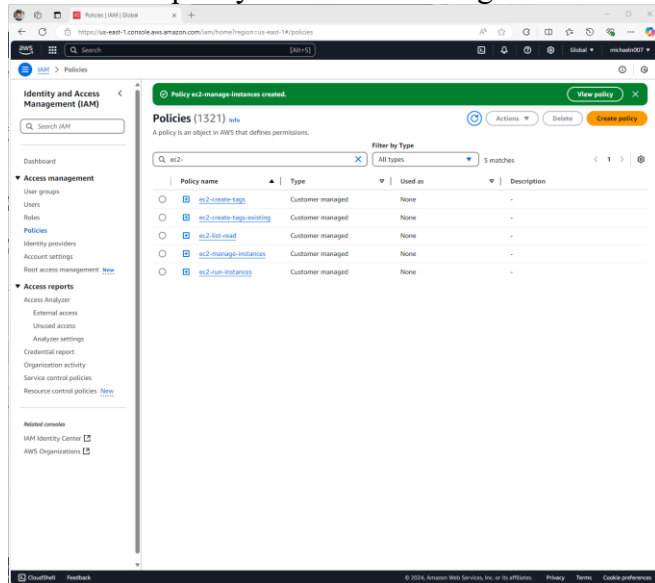
Creating an iam-restricted-list-read policy

2.1 Create Developer Role



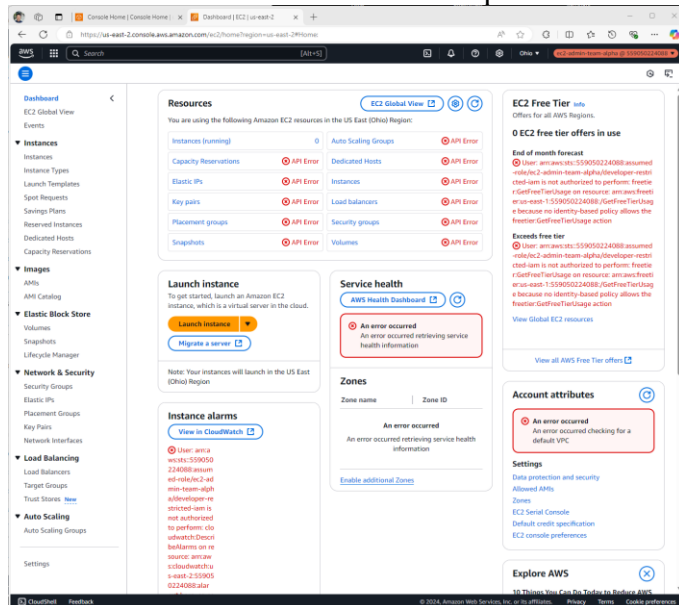
Creating a developer-restricted-iam role

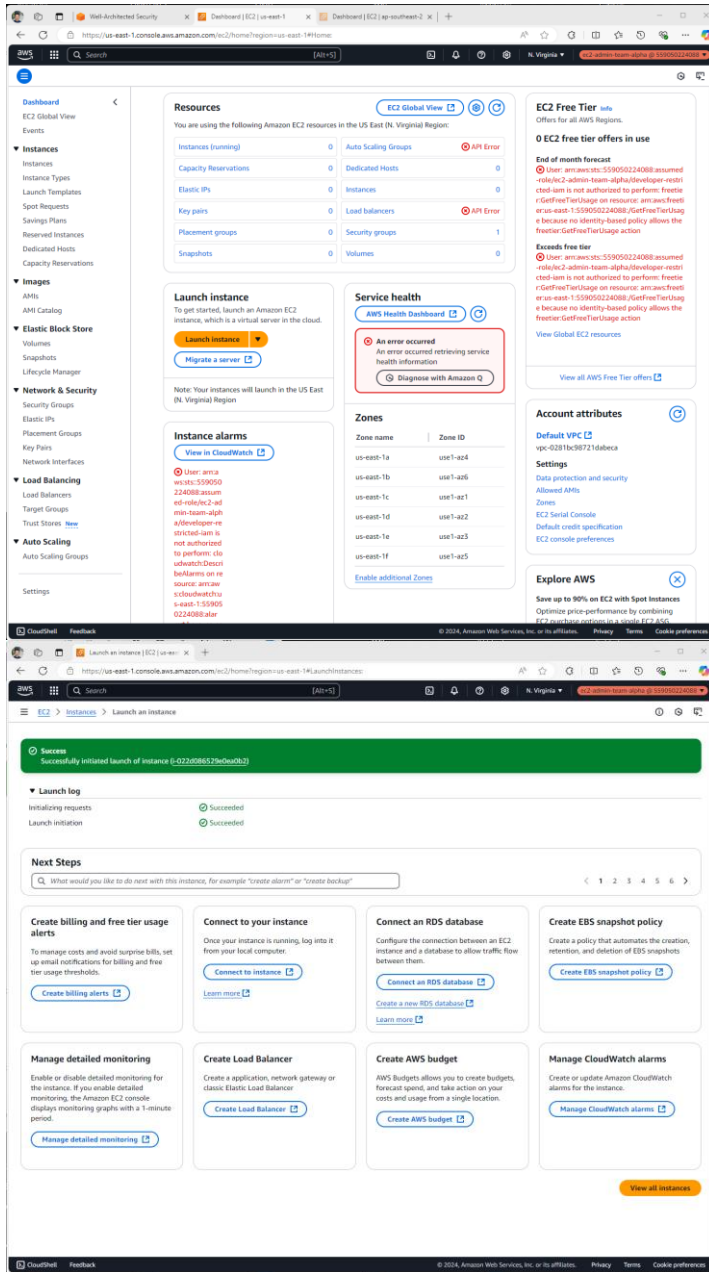
- 1.1 – Create policy named ec2-list-read
- 1.2 – Create policy named ec2-create-tags
- 1.3 – Create policy named ec2-create-tags-existing
- 1.4 – Create policy named ec2-run-instances
- 1.5 – Create policy named ec2-manage-instances



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

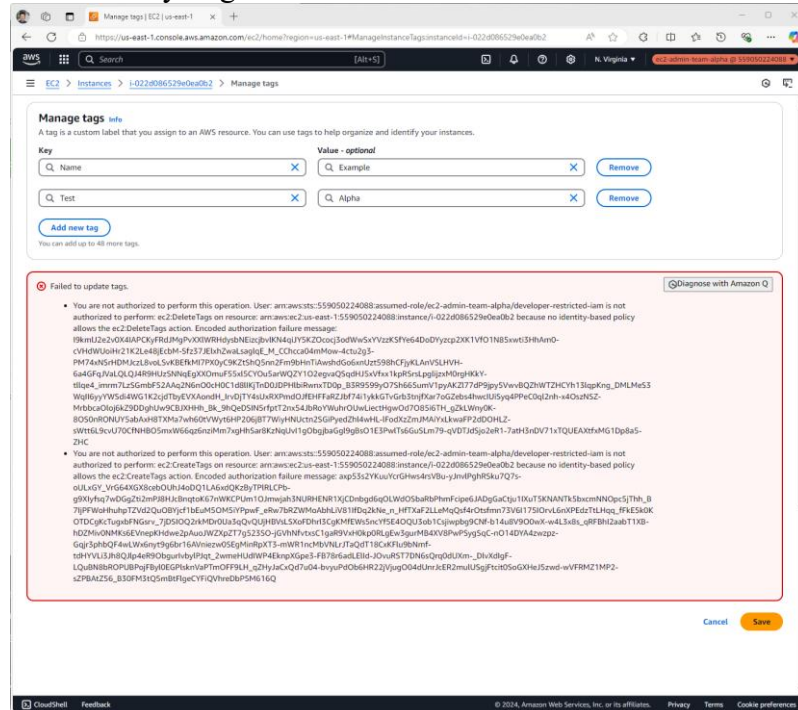
3.1-3.2 – Assume ec2-admin-team-alpha Role and Launch Instance With & Without Tags



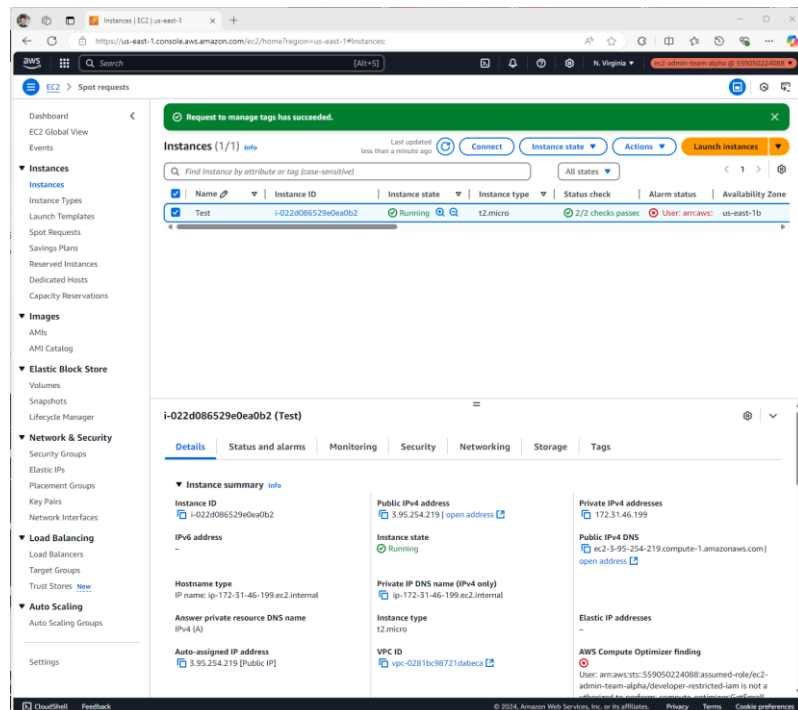


Successfully initiated launch of instance

3.3 – Modify Tags On Instances



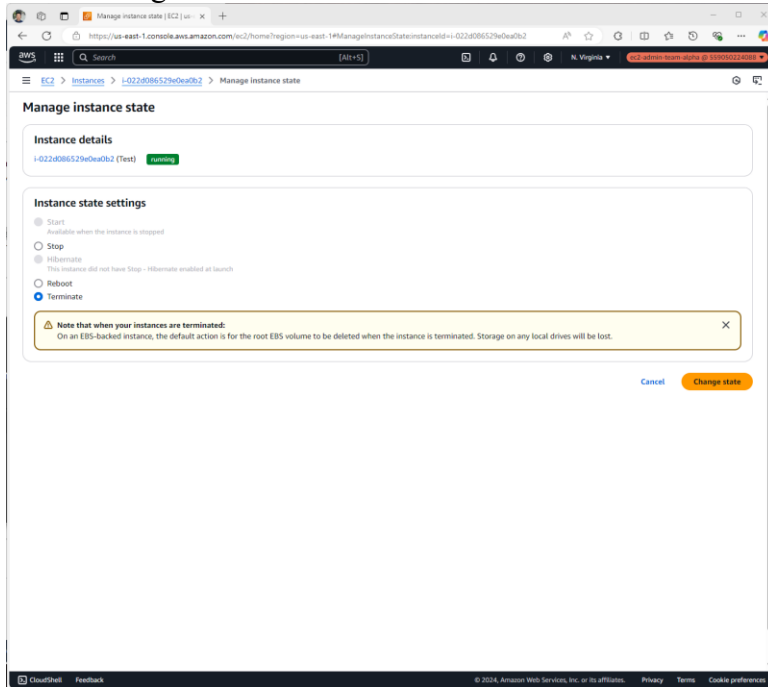
Managing tags of team key to test



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

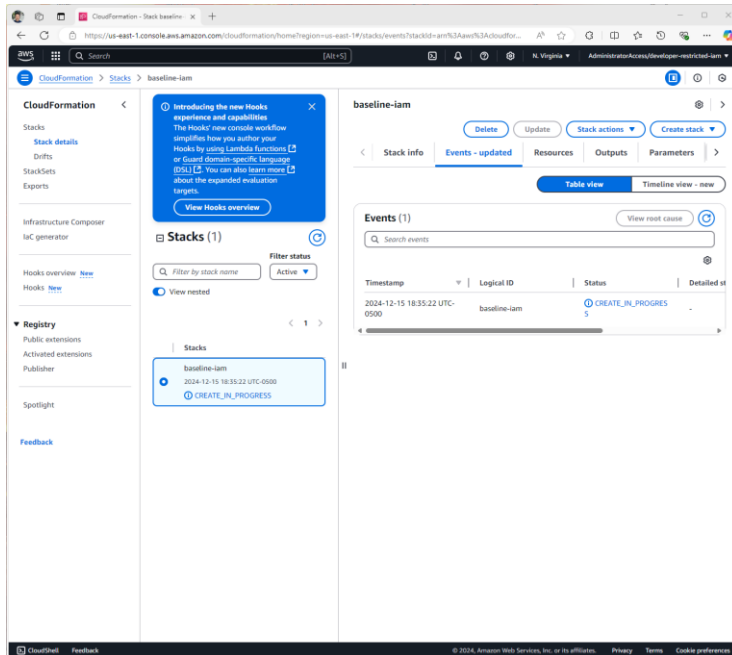


Terminating the instance of Test

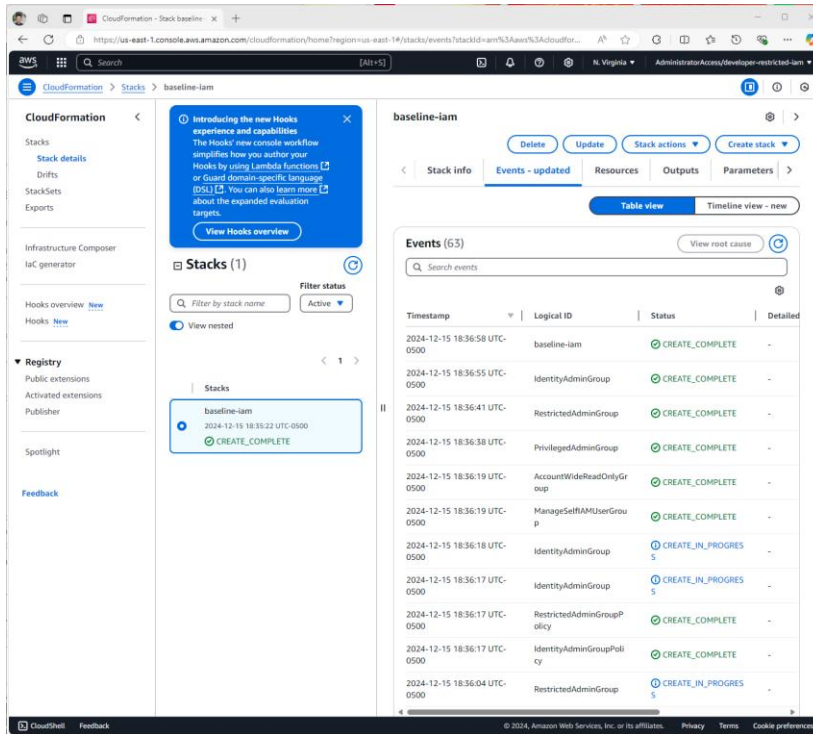
Professor Zhang, there was some mistakes along the way, so I created a new AWS account using the mgnguyen@bu.edu email address instead of my personal email address. So, therefore, some of the screenshots shows the other User Account ID instead.

c. Automated Deployment of IAM Groups and Roles

1.1 – Create AWS CloudFormation Stack

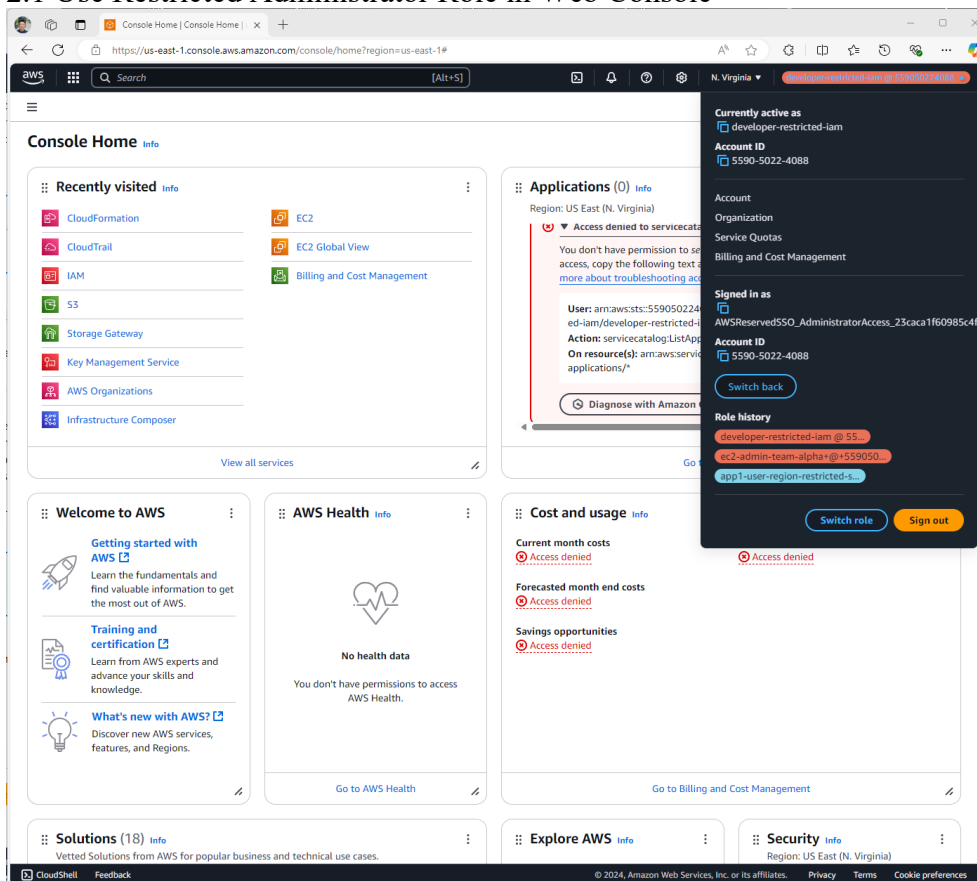


AWS CloudFormation Stack CREATE_IN_PROGRESS



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.