Assessment Task
Portfolio of Evidence

ICTCLD507_508_AT3_PE_TQM_v1.docx

Student Name		**Student Number**	
Unit Code/s & Name/s	ICTCLD507 Build and deploy resources on cloud platforms ICTCLD508 Manage infrastructure in cloud environments		
Cluster Name *If applicable*	Cloud Infrastructure		
Assessment Name	Design and Implement a Cloud based solution	**Assessment Task No.**	3 of 3
Assessment Due Date		**Date submitted**	/ /
Assessor Name			
Student Declaration: I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature.			
Student Signature		**Date**	/ /

Instructions to Student	**General Instructions:** This written assessment contains two (2) parts: ● Section 1 – Build and Deploy Resources on The Cloud Platform ● Section 2 – Manage Infrastructure in Cloud Environments The answers required for these tasks shall be written in plain English, using language that is understandable by a person of a technical level suitable for the case study.

Materials to be Supplied:

For the student to successfully complete this assessment they will need to acquire:

- A computer system installed with a current desktop operating system with appropriate internet browser, and office suite able to save in Microsoft Word .docx format, and current industry standard file formats
- Internet access
- Uptown IT documentation, located in Connect

Work, Health and Safety:

TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules[1], specifically as they relate to progress of study and assessment guidelines.

Assessment Criteria:

To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard:

- deploy and configure at least 6 of the following different types of cloud resources, including but not limited to
  - virtual machines
  - container services
  - load balancers and autoscaling
  - serverless functions
  - API gateways
  - block or object storage
  - managed databases
  - DNS
  - content delivery networks
- use cloud management console, cloud software development kits or command line tools

[1] http://tafeqld.edu.au/current-students/student-rules/

	● develop and execute test plans and demonstrate successful task completion

	● consider procedural improvements to produce repeatable and automated deployments by reducing manual processes ● monitor and manage inventory, changes and lifecycle of at least one cloud resource ● use cloud management console, cloud software development kits or command line tools ● collect and analyse cloud and system data and adjust resources accordingly ● summarise ways system operations in cloud environments can be automated to minimise manual intervention
Submission details (if relevant)	Insert your details on page 1 and sign the Student Declaration. Include this form with your submission. **Due:** Week 8 as per the unit study guide Submit the listed files below as per the instructions in the Connect online learning system stated on the Assessment Task 2 page. You are to submit the following files: ● *ICTCLD507_ICTCLD508_AT2_Report_yourname.docx* ● *ICTCLD507_ICTCLD508_AT2_Test_Plan_yourname.docx* Assessment to be submitted via: ● TAFE Queensland Learning Management System (Connect): *https://connect.tafeqld.edu.au/d2l/login* ● Username; 9 digit student number ● For password resets go to: *https://passwordreset.tafeqld.edu.au/default.aspx*
Instructions to Assessor	Student will require: ● Computer applications currently used in industry ● Support resources, including online, manuals and training booklets ● A computer system with a suitable current OS and access to the internet ● information and data sources required to design and implement cloud infrastructure ● specific requirements and industry standards, organisational procedures and legislative requirements, including business and functionality requirements as well as retention/lifecycle business policy, as required ● retention/lifecycle policy example as it relates to managing cloud infrastructure ● data to gather information from to determine output and user requirements, including user access and business protocols

	Work, Health and Safety: TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules[2], specifically as they relate to progress of study and assessment guidelines. **Level of Assistance:** Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but guide them to where to go to complete tasks individually. The teacher will make reasonable adjustment for students, as and when appropriate, after consultation with the Disability and Counselling team. **Assessment Criteria:** ● See Marking Criteria on Connect ● Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards. Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.
Note to Student	An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.

[2] http://tafeqld.edu.au/current-students/student-rules/

Case Study 1

Client's Details

Company Name: Gunda Online Shop (GO Shop)

GO Shop is a small online store which sells various items such as household goods, computer spare parts, cables, garden tools etc. The company uses an in-house developed web application software running on its own servers. The company has been operating with this system for a long time and the application has been fine tuned for their purpose. With the rapid increase in the business transactions during and the pandemic, the old hardware platform is pushed to limits. This has given rise to issues resulting in increased system administration tasks for in-house IT staff and the Senior system administrator is requesting more staff from the management to manage the systems.

After having several discussions with the Management, GO Shop decides to explore the possibility of implementing a cloud-based system so that the company does not need to maintain the in-house IT infrastructure.

Current Configuration IT Systems:

- Domain Controller
- Web Application Server
- Database Server
- File Server

Business Needs:

- Reliable servers with reduced hardware maintenance cost
- Maintain current level of System Administration staff
- Reduced utility costs for IT infrastructure
- Use the existing well-tuned online transaction system and the database
- Secure File storage
- High availability servers
- Access GO Shop application from anywhere in the world with minimum response time.

Technical Requirements:

- Cloud based solution
- Well defined Identity and Access Management
- Automation of Administrative tasks
- Containerised web applications
- Minimum latency of online transaction when accessed from different regions and countries
- Redundant IT infrastructure
- High availability of serves and transaction system
- Software development environment

Company Policies:

1. GO Shop is commitment to professionalism, ethical practices, equity, and social accountability implies a duty of care in relation to the use of information resources.
2. GO Shop is committed to protect the privacy of all the stake holders of the company.
3. The security of information is paramount to GO Shop and stress on implementing well architected access management system.
4. GO Shop will maintain all the transaction data in Australia.
5. The transaction WEB application is developed and maintained by GO Shop software development staff.
6. GO Shop always maintain a backup system so that the applications are available 24x7

Your Role

As a Senior System Administrator with GO Shop, management has requested you to design and implement a cloud-based solution for the company and configure appropriate management systems to ensure resource performance, resilience, and security.

Section 1: Build and Deploy Resources on The Cloud Platform

Part 1 – Prepare to Deploy Cloud Resources

1.1 List all of the necessary resources required for GO Shop according to the business needs and identify the corresponding cloud computing resources.

Some preface/context to the decisions I made and why.

There are multiple ways to convert an in house servers and their contents to the cloud. Since GO Shop is presumably running on monolithic-esque architecture style for its current system. The deployment style with roughly translate to that same style to the cloud for inherent simplicity and familiar control over the application, so a more granular approach will be the direction this identification will follow.

Resource	Cloud Resource	Comments
Resource	**Cloud Resource**	**Comments**
Domain Controller	AWS Directory Service (Simple AD)	Managed service for basic AD features.
Web Application Server	AWS Elastic Beanstalk	Managed service for easy deployment and scaling of applications.
Database Server	Amazon RDS (Relational oriented db management)	Managed relational database with Multi-AZ for high availability.
File Server	Amazon S3 Standard	Simple and durable storage service. Use SSE-S3 for encryption.
Software Dev Environment	AWS Cloud9	Cloud-based IDE, straightforward for development.
Identity and Access Management	AWS IAM	Define permissions and access. Enable MFA for security.

1.2 Identify organizational policies and procedures required for cloud technology resources

The information in the Case study has a specific segment for all the organizational policies.

1.GO Shop is commitment to professionalism, ethical practices, equity, and social accountability implies a duty of care in relation to the use of information resources.

2. GO Shop is committed to protect the privacy of all the stake holders of the company.

3. The security of information is paramount to GO Shop and stress on implementing well architected access management system.

4. GO Shop will maintain all the transaction data in Australia.

5. . The transaction WEB application is developed and maintained by GO Shop software development staff.

6. GO Shop always maintain a backup system so that the applications are available 24x7

1.3 Table the business purpose, use and plan of different cloud resources according to business needs

Could Resource	Business purpose, use and plan	Business needs
Amazon EC2	• Serverless compute power • Focus on application deployment • Need functioning computational power	Reduced hardware maintenance costs • Scalability without manual intervention
Amazon RDS	Managed relational database • Automated backups • Use as storage for high queried objects.	• Secure, reliable, and scalable data storage
AWS Directory Service	• Manage EC2 domain joining • User/group permissions • Management of company policy objects inside AWS using AD Connector to transport existing comapny structure	• Centralized identity management
AWS Elastic Beanstalk	• Rapid app deployment • Auto-scaling • Plan to use for quick fixes to remediate critical issues fast	• Quick application deployment and management
Amazon S3	• Store/retrieve files • High durability • Install ec2 instance onto S3 bucket	• Secure and reliable file storage
Amazon Cloud9	• Cloud based IDE • Collaborative coding • For the IT Team to collab in realtime alongside a video call for better communication and productivity.	•Centralized, web-based software development
AWS IAM	• User/access management. • Manage permissions employees and roles have inside the AWS cloud resources. • Setup MFA for security	• Security access control to cloud resources
AWS VPC	• Define the IP address range, subnets and configure route tables,	• Connects AWS services securely

	sgs ect	

Part 2 – Deploy and Configure Cloud Resources

2.1 Identify interfaces and tools required to perform repeatable and automatable tasks.

AWS Management Console

Purpose: Provides a web-based user interface to manage and monitor AWS services.

Use Case for GO Shop: Easy access to configure and monitor resources like EC2 instances, S3 buckets, RDS databases, etc.

AWS Command Line Interface (CLI)

Purpose: Offers a command-line shell to interact with AWS services.

Use Case for GO Shop: Automating deployment and configuration tasks through scripts.

AWS CloudFormation

Purpose: Allows users to define and provision AWS infrastructure using YAML or JSON templates.

Use Case for GO Shop: Define the entire AWS infrastructure in code to ensure repeatability and version control.

AWS Elastic Beanstalk CLI (EB CLI)

Purpose: A command-line interface to interact with AWS Elastic Beanstalk.

Use Case for GO Shop: Simplify the deployment of applications, manage application environments, and automate application deployments.

AWS Identity and Access Management (IAM)

Purpose: Manage access to AWS services and resources securely.

Use Case for GO Shop: Ensure that only authorized and authenticated users can access and modify resources.

AWS SDKs (Software Development Kits)

Purpose: Provides language-specific APIs to interact with AWS services.

Use Case for GO Shop: Integrate AWS services directly with the GO Shop application or automation scripts.

AWS Systems Manager

Purpose: Offers an interface to automate administration tasks.

Use Case for GO Shop: Automate routine management tasks such as patch management, apply OS configurations, and automate software installations.

2.2 Define the steps required to provision resources using flowcharts.

Using AWS architecture design i converted my basic bucket from yaml (json is objectively better) to this flowchart. Below is the template file.

GUNDA DO SHOP TEMPLATE V2

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  WebServerInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: ami-0c55b159cbfafe1f0
      InstanceType: t2.micro
      KeyName: MyKeyPair
      SecurityGroups:
        - Ref: WebServerSecurityGroup
      UserData:
        Fn::Base64: |
          #!/bin/bash
          yum install -y httpd
          systemctl start httpd
          systemctl enable httpd
          echo "<h1> GO GUNDA SHOP >:)</h1>" > /var/www/html/index.html

  WebServerSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: 'Enable HTTP access via port 80 locked down to the load balancer + SSH
access for IT Management''
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: '22'
          ToPort: '22'
          CidrIp: 0.0.0.0/0
        - IpProtocol: tcp
          FromPort: '80'
          ToPort: '80'
          CidrIp: 0.0.0.0/0

  WebsiteBucket:
    Type: 'AWS::S3::Bucket'
```

```
Properties:
  AccessControl: PublicRead
  WebsiteConfiguration:
    IndexDocument: index.html
```

2.3 Prepare a test plan to demonstrate successful completion of the deployment.

Test Plan for GO SHOP Post CloudFormation Deployment

Objective:

Verify that all AWS resources have been successfully created, configured, and are operational after the CloudFormation stack deployment.

Test Environment:

AWS CloudFormation with resources including AWS EC2, S3, and Security Groups.

Preconditions:

The CloudFormation stack for GO SHOP has been successfully deployed.

User has access to AWS Management Console and AWS CLI with necessary permissions.

Test Cases:

Test Case 1: Validate EC2 Instance

Description: Check that the EC2 instance has been created and is running.

Steps:

Go to the AWS Management Console.

Navigate to EC2 Dashboard.

Check that there is a running instance with the name associated with WebServerInstance in the CloudFormation template.

Expected Result:

EC2 instance is in the running state.

Instance type is t2.micro.

Key Pair associated is “MyKeyPair”.

Status: Pending / Pass / Fail

Test Case 2: Validate Security Group Configuration

Description: Ensure the Security Group has been configured correctly.

Steps:

In the EC2 Dashboard, click on “Security Groups”.

Find and select the Security Group associated with WebServerSecurityGroup in the CloudFormation template.

Check the Inbound Rules to ensure port 22 (SSH) and port 80 (HTTP) are open.

Expected Result:

Port 22 and 80 are open for inbound traffic.

Status: Pending / Pass / Fail

Test Case 3: Validate S3 Bucket Creation

Description: Ensure the S3 bucket has been created.

Steps:

Go to the S3 Dashboard in AWS Management Console.

Check for the bucket with the name associated with WebsiteBucket in the CloudFormation template.

Expected Result:

S3 bucket is present.

Bucket has public read access.

Status: Pending / Pass / Fail

Test Case 4: Validate EC2 Web Server Response

Description: Ensure the web server on EC2 is serving the correct content.

Steps:

Obtain the Public IP or DNS of the EC2 instance.

Open a web browser and navigate to http://<Public-IP-or-DNS>.

Expected Result:

Web page displays “GO GUNDA SHOP >:)”.

Status: Pending / Pass / Fail

2.4 Deploy and configure cloud resource (provide screen shots where appropriate)

on learner labs you need to deploy resources out of 6 lists

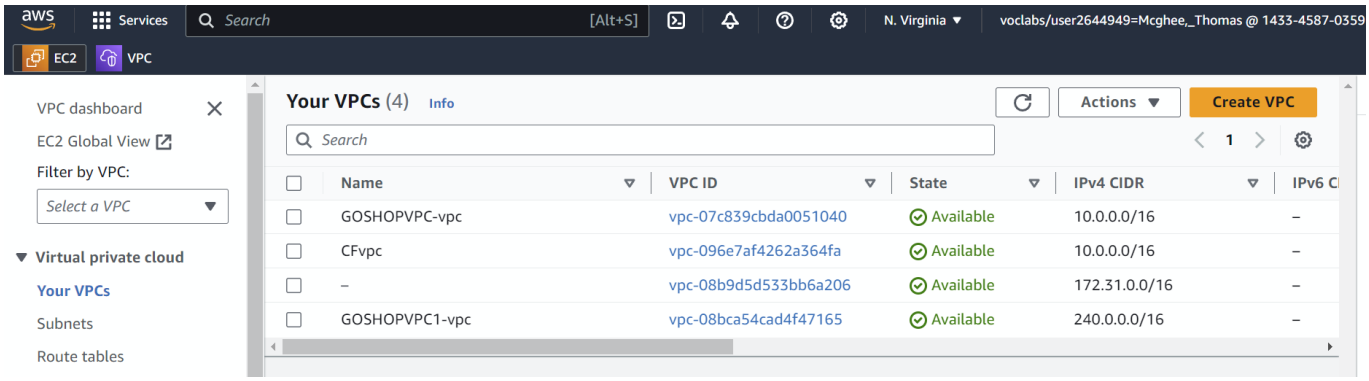
deploy these resources
deploy and configure at least 6 of the following different types of cloud resources, including but not limited to

- virtual machines

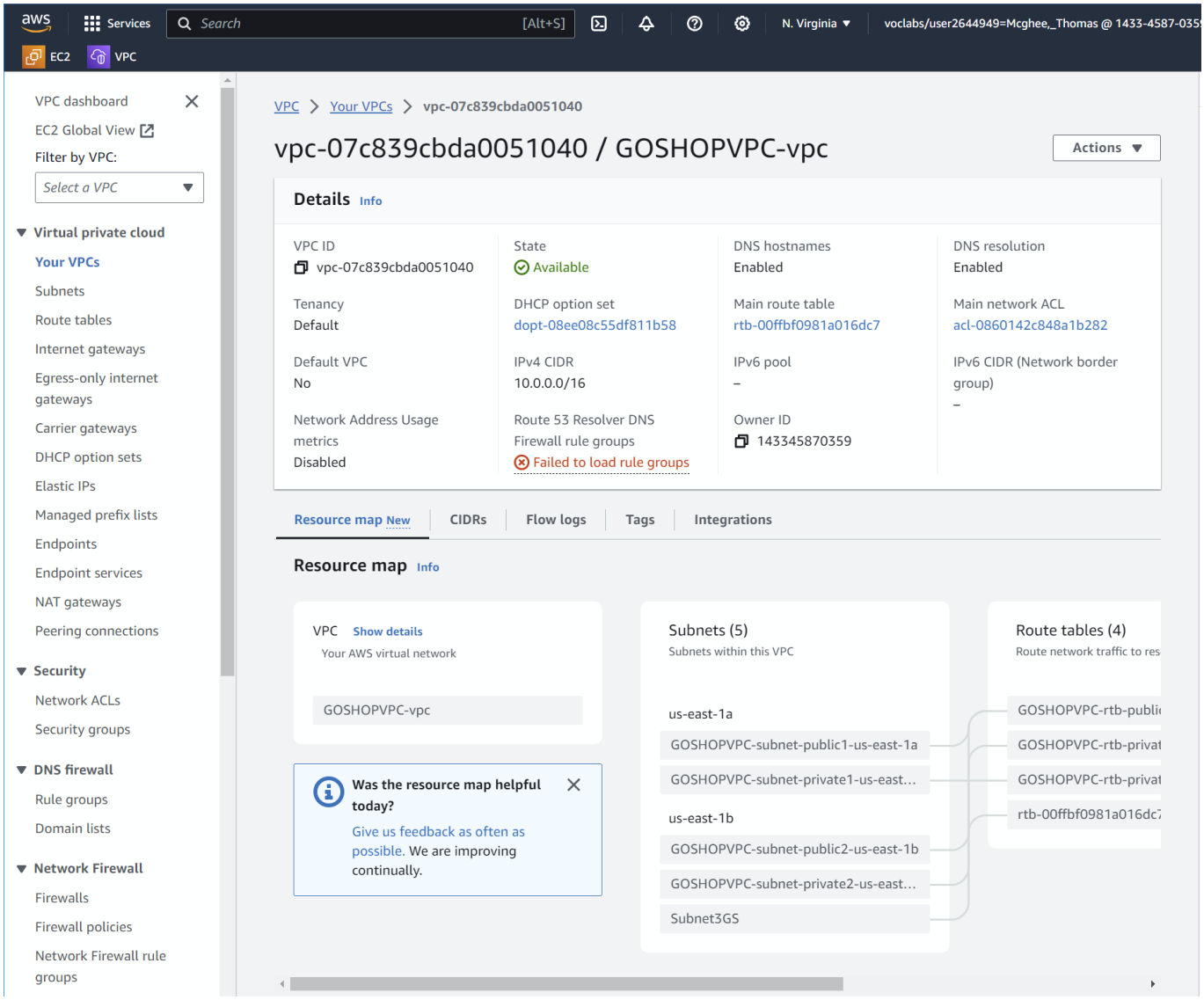
- container services
- load balancers and autoscaling
- serverless functions
- API gateways
- block or object storage
- managed databases
- DNS
- content delivery networks

there is a lab for route 53, use it, module lab, virtual machines should be able to do that.

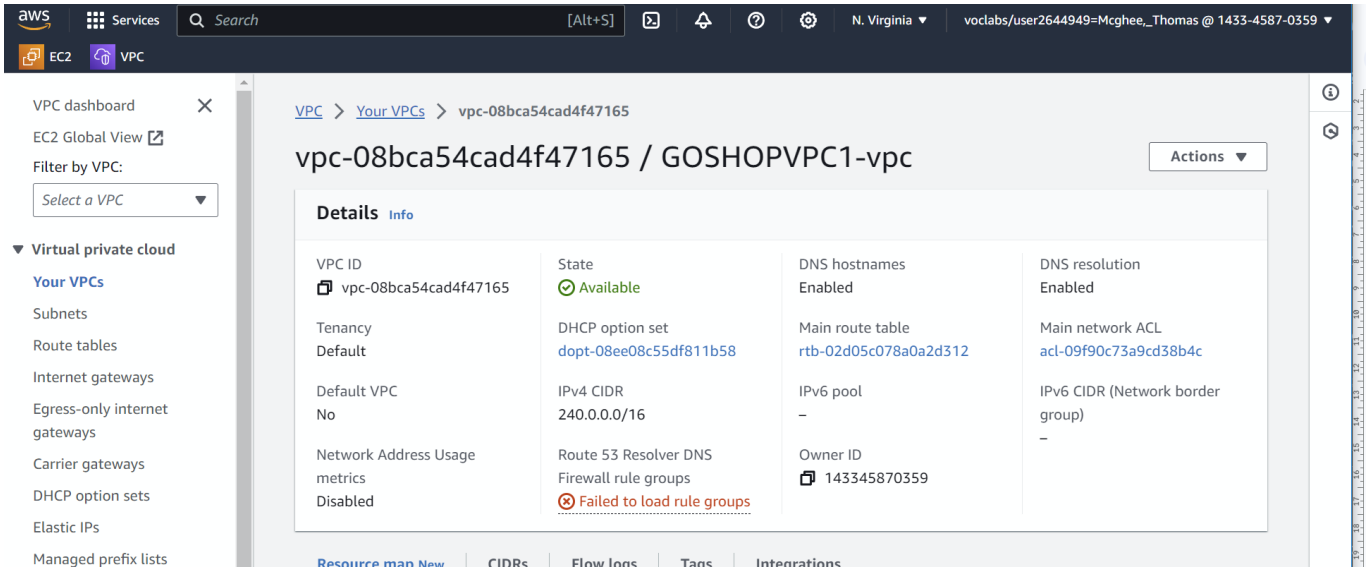
VPC CONFIGURATIONS



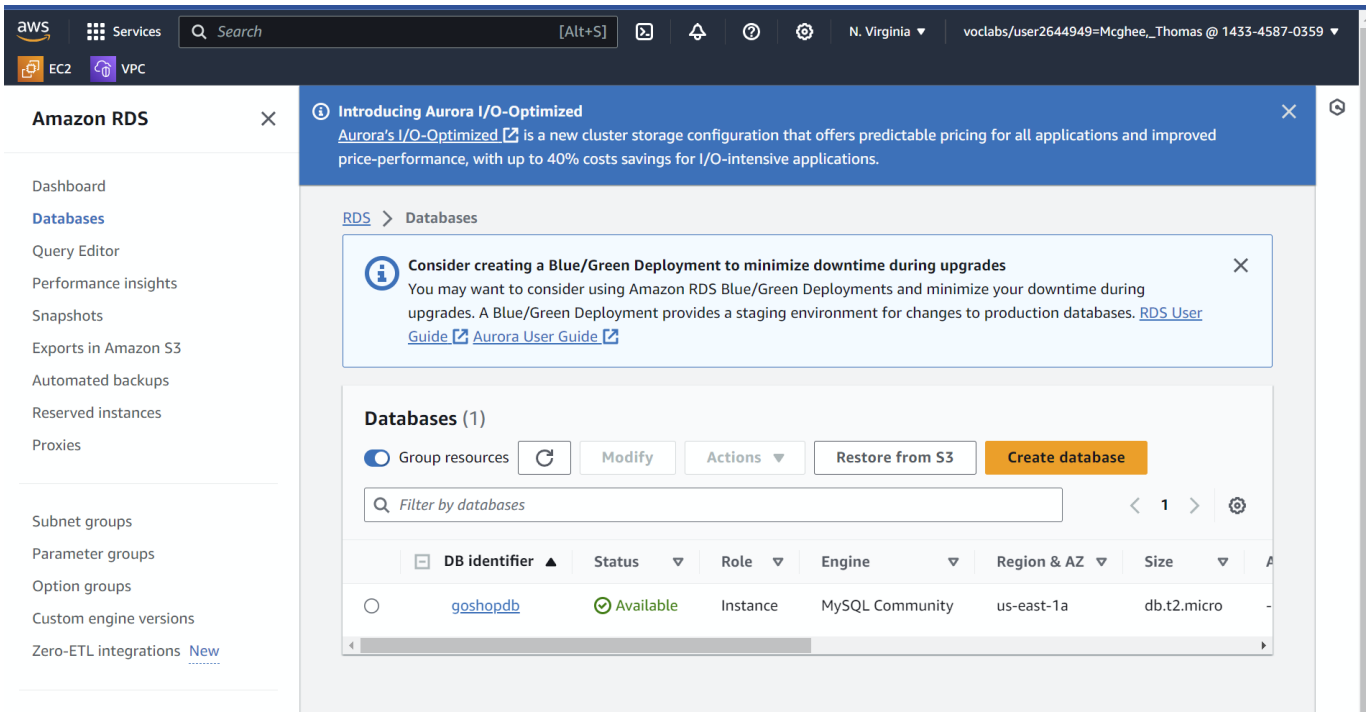
VPC0:


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 1433-4587-035
EC2
VPC
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
VPC > Your VPCs > vpc-07c839cbda0051040
vpc-07c839cbda0051040 / GOSHOPVPC-vpc
Actions
Details Info
VPC ID
vpc-07c839cbda0051040
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-08ee08c55df811b58
Main route table
rtb-00ffbf0981a016dc7
Main network ACL
acl-0860142c848a1b282
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups
Owner ID
143345870359
Resource map New
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
GOSHOPVPC-vpc
Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.
Subnets (5)
Subnets within this VPC
us-east-1a
GOSHOPVPC-subnet-public1-us-east-1a
GOSHOPVPC-subnet-private1-us-east...
us-east-1b
GOSHOPVPC-subnet-public2-us-east-1b
GOSHOPVPC-subnet-private2-us-east...
Subnet3GS
Route tables (4)
Route network traffic to res
GOSHOPVPC-rtb-publi
GOSHOPVPC-rtb-privat
GOSHOPVPC-rtb-privat
rtb-00ffbf0981a016dc7

VPC1:



RDS Instance Deployment:



ROUTE TABLES:

TABLE0:

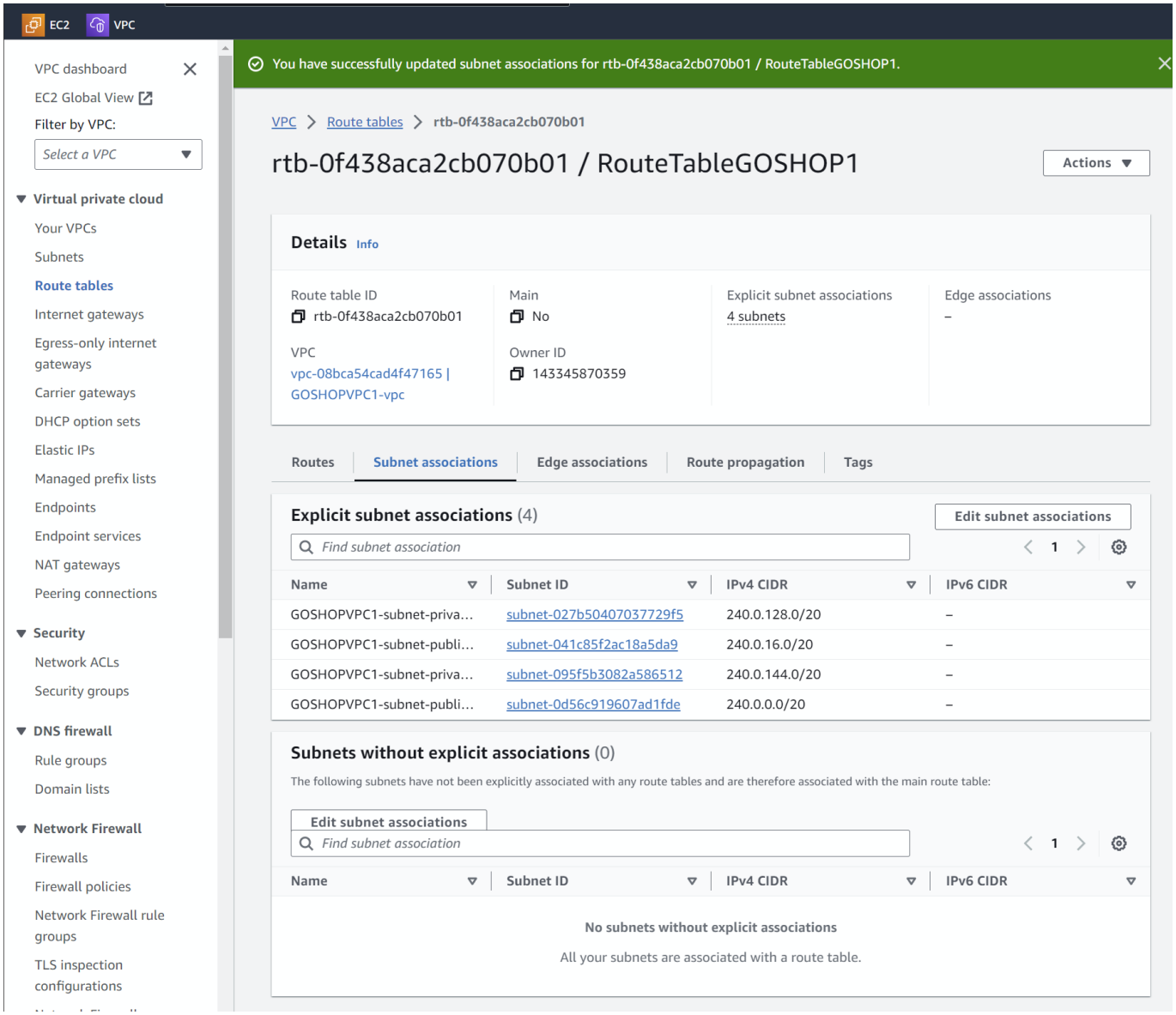
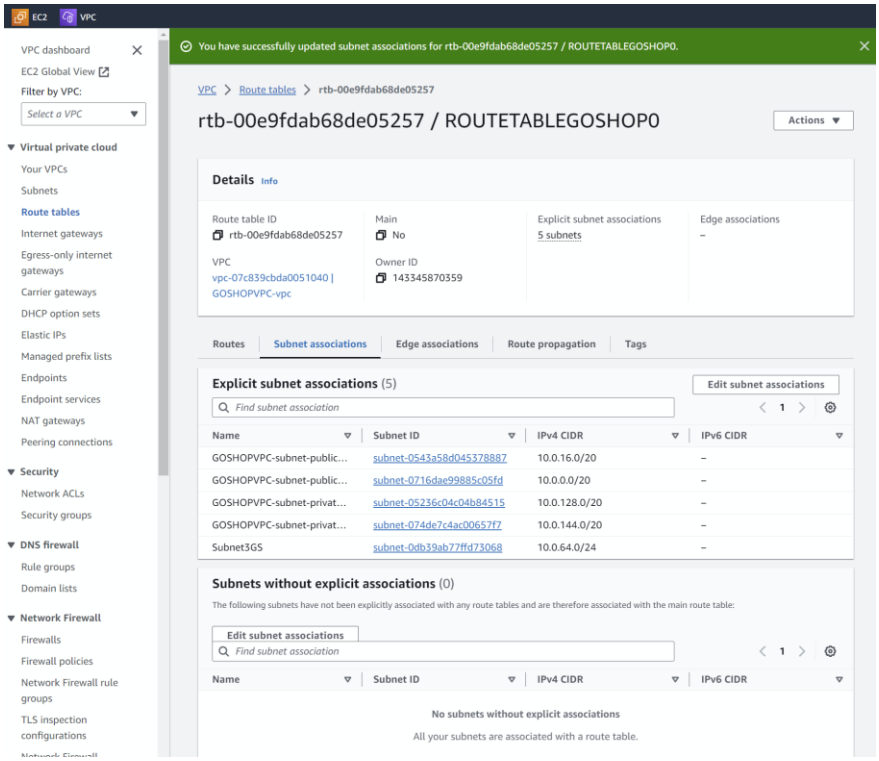
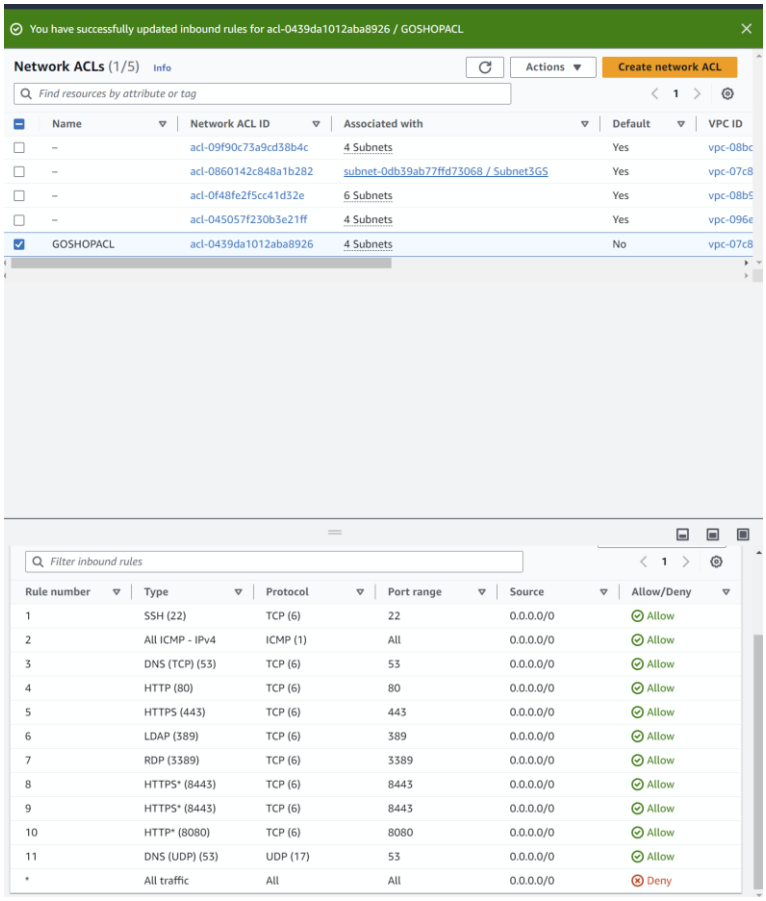


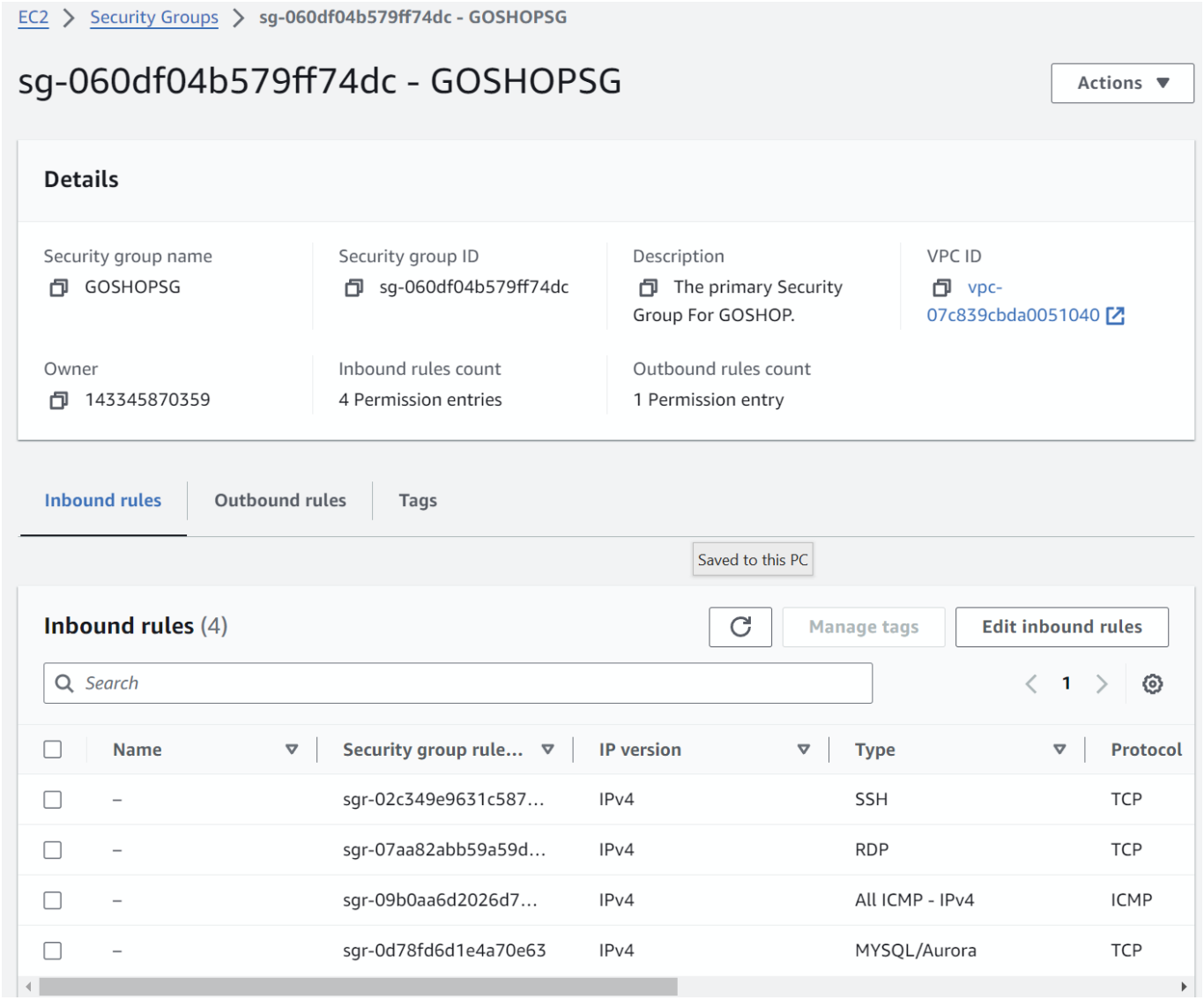
TABLE1:



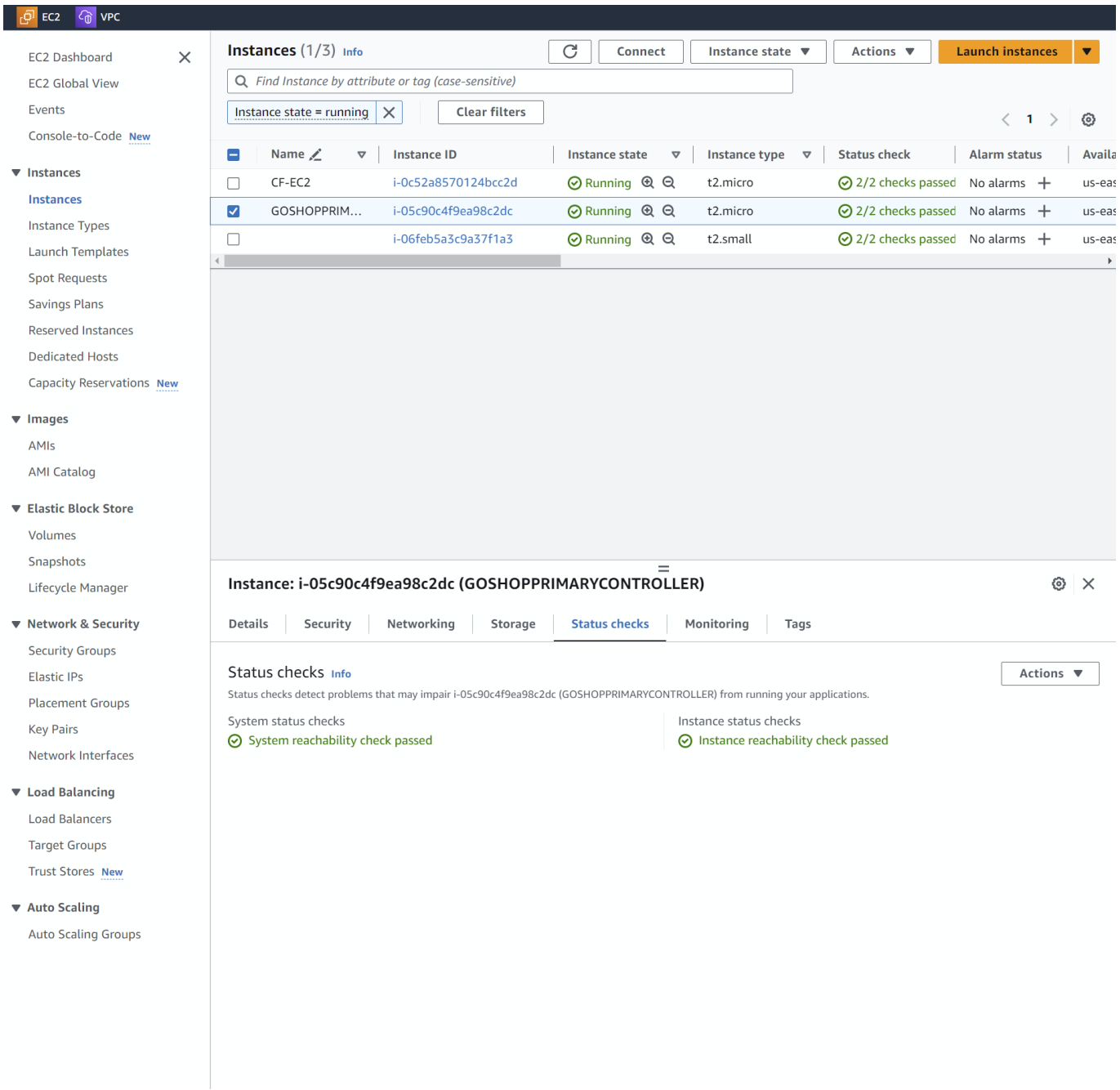
ACCESS CONTROL LISTS

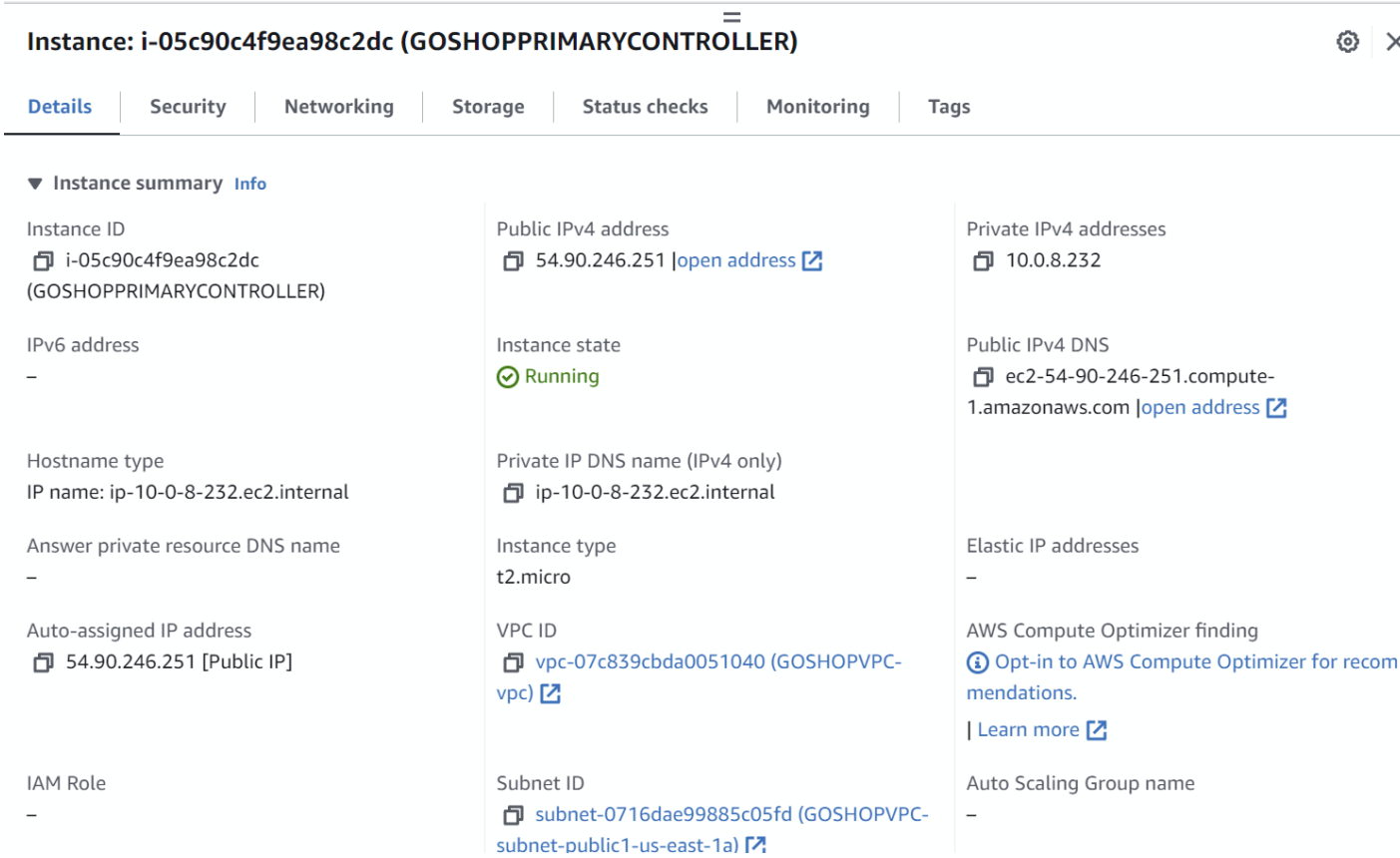


SECURITY GROUPS:

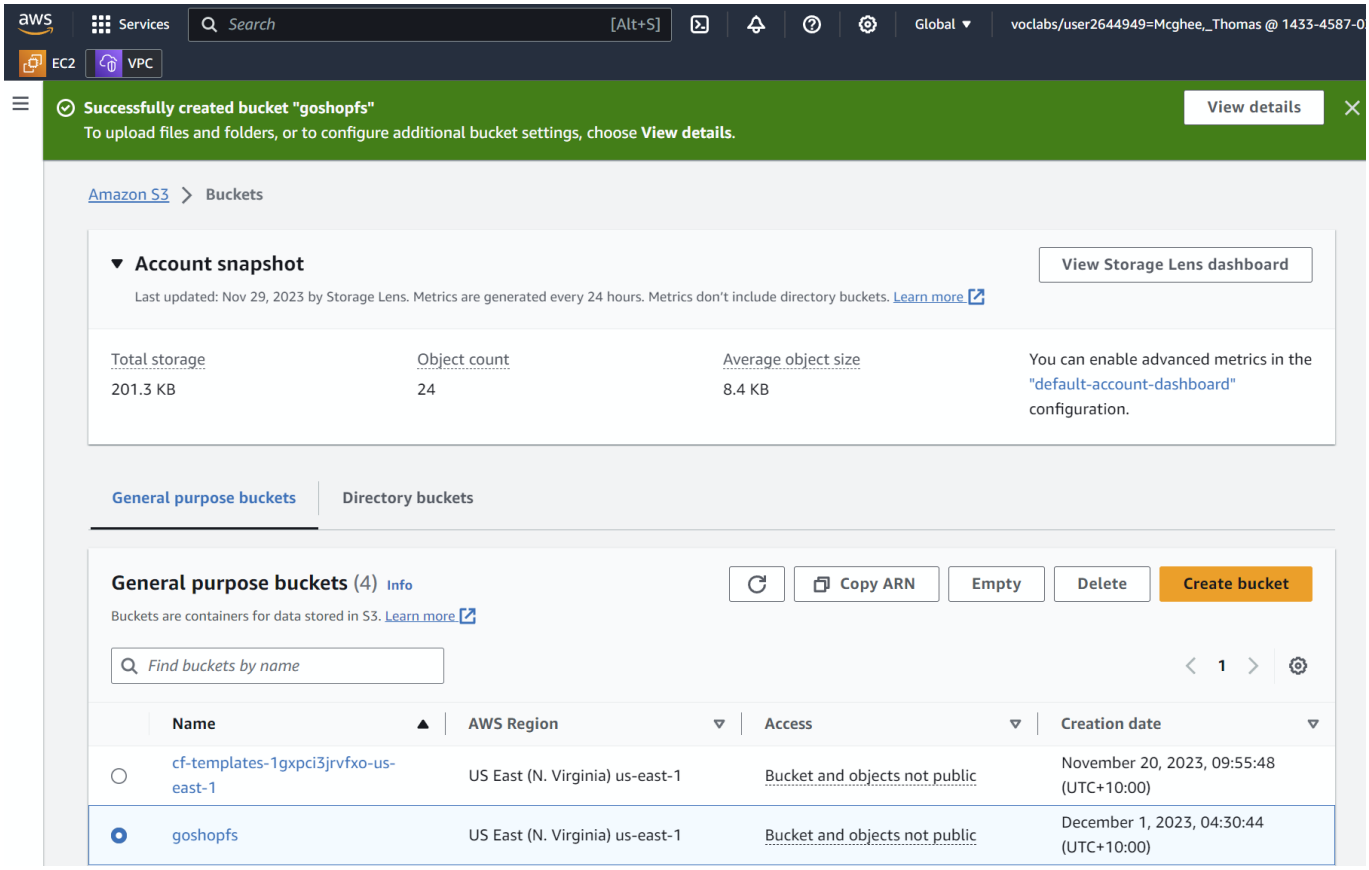


EC2 INSTANCES (DC AND DEFAULT [3rd]):

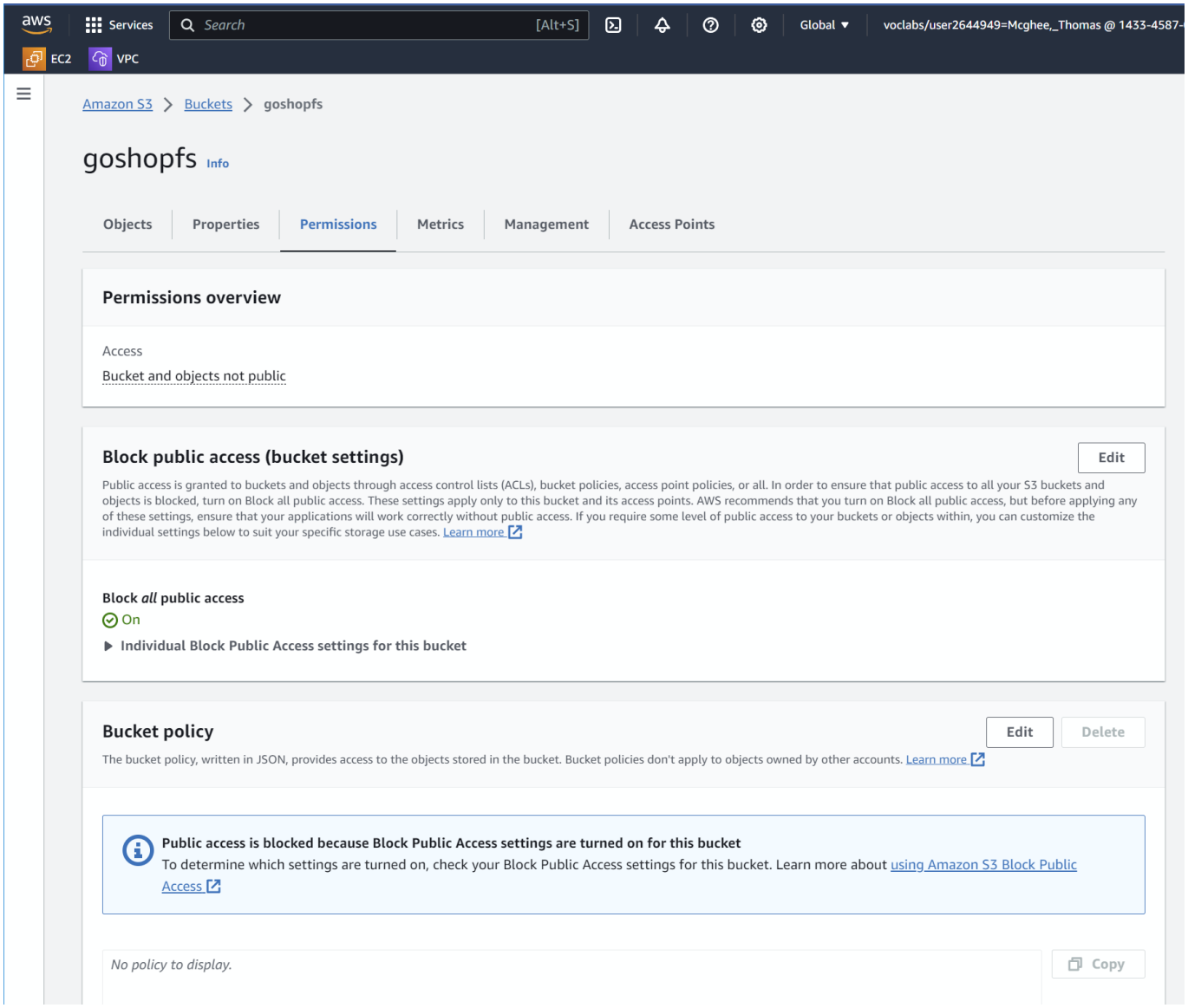




FILES SERVER DEPLOYMENT (S3)

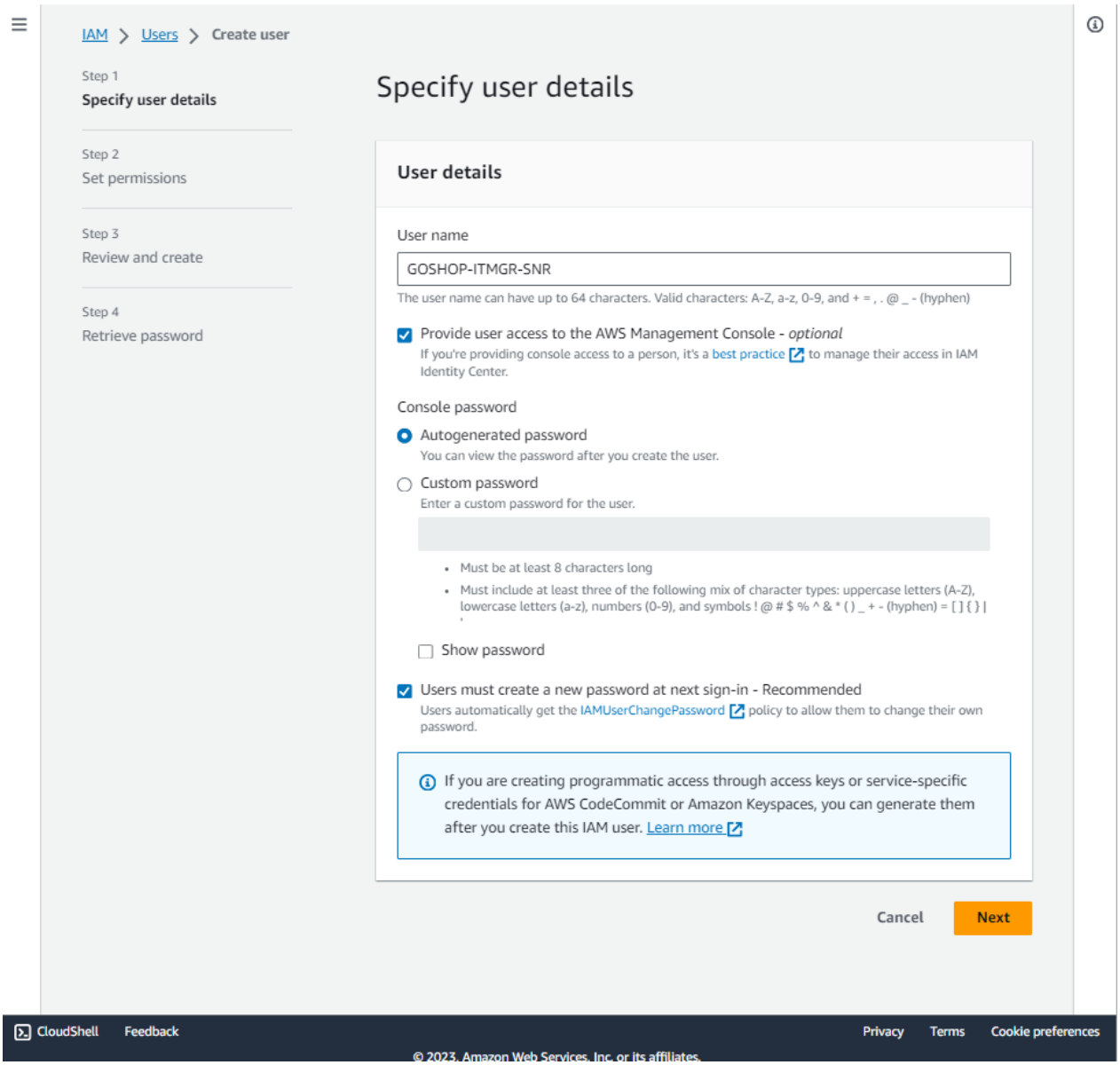


(BLOCKS RANDOM IPS ACCESSING FILESERVER) ^^^

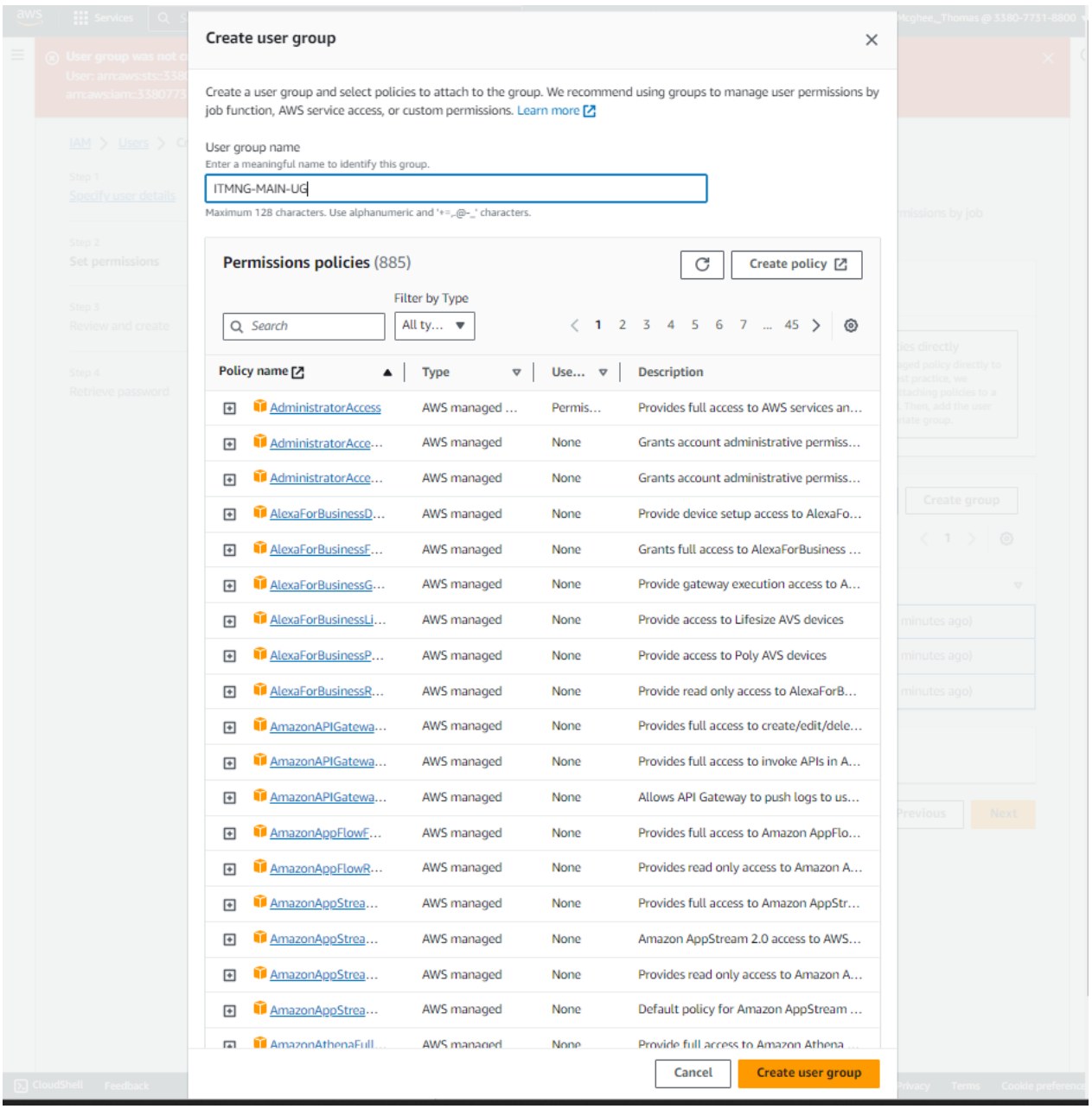

aws
Services
Search
[Alt+S]
Global
voclabs/user2644949=Mcghee,_Thomas @ 1433-4587-
EC2
VPC
Amazon S3
Buckets
goshopfs
goshopfs
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Bucket and objects not public
Block public access (bucket settings)
Edit
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
On
Individual Block Public Access settings for this bucket
Bucket policy
Edit
Delete
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access
No policy to display.
Copy

IAM

Creating IT Management IAM User



Creating new User Group With Administrator Access for Senior IT developer:

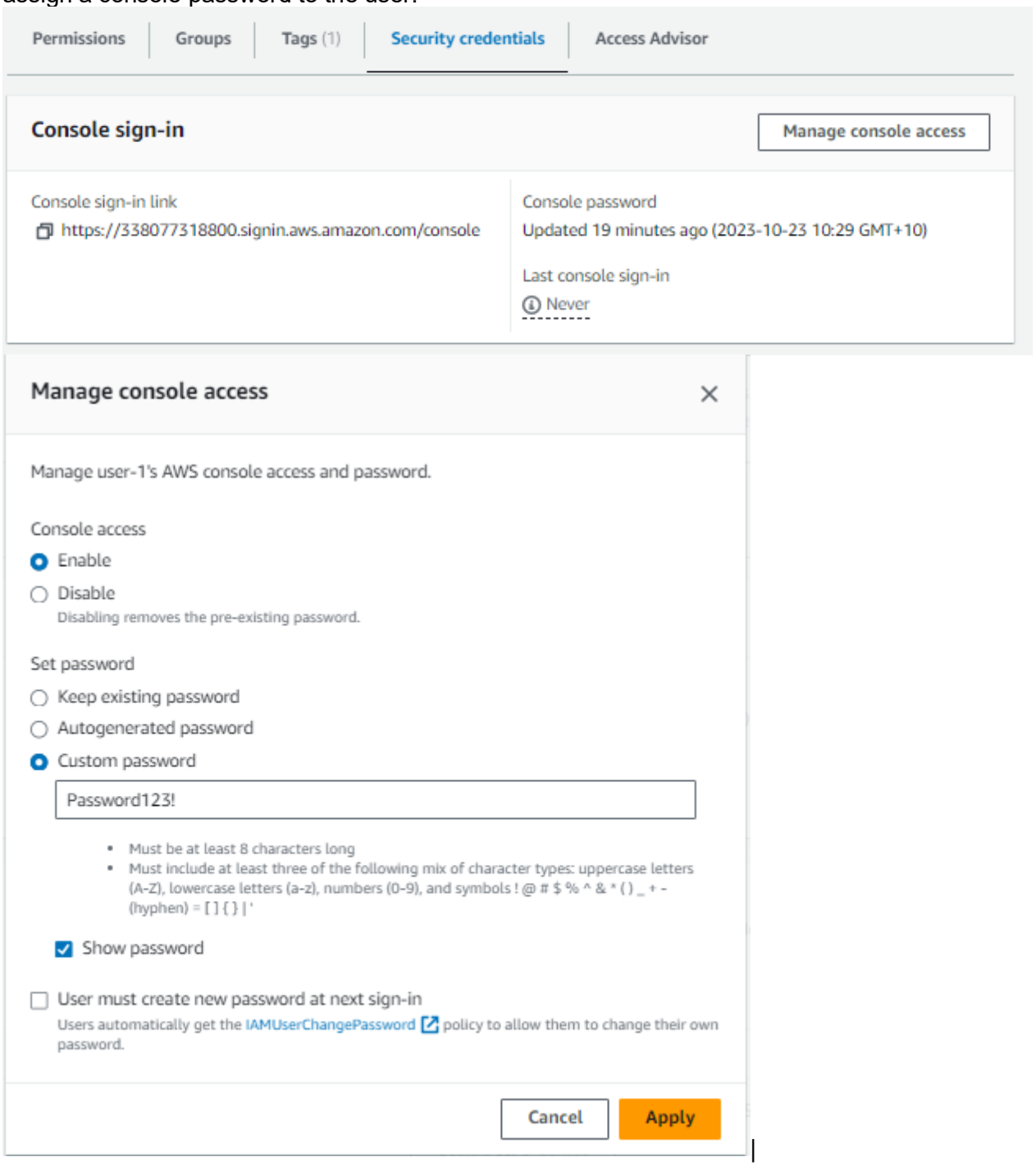


The (Administrator Access would be selected at the top - learner labs does not allow this) code is here:
(This Provides FULL Administrator access which is generally not recommended but will be used anyway)

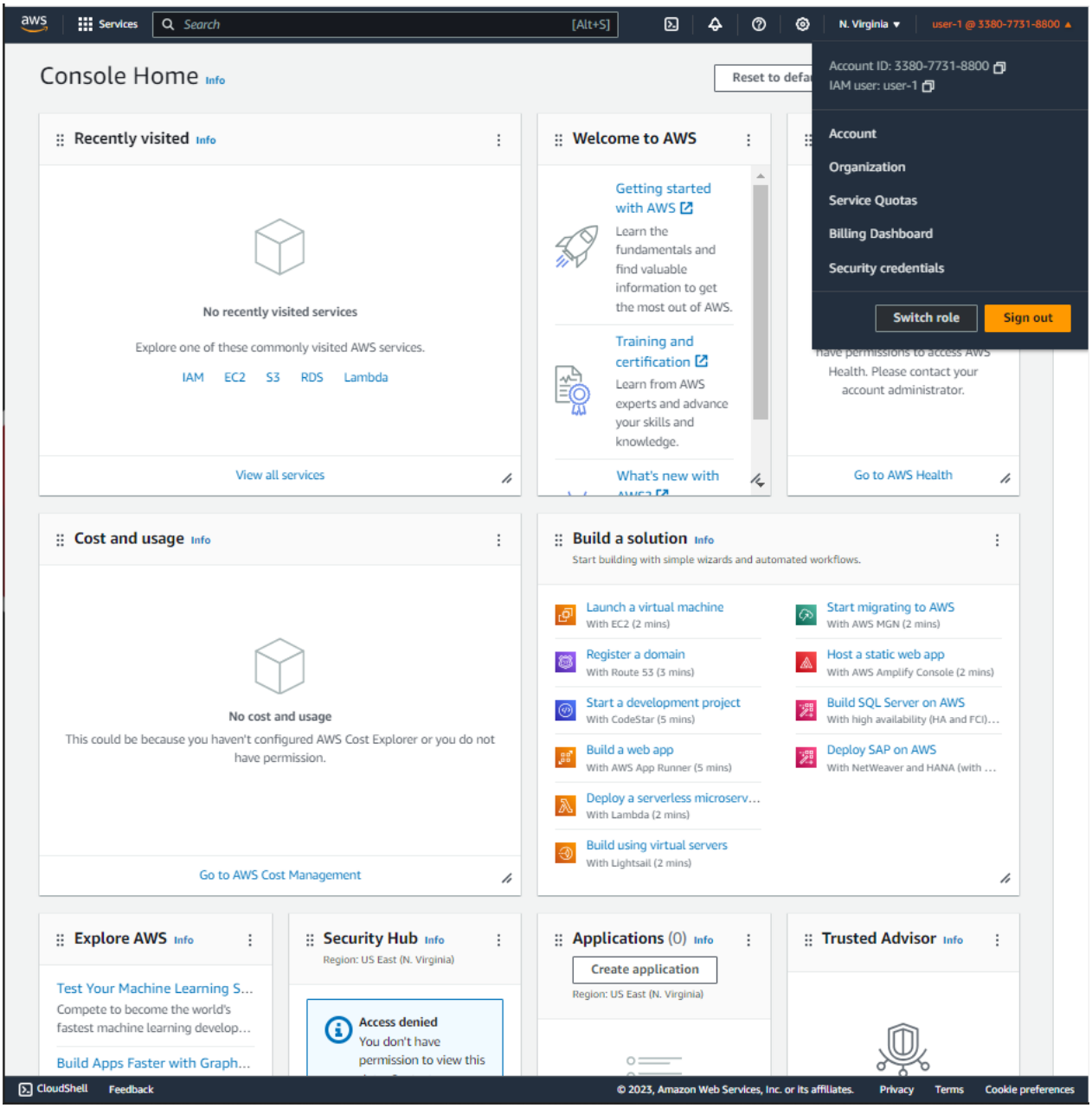
JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "*",
         "Resource": "*"
      }
   ]
}
```

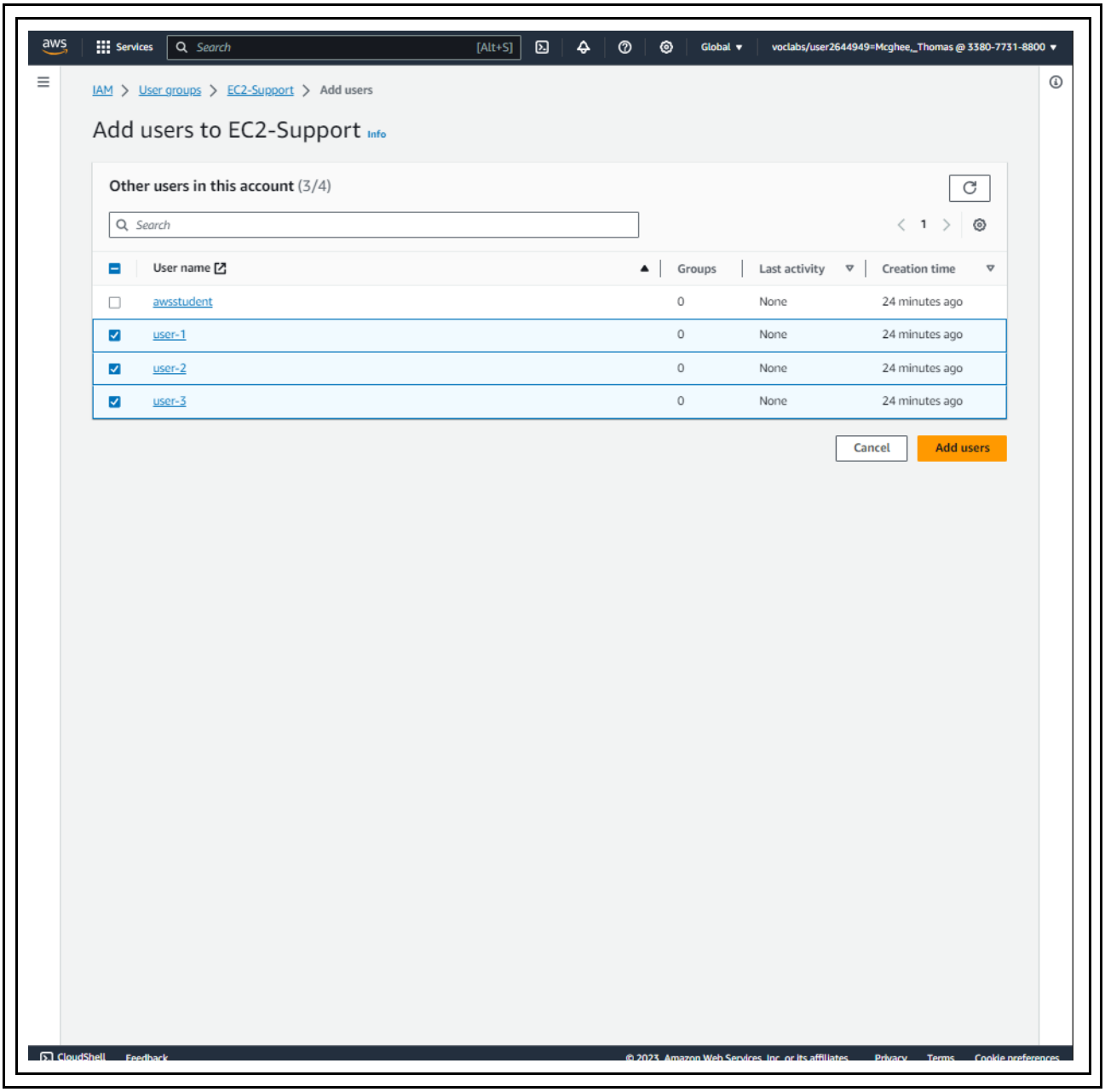
assign a console password to the user:



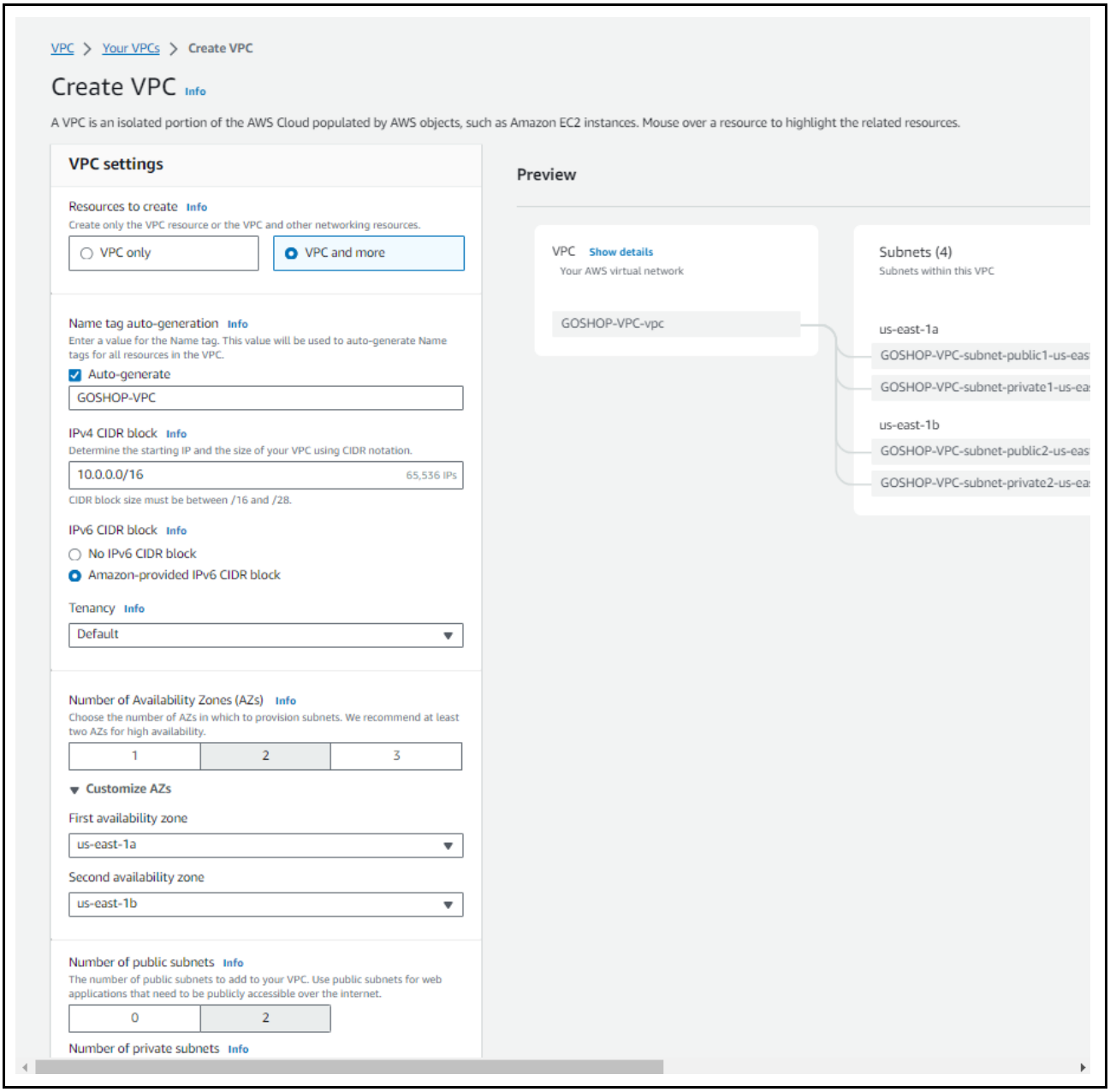
USER SIDE:
IT ADMIN ACCESS PAGE

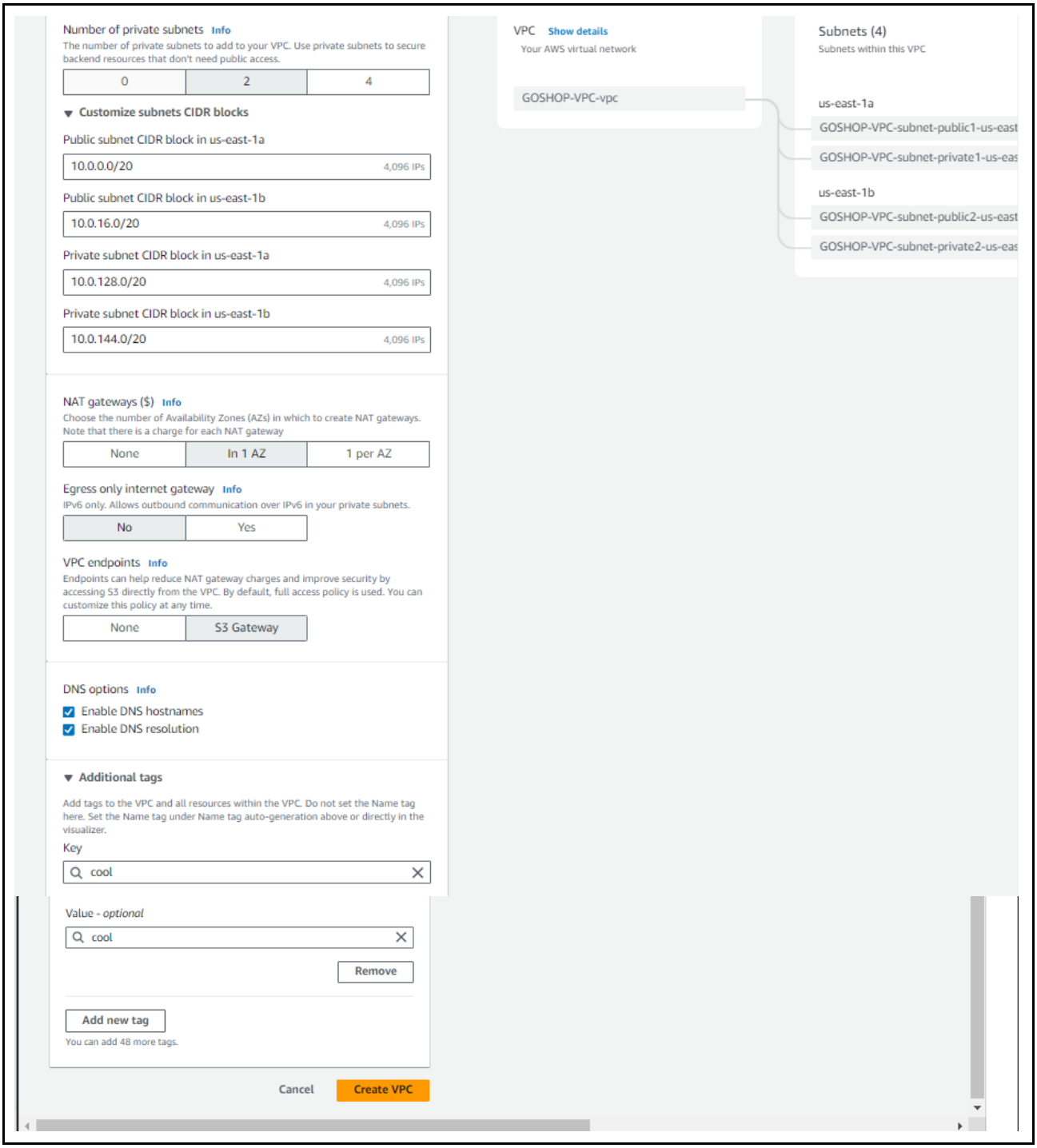


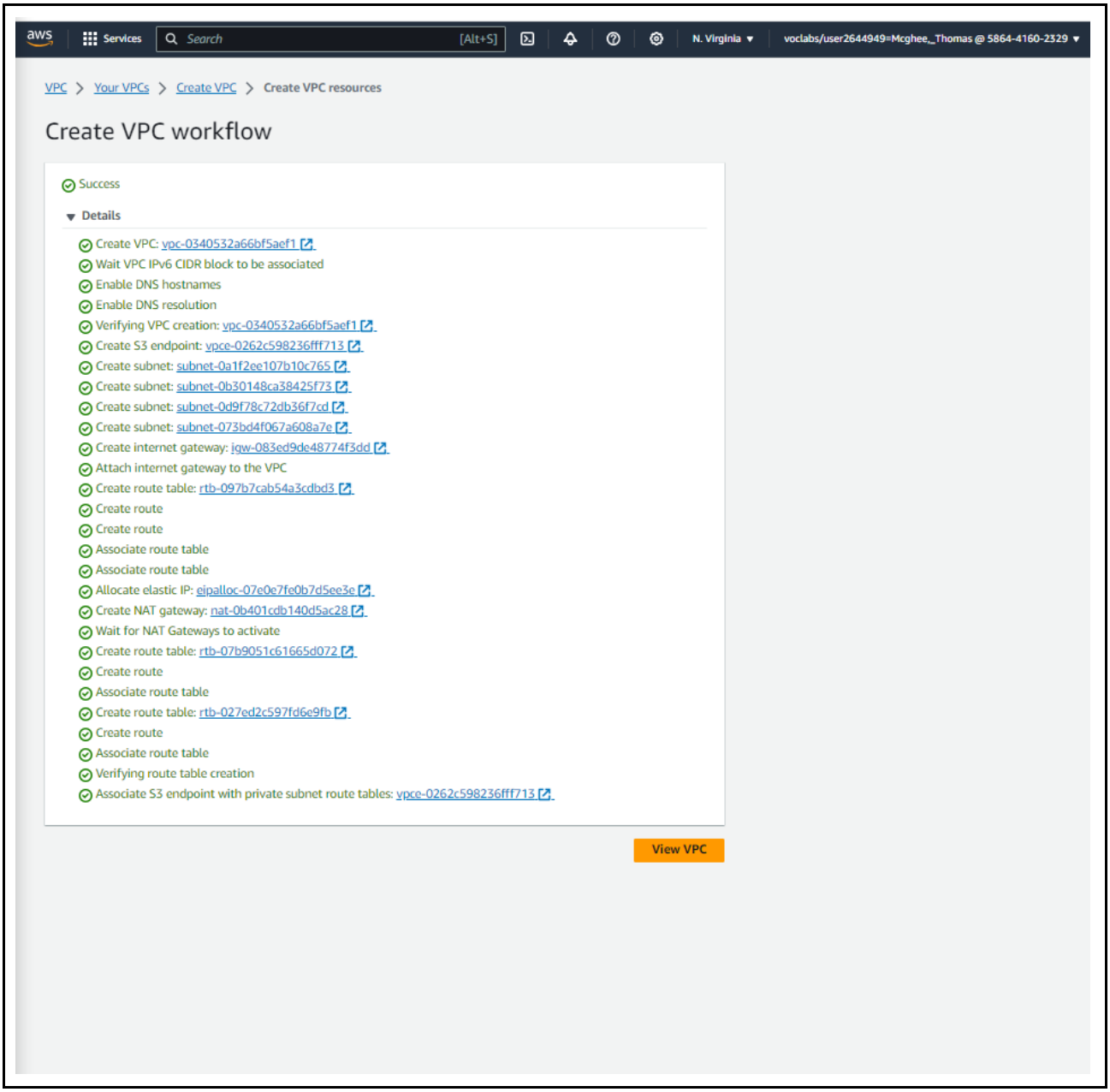
Adding IT SUPPORT IAM ROLES FOR GO SHOP INSTANCES

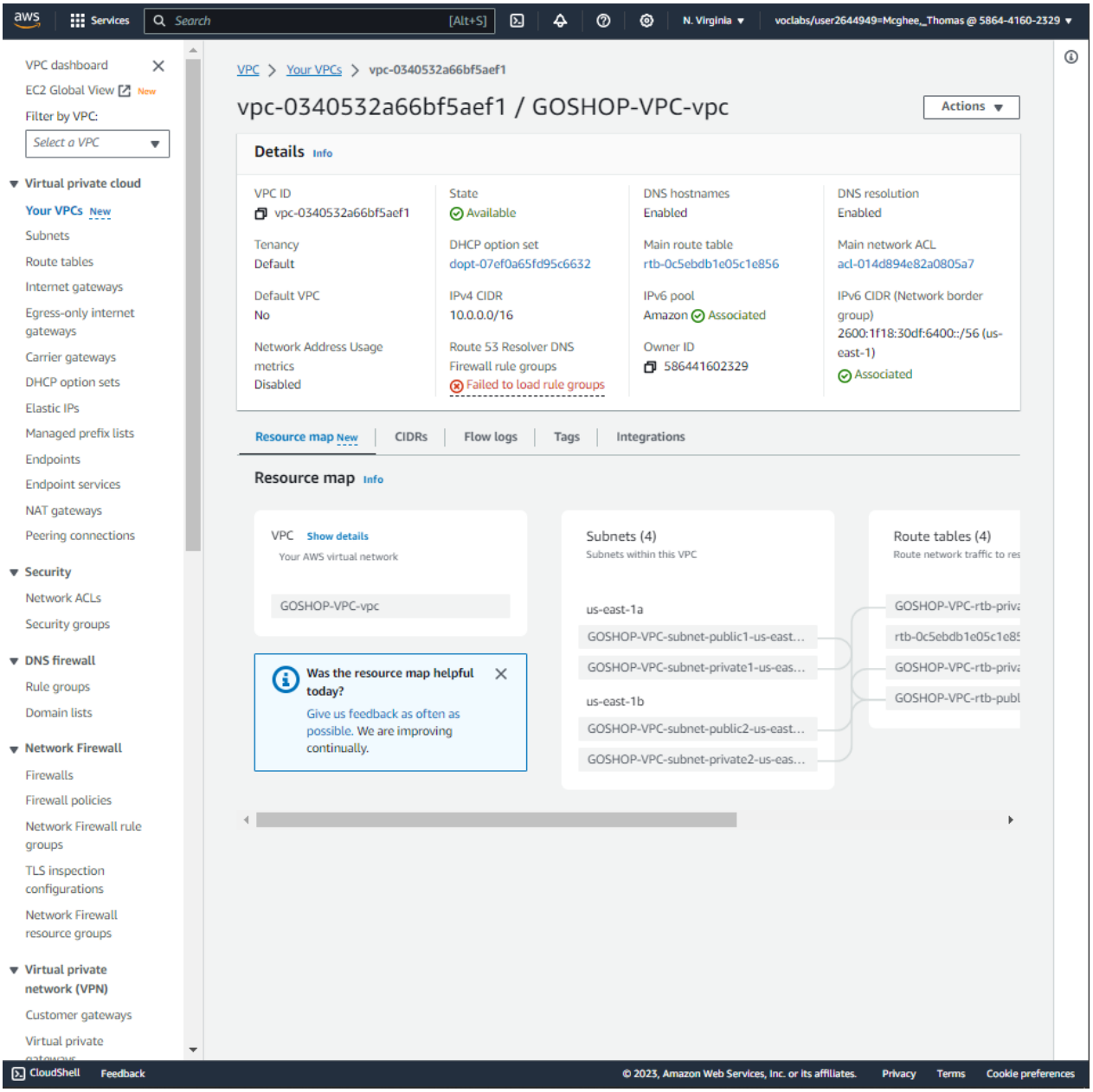


AWS VPC Config FOR GO SHOP


VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
GOSHOP-VPC
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16
65,536 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default
Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1
2
3
Customize AZs
First availability zone
us-east-1a
Second availability zone
us-east-1b
Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0
2
Number of private subnets Info
Preview
VPC Show details
Your AWS virtual network
GOSHOP-VPC-vpc
Subnets (4)
Subnets within this VPC
us-east-1a
GOSHOP-VPC-subnet-public1-us-eas
GOSHOP-VPC-subnet-private1-us-ea
us-east-1b
GOSHOP-VPC-subnet-public2-us-eas
GOSHOP-VPC-subnet-private2-us-ea


Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0
2
4
Customize subnets CIDR blocks
Public subnet CIDR block in us-east-1a
10.0.0.0/20
4,096 IPs
Public subnet CIDR block in us-east-1b
10.0.16.0/20
4,096 IPs
Private subnet CIDR block in us-east-1a
10.0.128.0/20
4,096 IPs
Private subnet CIDR block in us-east-1b
10.0.144.0/20
4,096 IPs
NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
None
In 1 AZ
1 per AZ
Egress only internet gateway Info
IPv6 only. Allows outbound communication over IPv6 in your private subnets.
No
Yes
VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None
S3 Gateway
DNS options Info
Enable DNS hostnames
Enable DNS resolution
Additional tags
Add tags to the VPC and all resources within the VPC. Do not set the Name tag here. Set the Name tag under Name tag auto-generation above or directly in the visualizer.
Key
cool
Value - optional
cool
Remove
Add new tag
You can add 48 more tags.
Cancel
Create VPC
VPC Show details
Your AWS virtual network
GOSHOP-VPC-vpc
Subnets (4)
Subnets within this VPC
us-east-1a
GOSHOP-VPC-subnet-public1-us-east
GOSHOP-VPC-subnet-private1-us-eas
us-east-1b
GOSHOP-VPC-subnet-public2-us-east
GOSHOP-VPC-subnet-private2-us-eas


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 5864-4160-2329
VPC > Your VPCs > Create VPC > Create VPC resources
Create VPC workflow
Success
Details
Create VPC: vpc-0340532a66bf5aef1
Wait VPC IPv6 CIDR block to be associated
Enable DNS hostnames
Enable DNS resolution
Verifying VPC creation: vpc-0340532a66bf5aef1
Create S3 endpoint: vpce-0262c598236fff713
Create subnet: subnet-0a1f2ee107b10c765
Create subnet: subnet-0b30148ca38425f73
Create subnet: subnet-0d9f78c72db36f7cd
Create subnet: subnet-073bd4f067a608a7e
Create internet gateway: igw-083ed9de48774f3dd
Attach internet gateway to the VPC
Create route table: rtb-097b7cab54a3cdbd3
Create route
Create route
Associate route table
Associate route table
Allocate elastic IP: eipalloc-07e0e7fe0b7d5ee3e
Create NAT gateway: nat-0b401cdb140d5ac28
Wait for NAT Gateways to activate
Create route table: rtb-07b9051c61665d072
Create route
Associate route table
Create route table: rtb-027ed2c597fd6e9fb
Create route
Associate route table
Verifying route table creation
Associate S3 endpoint with private subnet route tables: vpce-0262c598236fff713
View VPC



Cloudformation template: (with extra subnet for added control)

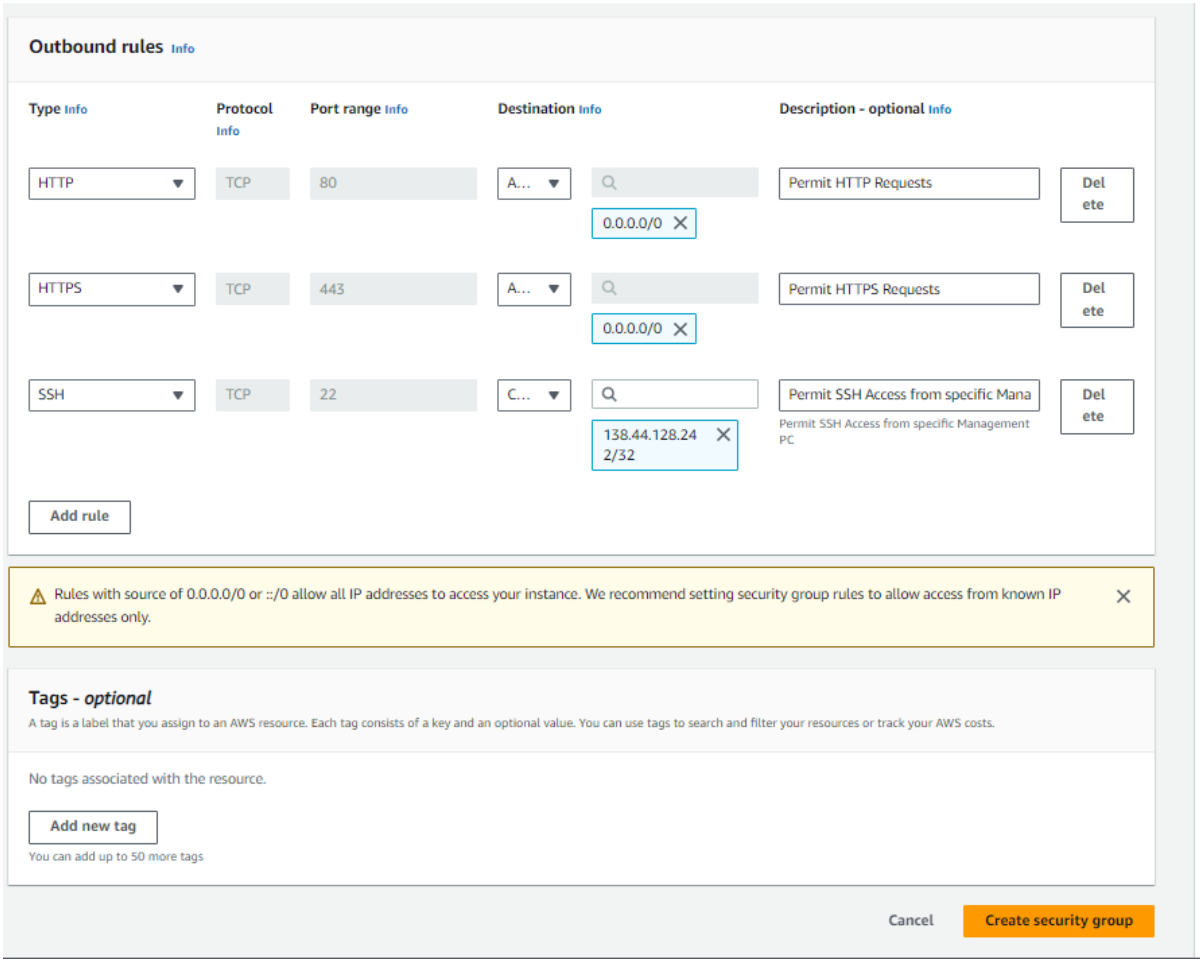
AWSTemplateFormatVersion: '2010-09-09'
Description: GoShop VPC CloudFormation Template
 	
Resources:
  GoShopVPC:
  Type: AWS::EC2::VPC
  Properties:
  CidrBlock: 10.0.0.0/16
  EnableDnsHostnames: true
  EnableDnsSupport: true
  Tags:
  - Key: Name

```
        Value: GOSHOP-VPC

PublicSubnetA:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.0.0/20
    AvailabilityZone: us-east-1a
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: GOSHOP-PublicSubnet-A

PublicSubnetB:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.16.0/20
    AvailabilityZone: us-east-1b
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: GOSHOP-PublicSubnet-B

PublicSubnetC:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.32.0/20
    AvailabilityZone: us-east-1c
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: GOSHOP-PublicSubnet-C

PrivateSubnetA:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.128.0/20
    AvailabilityZone: us-east-1a
    Tags:
      - Key: Name
        Value: GOSHOP-PrivateSubnet-A

PrivateSubnetB:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.144.0/20
    AvailabilityZone: us-east-1b
    Tags:
      - Key: Name
        Value: GOSHOP-PrivateSubnet-B
```

```
PrivateSubnetC:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref GoShopVPC
    CidrBlock: 10.0.160.0/20
    AvailabilityZone: us-east-1c
    Tags:
      - Key: Name
        Value: GOSHOP-PrivateSubnet-C

InternetGateway:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: GOSHOP-IGW

AttachGateway:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    VpcId: !Ref GoShopVPC
    InternetGatewayId: !Ref InternetGateway

PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref GoShopVPC
    Tags:
      - Key: Name
        Value: GOSHOP-PublicRouteTable

DefaultPublicRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway

AssociatePublicSubnetA:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    SubnetId: !Ref PublicSubnetA
    RouteTableId: !Ref PublicRouteTable

AssociatePublicSubnetB:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    SubnetId: !Ref PublicSubnetB
    RouteTableId: !Ref PublicRouteTable

AssociatePublicSubnetC:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
```

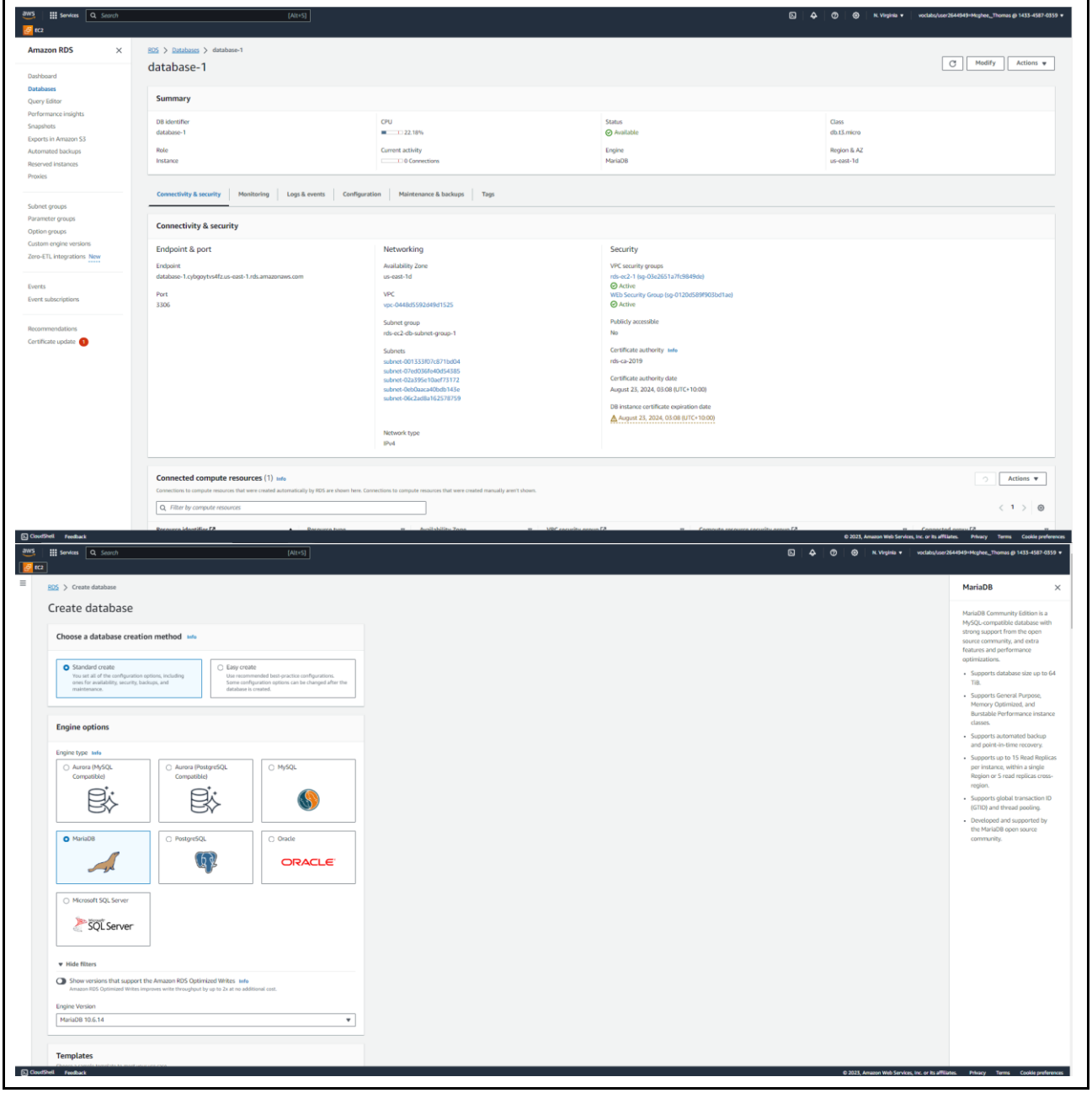
```
    SubnetId: !Ref PublicSubnetC
    RouteTableId: !Ref PublicRouteTable

Outputs:
  VPCId:
    Description: The ID of the VPC
    Value: !Ref GoShopVPC
```

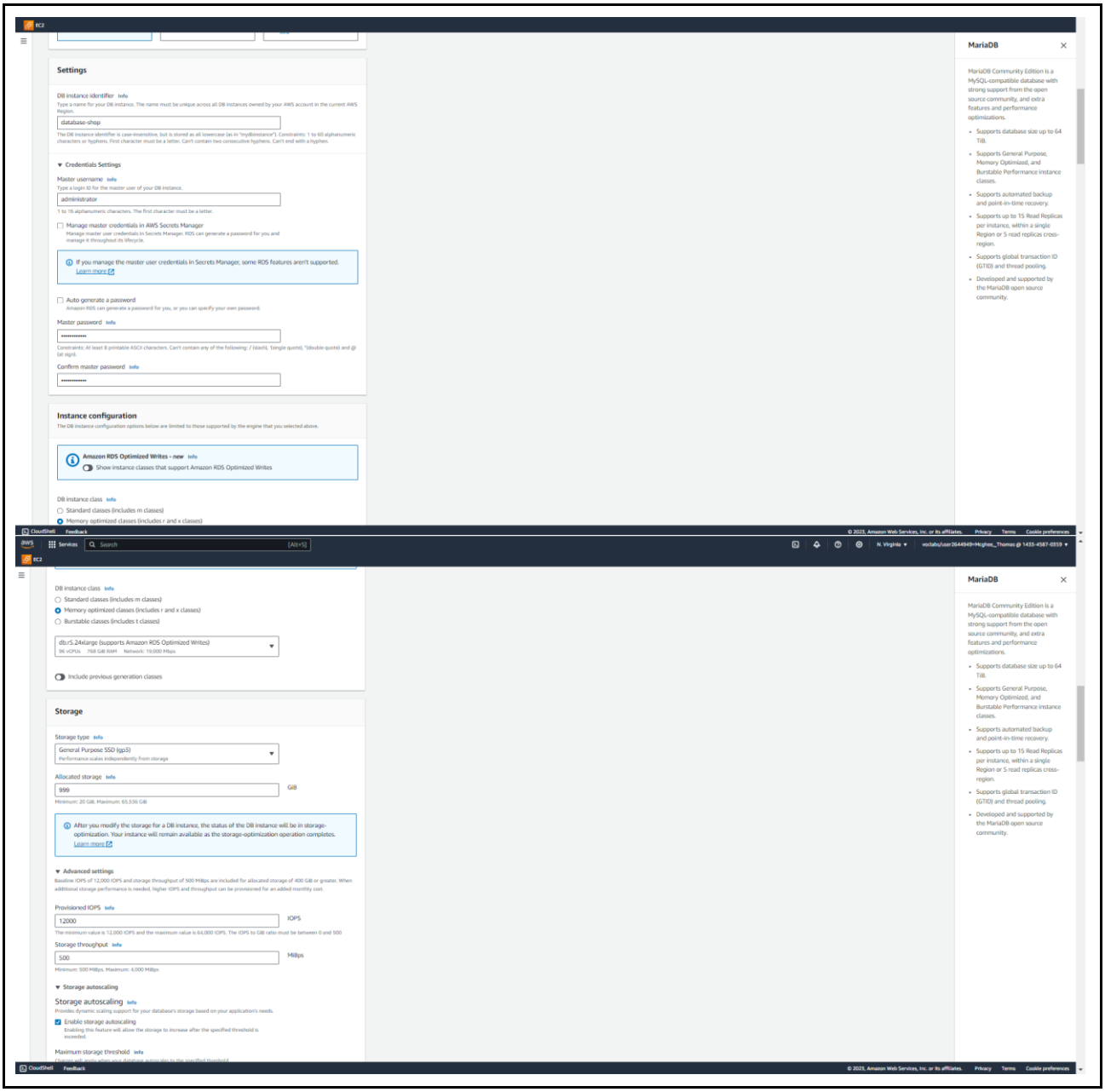
Creating SG for VPC

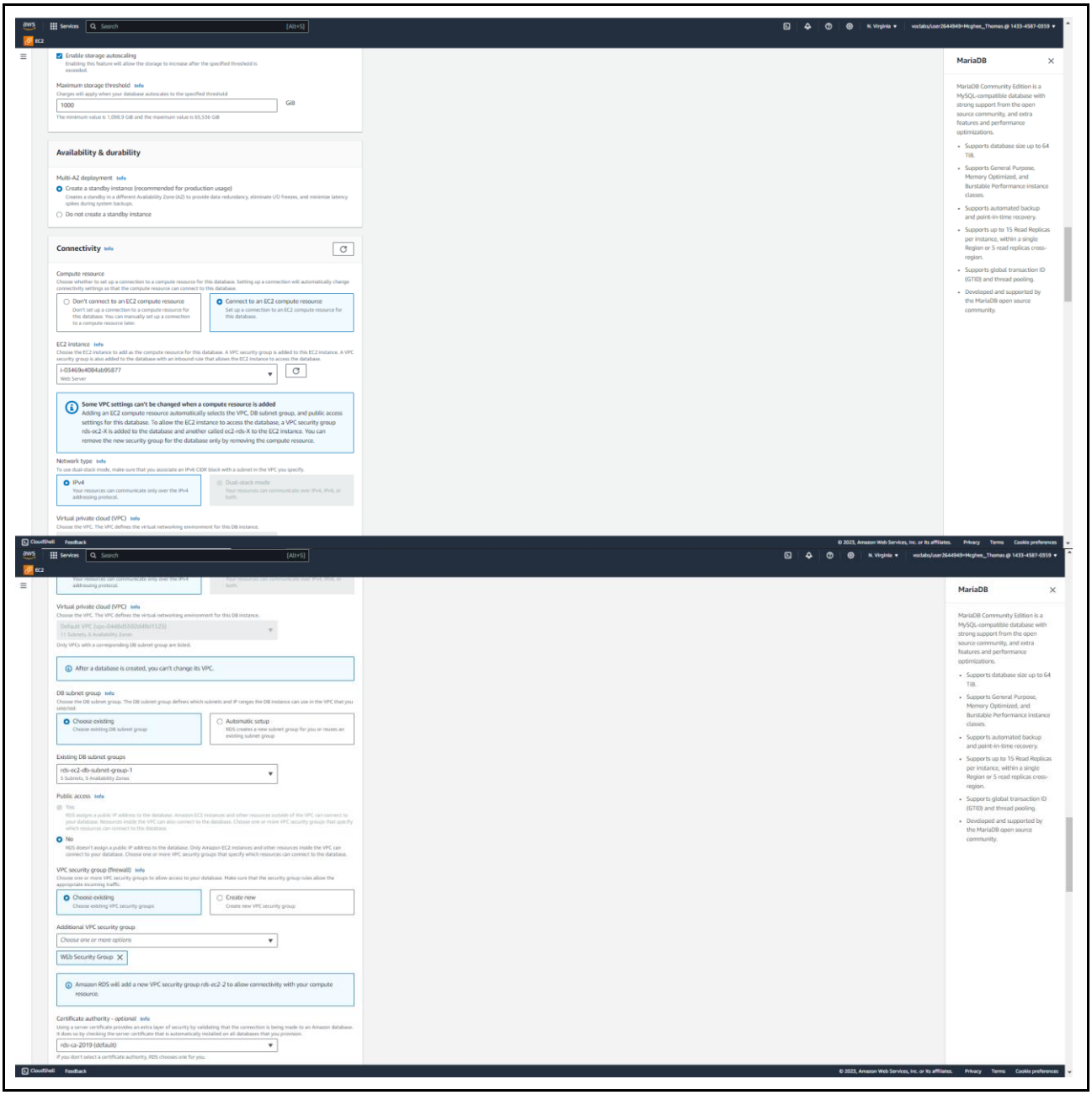


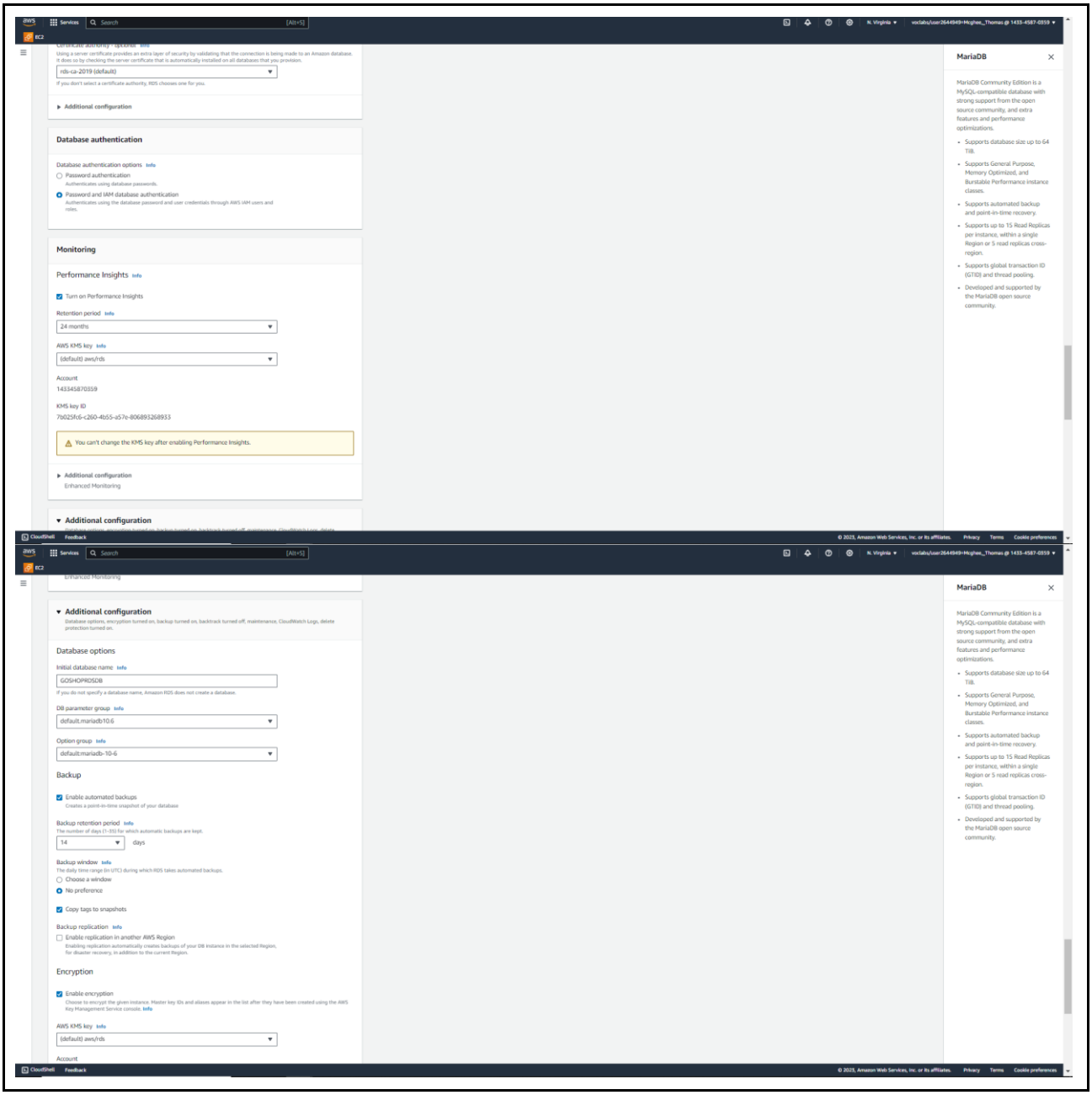
Allows SSH access from specific Management PC with allocate IP address at company location.

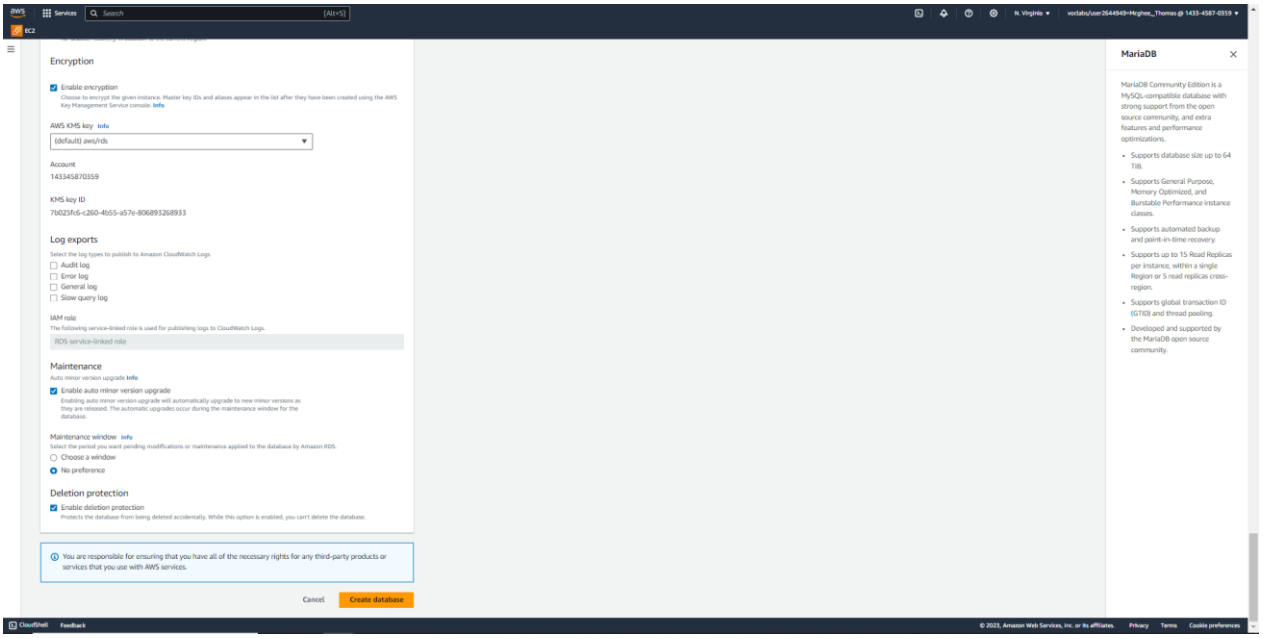
AWS RDS for GO SHOP




Settings
DB instance identifier
database-shop
Credentials Settings
Master username
administrator
Manage master credentials in AWS Secrets Manager
Auto generate a password
Master password
Confirm master password
Instance configuration
Amazon RDS Optimized Writes - new
DB instance class
Standard classes (includes m classes)
Memory optimized classes (includes r and x classes)
MariaDB
MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
Supports global transaction ID (GTID) and thread pooling.
Developed and supported by the MariaDB open source community.
Burstable classes (includes t classes)
db.r5.24xlarge (supports Amazon RDS Optimized Writes)
Include previous generation classes
Storage
Storage type
General Purpose SSD (gp3)
Allocated storage
999
GiB
Advanced settings
Provisioned IOPS
12000
IOPS
Storage throughput
500
MiBps
Storage autoscaling
Enable storage autoscaling
Maximum storage threshold


Enable storage autoscaling
Maximum storage threshold
1000
GiB
Availability & durability
Multi-AZ deployment
Create a standby instance (recommended for production usage)
Do not create a standby instance
Connectivity
Compute resource
Don't connect to an EC2 compute resource
Connect to an EC2 compute resource
EC2 instance
i-03469e4084ab95877
Web Server
Some VPC settings can't be changed when a compute resource is added
Network type
IPv4
Dual-stack mode
Virtual private cloud (VPC)
MariaDB
MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
Supports global transaction ID (GTID) and thread pooling.
Developed and supported by the MariaDB open source community.
Virtual private cloud (VPC)
After a database is created, you can't change its VPC.
DB subnet group
Choose existing
Automatic setup
Existing DB subnet groups
rds-ec2-db-subnet-group-1
Public access
No
VPC security group (firewall)
Choose existing
Create new
Additional VPC security group
Choose one or more options
WEb Security Group
Amazon RDS will add a new VPC security group rds-ec2-2 to allow connectivity with your compute resource.
Certificate authority - optional
rds-ca-2019 (default)


Database authentication
Database authentication options
Password authentication
Password and IAM database authentication
Monitoring
Performance Insights
Turn on Performance Insights
Retention period
24 months
AWS KMS key
(default) aws/rds
Account
143345870359
KMS key ID
7b025fc6-c260-4b55-a57e-806893268933
You can't change the KMS key after enabling Performance Insights.
Additional configuration
Enhanced Monitoring
Additional configuration
Database options
Initial database name
GOSHOPRDSDB
DB parameter group
default.mariadb10.6
Option group
default:mariadb-10-6
Backup
Enable automated backups
Backup retention period
14
days
Backup window
Choose a window
No preference
Copy tags to snapshots
Backup replication
Enable replication in another AWS Region
Encryption
Enable encryption
AWS KMS key
(default) aws/rds
Account
MariaDB
MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
Supports global transaction ID (GTID) and thread pooling.
Developed and supported by the MariaDB open source community.

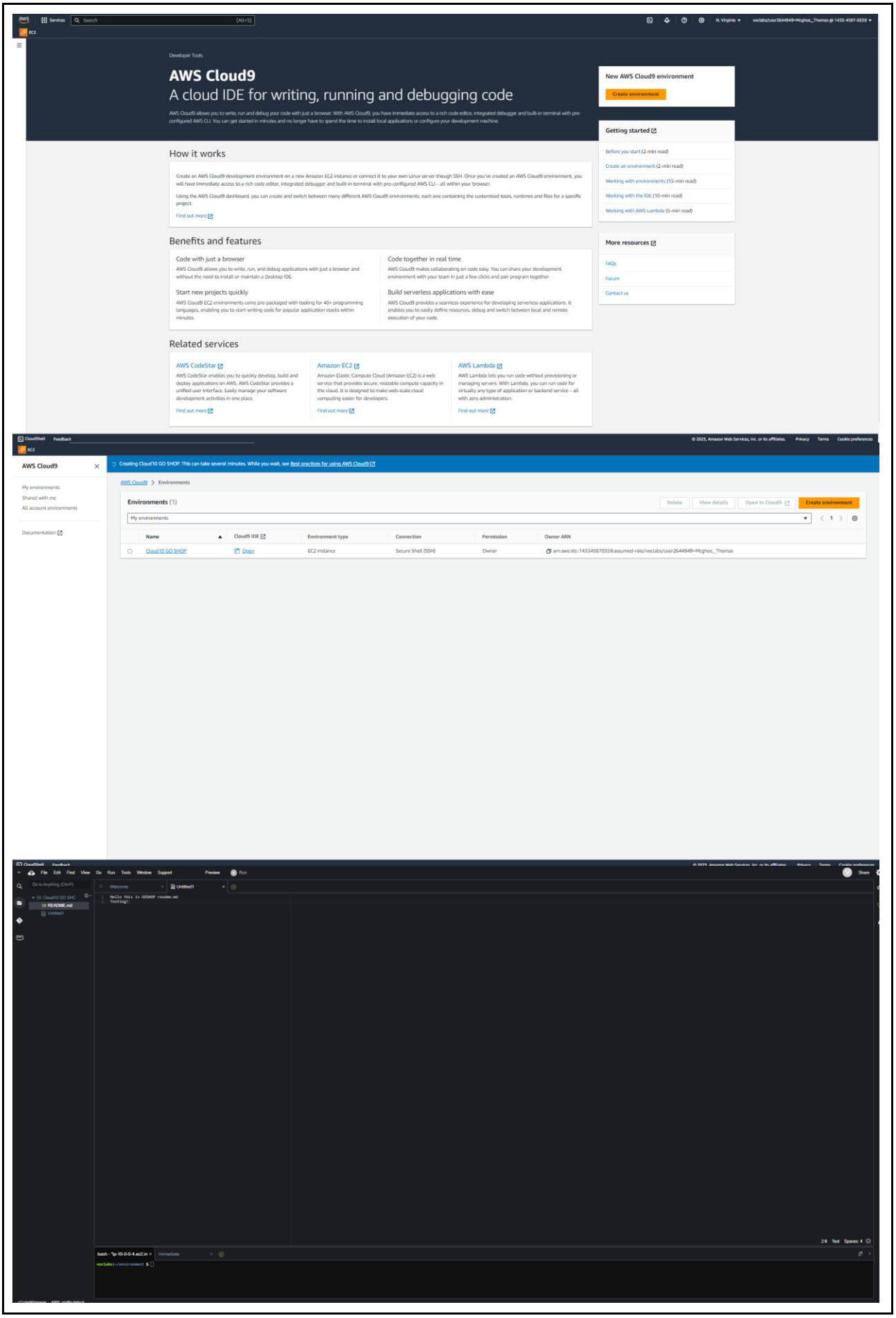


YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  MyDB:
    Type: AWS::RDS::DBInstance
    Properties:
      DBInstanceIdentifier: database-shop
      MasterUsername: administrator
      MasterUserPassword: 'your_secure_password'
      DBInstanceClass: db.r5.24xlarge
      AllocatedStorage: 999
      StorageType: gp3
      Iops: 12000
      StorageThroughput: 500
      MaxAllocatedStorage: 1000
      Engine: mariadb
      EngineVersion: 10.6.14
      MultiAZ: true
      PubliclyAccessible: true
      VPCSecurityGroups:
        - Ref: MyDBSecurityGroup
      DBSubnetGroupName: rds-ec2-db-subnet-group-1
      DBName: GOSHOPRDSDB
      BackupRetentionPeriod: 14
      CopyTagsToSnapshot: true
      EnableCloudwatchLogsExports:
        - audit
        - error
        - general
        - slowquery
      KmsKeyId: 'arn:aws:kms:your-region:your-account-id:key/your-key-id'
      StorageEncrypted: true
      DeletionProtection: true
```

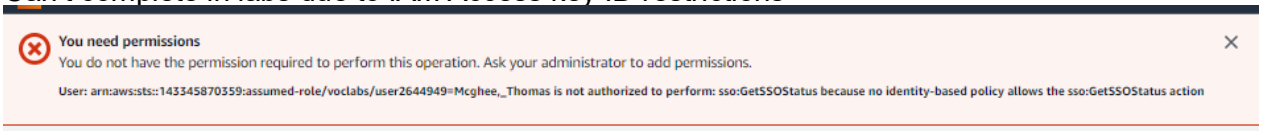
```
MyDBSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: MariaDB Security Group
    VpcId: 'your-vpc-id'
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 3306
        ToPort: 3306
        CidrIp: 'your-ip-address/32'

RDSOptionGroup:
  Type: 'AWS::RDS::OptionGroup'
  Properties:
    EngineName: mariadb
    MajorEngineVersion: '10.6'
    OptionGroupDescription: MariaDB Option Group
    OptionConfigurations:
      - OptionName: 'your-option-name'
        OptionSettings:
          - Name: 'name-of-setting'
            Value: 'value-of-setting'

RDSDBParameterGroup:
  Type: 'AWS::RDS::DBParameterGroup'
  Properties:
    Description: MariaDB Parameter Group
    Family: mariadb10.6
    Parameters:
      parameter_name1: 'value1'
      parameter_name2: 'value2'
```

USING CLOUD9 ENV

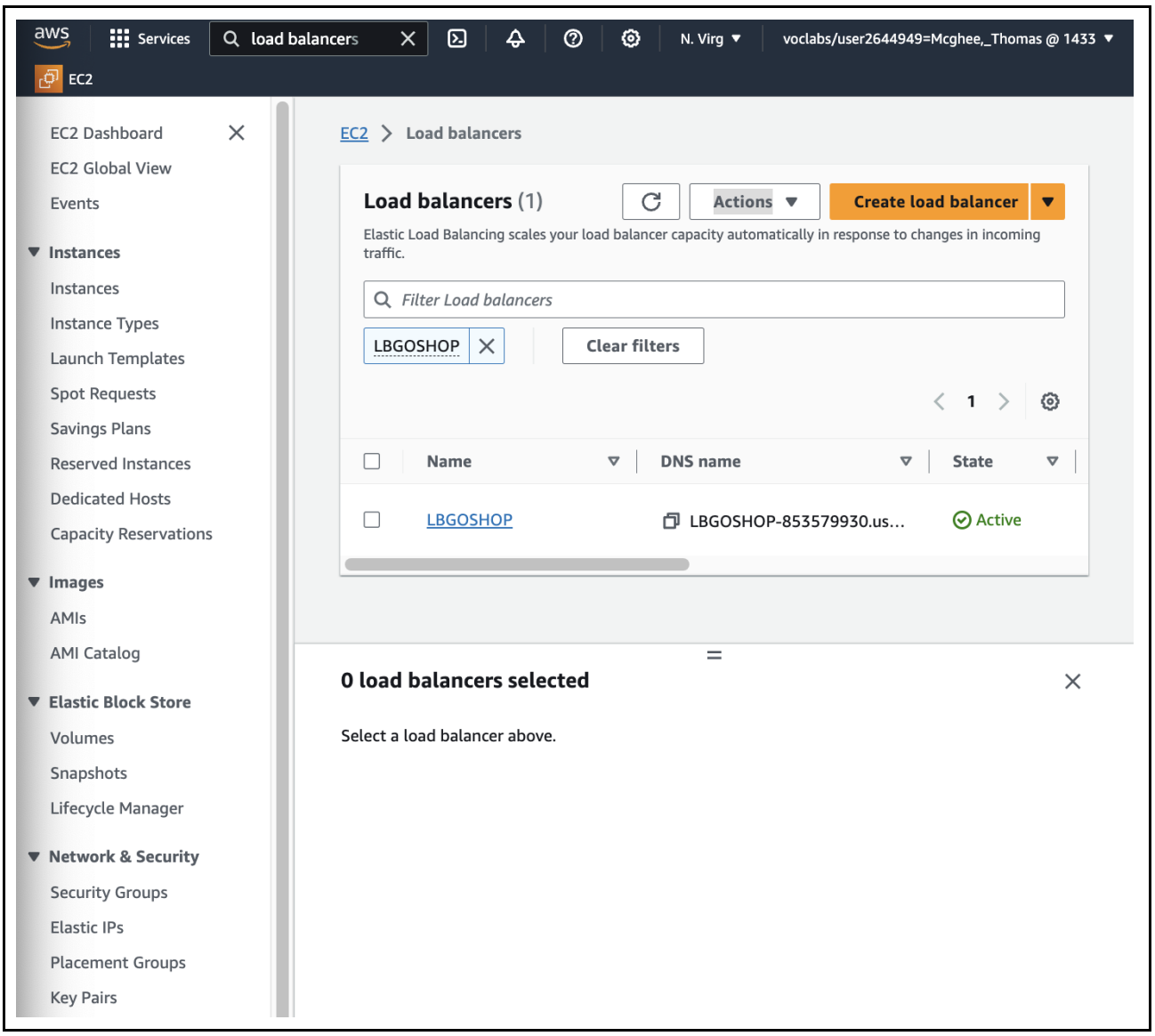

Developer Tools
AWS Cloud9
A cloud IDE for writing, running and debugging code
New AWS Cloud9 environment
Create environment
Getting started
How it works
Benefits and features
Code with just a browser
Code together in real time
Start new projects quickly
Build serverless applications with ease
Related services
AWS CodeStar
Amazon EC2
AWS Lambda
More resources
FAQs
Forum
Contact us
AWS Cloud9
Environments (1)
Create environment
Cloud10 GO SHOP
EC2 instance
Secure Shell (SSH)
Owner

AZURE AWS AD

Can’t complete in labs due to IAM Access key ID restrictions

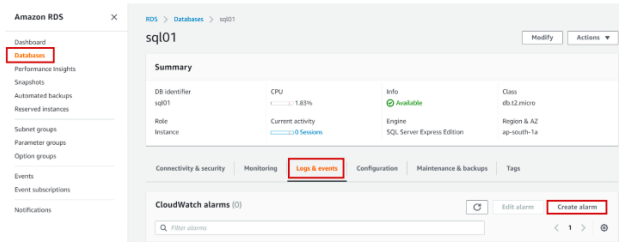
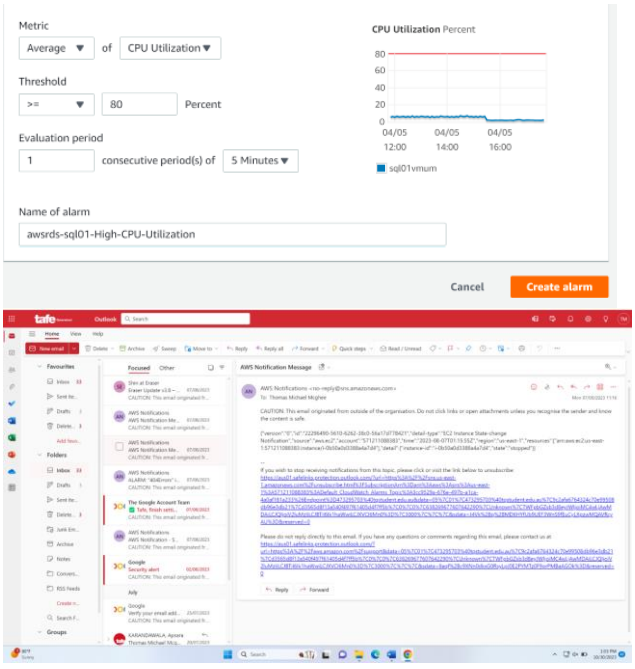


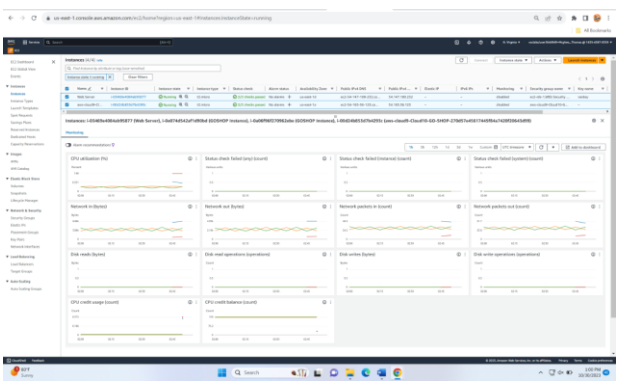
Load Balancer



2.5 Configure required monitoring of cloud resources (provide screen shots where appropriate)

RDS Alarm - When CPU usage of the ami instance is equal to or exceeds ~80%

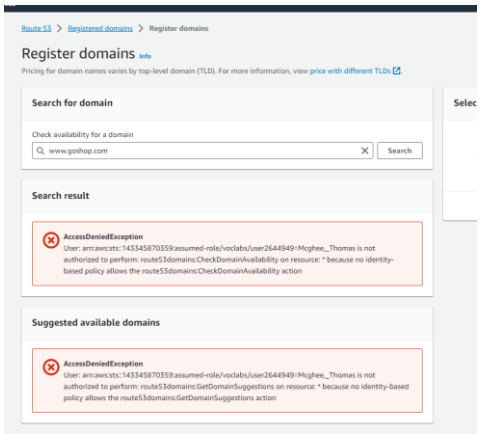
Inside shell of amazon RDS (logs & events tab has monitoring services)	
Create alarm to average out usage for every 5 mins, that way if the cpu util has been averaged at 80% or over for 5 minutes, it will alert either via email or in the panel dashboard.	

Monitoring of EC2 instances.	

Part 3 – Test the environment

Use the test plan prepared in 2.3 to test your cloud deployment and demonstrate that it meets the requirements and business needs. If problems are encountered during the test, use appropriate troubleshooting techniques to resolve the issues and document.

Issues arose around DNS Route 53 and setting it up around learner labs.
to fix this issue, I used a specific learner lab which mitigated this issue in how to theoretically successfully run it. Wasn't possible in learner labs with my current knowledge.



All other tests were successful

Objective:

Verify that all AWS resources have been successfully created, configured, and are operational after the CloudFormation stack deployment.

Test Environment:

AWS CloudFormation with resources including AWS EC2, S3, and Security Groups.

Preconditions:

The CloudFormation stack for GO SHOP has been successfully deployed.

User has access to AWS Management Console and AWS CLI with necessary permissions.

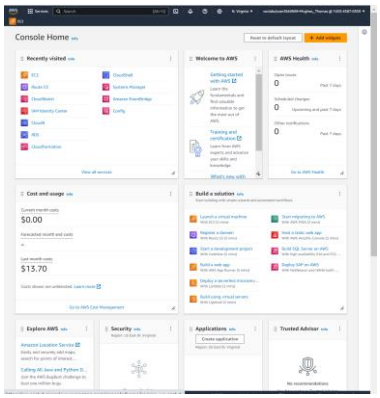
Test Cases:

Test Case 1: Validate EC2 Instance

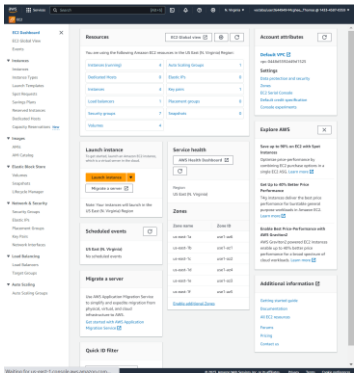
Description: Check that the EC2 instance has been created and is running.

Steps:

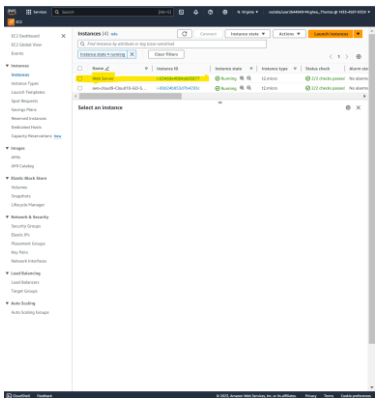
Go to the AWS Management Console.



Navigate to EC2 Dashboard.



Check that there is a running instance with the name associated with WebServerInstance in the CloudFormation template.



Expected Result:

EC2 instance is in the running state.

☑

Instance type is t2.micro.

☑

Key Pair associated is “MyKeyPair”.

☑

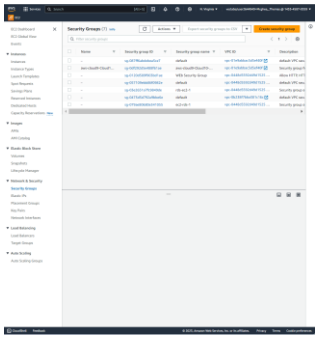
Status: ☑

Test Case 2: Validate Security Group Configuration

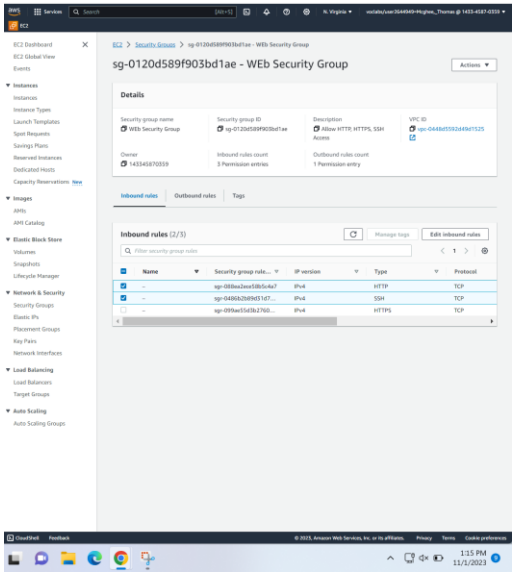
Description: Ensure the Security Group has been configured correctly.

Steps:

In the EC2 Dashboard, click on “Security Groups”.



Find and select the Security Group associated with WebServerSecurityGroup in the CloudFormation template.



Check the Inbound Rules to ensure port 22 (SSH) and port 80 (HTTP) are open.

Expected Result:

Port 22 and 80 are open for inbound traffic. ☑

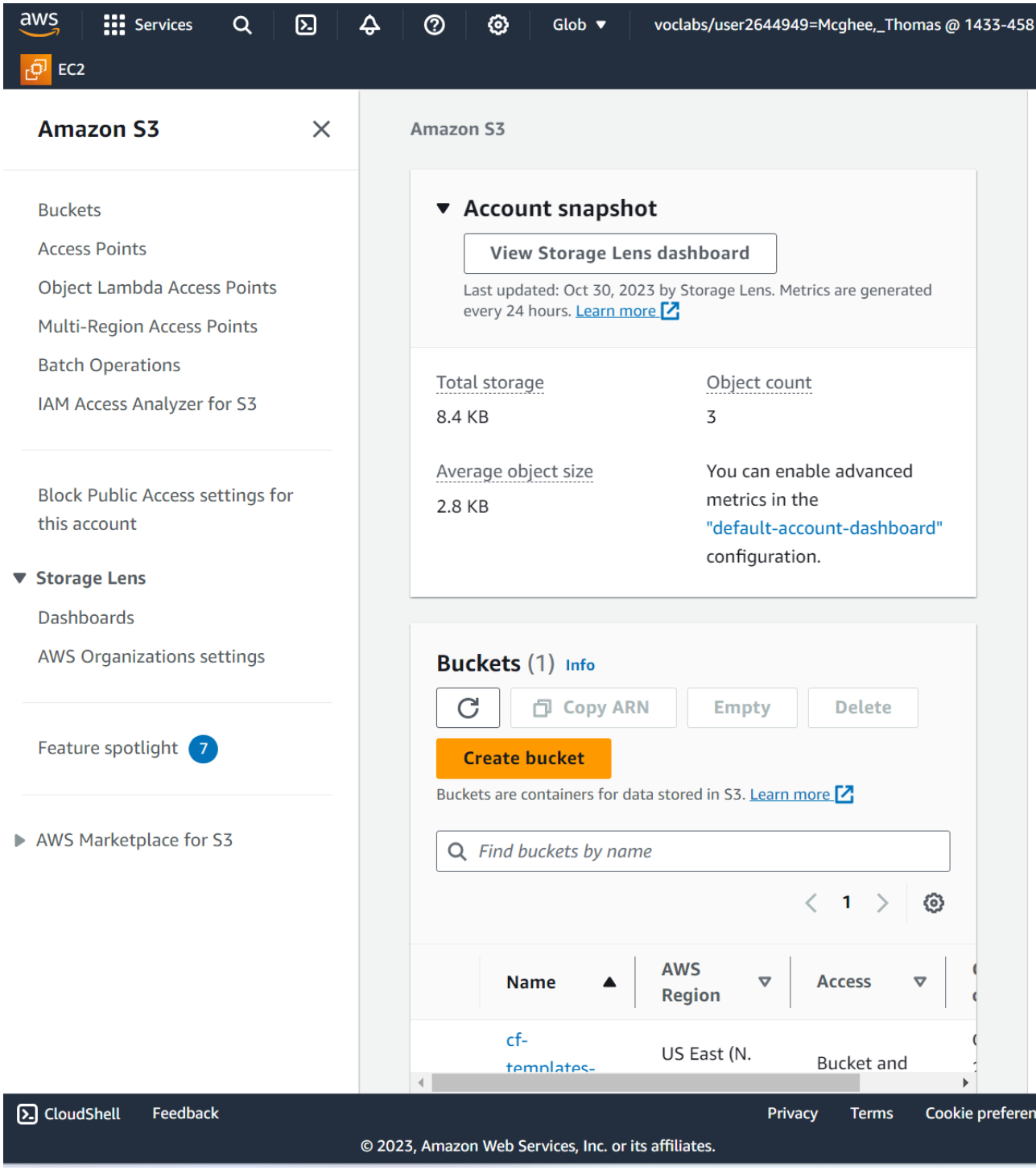
Status: Pending / Pass / Fail ☑

Test Case 3: Validate S3 Bucket Creation

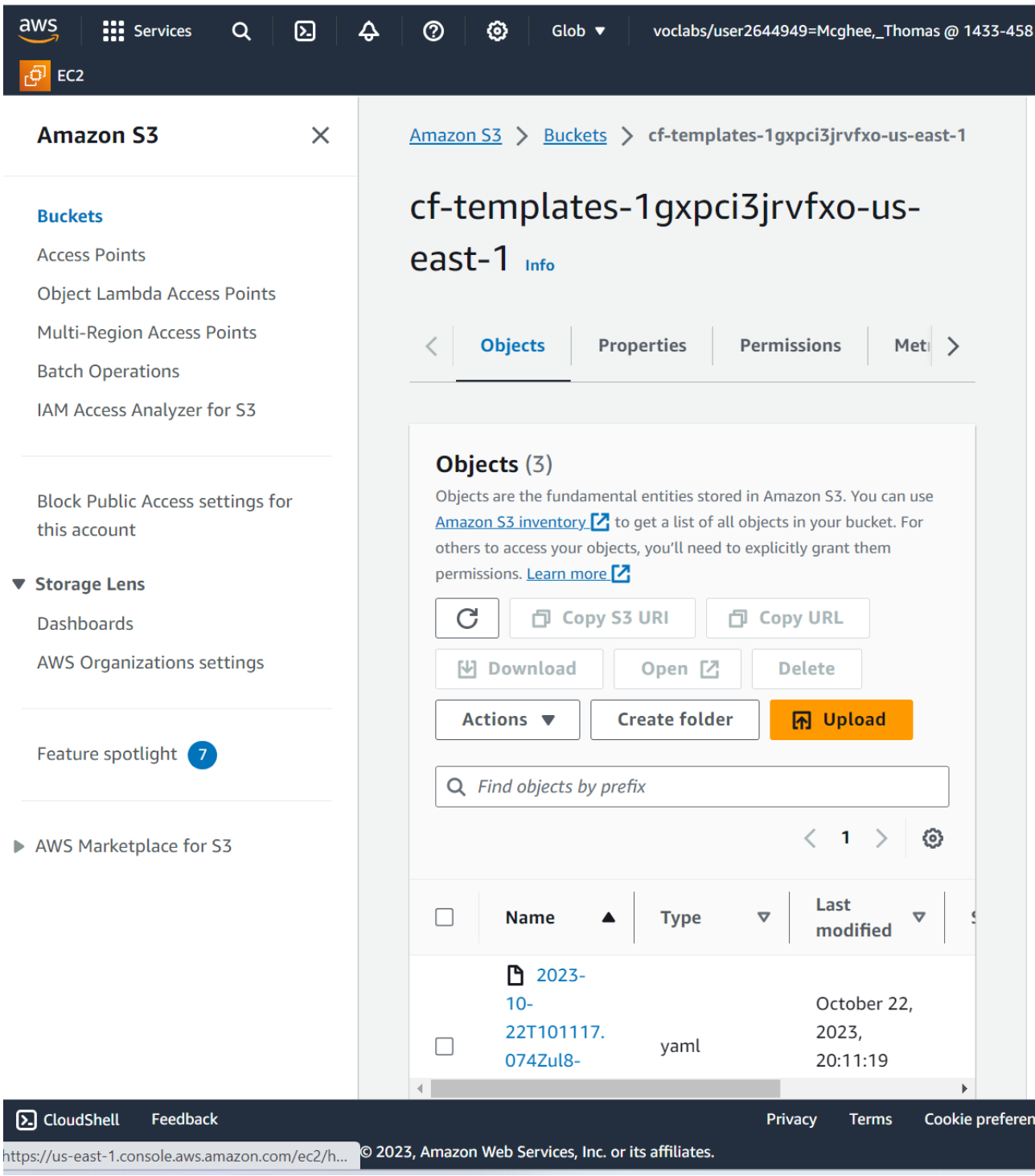
Description: Ensure the S3 bucket has been created.

Steps:

Go to the S3 Dashboard in AWS Management Console.



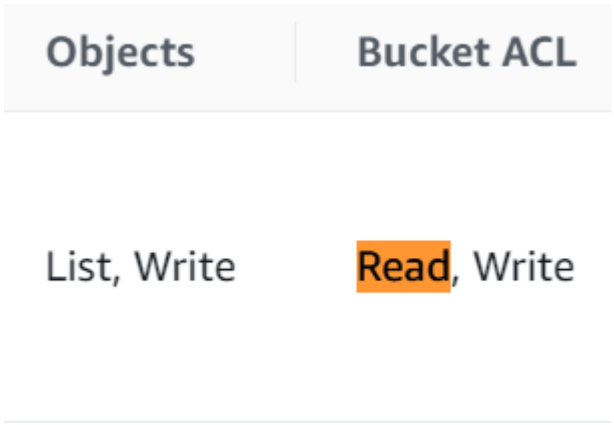
Check for the bucket with the name associated with WebsiteBucket in the CloudFormation template.



Expected Result:

S3 bucket is present. ☑

Bucket has public read access. ☑



Status: Pending / Pass / Fail

Test Case 4: Validate EC2 Web Server Response

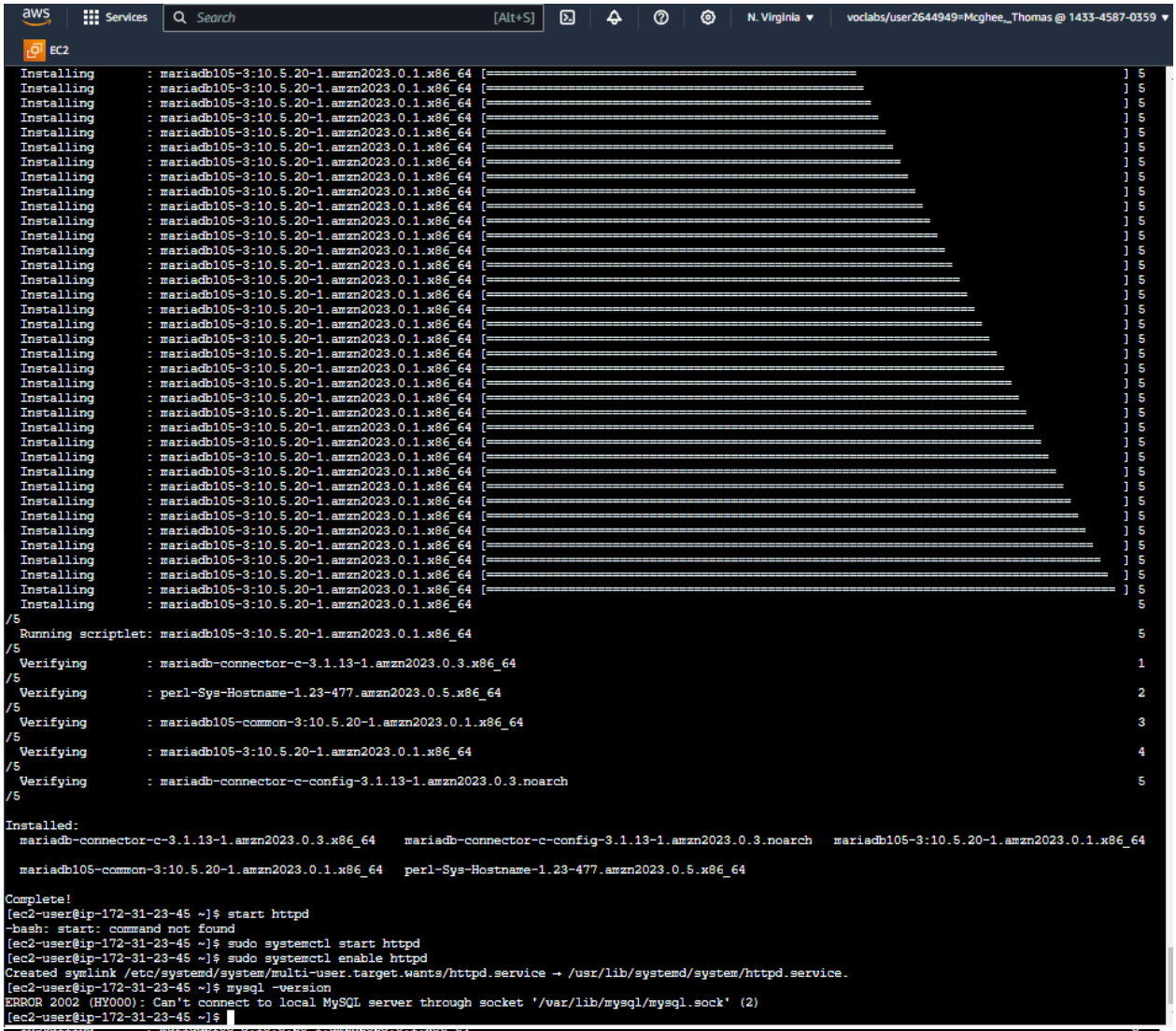
Description: Ensure the web server on EC2 is serving the correct content.

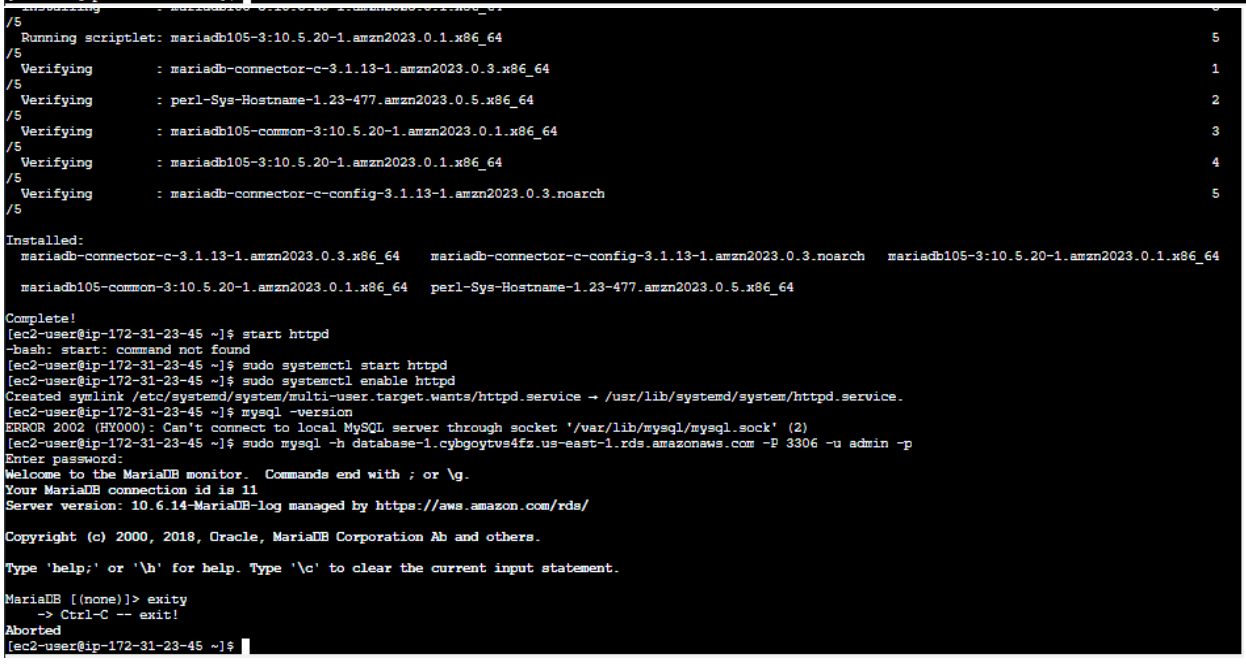
Steps:

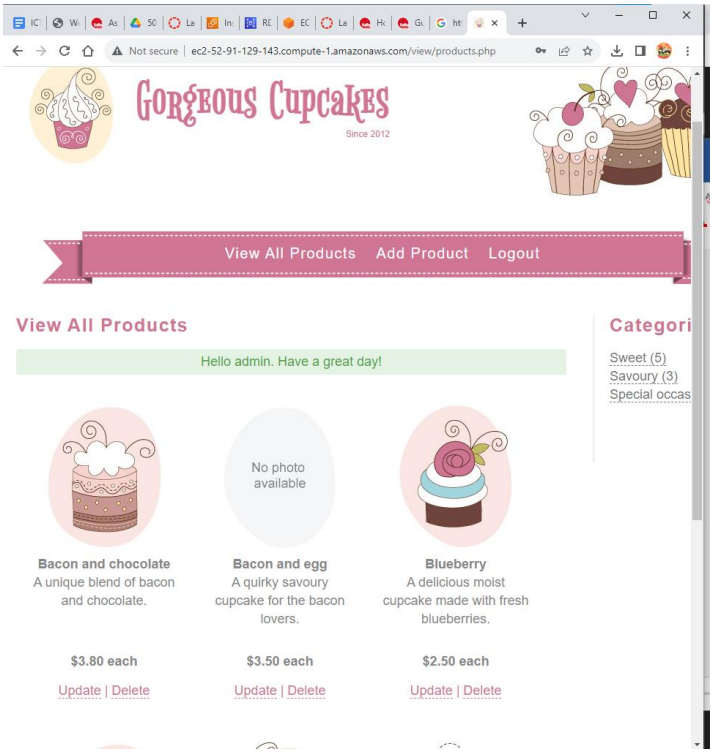
Obtain the Public IP or DNS of the EC2 instance.

Open a web browser and navigate to http://<Public-IP-or-DNS>.

Expected Result:


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 1433-4587-0359
EC2
Installing : mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
Running scriptlet: mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64
Verifying : perl-Sys-Hostname-1.23-477.amzn2023.0.5.x86_64
Verifying : mariadb105-common-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch
Installed:
mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64
mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch
mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
mariadb105-common-3:10.5.20-1.amzn2023.0.1.x86_64
perl-Sys-Hostname-1.23-477.amzn2023.0.5.x86_64
Complete!
[ec2-user@ip-172-31-23-45 ~]$ start httpd
-bash: start: command not found
[ec2-user@ip-172-31-23-45 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-23-45 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-172-31-23-45 ~]$ mysql -version
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
[ec2-user@ip-172-31-23-45 ~]$


Running scriptlet: mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64
Verifying : perl-Sys-Hostname-1.23-477.amzn2023.0.5.x86_64
Verifying : mariadb105-common-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
Verifying : mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch
Installed:
mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64
mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch
mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64
mariadb105-common-3:10.5.20-1.amzn2023.0.1.x86_64
perl-Sys-Hostname-1.23-477.amzn2023.0.5.x86_64
Complete!
[ec2-user@ip-172-31-23-45 ~]$ start httpd
-bash: start: command not found
[ec2-user@ip-172-31-23-45 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-23-45 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-172-31-23-45 ~]$ mysql -version
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (2)
[ec2-user@ip-172-31-23-45 ~]$ sudo mysql -h database-1.cybgoytvs4fz.us-east-1.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 10.6.14-MariaDB-log managed by https://aws.amazon.com/rds/
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> exity
-> Ctrl-C -- exit!
Aborted
[ec2-user@ip-172-31-23-45 ~]$

1. 

   Web page displays “GO GUNDA SHOP >:) in title”. ☑

   Status: Pending / Pass / Fail ☑

Part 4 – Documentation

Prepare a report outlining the procedures, outcomes, and any recommendations to reduce manual elements through automation. Present the report to the General Manager for final sign-off.

GO Shop
Cloud-Based Infrastructure Automation Report

Date: 10/1/2023
Prepared by: Tom McGhee
Position: Senior Sys Admin
Reviewed by: General manager

1. Executive Summary

   This report details the initiatives taken to automate the management and operation of GO Shop’s IT infrastructure, post-migration to Amazon Web Services (AWS). By leveraging various AWS

services and automation tools, we aim to optimize resource performance, enhance resilience, and fortify security, all while maintaining our current level of System Administration staff.

2. Introduction

GO Shop has transitioned to a cloud-based infrastructure to accommodate the surge in business transactions and alleviate the stress on our old hardware platform. The next strategic step is to maximize the efficiency of our cloud resources through automation, ensuring high availability, secure storage, and global accessibility of the GO Shop application.

3. Automation Procedures

3.1 Infrastructure as Code (IaC)

AWS CloudFormation: Used to automate the provisioning and management of AWS resources, ensuring consistency and compliance with company policies.

3.2 Continuous Integration and Continuous Deployment (CI/CD)

AWS CodePipeline: Automated the deployment process of our web application, ensuring quicker and more reliable updates.

3.3 Auto-Scaling and Load Balancing

AWS Auto Scaling: Configured to automatically adjust the number of EC2 instances based on demand, ensuring high availability and cost-efficiency.

3.4 Monitoring and Management

AWS CloudWatch: Automated monitoring of resource utilization and setting up alerts for proactive issue resolution.

AWS Lambda: Used to run scripts in response to events, automating various administrative tasks.

4. Outcomes

Reduced Manual Efforts: Significantly reduced the time and effort required for system administration tasks.

Enhanced Performance and Availability: Achieved consistent performance and high availability of the GO Shop application.

Cost Efficiency: Optimized resource utilization, resulting in cost savings.

Global Accessibility: Ensured that the GO Shop application is accessible worldwide with minimal latency.

5. Recommendations for Further Automation

5.1 Advanced Monitoring and Alerts

Implement AI-driven monitoring tools: Tools like AWS CloudTrail for tracking user activity and API usage.

5.2 Disaster Recovery Automation

AWS Backup: Automate and centralize the backup of data across AWS services.

5.3 Security Automation

AWS Security Hub: Automate security checks to ensure compliance with company policies.

7. Approval for Implementation

[General Manager]

Signature: _____

Date: 11/1/2023

Section 2: Manage Infrastructure in Cloud Environments

Part 5 – Inventory and change management of cloud resources

5.1 Identify tagging policy and categorize resources according to business needs

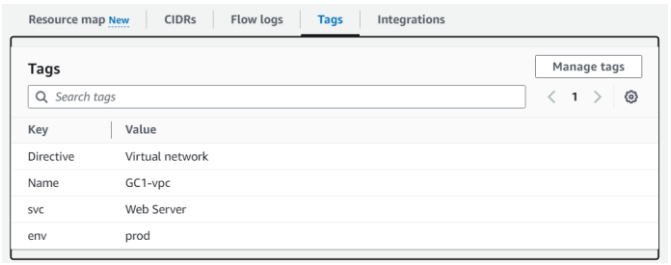
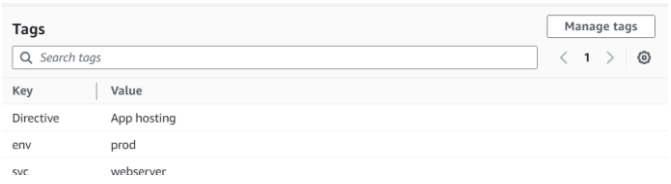
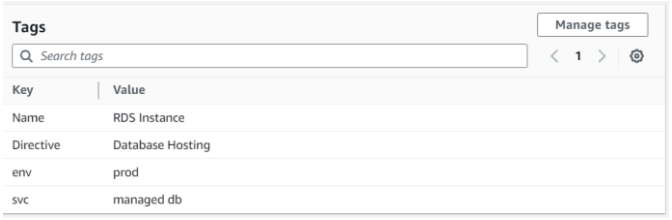
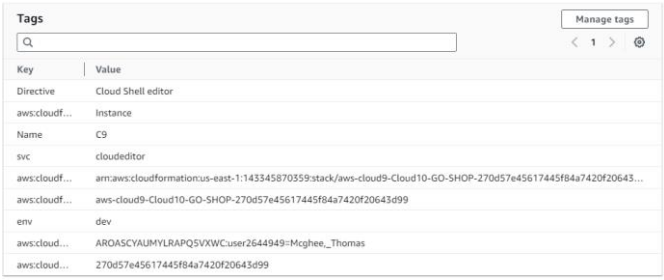
Category	Tag Key	Tag Value
Company	Company	GO Shop
Department	Department	IT
		Sales
		Marketing
SSH Access	SSH Access	Allowed
		Not Allowed
Environment	Environment	Production
		Staging
		Development
Service	Service	SSH Access
		Web Server
		Database
		Load Balancer

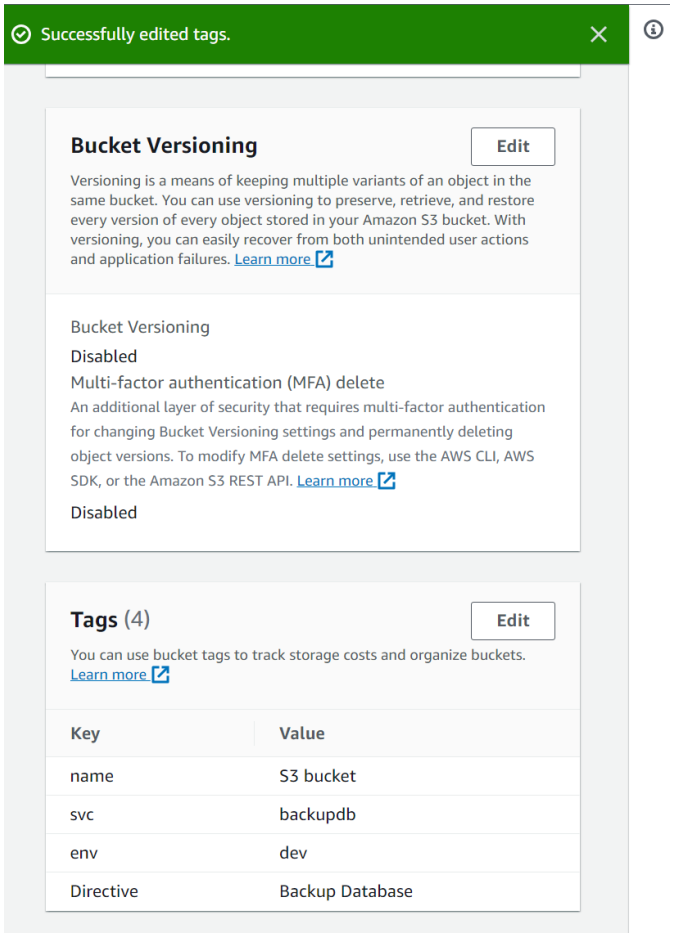
Category	Tag Key	Tag Value
Company	Company	GO Shop
Department	Department	IT

ICTCLD507_508_AT3_PE_TQ

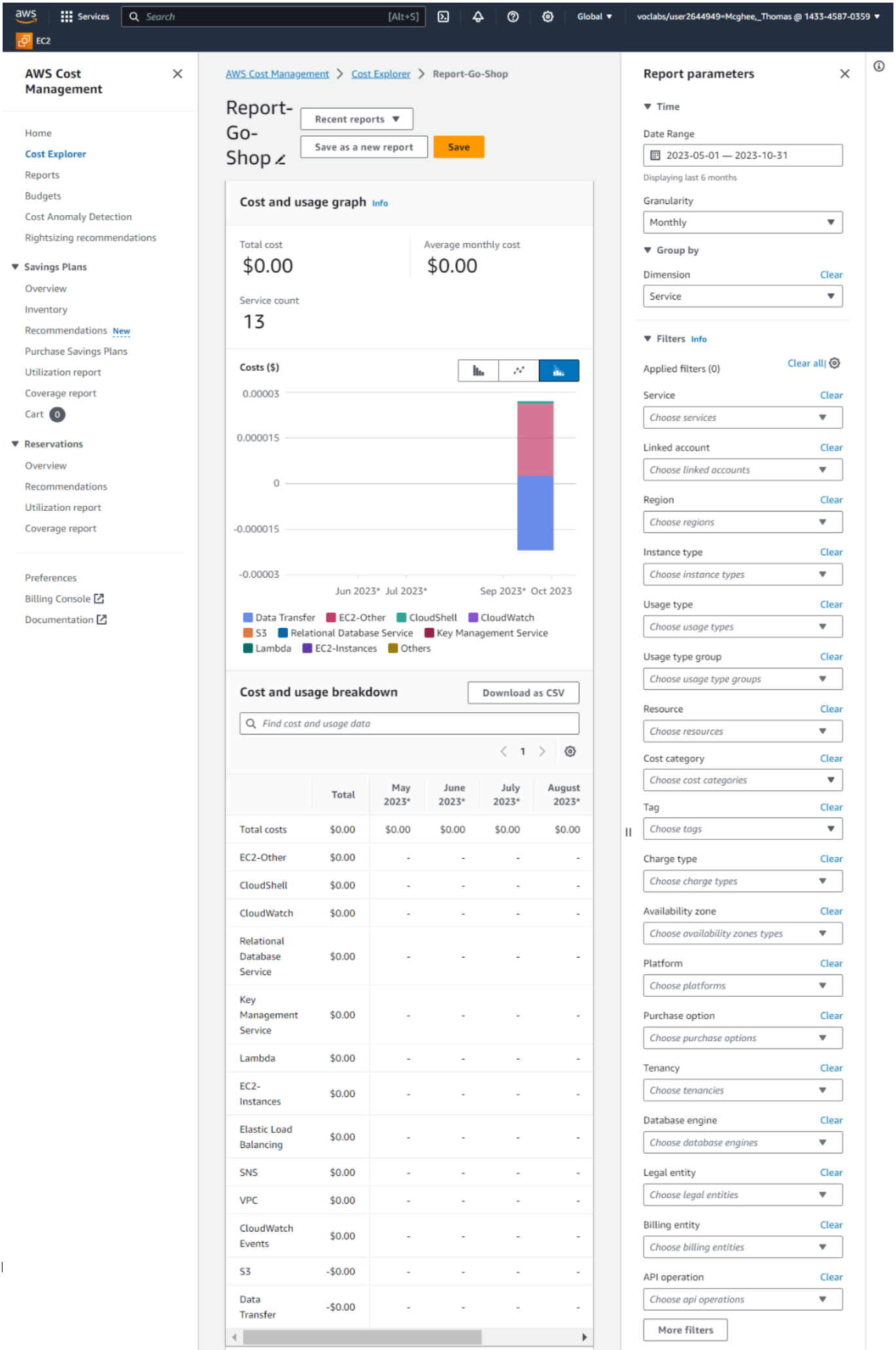
M_v1.docx

5.2 Update resources according to tagging policy and build and maintain inventory of cloud resources

Cloud Resource	Tag
VPC	
EC2	
RDS	
C9	

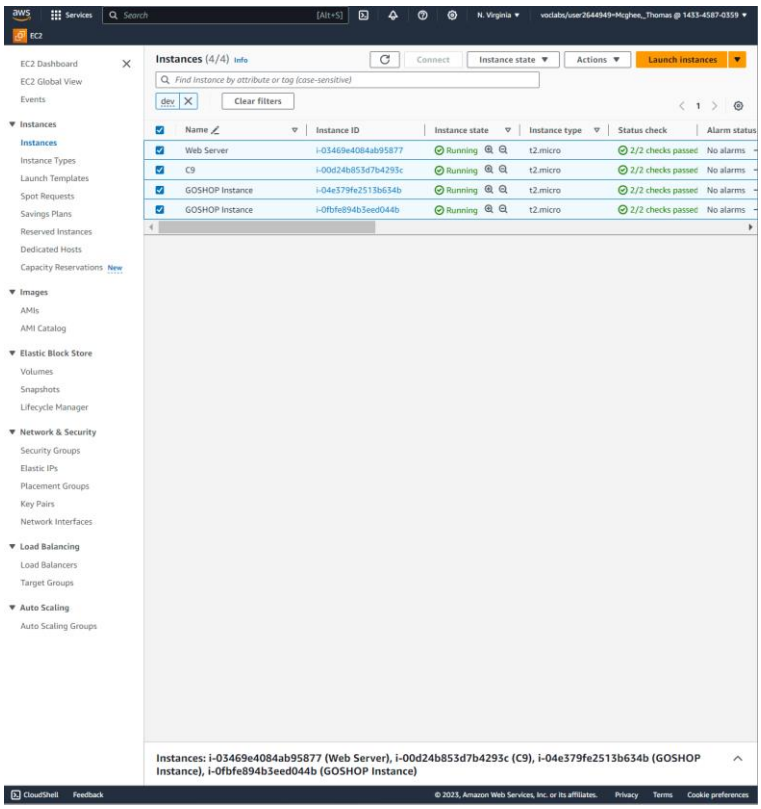
S3 Bucket	

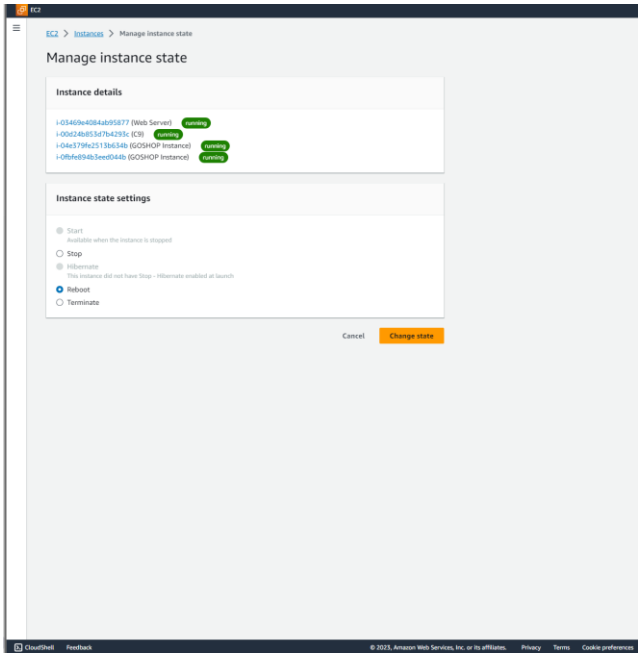
5.3 Generate a report of resources based on category

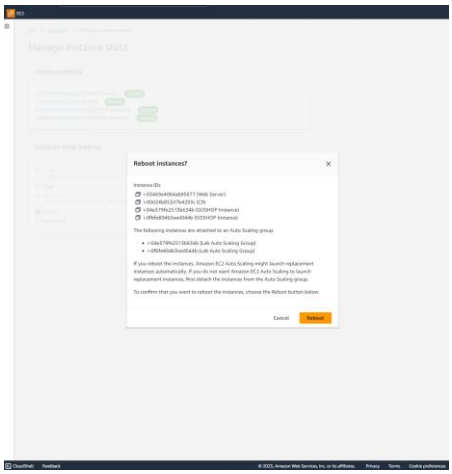

aws
Services
Search
[Alt+S]
Global
voclabs/user2644949=Mcghee,_Thomas @ 1433-4587-0359
EC2
AWS Cost Management
Home
Cost Explorer
Reports
Budgets
Cost Anomaly Detection
Rightsizing recommendations
Savings Plans
Overview
Inventory
Recommendations New
Purchase Savings Plans
Utilization report
Coverage report
Cart 0
Reservations
Overview
Recommendations
Utilization report
Coverage report
Preferences
Billing Console
Documentation
AWS Cost Management > Cost Explorer > Report-Go-Shop
Report-Go-Shop
Recent reports
Save as a new report
Save
Cost and usage graph Info
Total cost
$0.00
Average monthly cost
$0.00
Service count
13
Costs ($)
0.00003
0.000015
0
-0.000015
-0.00003
Jun 2023* Jul 2023* Sep 2023* Oct 2023
Data Transfer
EC2-Other
CloudShell
CloudWatch
S3
Relational Database Service
Key Management Service
Lambda
EC2-Instances
Others
Cost and usage breakdown
Download as CSV
Find cost and usage data
1
Total
May 2023*
June 2023*
July 2023*
August 2023*
Total costs $0.00 $0.00 $0.00 $0.00 $0.00
EC2-Other $0.00 - - - -
CloudShell $0.00 - - - -
CloudWatch $0.00 - - - -
Relational Database Service $0.00 - - - -
Key Management Service $0.00 - - - -
Lambda $0.00 - - - -
EC2-Instances $0.00 - - - -
Elastic Load Balancing $0.00 - - - -
SNS $0.00 - - - -
VPC $0.00 - - - -
CloudWatch Events $0.00 - - - -
S3 -$0.00 - - - -
Data Transfer -$0.00 - - - -
Report parameters
Time
Date Range
2023-05-01 — 2023-10-31
Displaying last 6 months
Granularity
Monthly
Group by
Dimension
Clear
Service
Filters Info
Applied filters (0)
Clear all
Service
Choose services
Linked account
Choose linked accounts
Region
Choose regions
Instance type
Choose instance types
Usage type
Choose usage types
Usage type group
Choose usage type groups
Resource
Choose resources
Cost category
Choose cost categories
Tag
Choose tags
Charge type
Choose charge types
Availability zone
Choose availability zones types
Platform
Choose platforms
Purchase option
Choose purchase options
Tenancy
Choose tenancies
Database engine
Choose database engines
Legal entity
Choose legal entities
Billing entity
Choose billing entities
API operation
Choose api operations
More filters

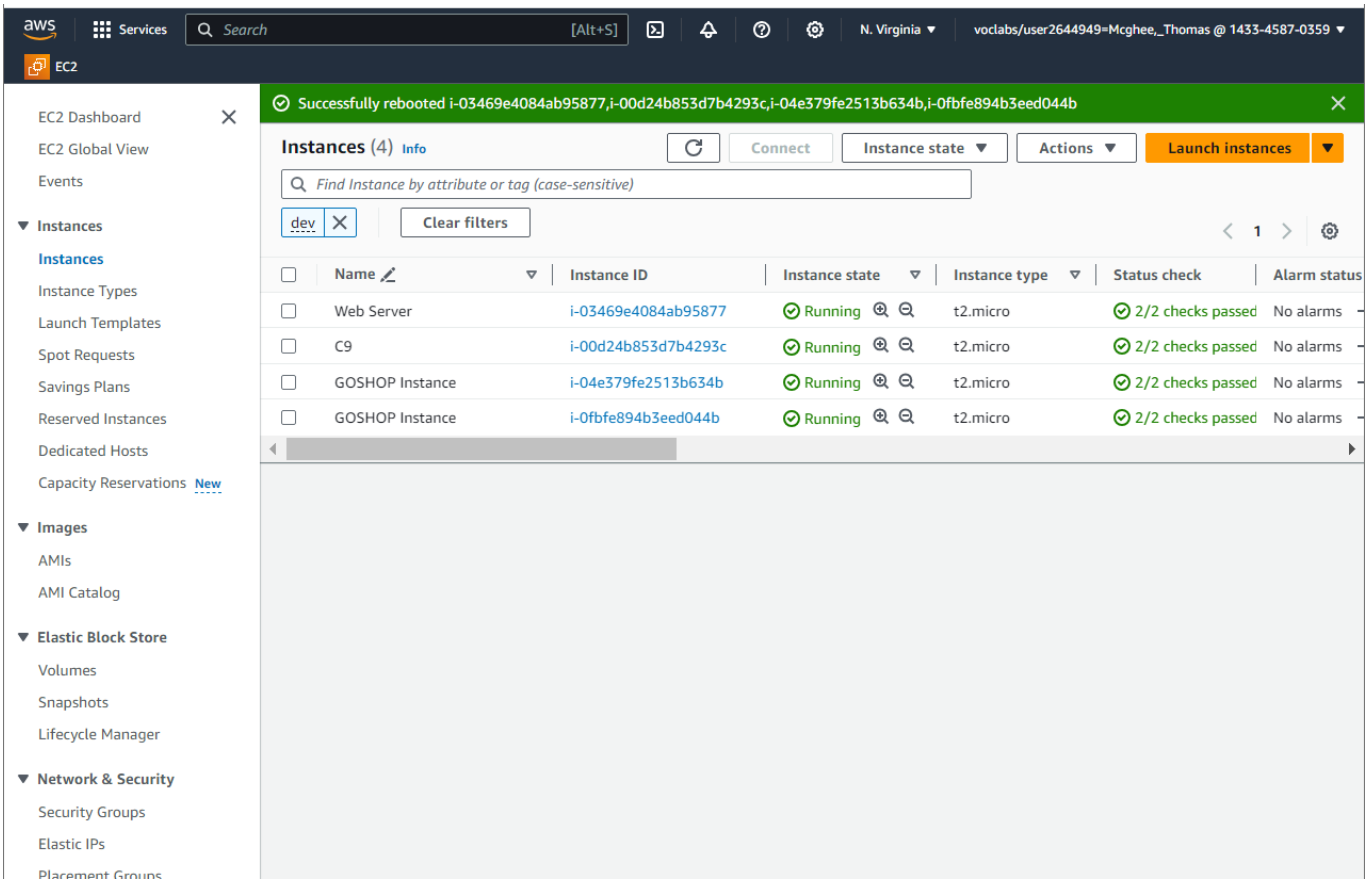
5.4 Conduct maintenance with resources in specific category

Rebooting entire “dev” environment inside of the cloud 9 ec2 instance




EC2
EC2 > Instances > Manage instance state
Manage instance state
Instance details
i-03469e4084ab95877 (Web Server) running
i-00d24b853d7b4293c (C9) running
i-04e379fe25133b634b (GOSHOP Instance) running
i-0fbfe894b3eed044b (GOSHOP Instance) running
Instance state settings
Start
Available when the instance is stopped
Stop
Hibernate
This instance did not have Stop - Hibernate enabled at launch
Reboot
Terminate
Cancel
Change state
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Reboot instances?
Cancel
Reboot



Part 6 – Audit and change management of cloud resources (provide screen shots)

6.1 Identify configuration policy according to business needs

Search on the internet what kind of configuration policies you can configure on the cloud

Mandatory Two-Factor Authentication (2FA) Policy

All user accounts within the cloud environment, particularly those with administrative privileges, must have two-factor authentication (2FA) enabled to enhance security measures. This policy applies across all departments and is overseen by the IT Security and IT Operations teams.

Users are required to configure 2FA using an authenticator app (like Google Authenticator or Authy) or SMS verification as part of their login process.

IT administrators will periodically audit accounts to verify 2FA compliance.

Accounts found non-compliant with 2FA requirements will be subject to restricted access until 2FA is enabled.

Mandatory Tagging Policy:

Every resource in the cloud must have the following tags:

'CostCentre': Identifies the department or project budget responsible for the cost. Example: 'CostCentre:IT-Dept'.

'Name': A descriptive name for the resource. Example: 'Name:Prod-WebServer-01'.

'Owner': The individual or team responsible for the resource. Example: 'Owner:JohnSmith'.

Block Storage Attachment Policy:

Every EC2 instance must have block storage (EBS) attached.

Example: All EC2 instances, especially those handling databases or requiring persistent storage, should have an EBS volume attached with a minimum specified capacity, such as 100 GB.

CloudTrail for S3 Monitoring:

Enable CloudTrail for S3 event logging, very S3 bucket must have an associated CloudTrail log.

Data Security and Encryption:

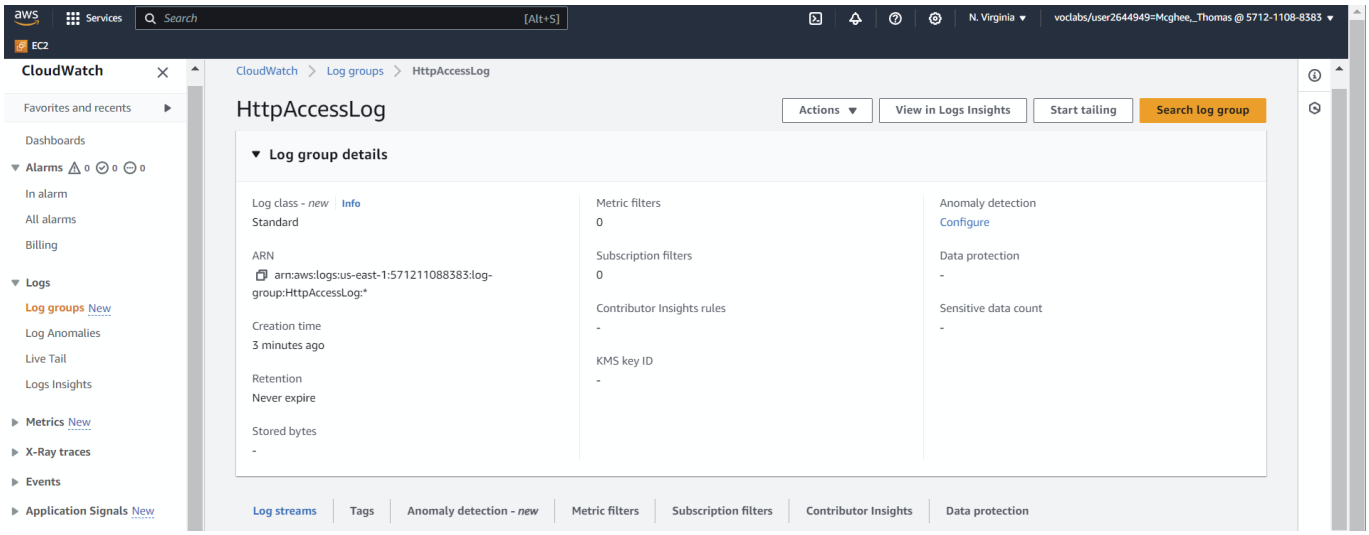
Encrypt sensitive data at rest and in transit, use AES-256 encryption for all stored data and TLS for data in transit.

extra: Both the tagging policies and configuration policies are needed because whilst the configuration policy establishes the technical standards and security practices, the tagging policy enables effective implementation, tracking, and management of these configurations within the organization's cloud environment. This combination ensures that GO Shop's cloud resources are not only well-configured but also easily manageable, secure, and aligned with business objectives.

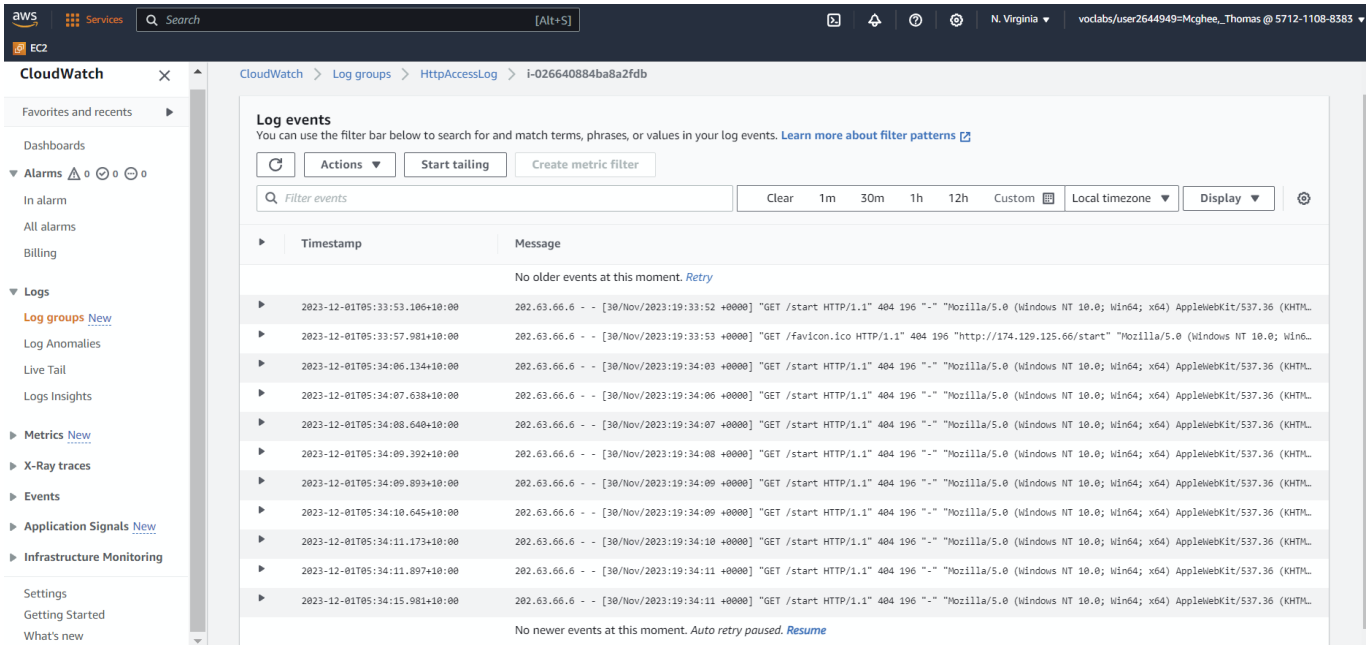
6.2 Enable logging of cloud-based events

(FOLLOWED LEARNER LABS OPERATIONS MODULE 9- Monitoring and Security [Lab 6 - Monitoring Infrastructure | TASK {1-2}])

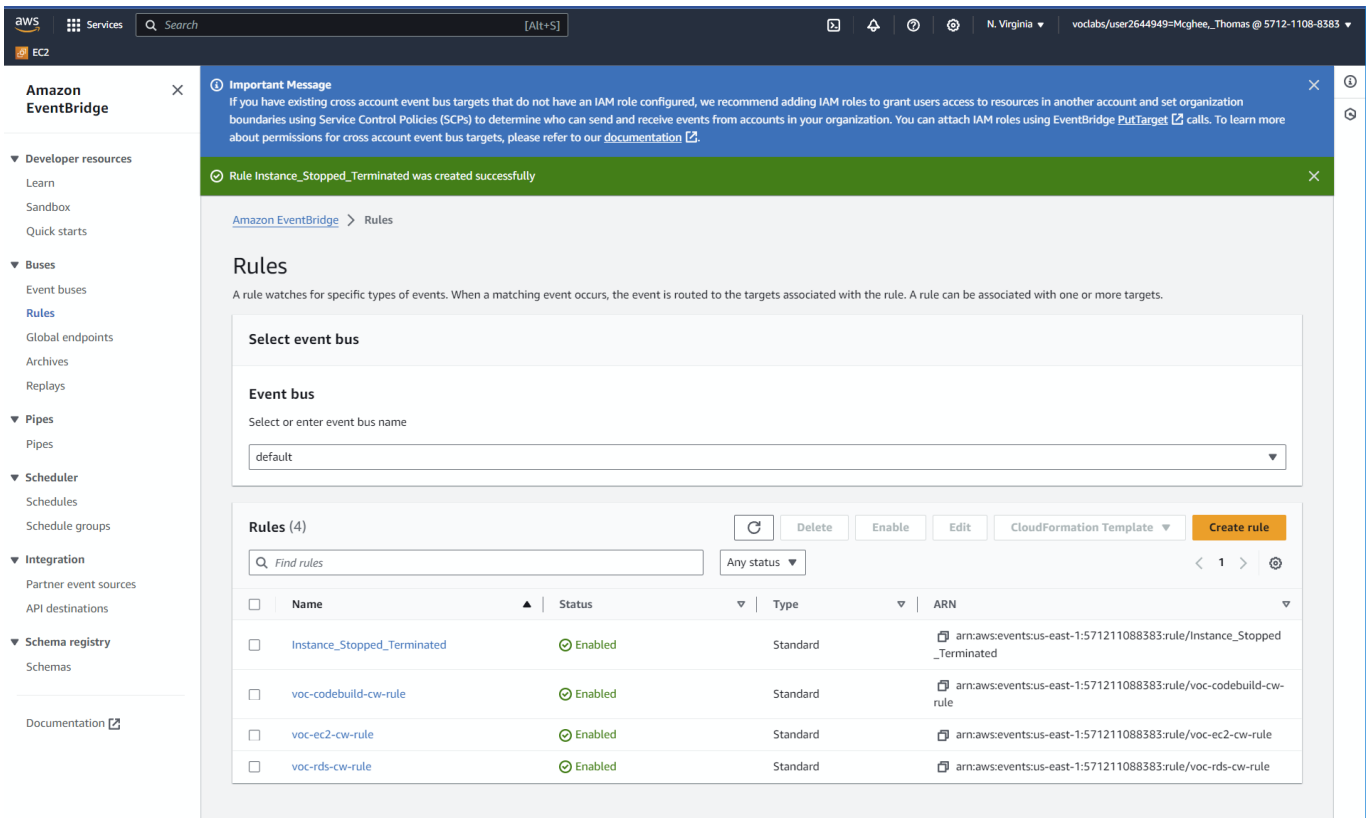
TASK 1 OUTPUT:



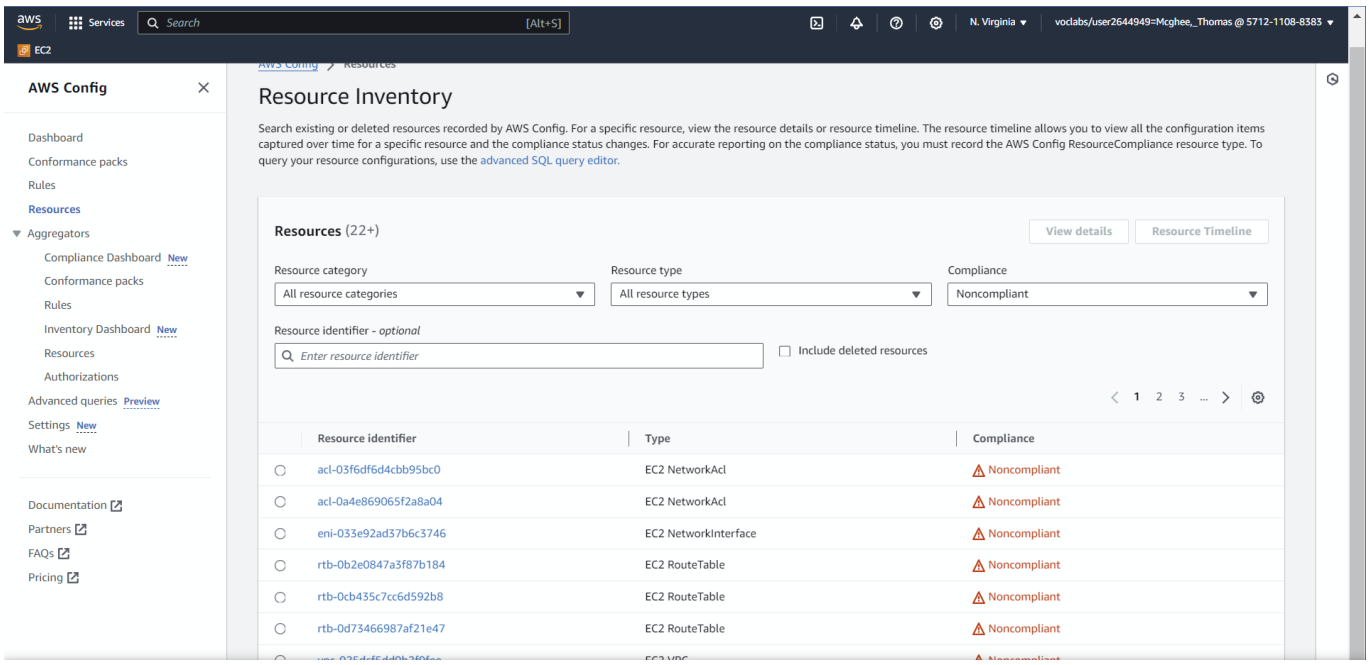
TASK2 OUTPUT:

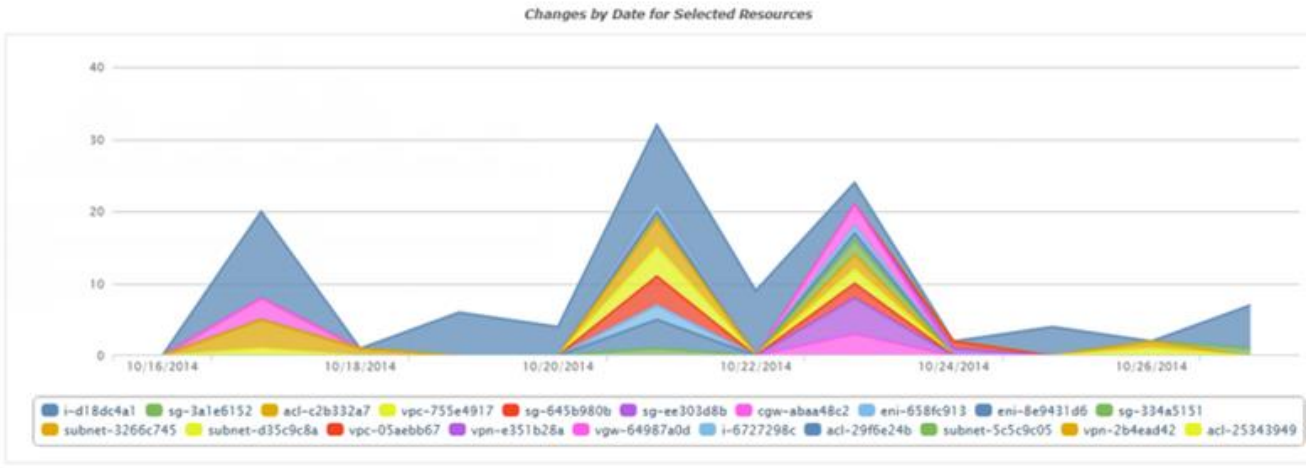


HERE IS WHAT I THINK SHOULD BE HERE {TASK 4}



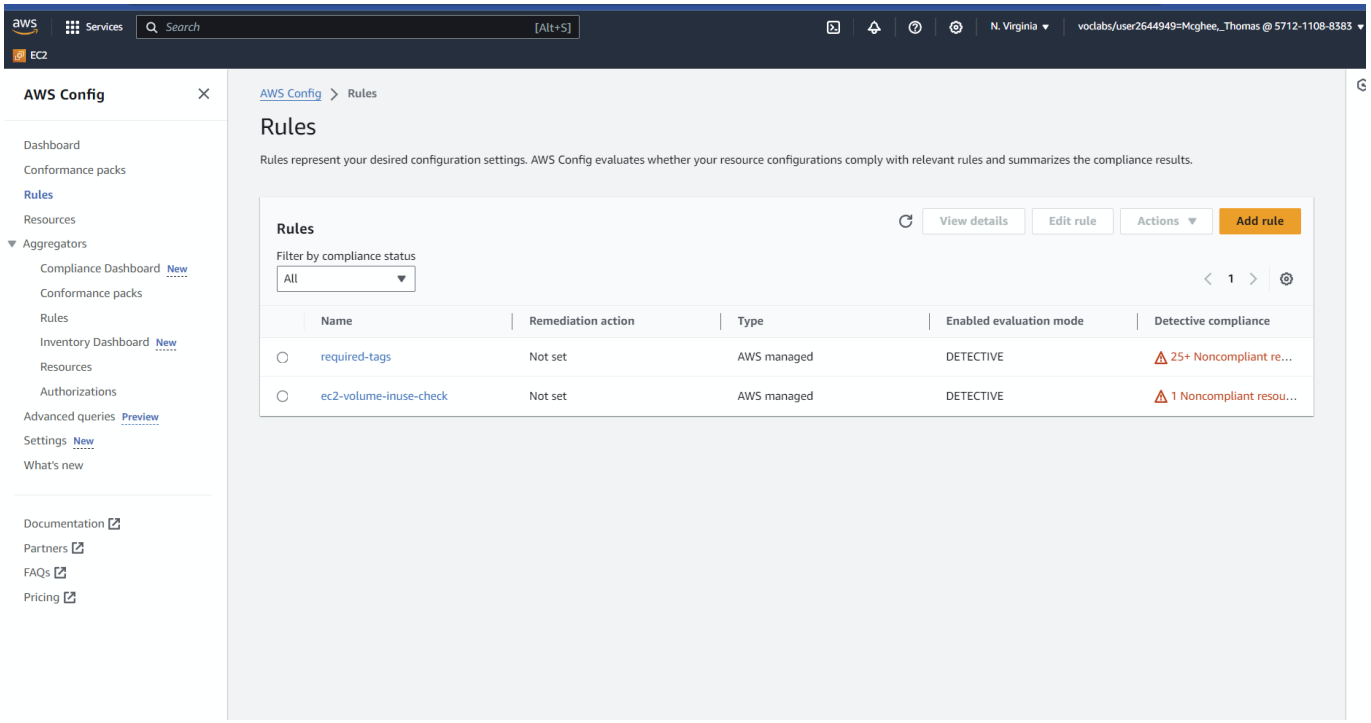
6.3 Collect and track changes to cloud resource configuration

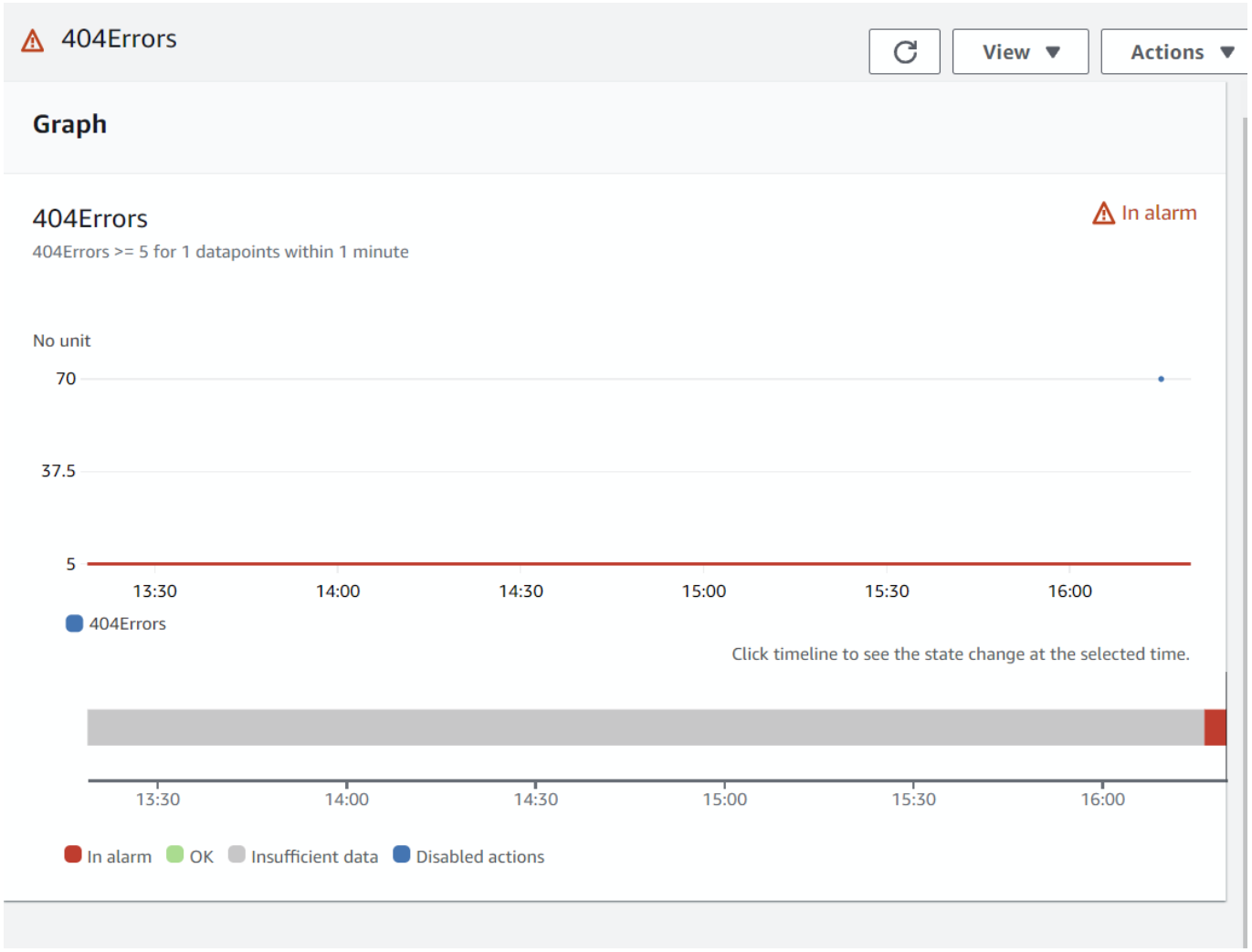


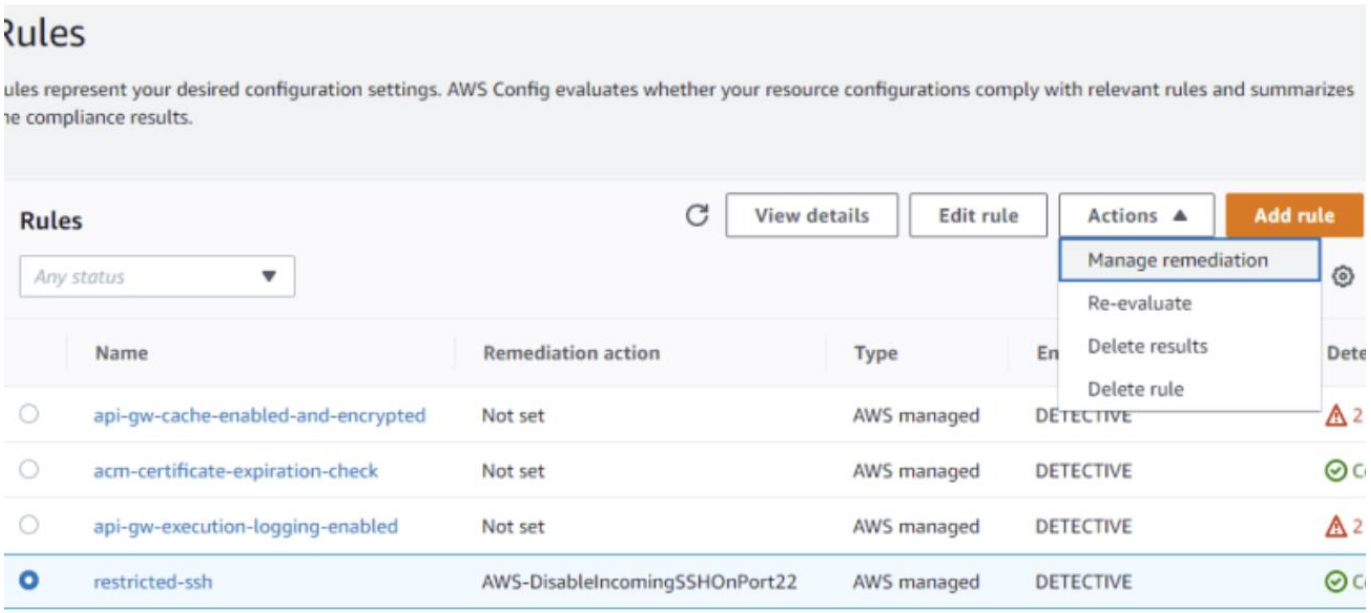


Resource ID	AWS Service
i-d18dc4a1	EC2 Instance
sg-3a1e6152	EC2 Security Group
acl-c2b332a7	Network ACL
vpc-755e4917	VPC
sg-645b980b	EC2 Security Group

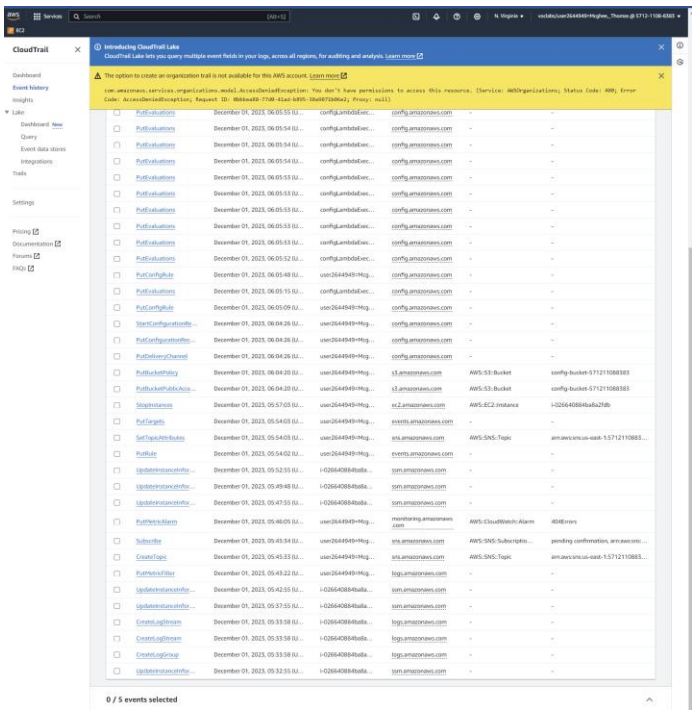
6.4 Apply configuration policy to resource and alert non-conformance




404Errors
View
Actions
Graph
404Errors
In alarm
404Errors >= 5 for 1 datapoints within 1 minute
No unit
70
37.5
5
13:30
14:00
14:30
15:00
15:30
16:00
404Errors
Click timeline to see the state change at the selected time.
13:30
14:00
14:30
15:00
15:30
16:00
In alarm
OK
Insufficient data
Disabled actions


Rules
ules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes
ne compliance results.
Rules
View details
Edit rule
Actions
Add rule
Manage remediation
Re-evaluate
Delete results
Delete rule
Any status
Name
Remediation action
Type
En
Dete
api-gw-cache-enabled-and-encrypted
Not set
AWS managed
DETECTIVE
acm-certificate-expiration-check
Not set
AWS managed
DETECTIVE
api-gw-execution-logging-enabled
Not set
AWS managed
DETECTIVE
restricted-ssh
AWS-DisableIncomingSSHOnPort22
AWS managed
DETECTIVE

6.5 Utilize audit logs and determine details and changes from configurations



Part 7 – Monitoring, logging, and alarming

7.1 Define capacity limits for cloud resources according to business needs

These ones are cloud resources for example a ec2 instance for db, 2 vpc, what kind of capacity you would need for a particular application.c there is no right or wrong answer but just express in terms of ec2 instance memory and cpu. and also something like amazon rds something called iops and size of the database and also capacity limits and also auto scaling capacity limits.look at foundation course lab 6 so you can get some idea of capacity.

Cloud Resource	Limit
EC2 Instance (Web Server)	
Instance Type	m5.large
vCPU	2
Memory	8 GiB
EC2 Auto Scaling (Web Server)	
Minimum Capacity	2 instances
Desired Capacity	4 instances

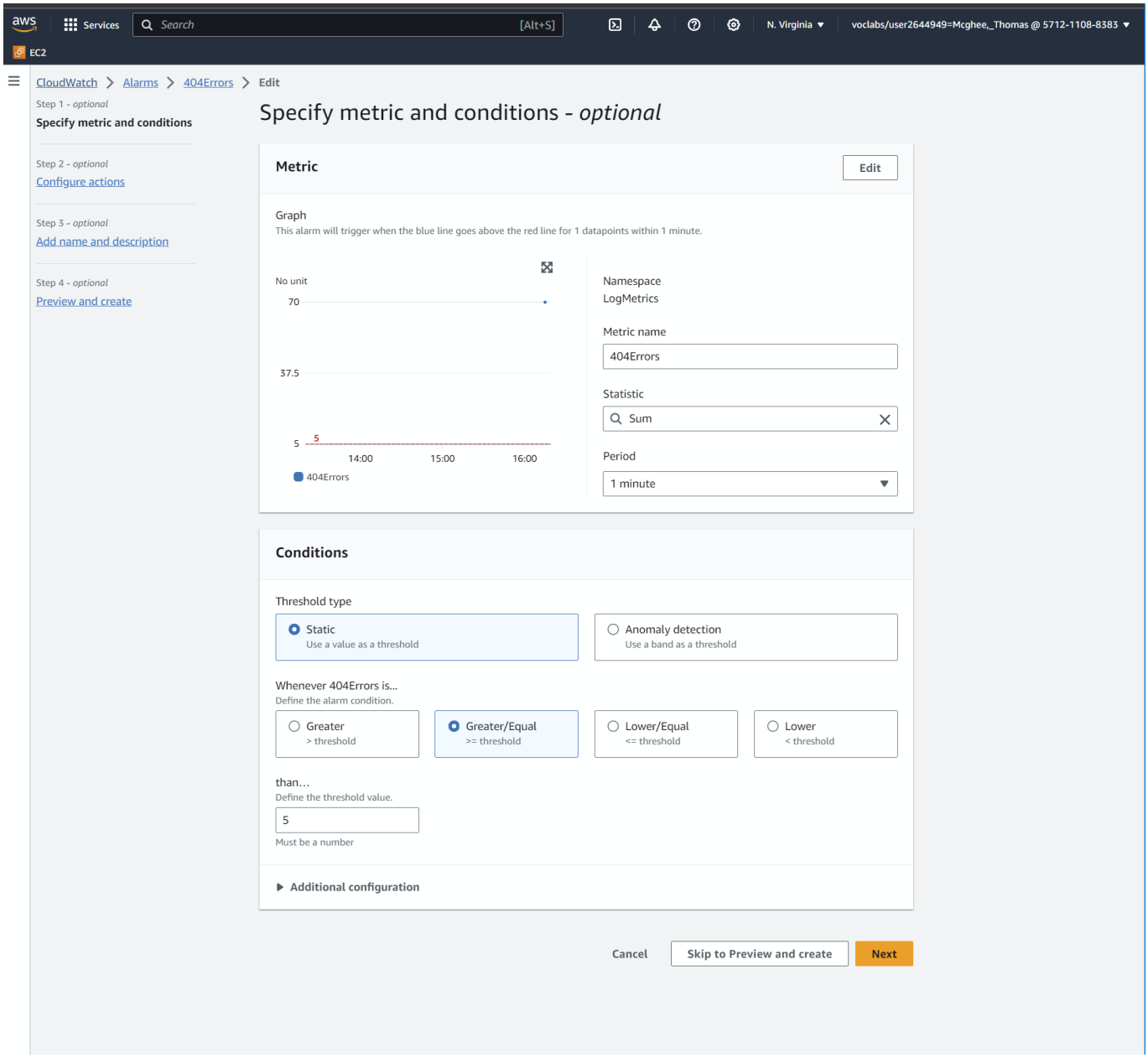
Maximum Capacity	10 instances
EC2 Instance (Database Server)	
Instance Type	r5.large
vCPU	2
Memory	16 GiB
Amazon RDS	
DB Instance Class	db.m4.large
Allocated Storage	200 GB
IOPS	Provisioned 1000 IOPS
Storage Auto Scaling Threshold	75% of allocated storage

Maximum Storage Threshold	500 GB
Amazon VPC	
Number of VPCs	2 (production and staging/testing)
Subnets	Multiple according to best practices
Elastic Load Balancer (ELB)	
Type	Application Load Balancer (ALB)
Capacity	Scales automatically with incoming traffic
Auto Scaling Group for EC2	
Target Tracking Scaling	Based on average CPU utilization or network
Scheduled Scaling	Increase instances for known load increases

Dynamic Scaling	Respond to CloudWatch alarms
CloudWatch Alarms	
EC2 Monitoring	CPU Utilization, Network In/Out, Disk Ops
RDS Monitoring	CPU Utilization, Freeable Memory, IOPS, Storage

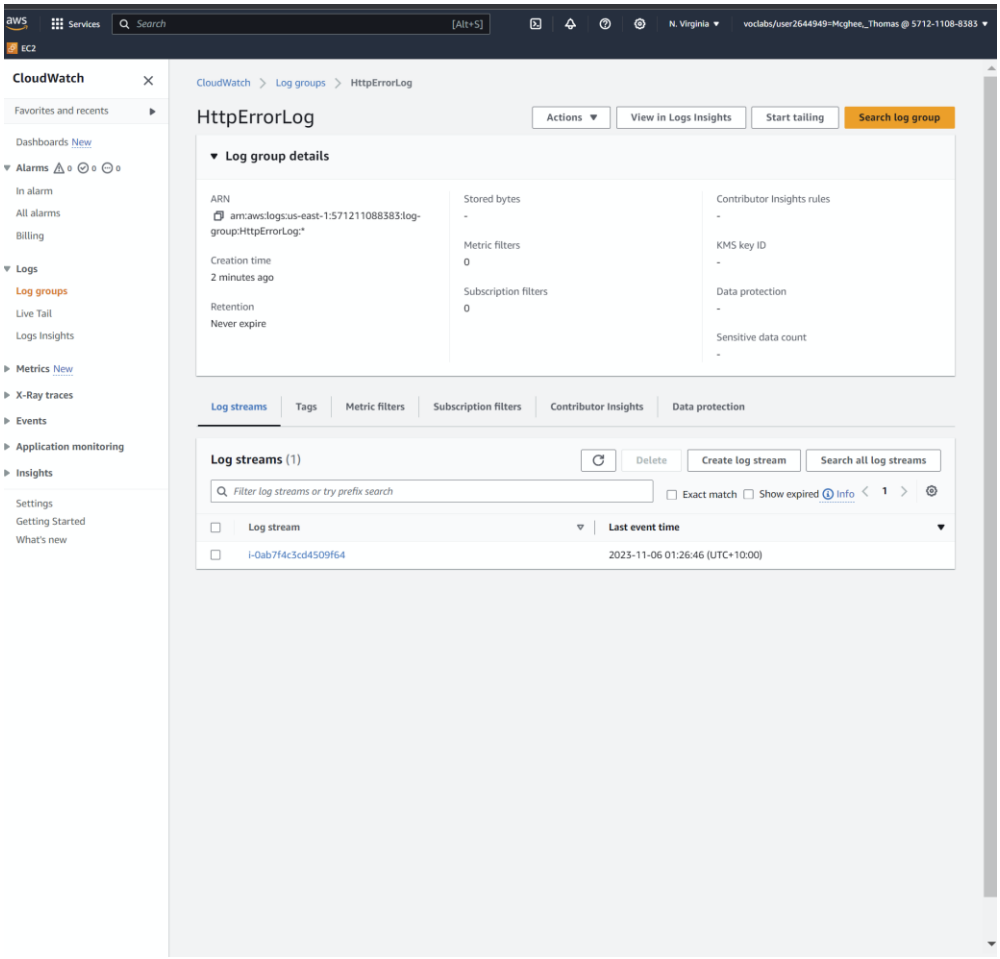
7.2 Configure metrics and alarm when limits are exceeded (provide screen shot)

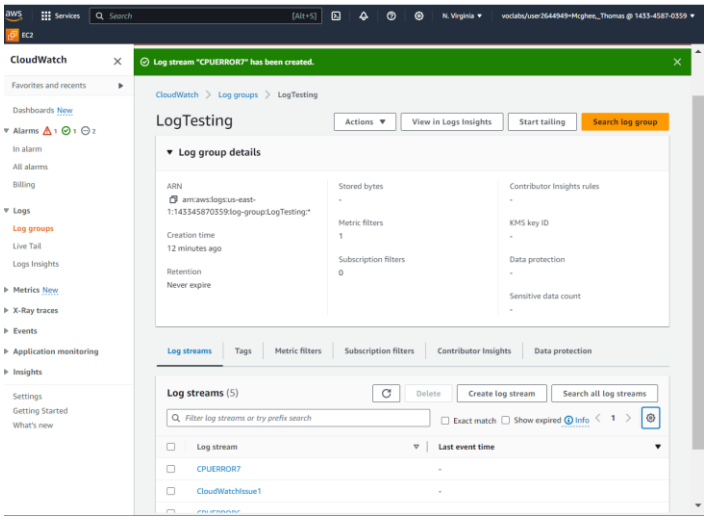
Find foundation inside lab 6 again, take a screenshot from that lab 6



7.3 Capture and store resource and system logs (provide screen shot)\

You can take a screenshot of log events and a screenshot of that lab


CloudWatch
CloudWatch > Log groups > HttpErrorLog
HttpErrorLog
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
ARN
arn:aws:logs:us-east-1:571211088383:log-group:HttpErrorLog:*
Creation time
2 minutes ago
Retention
Never expire
Stored bytes
-
Metric filters
0
Subscription filters
0
Contributor Insights rules
-
KMS key ID
-
Data protection
-
Sensitive data count
-
Log streams
Tags
Metric filters
Subscription filters
Contributor Insights
Data protection
Log streams (1)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired
Info
Log stream
Last event time
i-0ab7f4c3cd4509f64
2023-11-06 01:26:46 (UTC+10:00)

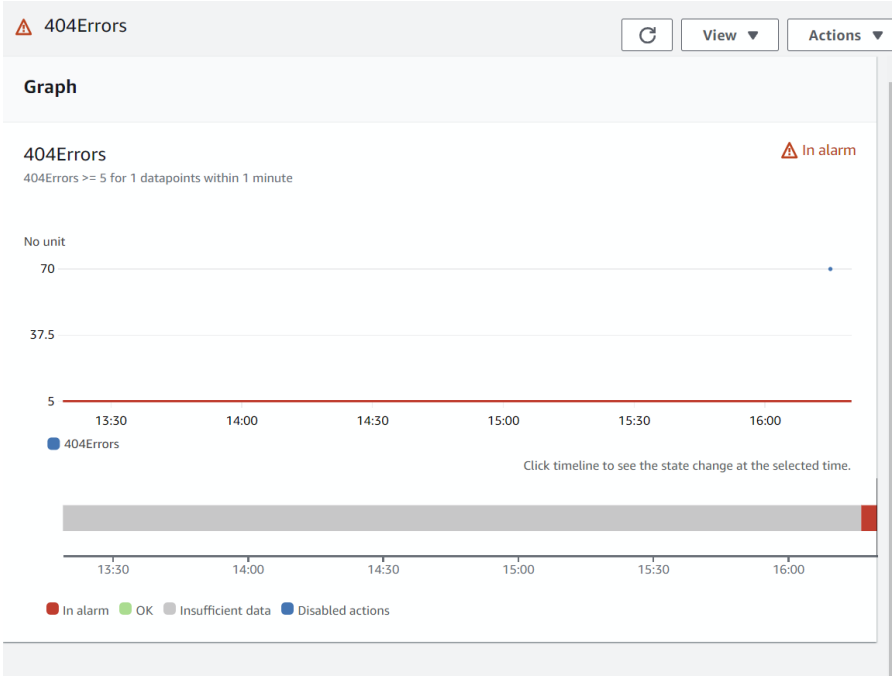

Log stream "CPUERROR7" has been created.
CloudWatch
CloudWatch > Log groups > LogTesting
LogTesting
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
ARN
arn:aws:logs:us-east-1:143345870359:log-group:LogTesting:*
Creation time
12 minutes ago
Retention
Never expire
Stored bytes
-
Metric filters
1
Subscription filters
0
Contributor Insights rules
-
KMS key ID
-
Data protection
-
Sensitive data count
-
Log streams
Tags
Metric filters
Subscription filters
Contributor Insights
Data protection
Log streams (5)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired
Info
Log stream
Last event time
CPUERROR7
CloudWatchIssue1

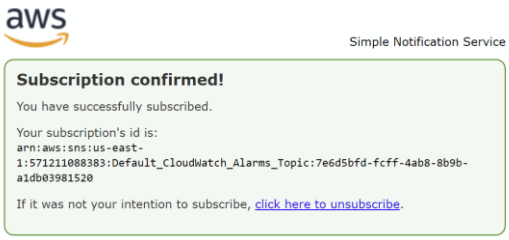
ICTCLD507_508_AT3_PE_TQ

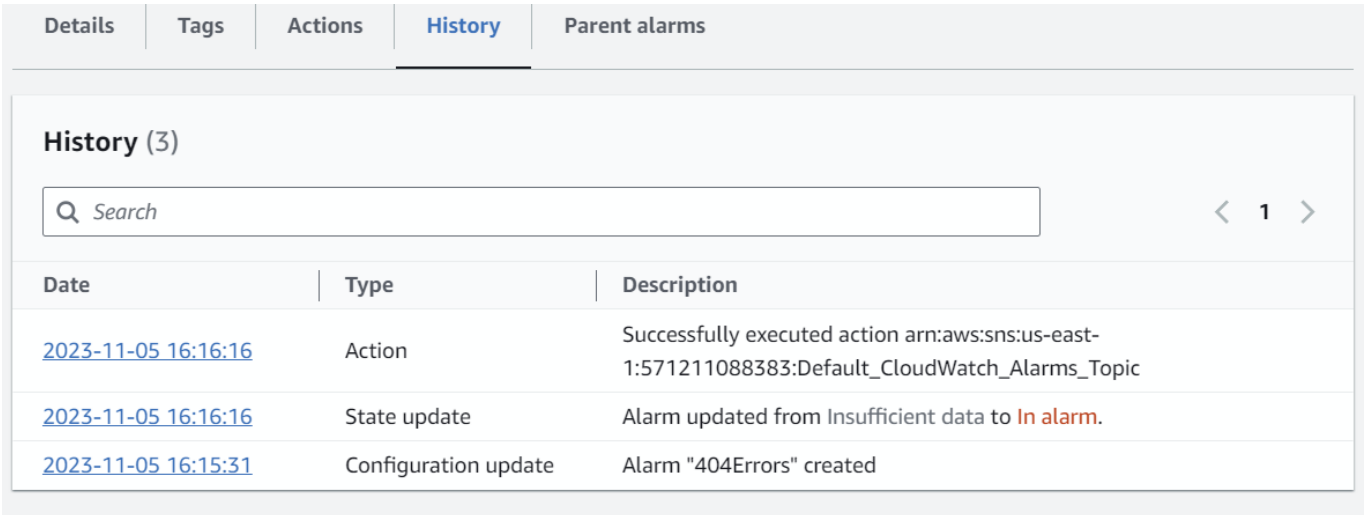
M_v1.docx

7.4 Test capacity to trigger alarms and review logs of incident (provide screen shot)

In this lab, you are asked to run the workload and then take a screenshot of the alarms it will generate an alarm and also send an email, take a screenshot of either one.

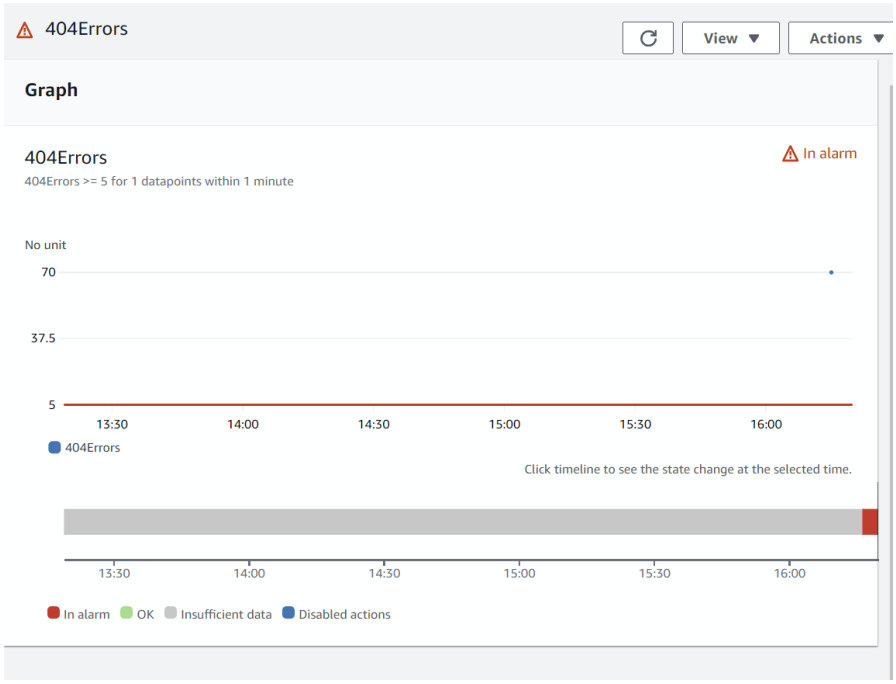


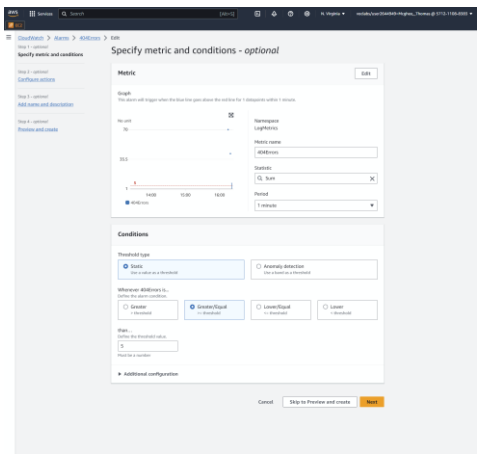




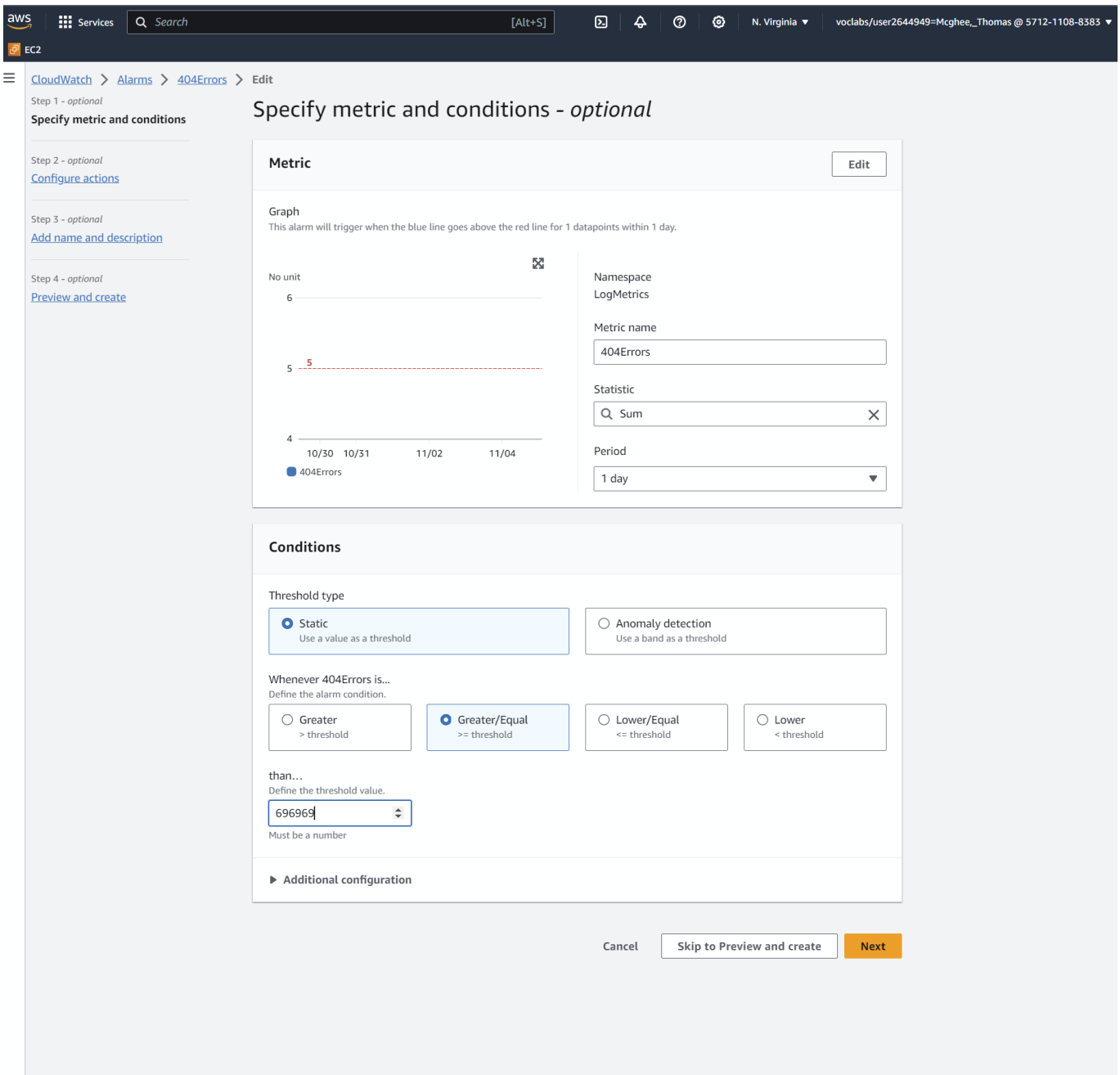
7.5 Manage capacity of resource to remove alarm (provide screen shot)

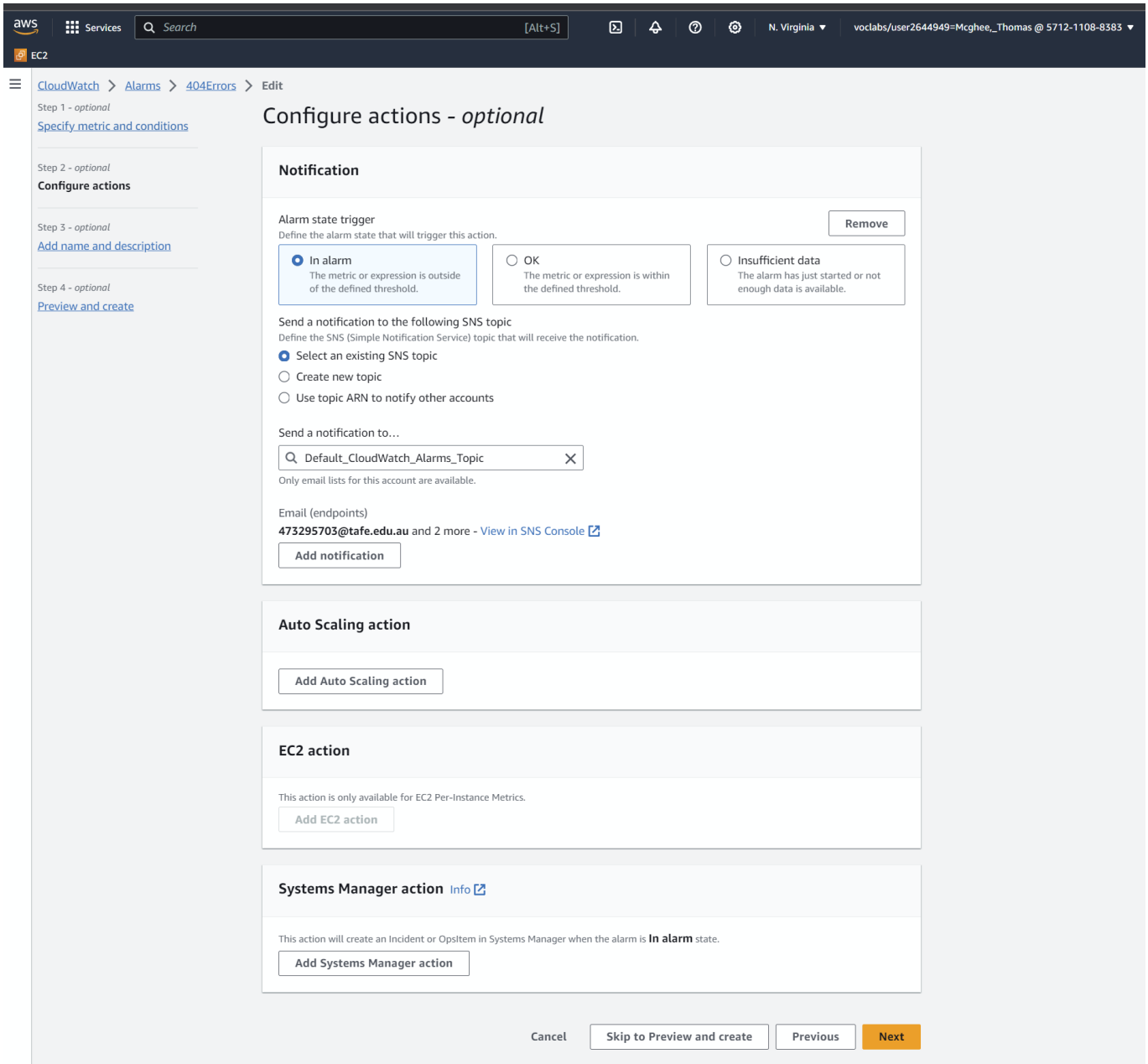
You need to increase the capacity and remove the alarm and take a screenshot without the alarm and put it there. note down what im saying, and remember this is one of the labs set cpu util to 80% to remove the alarm.

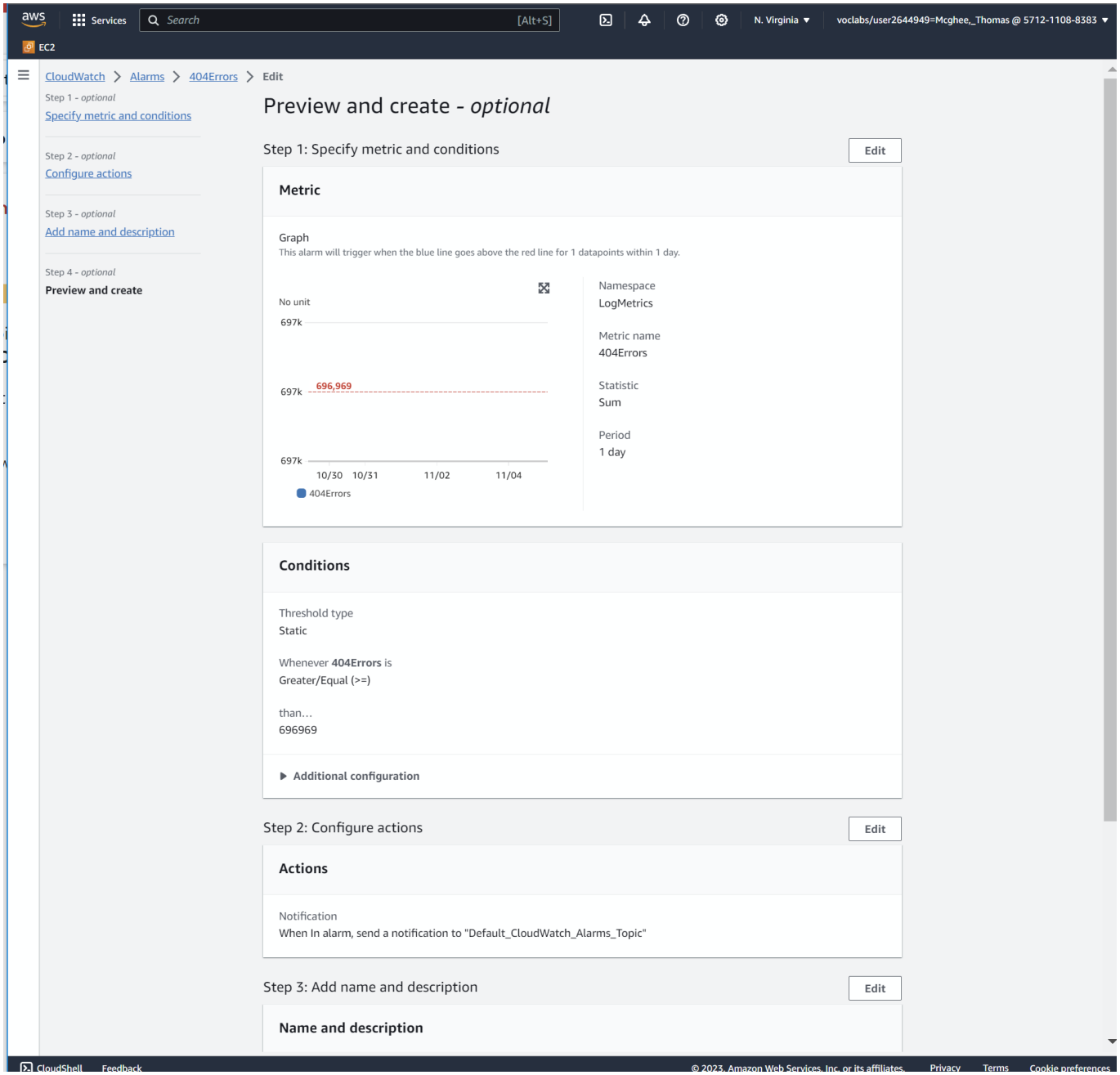




Changed to ->


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 5712-1108-8383
EC2
CloudWatch
Alarms
404Errors
Edit
Step 1 - optional
Specify metric and conditions
Step 2 - optional
Configure actions
Step 3 - optional
Add name and description
Step 4 - optional
Preview and create
Specify metric and conditions - optional
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.
No unit
6
5
5
4
10/30
10/31
11/02
11/04
404Errors
Namespace
LogMetrics
Metric name
404Errors
Statistic
Sum
Period
1 day
Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever 404Errors is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
696969
Must be a number
Additional configuration
Cancel
Skip to Preview and create
Next


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 5712-1108-8383
EC2
CloudWatch
Alarms
404Errors
Edit
Step 1 - optional
Specify metric and conditions
Step 2 - optional
Configure actions
Step 3 - optional
Add name and description
Step 4 - optional
Preview and create
Configure actions - optional
Notification
Alarm state trigger
Define the alarm state that will trigger this action.
Remove
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is within the defined threshold.
Insufficient data
The alarm has just started or not enough data is available.
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Send a notification to...
Default_CloudWatch_Alarms_Topic
Only email lists for this account are available.
Email (endpoints)
473295703@tafe.edu.au and 2 more - View in SNS Console
Add notification
Auto Scaling action
Add Auto Scaling action
EC2 action
This action is only available for EC2 Per-Instance Metrics.
Add EC2 action
Systems Manager action
Info
This action will create an Incident or OpsItem in Systems Manager when the alarm is In alarm state.
Add Systems Manager action
Cancel
Skip to Preview and create
Previous
Next


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2644949=Mcghee,_Thomas @ 5712-1108-8383
EC2
CloudWatch > Alarms > 404Errors > Edit
Step 1 - optional
Specify metric and conditions
Step 2 - optional
Configure actions
Step 3 - optional
Add name and description
Step 4 - optional
Preview and create
Preview and create - optional
Step 1: Specify metric and conditions
Edit
Metric
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.
No unit
697k
696,969
10/30
10/31
11/02
11/04
404Errors
Namespace
LogMetrics
Metric name
404Errors
Statistic
Sum
Period
1 day
Conditions
Threshold type
Static
Whenever 404Errors is
Greater/Equal (>=)
than...
696969
Additional configuration
Step 2: Configure actions
Edit
Actions
Notification
When In alarm, send a notification to "Default_CloudWatch_Alarms_Topic"
Step 3: Add name and description
Edit
Name and description
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Part 8 – Manage storage life cycle (provide screen shots)

8.1 Identify data retention policy according to business needs and cloud resources

This one you need to write down the policies, tax related documents will be kept for 5 years, customer policies will be kept for 3 years (these are just examples).

Data Inventory: "We have cataloged all types of telecommunications data in our possession to ensure a comprehensive understanding of our data retention responsibilities."
Data Encryption and Protection:

- "All telecommunications data stored within our AWS services is encrypted at rest using AWS Key Management Service (KMS)."
- "We ensure that data in transit is secured and encrypted using protocols like TLS."

Database Storage with Amazon RDS:

- "Our telecommunications data is securely stored in Amazon RDS databases, configured to retain automated backups for a period of at least 2 years."
- "RDS instances handling telecommunications data are encrypted using keys managed by AWS KMS."

File Storage with Amazon S3:

- "We use Amazon S3 for any additional file storage requirements, with versioning and MFA Delete features enabled for added data protection."
- "A lifecycle policy is in place to retain data within Amazon S3 for a minimum of 2 years."

Logging and Monitoring:

- "AWS CloudTrail is active across our AWS environment, ensuring all API calls and activities are logged."
- "AWS CloudWatch monitors our resources for unauthorized access or changes, with alarms set up to notify us of any suspicious activity."

Access Control:

- "Access to telecommunications data is strictly controlled using AWS Identity and Access Management (IAM), ensuring users have the least privilege necessary."
- "Regular audits of IAM policies and user access levels are conducted to maintain a secure environment."

Regular Audits and Reviews: "We conduct regular audits of our AWS environment and our data retention practices to ensure ongoing compliance with the Telecommunications (Interception and Access) Act."
Documentation and Reporting: "Comprehensive documentation of our data retention policies, AWS service configurations, and access controls is maintained and readily available for reporting purposes."
Legal and Compliance Consultation: "We engage with legal and compliance experts familiar with Australian telecommunications law to regularly review and validate our data retention practices."
Exemptions and Variations: "If necessary, we are prepared to proactively apply for exemptions or variations to our data retention obligations, providing clear and valid reasons for such requests."

By adhering to these statements and implementing the described practices, AWS users can ensure that they are in compliance with the Telecommunications (Interception and Access) Act 1979, maintaining the security and accessibility of telecommunications data for lawful access by authorized agencies. Especially regarding GOSHOP.

8.2 Configure storage to automatically comply with retention policy

S3 Service Selection:

The S3 service was located and selected within the AWS Console using the search functionality.

Bucket Details:

The intended S3 bucket was located in the list and selected to open its detail page.

Lifecycle Policy Configuration:

Within the bucket detail page, the "Management" tab was navigated to.

The "Lifecycle" option was chosen to add or modify the lifecycle rules.

Rule Specification:

A new lifecycle rule was initiated with the "Add lifecycle rule" action.

A nomenclature, such as "DataRetentionRule," was assigned to the rule.

Transition and Expiration Settings:

Transition actions were defined to move objects to the Standard-IA class after 30 days for current versions and after 60 days for noncurrent versions.

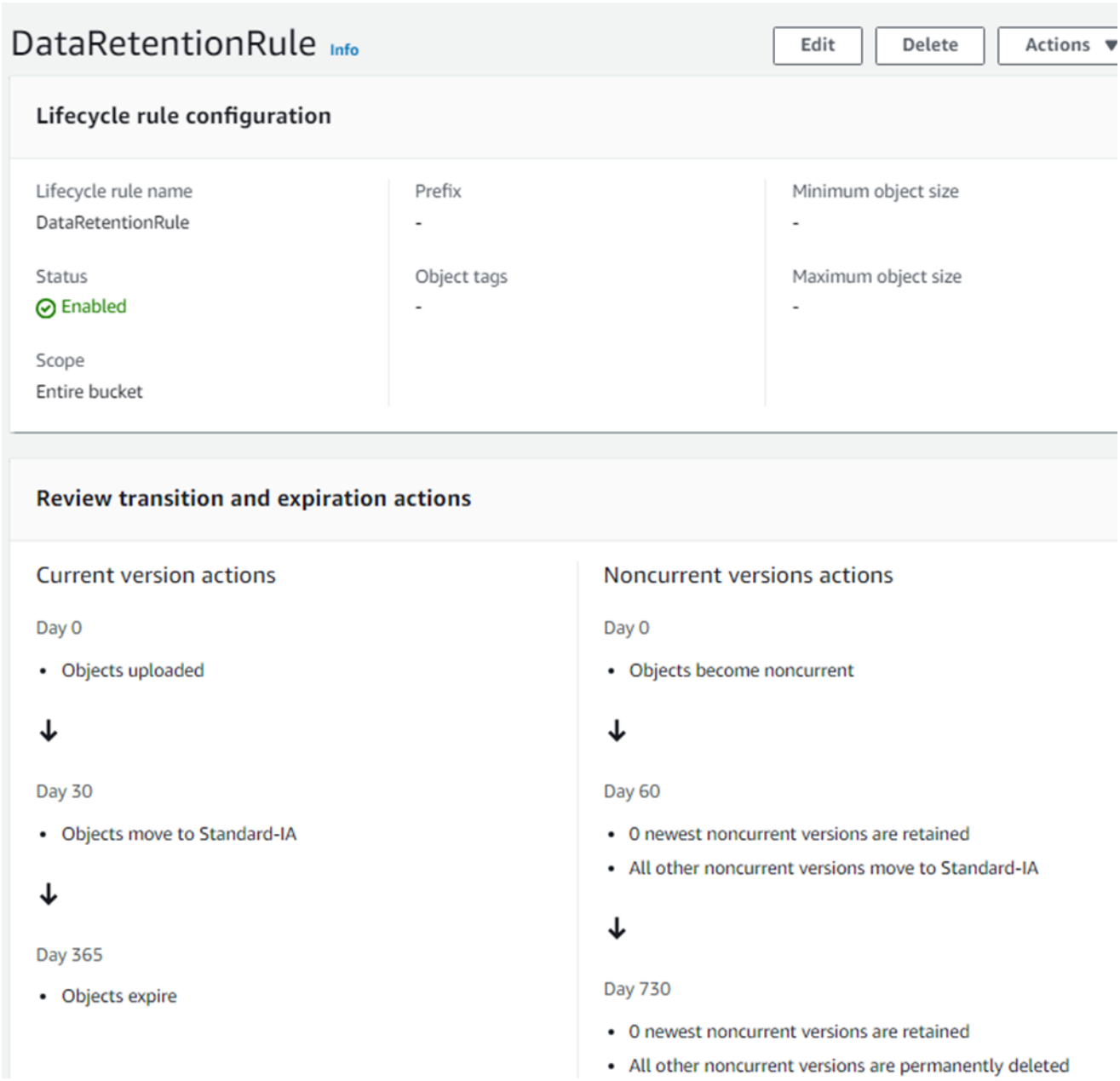
Expiration actions were established to delete current versions after 365 days and noncurrent versions after 730 days.

Policy Review and Implementation:

The lifecycle policy settings were reviewed for accuracy.

Upon confirmation of the correct settings, the "Save" button was utilized to implement the rule.

8.3 Confirm that retention policy is applied to target storage



Part 9 – Documentation

9.1 Document resource tagging and inventory management according to business needs

Basically documentation about resource tagging and you need to describe what tags you created, why you used it, why you use tags, that kind of thing.

Service Tags (svc:): This tag prefix was used to identify the service type, such as svc:webapp for the web application servers and svc:database for database servers.

Environment Tags (env:): These tags identify the environment in which the resource operates, like env:production for production systems and env:development for development systems.

Directive Tags (directive:): Directive tags are used to apply certain policies or rules, such as directive:webhosting for resources that have cost-saving measures applied, or directive:database for resources that must meet certain compliance standards.

Name Tags (name:): This simple yet critical tag is used for the name of the resource, for example, name:RDSdatabse or name:webapp.

Each tag was chosen to reflect a specific attribute of the resource it is attached to, thus enabling more effective filtering, reporting, and management of resources in the cloud environment.

9.2 Document cloud audit and change management configuration

Done section 6, so what you did in section 6 you need tyo describe it here

The documentation for the cloud audit and change management configuration includes detailed procedures and protocols on how the configuration policies are implemented and enforced. This ensures compliance with GO Shop's business needs and regulatory requirements, particularly concerning the operation of their cloud-based systems in Australia.

The configuration policy setup follows the defined roles and responsibilities:

Administrative Roles: Enforces policies that dictate permissions and access controls in alignment with each role's responsibilities, ensuring that administrators have the necessary rights to manage the cloud infrastructure without over-privileged access.

Development Team Roles: Configuration policies for the development team are designed to support a robust software development lifecycle, providing developers with permissions required for continuous integration/continuous deployment (CI/CD) processes while safeguarding against unauthorized changes.

IT Security Roles: Focuses on policies that manage and monitor security configurations, alert settings, and ensure that the security team has audit rights to oversee the security posture of the cloud

environment.

Support and Business Operation Roles: Policies for support and business operation roles are set to provide adequate access to systems required for customer support, inventory management, and business continuity without compromising sensitive data.

User Roles: Employees are granted basic access sufficient for their operational needs, subject to regular review and adjustment as needed.

External Roles: Third-party vendors and auditors are assigned limited and auditable access rights, ensuring they can perform their tasks without impacting the security and integrity of the cloud resources.

The specific cloud-based event logging and configuration tracking are detailed as follows:

CloudTrail Configuration: CloudTrail is configured to log all API calls, sign-in events, and resource changes. This ensures that any configuration change can be audited to determine who made the change, when it was made, and what exactly was changed.

AWS Config Setup: AWS Config is set to monitor resource configurations, with a "1-click setup" for immediate deployment. It tracks resource states over time for audit purposes, though the exact setup is limited by the permissions available in the Learner Labs environment.

Athena and QuickSight Integration: Athena is used to query the configuration state of resources like EC2 instances, with QuickSight leveraging Athena's data to create visualizations and reports that provide insights into resource states and compliance with established configuration policies.

Given the limitation within the Learner Labs, the exact implementation details such as the DDL for Athena and the subsequent QuickSight reporting may not be deployable within the lab environment. However, the proposed architecture and tagging policy facilitate the creation of a comprehensive view of the resource state and configuration changes over time, which is critical for auditing and compliance purposes.

The finalization of the documentation ensures all configurations and changes are captured and can be reviewed by the required personnel, including Cloud Administrators, IT Security Officers, Compliance Managers, and Auditors, to maintain operational integrity and compliance with company policies and external regulations.

9.3 Document run book for actions according to configured alarm

how you configure those alarms and capacity ect

Configured alarms, through tools like Amazon CloudWatch, initiate the following actions:

An SNS notification is sent to the designated IT personnel.

An automated scaling or healing action is executed if the alarm threshold is crossed, for example, creating an additional instance (directive:auto-scale).

In case of critical failures, an automated process is initiated to perform predefined recovery actions.

9.4 Document storage configuration according to business needs

How you configure lifecycle

The Amazon S3 storage lifecycle has been configured with the following policies:

- Transition to Infrequent Access (directive:cost-saving): After 30 days to move less frequently accessed data to a cost-effective storage tier.
- Archival (directive:long-term-storage): After 60 days, the data is transferred to Glacier for archival purposes.
- Expiry (directive:cleanup): Non-critical data is scheduled for deletion after 1 year to comply with data retention policies.

9.5 Finalize documentation and submit it to required personnel.

All the documentation for the configuration of the cloud resources, tagging, auditing, alarm response, and storage lifecycle management was compiled into a comprehensive report. This report was reviewed for accuracy and completeness, and a signature block was included at the end of the document to ensure authenticity and accountability.

This document was then submitted to the relevant personnel at GO Shop for review and approval, in accordance with the company's procedures for IT system changes.

Submission Details:

Name: Tom Mcghee	Name: Head IT Manager
Signature:	Signature:

Date: 10/10/23

Date:10/10/23

End of Assessment