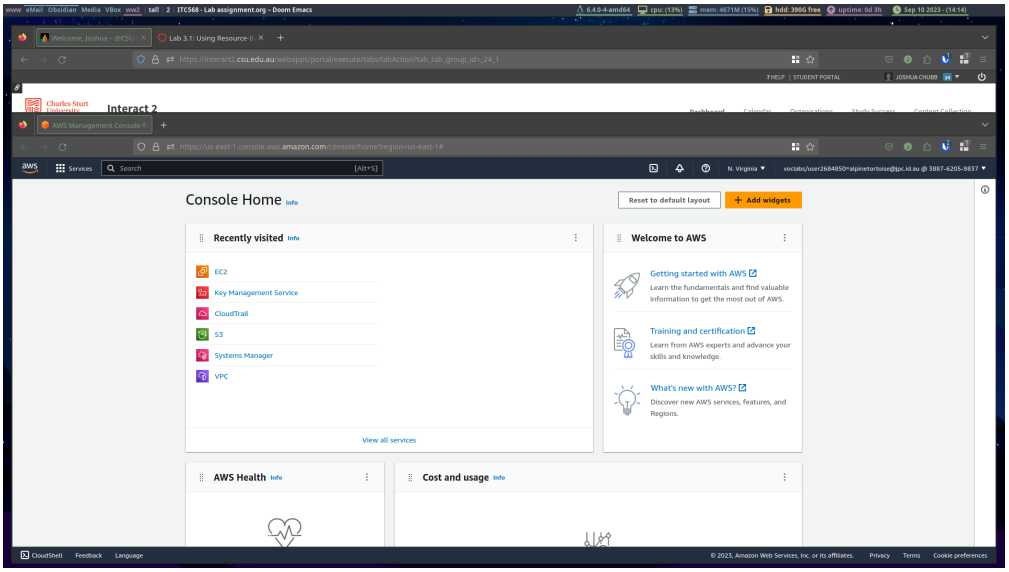
ITC568 - Lab assignment

Joshua Chubb

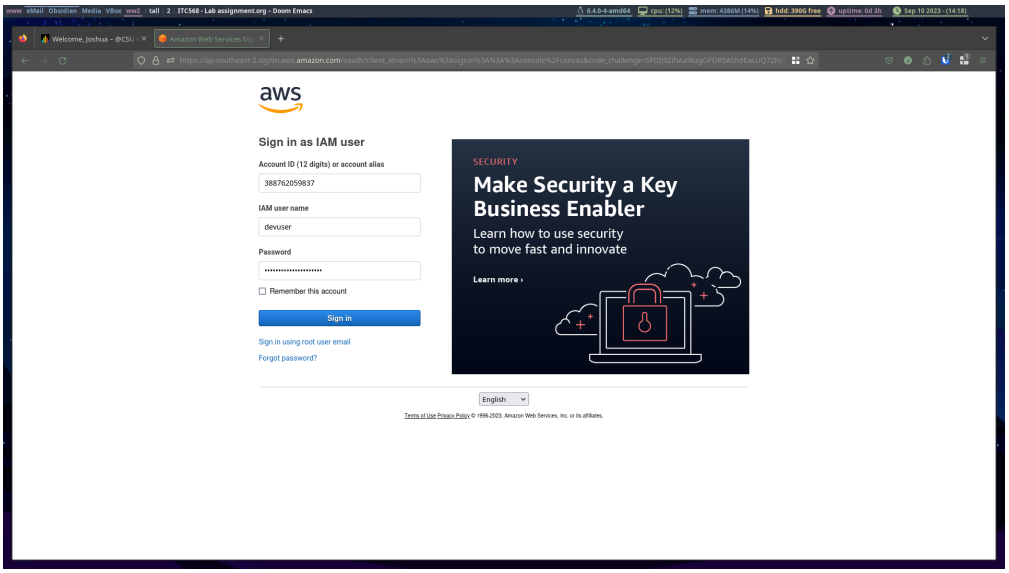
September 10, 2023

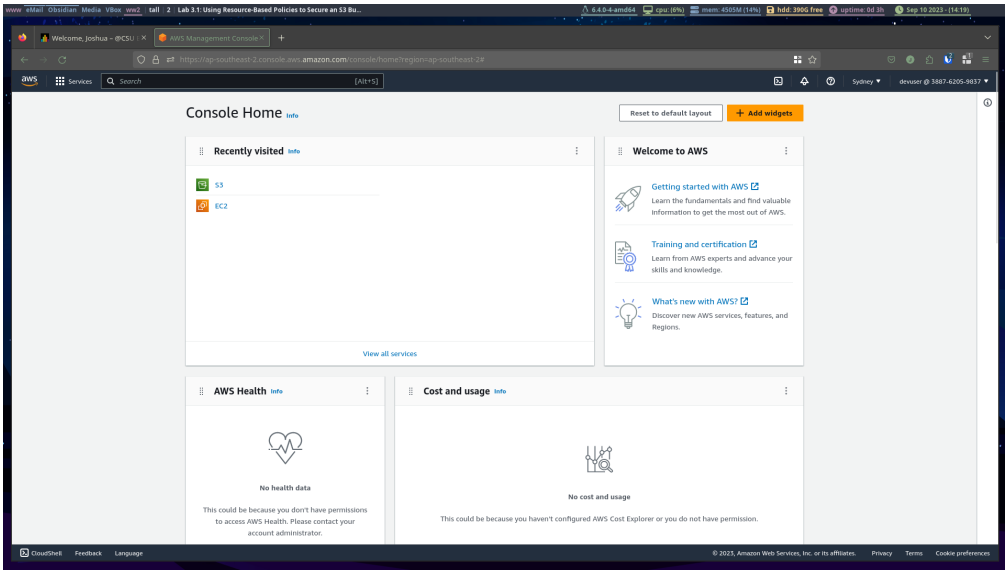
Contents

1 Lab 3.1: Using Resource-Based Policies to Secure an S3 Bucket

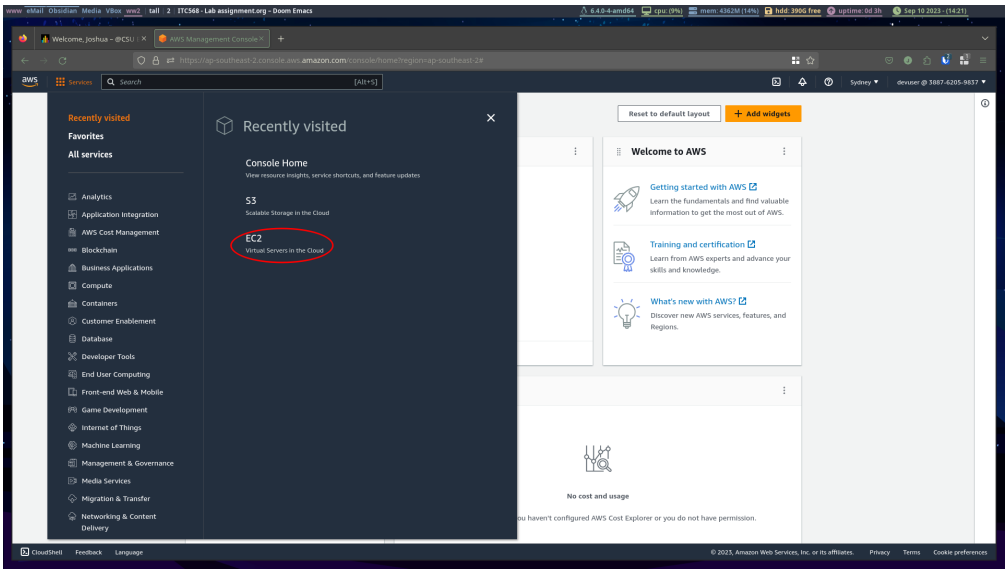


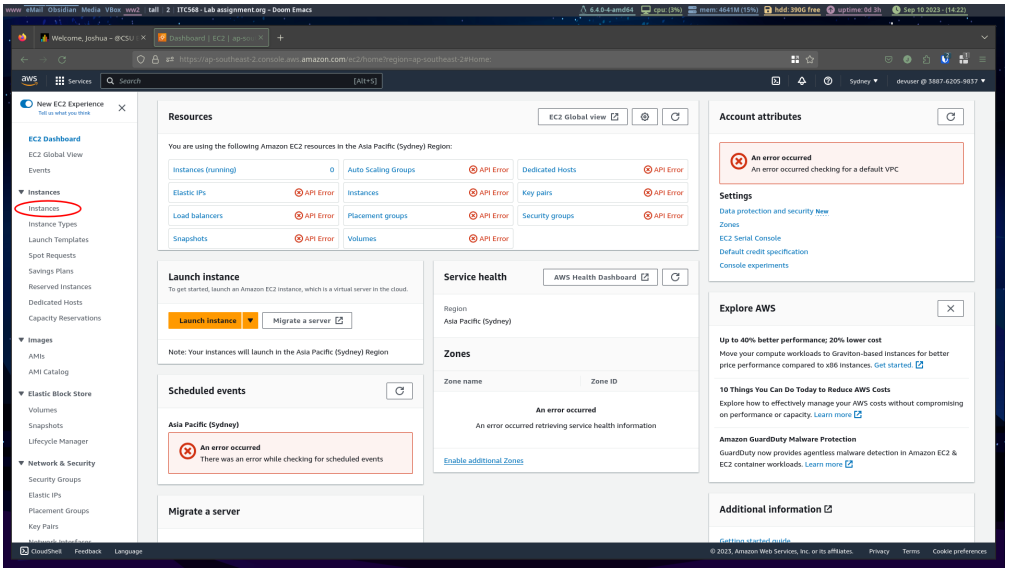
1.1 Task 1: Login to AWS as devuser

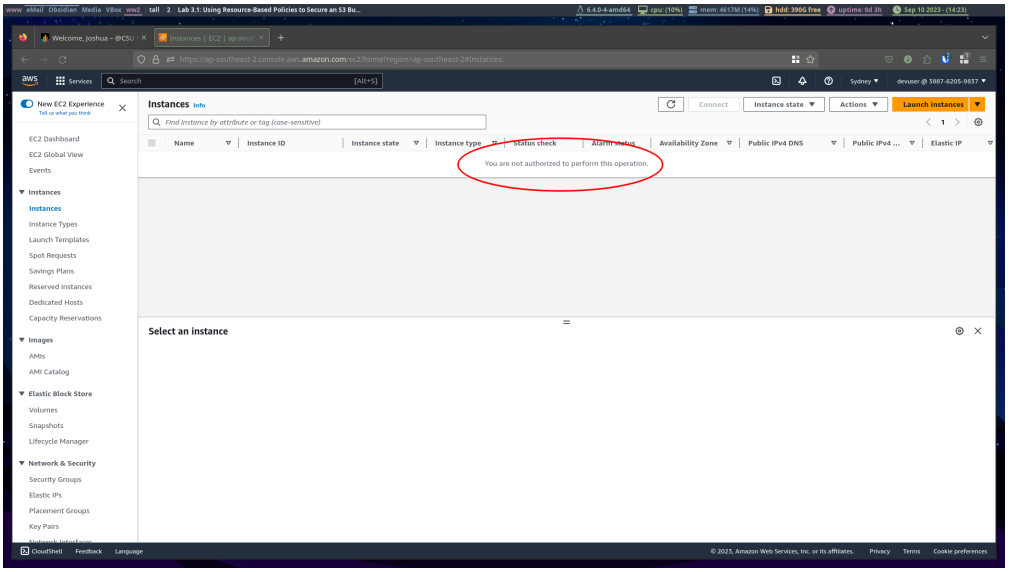


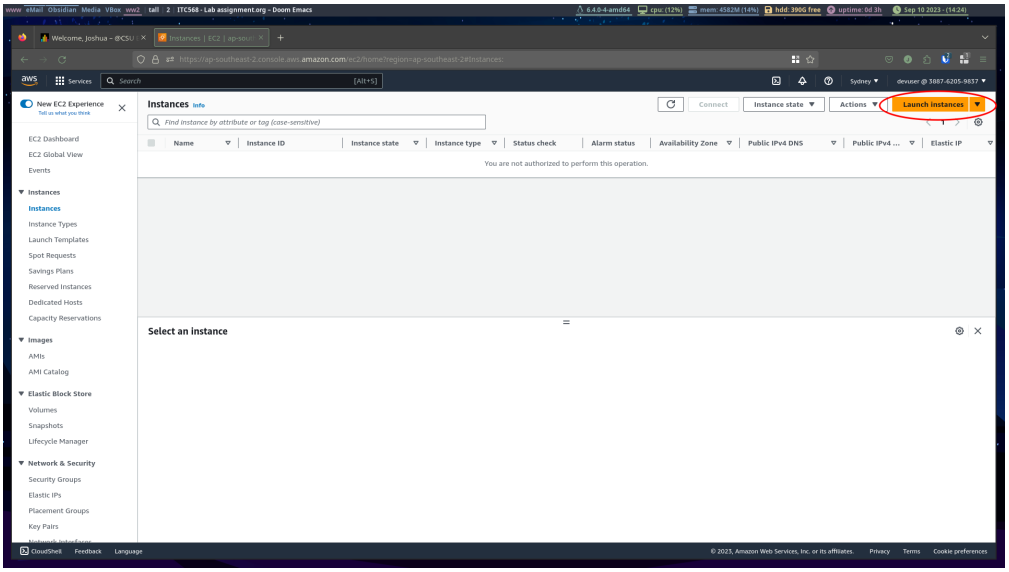


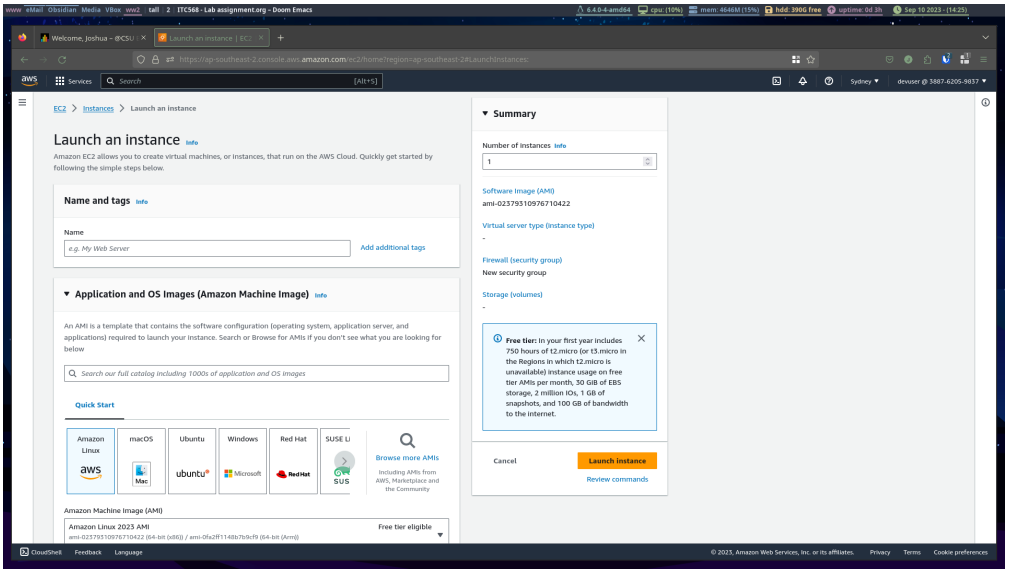
1.2 Task 2: Attempting Read-Level Access

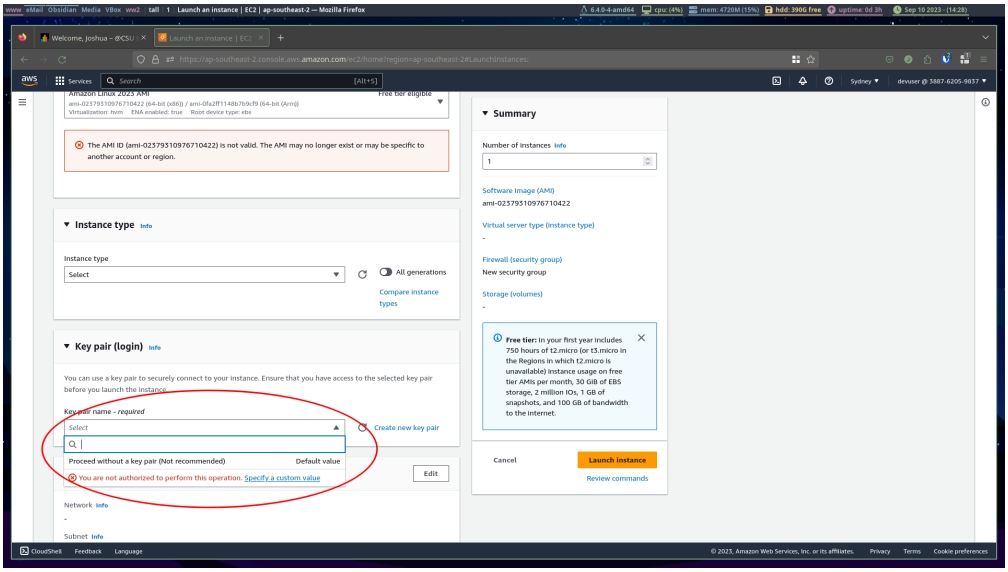


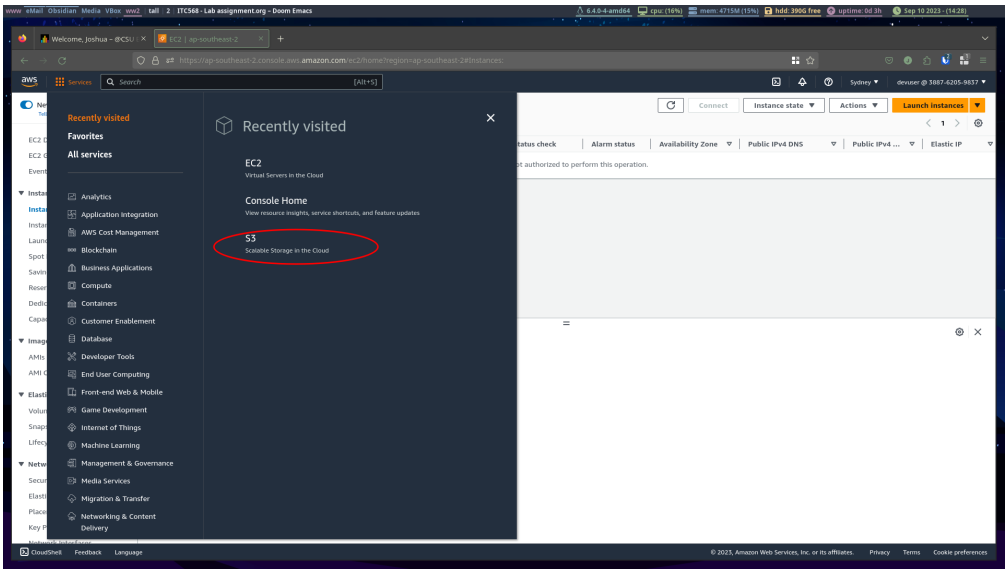

Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Account attributes
An error occurred
An error occurred checking for a default VPC
Settings
Data protection and security New
Zones
EC2 Serial Console
Default credit specification
Console experiments
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the Asia Pacific (Sydney) Region
Service health
AWS Health Dashboard
Region
Asia Pacific (Sydney)
Zones
Zone name
Zone ID
An error occurred
An error occurred retrieving service health information
Enable additional Zones
Explore AWS
Up to 40% better performance; 20% lower cost
Move your compute workloads to Gravitron-based instances for better price performance compared to x86 instances. Get started.
10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more
Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more
Scheduled events
Asia Pacific (Sydney)
An error occurred
There was an error while checking for scheduled events
Migrate a server
Additional information
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

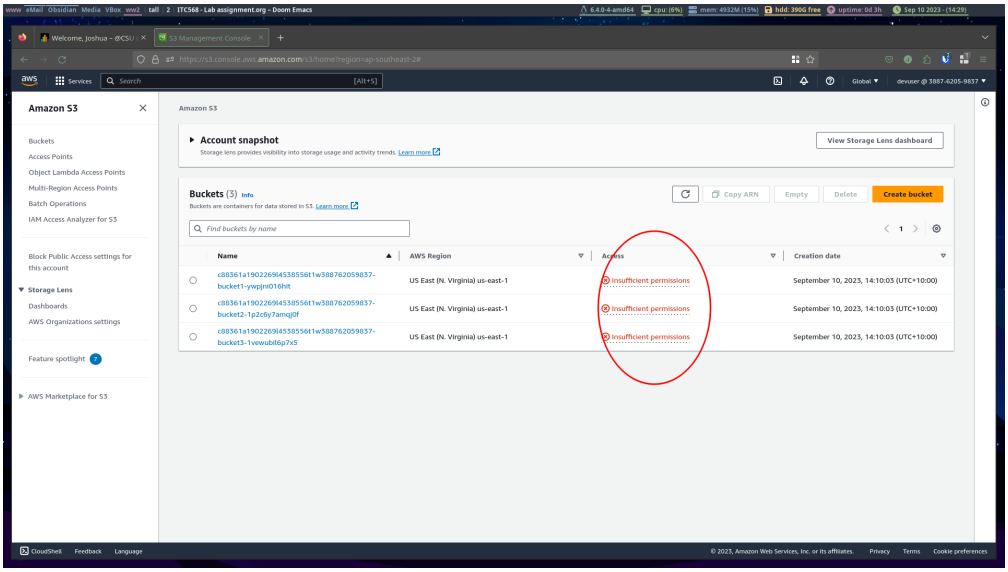

Instances Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
You are not authorized to perform this operation.
Select an instance
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Instances Info
Launch instances
Actions
Connect
Instance state
You are not authorized to perform this operation.
Select an instance

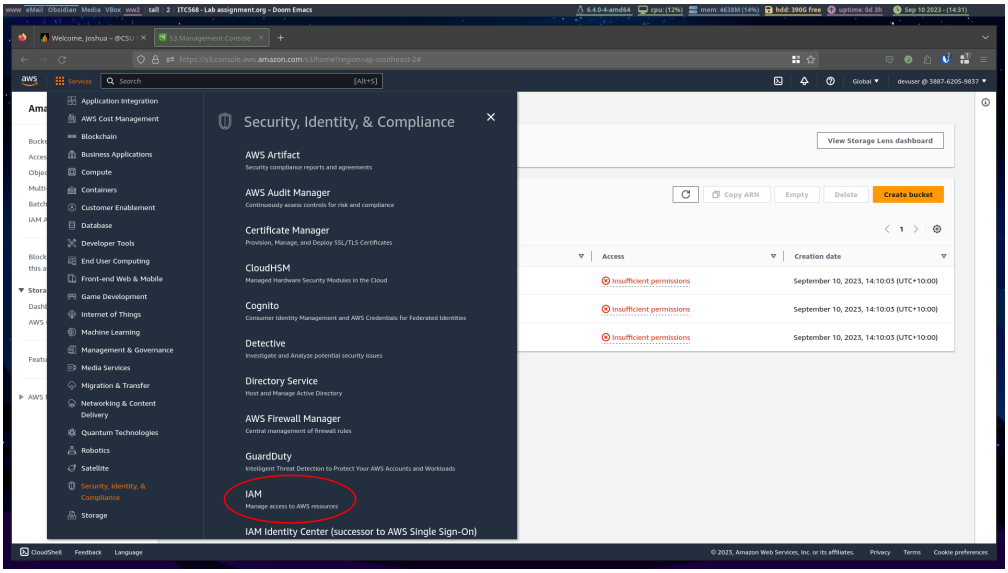

Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Application and OS Images (Amazon Machine Image) Info
Summary
Number of instances Info
Software Image (AMI)
ami-02379310976710422
Virtual server type (instance type)
Firewall (security group)
New security group
Storage (volumes)
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands

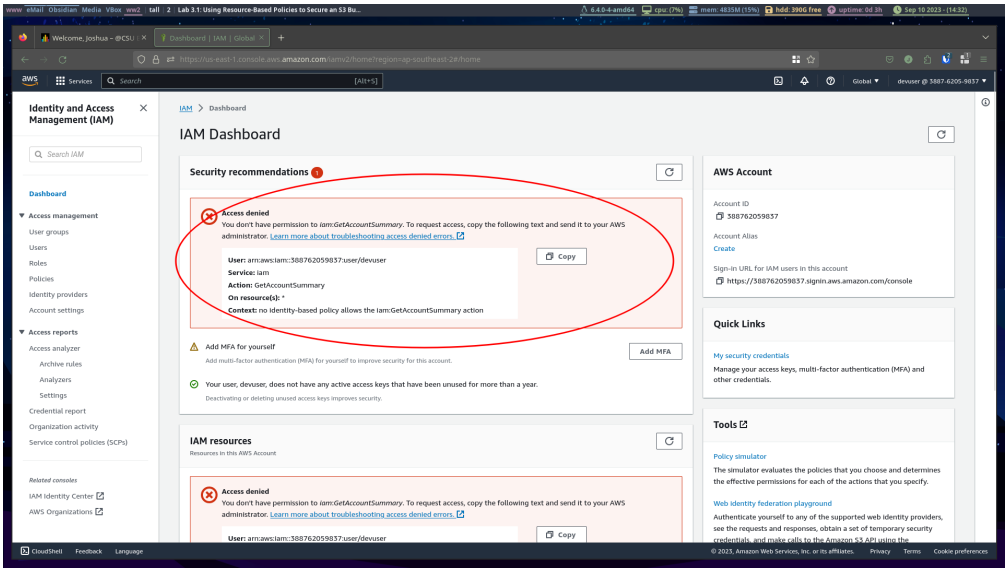

Launch an instance | EC2 | ap-southeast-2 — Mozilla Firefox
Welcome, Joshua – @CSU
Launch an instance | EC2
https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#LaunchInstances:
Services
Search
[Alt+S]
Sydney
devuser @ 3887-6205-9837
Amazon Linux 2023 AMI
Free tier eligible
The AMI ID (ami-02379310976710422) is not valid. The AMI may no longer exist or may be specific to another account or region.
Summary
Number of instances Info
1
Software Image (AMI)
ami-02379310976710422
Virtual server type (instance type)
-
Firewall (security group)
New security group
Storage (volumes)
-
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Instance type Info
Instance type
Select
All generations
Compare instance types
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Select
Create new key pair
Proceed without a key pair (Not recommended)
Default value
You are not authorized to perform this operation. Specify a custom value
Edit
Network Info
-
Subnet Info
Cancel
Launch instance
Review commands
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

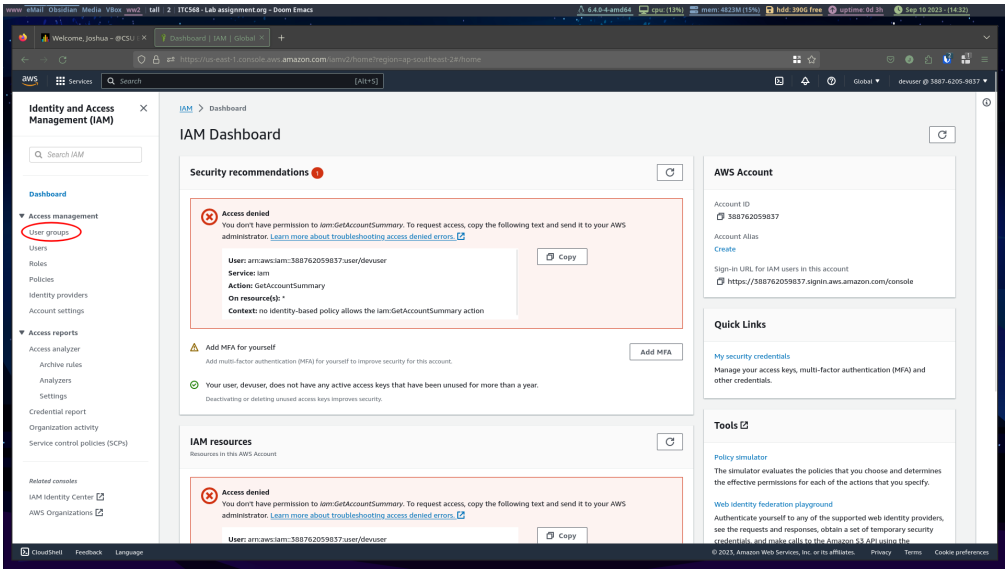

ITC568 - Lab assignment.org - Doom Emacs
Welcome, Joshua – @CSU
EC2 | ap-southeast-2
https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#Instances:
Services
Search
[Alt+S]
Sydney
devuser @ 3887-6205-9837
Connect
Instance state
Actions
Launch instances
Recently visited
Favorites
All services
Recently visited
EC2
Virtual Servers in the Cloud
Console Home
View resource insights, service shortcuts, and feature updates
S3
Scalable Storage in the Cloud
Analytics
Application Integration
AWS Cost Management
Blockchain
Business Applications
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Internet of Things
Machine Learning
Management & Governance
Media Services
Migration & Transfer
Networking & Content Delivery
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

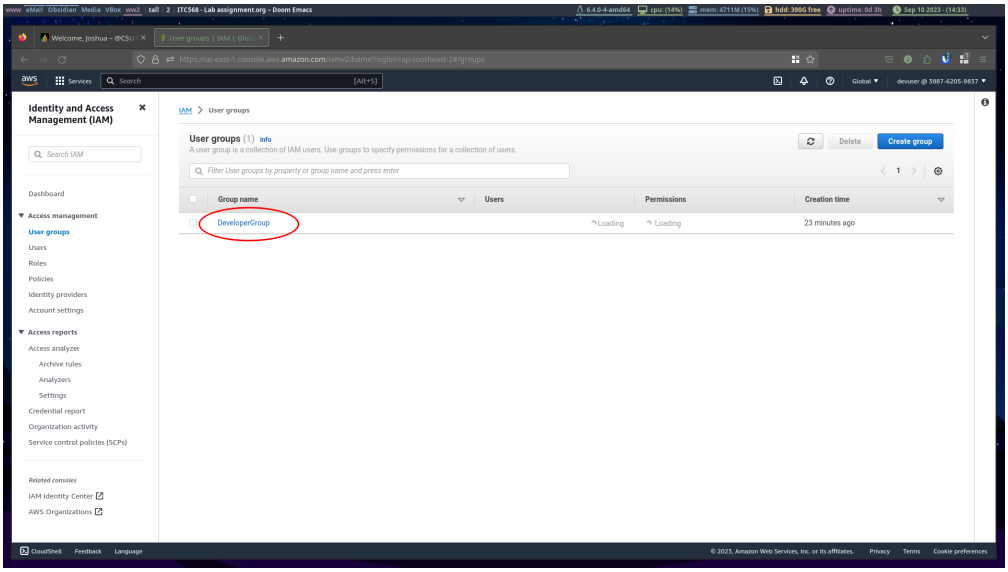


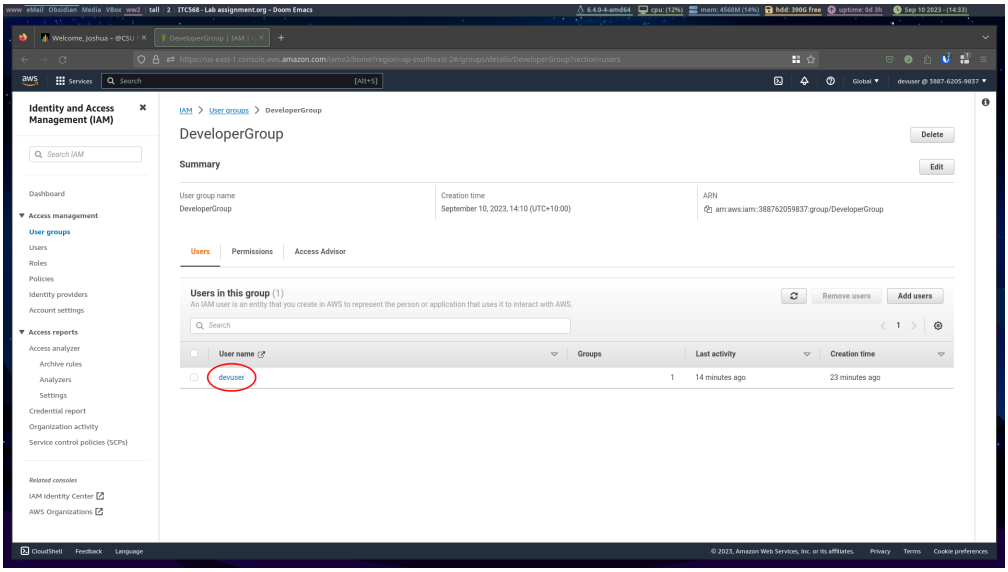
1.3 Task 3: Analyzing the identity-based policy applied to the IAM user

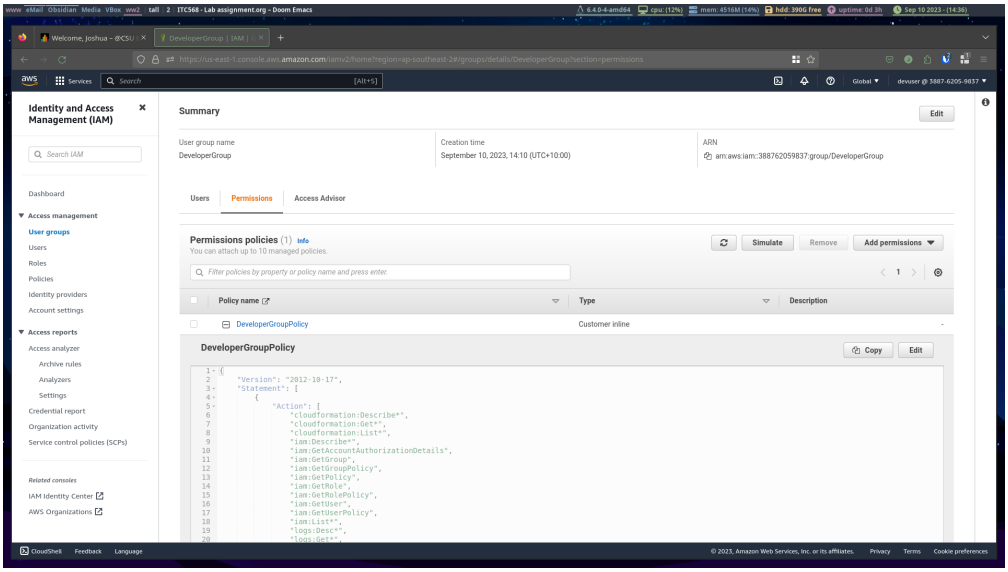



Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
IAM Identity Center
AWS Organizations
IAM > Dashboard
IAM Dashboard
Security recommendations
Access denied
You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
Copy
User: arn:aws:iam::388762059837:user/devuser
Service: iam
Action: GetAccountSummary
On resource(s): *
Context: no identity-based policy allows the iam:GetAccountSummary action
Add MFA for yourself
Add multi-factor authentication (MFA) for yourself to improve security for this account.
Add MFA
Your user, devuser, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.
IAM resources
Resources in this AWS Account
Access denied
You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
Copy
User: arn:aws:iam::388762059837:user/devuser
AWS Account
Account ID
388762059837
Account Alias
Create
Sign-in URL for IAM users in this account
https://388762059837.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
IAM Identity Center
AWS Organizations
IAM > Dashboard
IAM Dashboard
Security recommendations
Access denied
You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
Copy
User: arn:aws:iam::388762059837:user/devuser
Service: iam
Action: GetAccountSummary
On resource(s): *
Context: no identity-based policy allows the iam:GetAccountSummary action
Add MFA for yourself
Add multi-factor authentication (MFA) for yourself to improve security for this account.
Add MFA
Your user, devuser, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.
IAM resources
Resources in this AWS Account
Access denied
You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
Copy
User: arn:aws:iam::388762059837:user/devuser
AWS Account
Account ID
388762059837
Account Alias
Create
Sign-in URL for IAM users in this account
https://388762059837.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Identity and Access Management (IAM)
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Group name
Users
Permissions
Creation time
DeveloperGroup
Loading
Loading
23 minutes ago


Identity and Access Management (IAM)
IAM > User groups > DeveloperGroup
DeveloperGroup
Delete
Summary
Edit
User group name
DeveloperGroup
Creation time
September 10, 2023, 14:10 (UTC+10:00)
ARN
arn:aws:iam::388762059837:group/DeveloperGroup
Users
Permissions
Access Advisor
Users in this group (1)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove users
Add users
User name
Groups
Last activity
Creation time
devuser
1
14 minutes ago
23 minutes ago



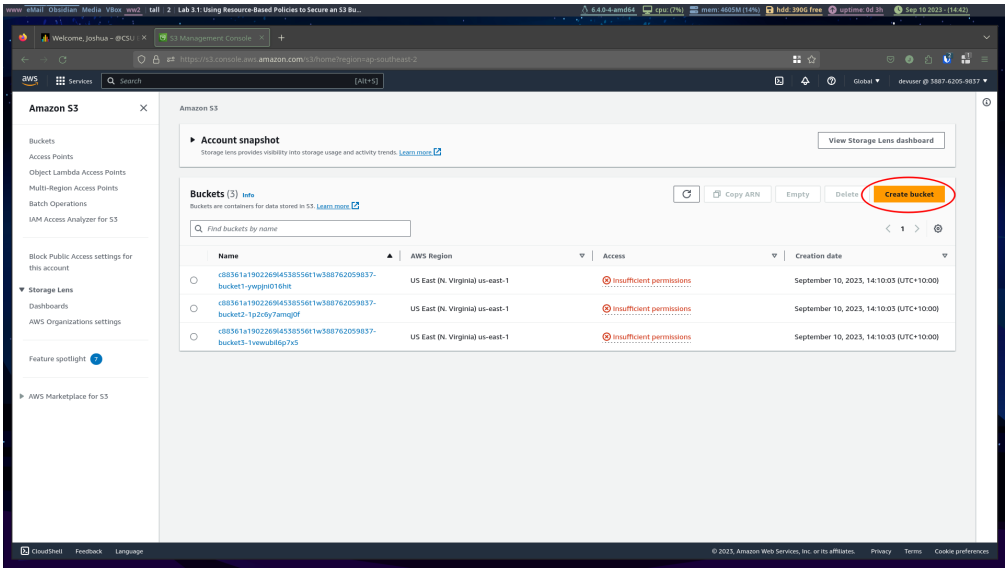
1.3.1 DeveloperGroup policy

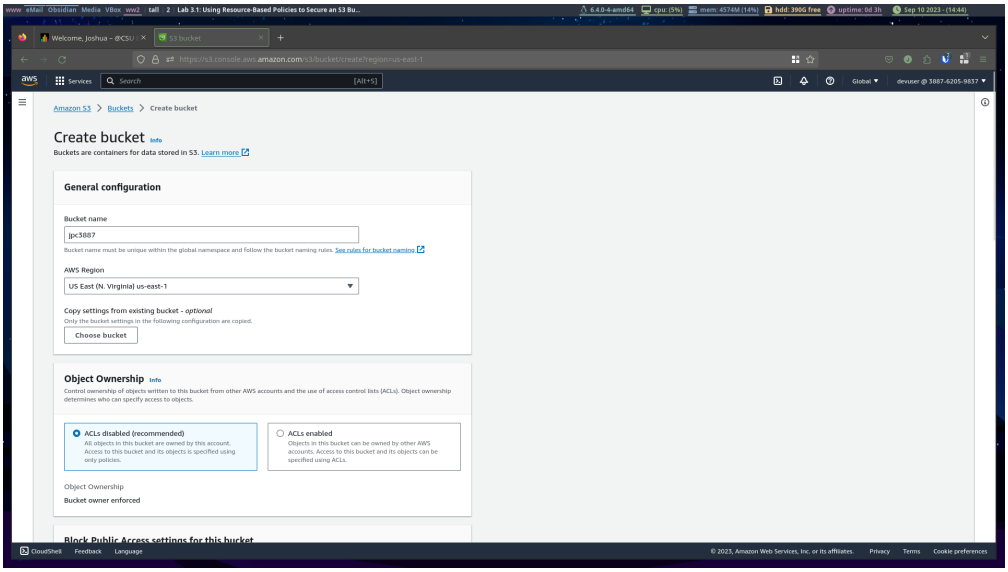
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudformation:Describe*",
                "cloudformation:Get*",
                "cloudformation:List*",
                "iam:Describe*",
                "iam:GetAccountAuthorizationDetails",
                "iam:GetGroup",
                "iam:GetGroupPolicy",
                "iam:GetPolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:List*",
                "logs:Desc*",
                "logs:Get*",
                "logs:List*",
                "s3:CreateBucket",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketPublicAccessBlock",
                "sts:AssumeRole"
```

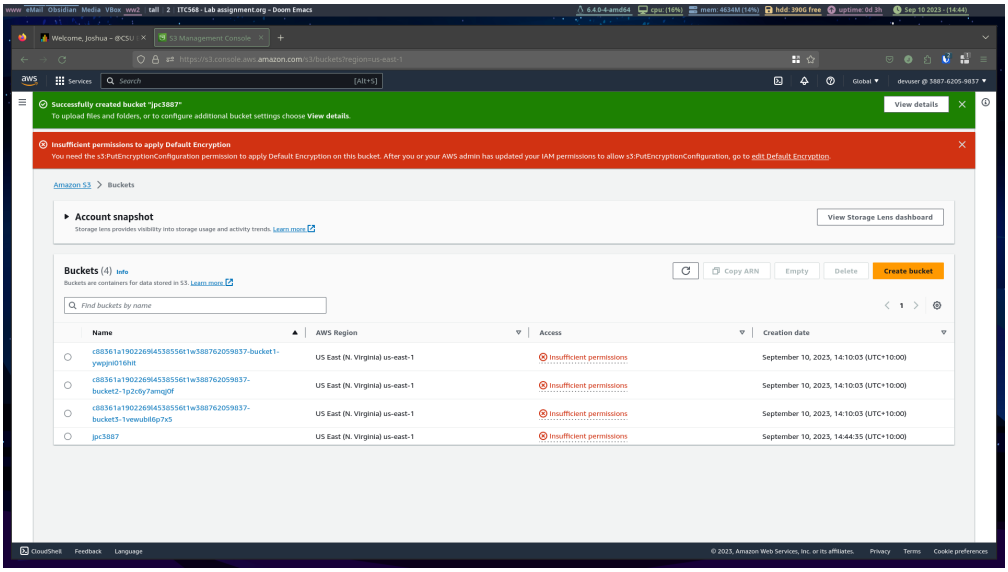
```
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

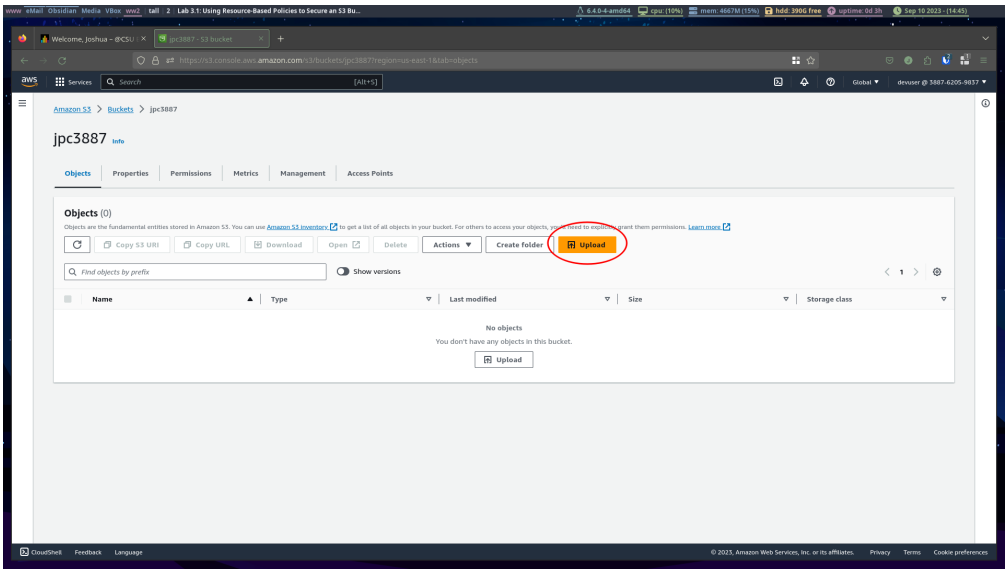
We see in the DeveloperGroupPolicy JSON that there are no EC2 roles and only limited S3 object-related actions.

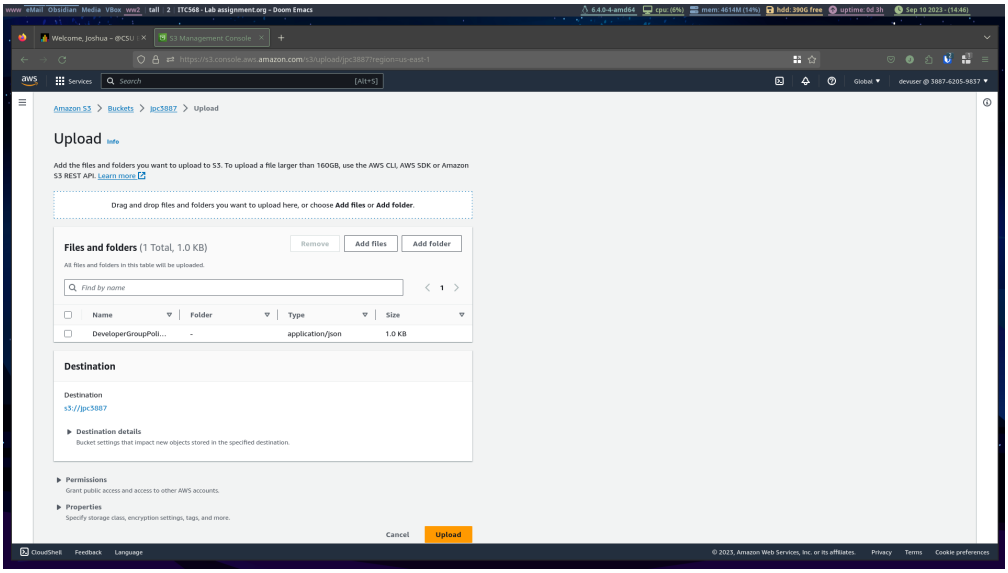
1.4 Task 4: Attempting write-level access to AWS services

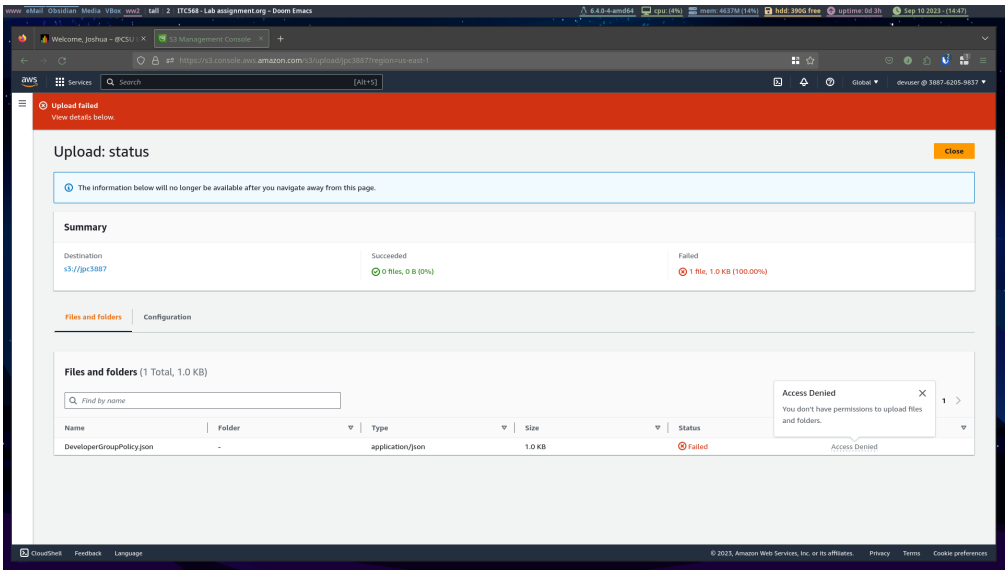





Successfully created bucket "jpc3887"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Insufficient permissions to apply Default Encryption
You need the s3:PutEncryptionConfiguration permission to apply Default Encryption on this bucket. After you or your AWS admin has updated your IAM permissions to allow s3:PutEncryptionConfiguration, go to edit Default Encryption.
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (4) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
c88361a19022694538556t1w388762059837-bucket1-ywpjnvl016hit
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
c88361a19022694538556t1w388762059837-bucket2-1p2c6y7amqi0f
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
c88361a19022694538556t1w388762059837-bucket3-1vewubll6p7x5
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
jpc3887
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:44:35 (UTC+10:00)
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3 > Buckets > jpc3887
jpc3887 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



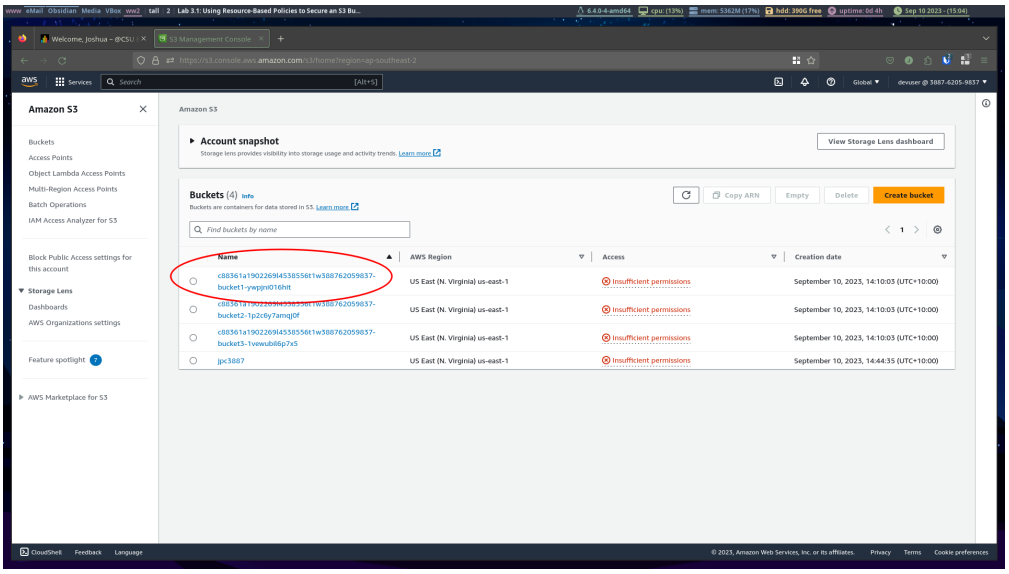


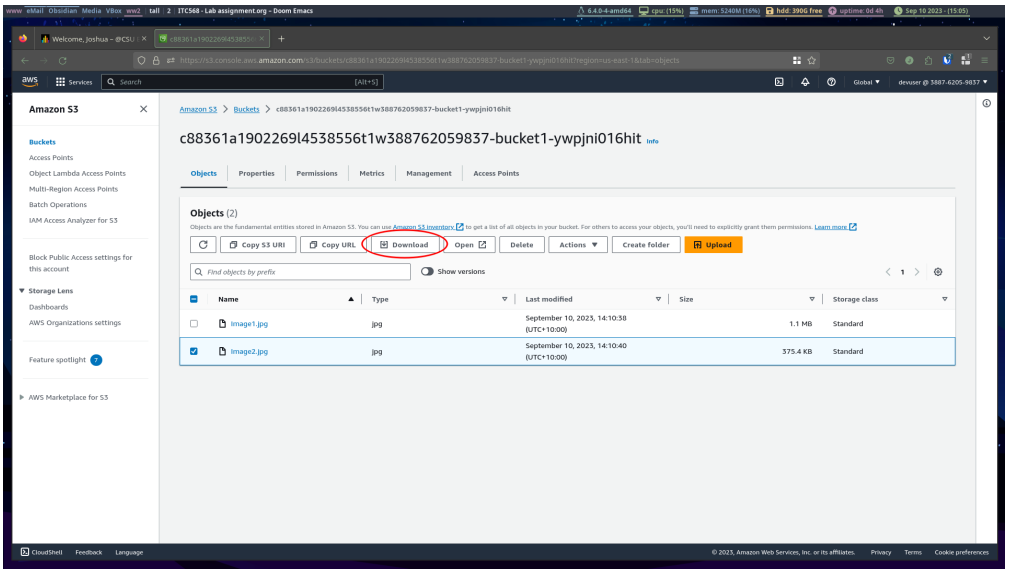
We see in the DeveloperGroupPolicy that there are only the folloring actions are available.

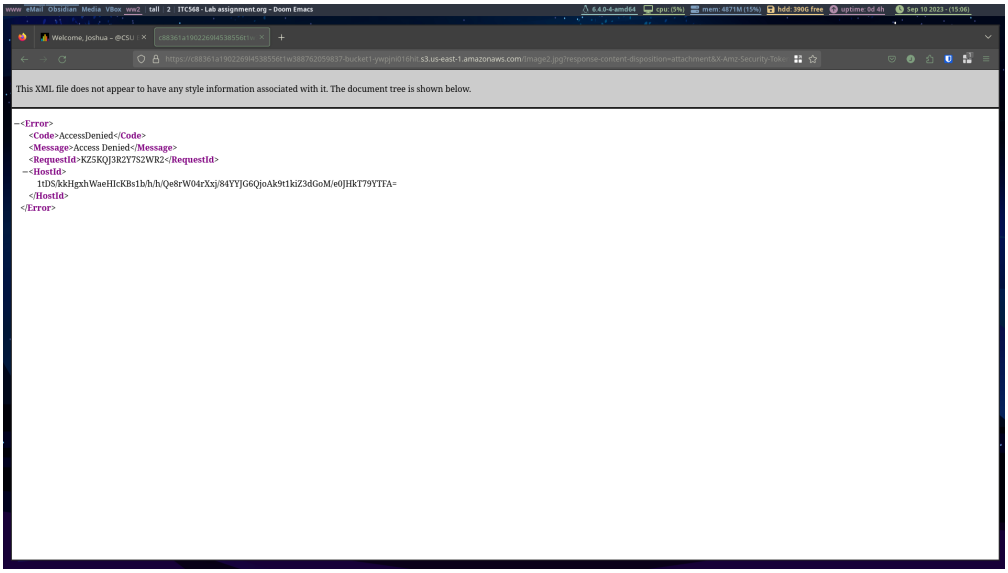
```
"s3:CreateBucket",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:PutAccountPublicAccessBlock",
"s3:PutBucketOwnershipControls",
"s3:PutBucketPublicAccessBlock"
```

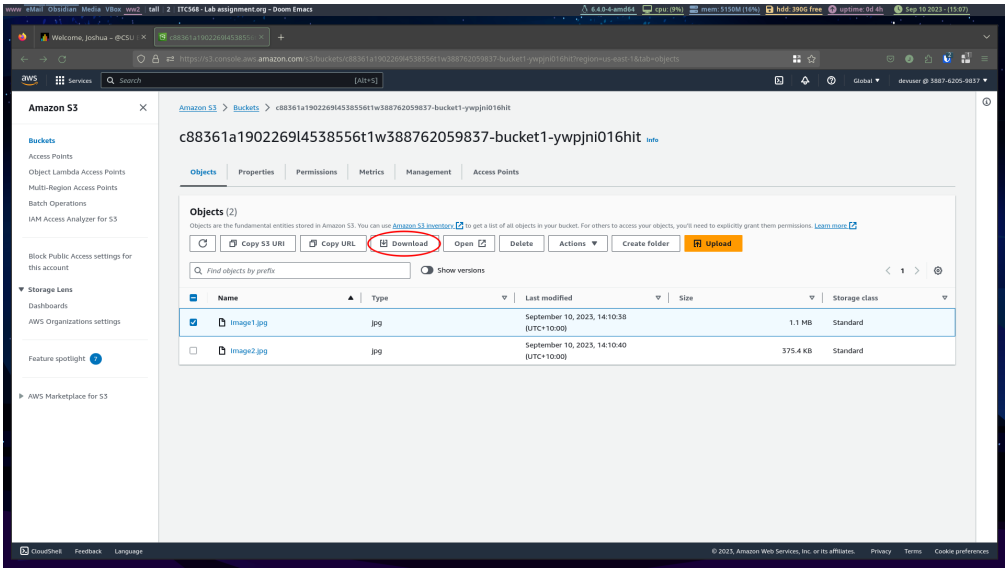
Here, there isn't statements for uploading files

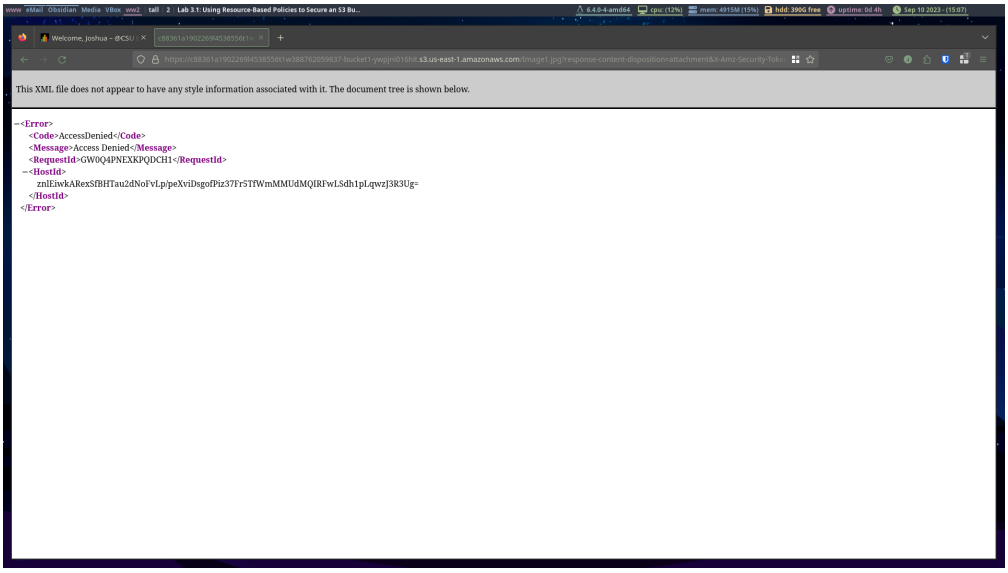
1.5 Task 5: Assuming an IAM role and reviewing a resource-based policy

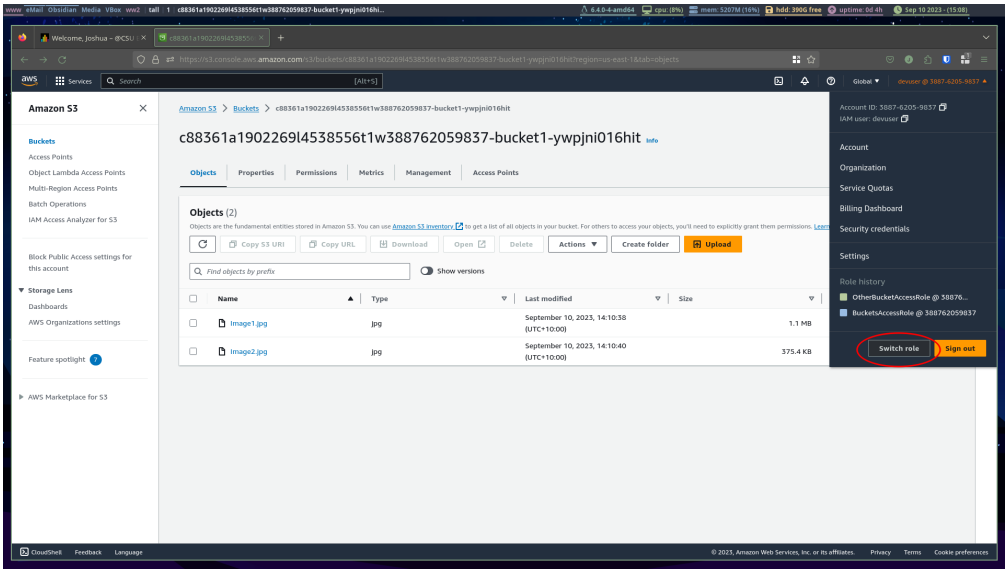


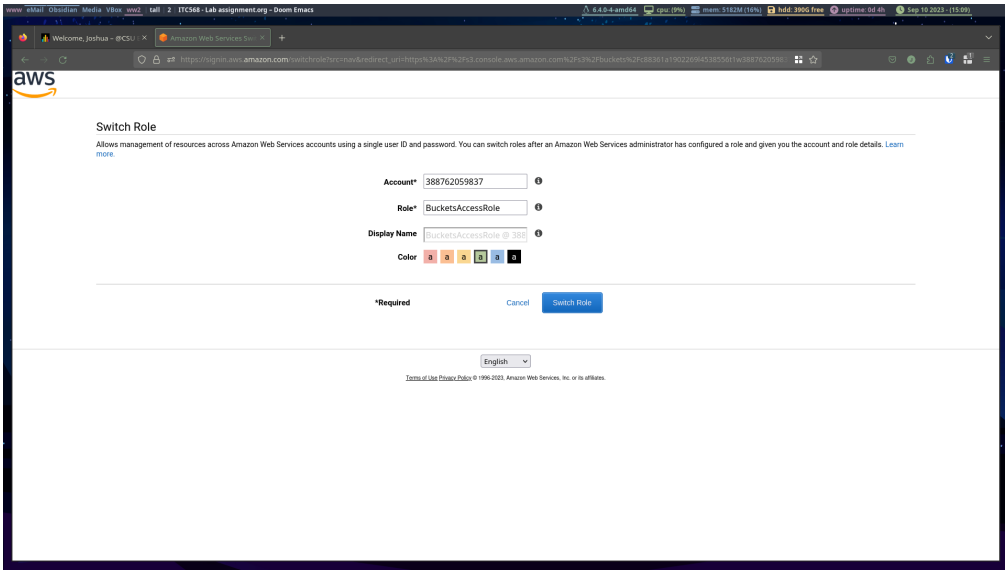


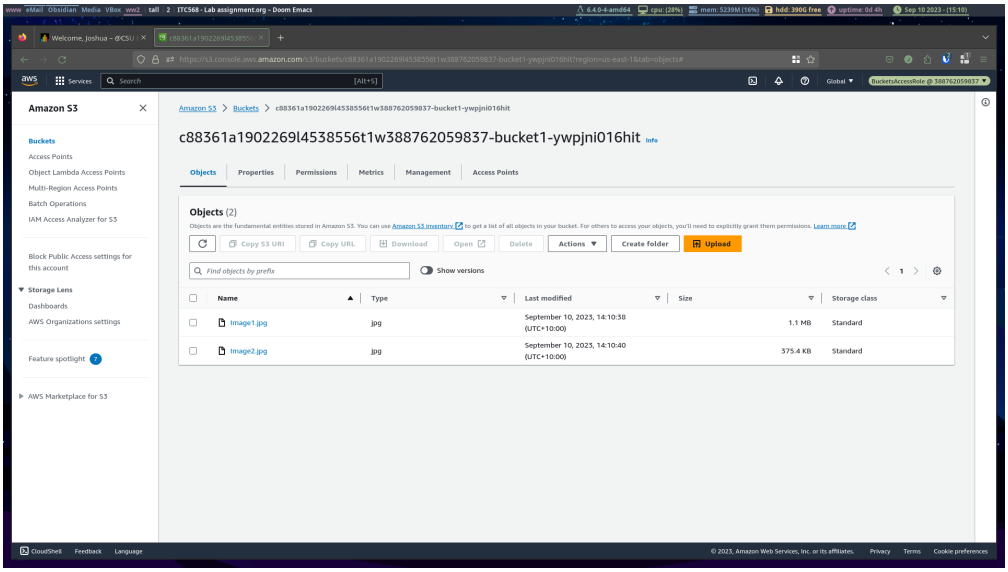

This XML file does not appear to have any style information associated with it. The document tree is shown below.
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>KZ5KQJ3R2Y7S2WR2</RequestId>
<HostId>
1tDS/kkHgxhWaeHIcKBs1b/h/h/Qe8rW04rXxj/84YYJG6QjoAk9t1kiZ3dGoM/e0JHkT79YTFA=
</HostId>
</Error>

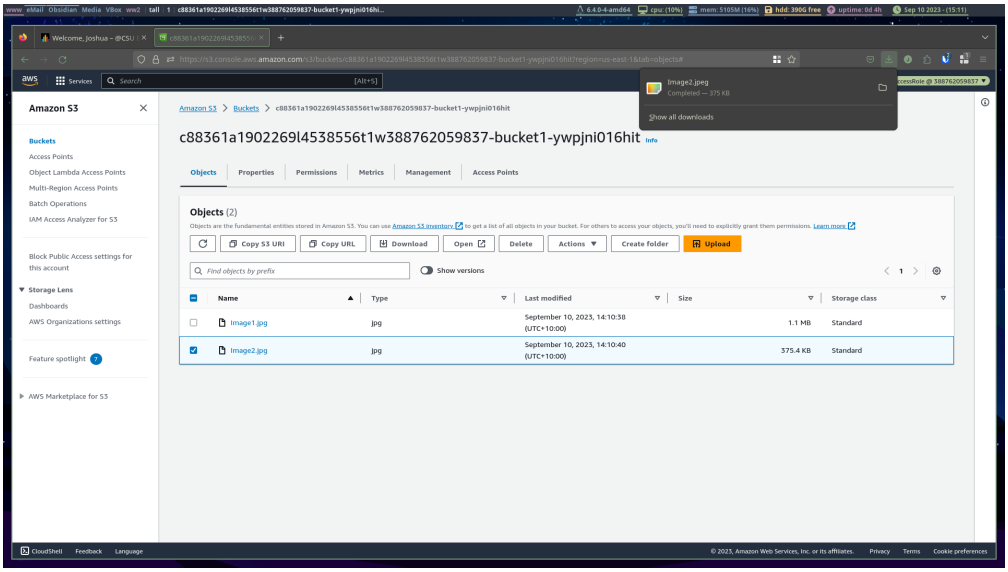

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
Image1.jpg
jpg
September 10, 2023, 14:10:38 (UTC+10:00)
1.1 MB
Standard
Image2.jpg
jpg
September 10, 2023, 14:10:40 (UTC+10:00)
375.4 KB
Standard
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences


This XML file does not appear to have any style information associated with it. The document tree is shown below.
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>GW0Q4PNEXKPQDCH1</RequestId>
<HostId>
znlEiwkARexSfBHTau2dNoFvLp/peXviDsgofPiz37FrSTfWmMMUdMQIRFwLSdh1pLqwzJ3R3Ug=
</HostId>
</Error>


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Image1.jpg
jpg
September 10, 2023, 14:10:38 (UTC+10:00)
1.1 MB
Image2.jpg
jpg
September 10, 2023, 14:10:40 (UTC+10:00)
375.4 KB
Account
Organization
Service Quotas
Billing Dashboard
Security credentials
Settings
Role history
OtherBucketAccessRole @ 38876...
BucketsAccessRole @ 388762059837
Switch role
Sign out
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Switch Role
Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. Learn more.
Account* 388762059837
Role* BucketsAccessRole
Display Name BucketsAccessRole @ 388
Color
*Required
Cancel
Switch Role
English


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
Image1.jpg
jpg
September 10, 2023, 14:10:38 (UTC+10:00)
1.1 MB
Standard
Image2.jpg
jpg
September 10, 2023, 14:10:40 (UTC+10:00)
375.4 KB
Standard
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
Image1.jpg
jpg
September 10, 2023, 14:10:38 (UTC+10:00)
1.1 MB
Standard
Image2.jpg
jpg
September 10, 2023, 14:10:40 (UTC+10:00)
375.4 KB
Standard
Image2.jpeg
Completed — 375 KB
Show all downloads
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

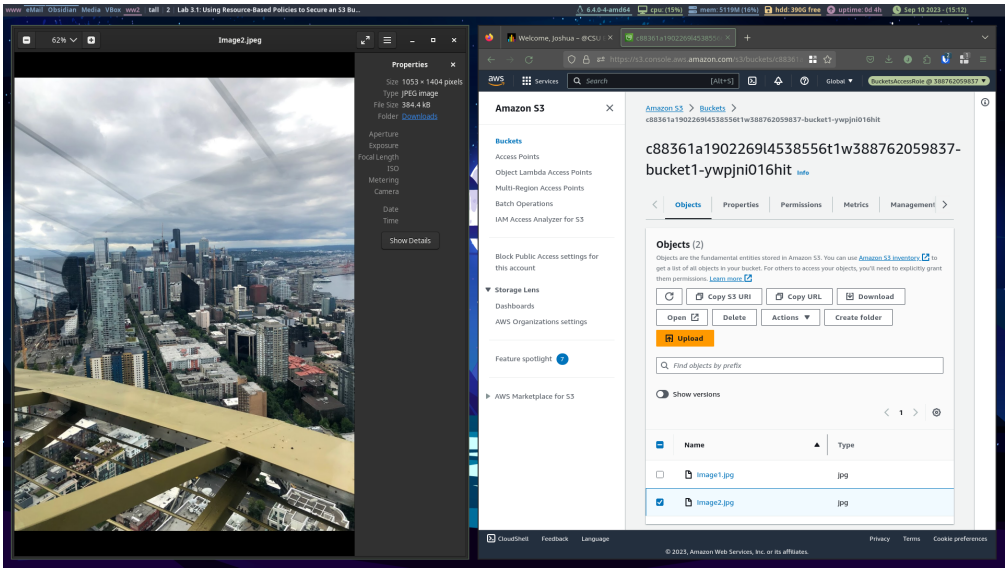
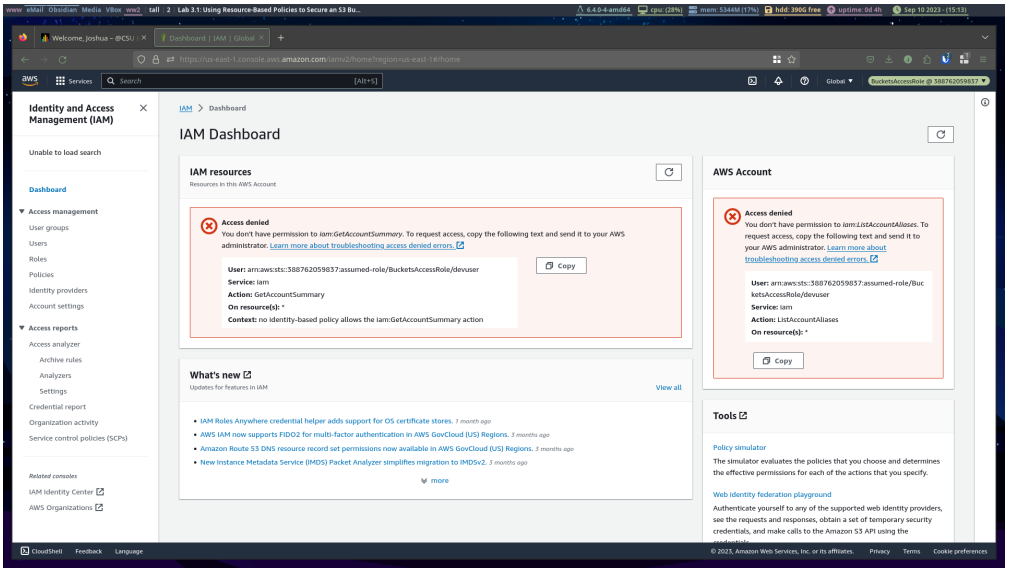
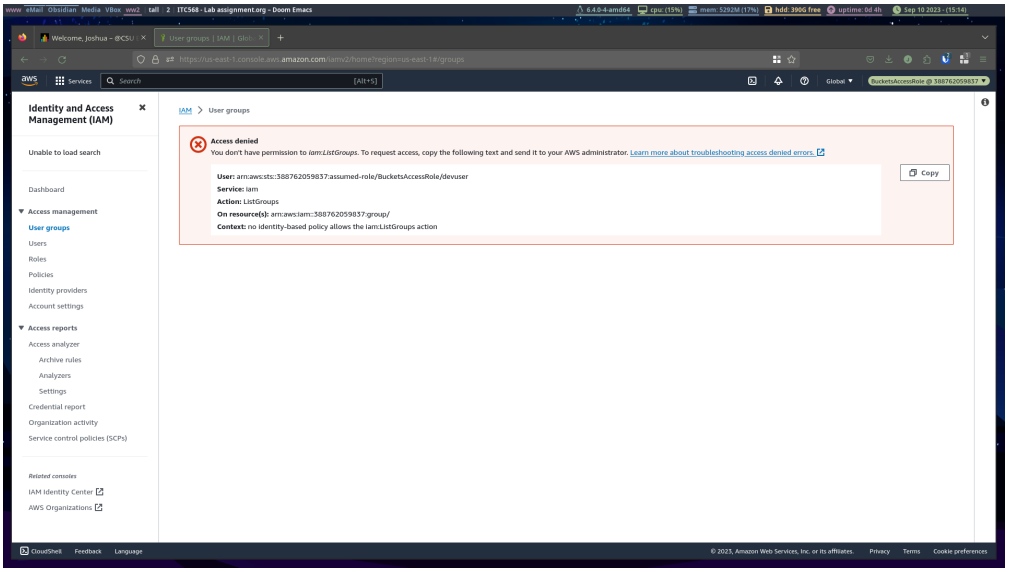
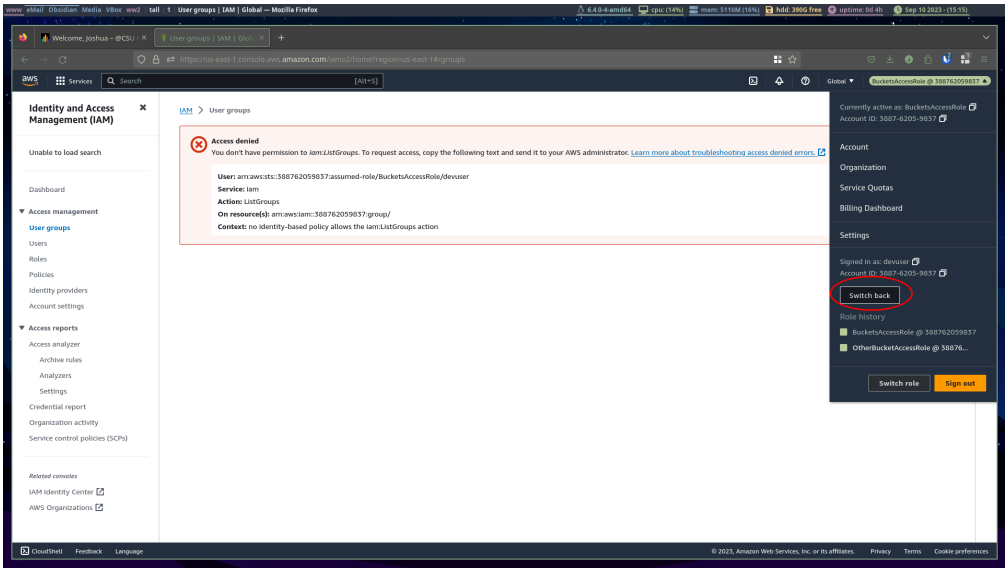
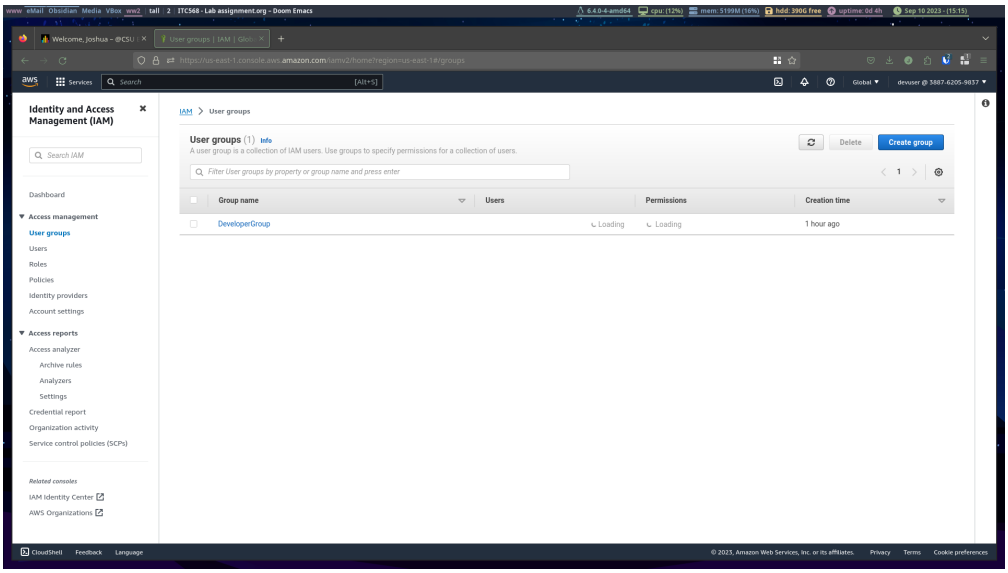


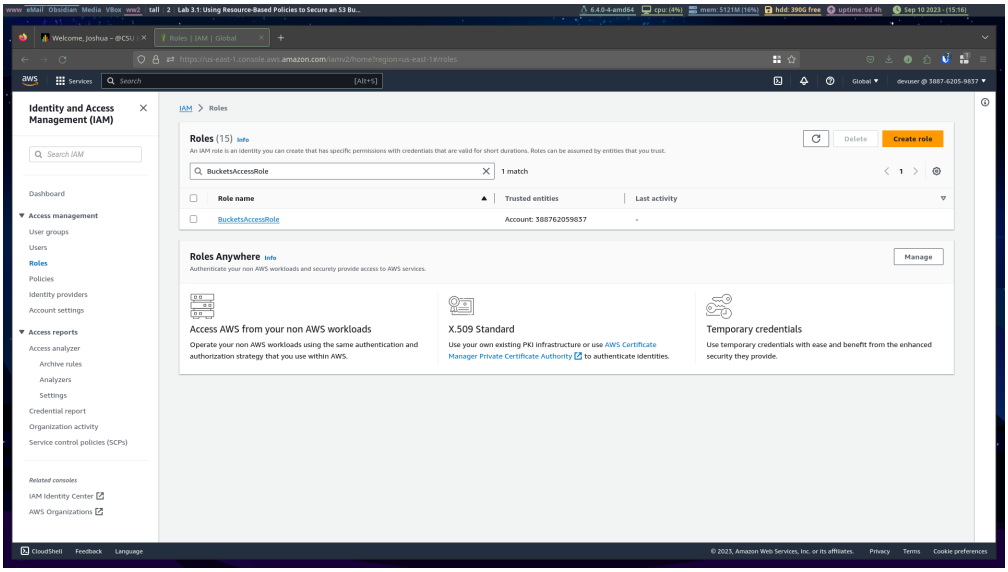
Image2.jpeg
Properties
Size 1053 × 1404 pixels
Type JPEG image
File Size 384.4 kB
Folder Downloads
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time
Show Details
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
c88361a1902269l4538556t1w388762059837-bucket1-ywpjni016hit
Objects
Properties
Permissions
Metrics
Management
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Image1.jpg
jpg
Image2.jpg
jpg
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

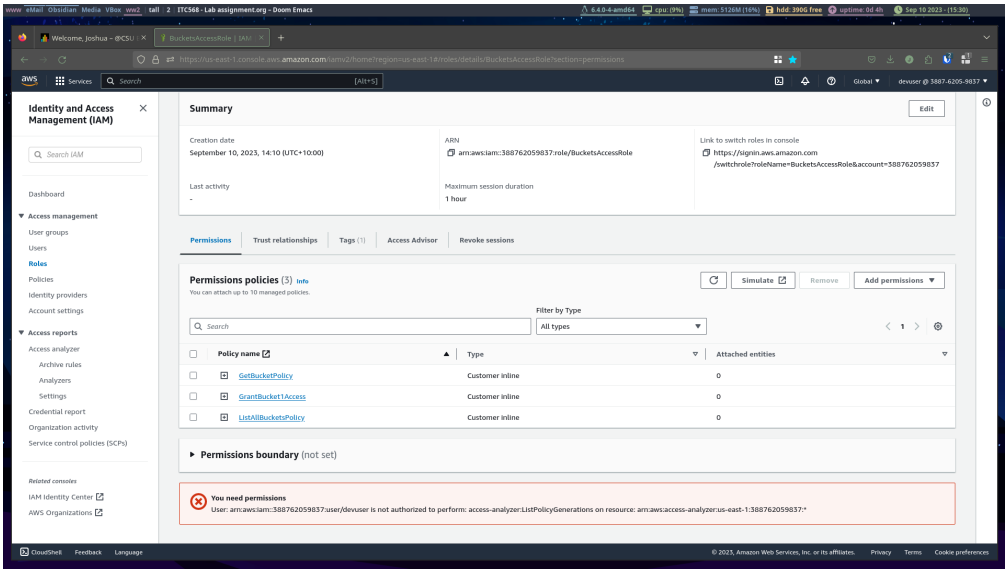

Identity and Access Management (IAM)
IAM Dashboard
IAM resources
Access denied
You don't have permission to iam:GetAccountSummary. To request access, copy the following text and send it to your AWS administrator.
Copy
AWS Account
Access denied
You don't have permission to iam:ListAccountAliases. To request access, copy the following text and send it to your AWS administrator.
What's new
Tools
Policy simulator
Web identity federation playground

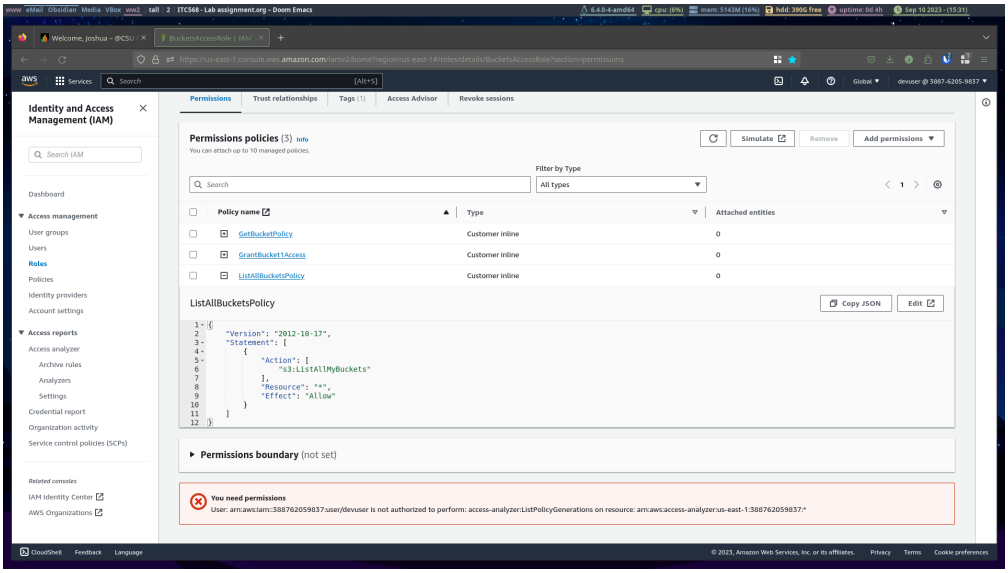

Identity and Access Management (IAM)
User groups
Access denied
You don't have permission to iam:ListGroups. To request access, copy the following text and send it to your AWS administrator.
Copy

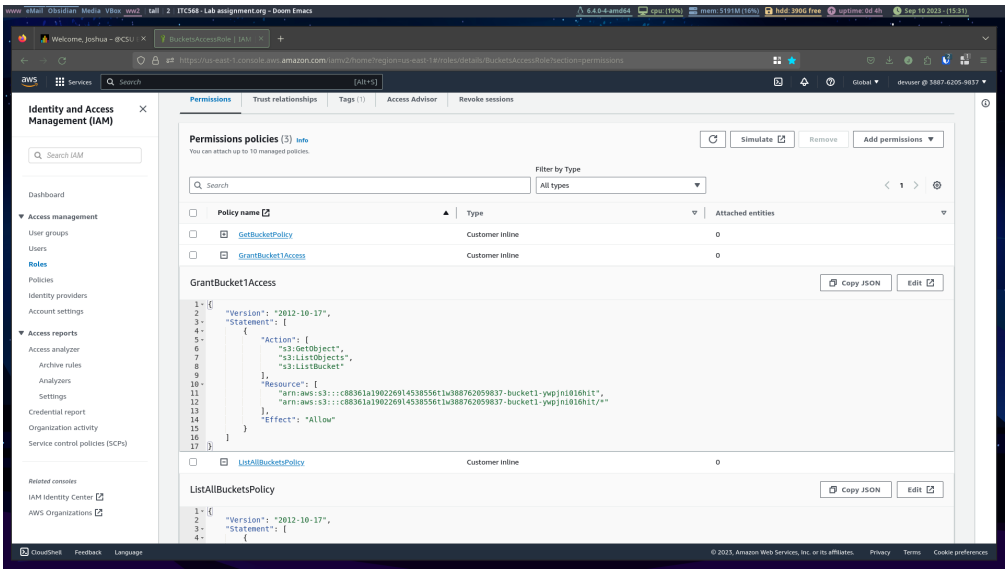

Identity and Access Management (IAM)
Access denied
You don't have permission to iam:ListGroups. To request access, copy the following text and send it to your AWS administrator.
User: arn:aws:sts::388762059837:assumed-role/BucketsAccessRole/devuser
Service: iam
Action: ListGroups
On resource(s): arn:aws:iam::388762059837:group/
Context: no identity-based policy allows the iam:ListGroups action
Switch back
Switch role
Sign out


Identity and Access Management (IAM)
User groups (1)
Delete
Create group
Group name
Users
Permissions
Creation time
DeveloperGroup
1 hour ago


Identity and Access Management (IAM)
IAM > Roles
Roles (15) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
BucketsAccessRole
1 match
Role name
Trusted entities
Last activity
BucketsAccessRole
Account: 388762059837
Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.
Manage
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.


Identity and Access Management (IAM)
Summary
Edit
Creation date
September 10, 2023, 14:10 (UTC+10:00)
ARN
arn:aws:iam::388762059837:role/BucketsAccessRole
Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=BucketsAccessRole&account=388762059837
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags (1)
Access Advisor
Revoke sessions
Permissions policies (3) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached entities
GetBucketPolicy
Customer inline
0
GrantBucket1Access
Customer inline
0
ListAllBucketsPolicy
Customer inline
0
Permissions boundary (not set)
You need permissions
User: arn:aws:iam::388762059837:user/devuser is not authorized to perform: access-analyzer:ListPolicyGenerations on resource: arn:aws:access-analyzer:us-east-1:388762059837:*

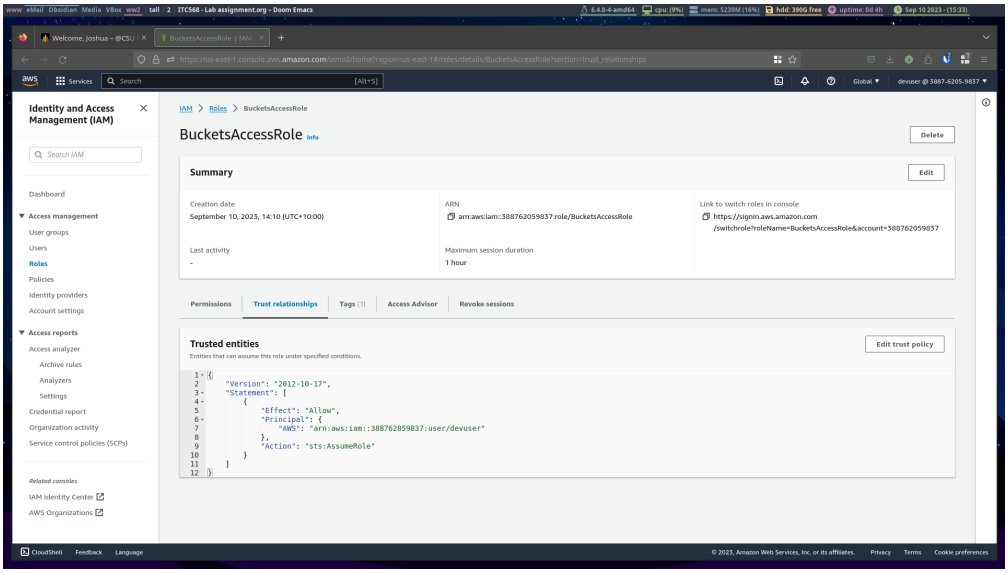


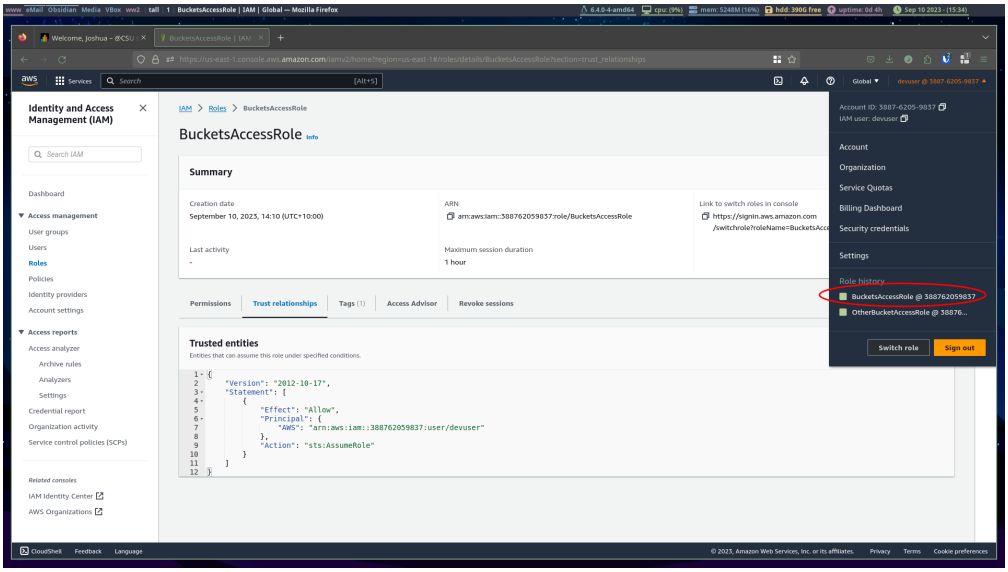


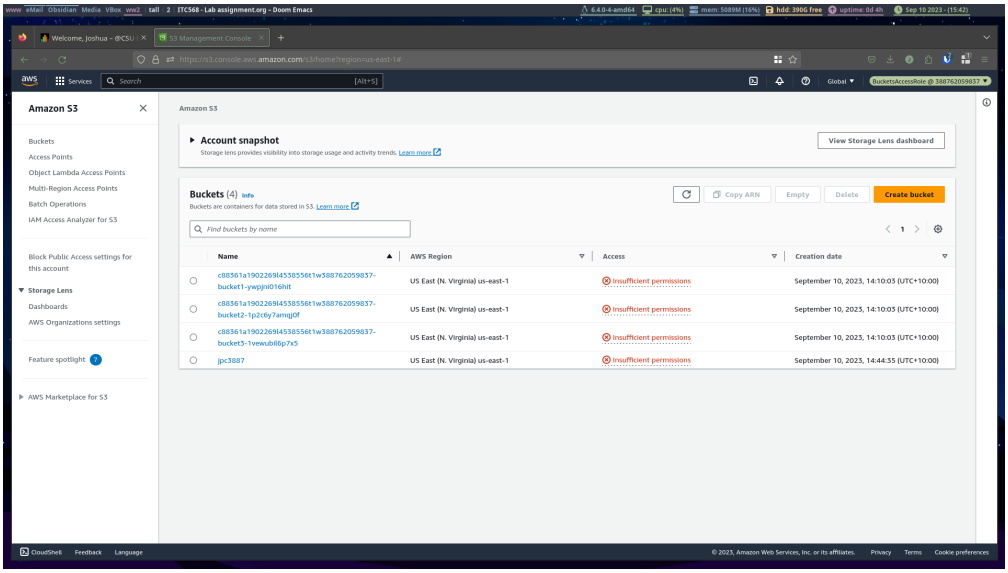
1.5.1 GrantBucket1Access.json

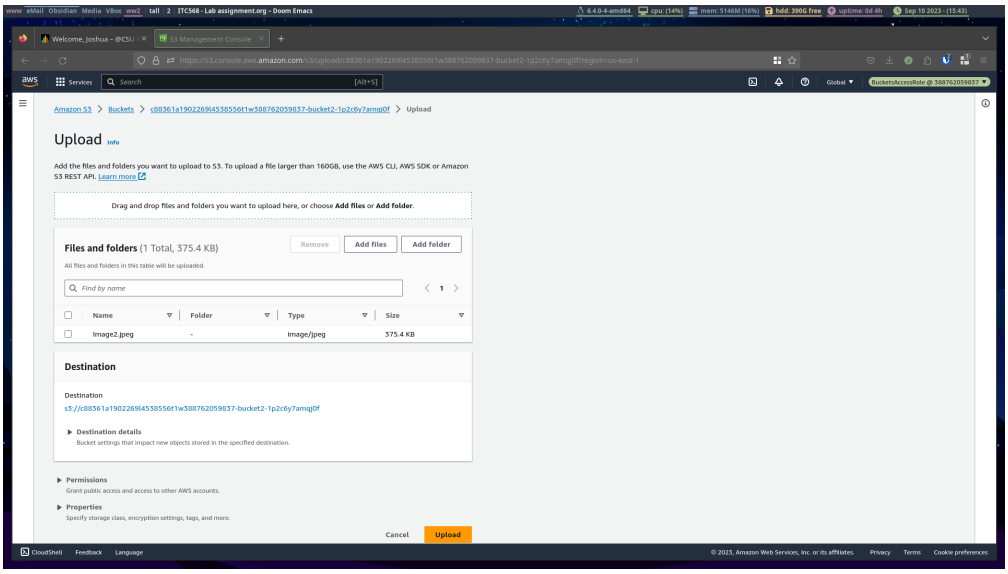
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:ListObjects",
                "s3:ListBucket"
            ],
            "Resource": [
```

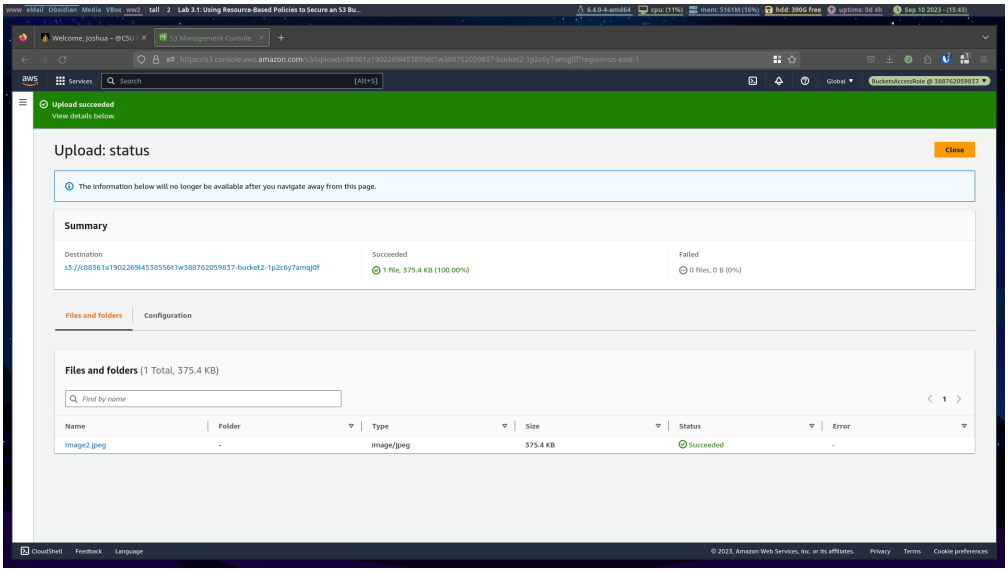
```
                "arn:aws:s3:::c88361a190226914538556t1w388762059837-bucket1-ywpjni016hit",
                "arn:aws:s3:::c88361a190226914538556t1w388762059837-bucket1-ywpjni016hit/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```



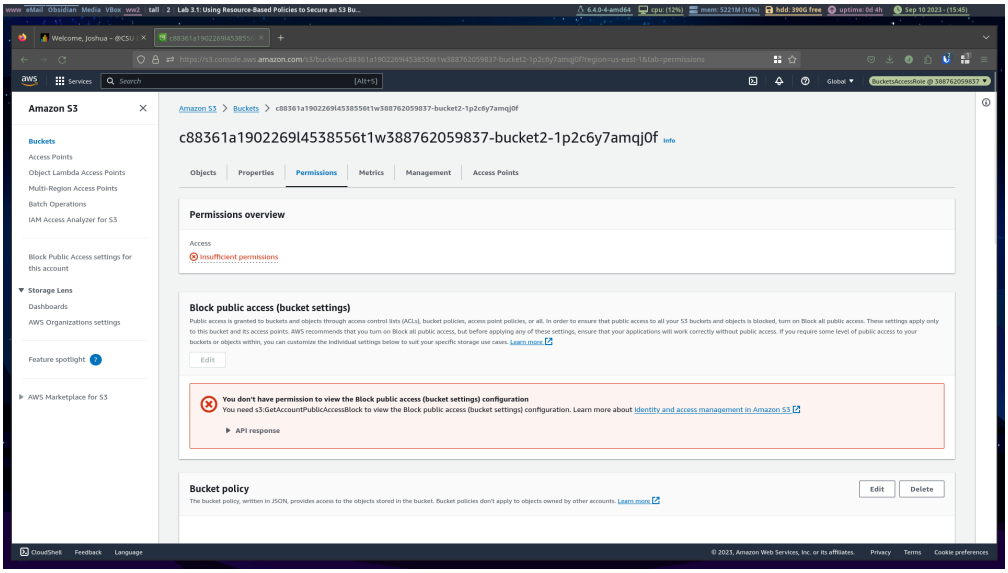


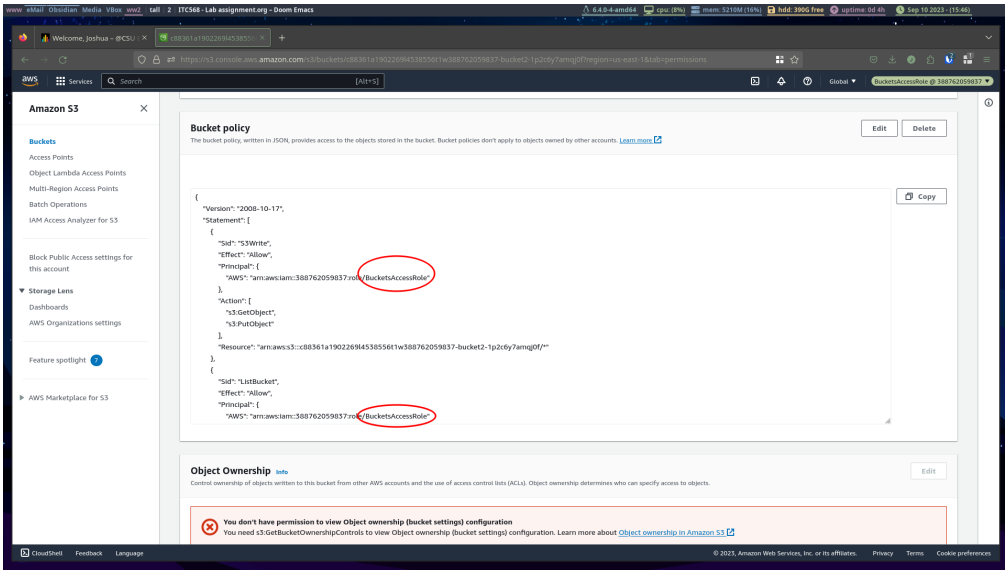

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (4) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
c88361a1902269l4538556t1w388762059837-bucket1-ywpjnl016hit
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
c88361a1902269l4538556t1w388762059837-bucket2-1p2c6y7amqj0f
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
c88361a1902269l4538556t1w388762059837-bucket3-1vewubli6p7x5
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:10:03 (UTC+10:00)
jpc3887
US East (N. Virginia) us-east-1
Insufficient permissions
September 10, 2023, 14:44:55 (UTC+10:00)
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket2-1p2c6y7amqj0f > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 375.4 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
Image2.jpeg
-
image/jpeg
375.4 KB
Destination
Destination
s3://c88361a1902269l4538556t1w388762059837-bucket2-1p2c6y7amqj0f
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

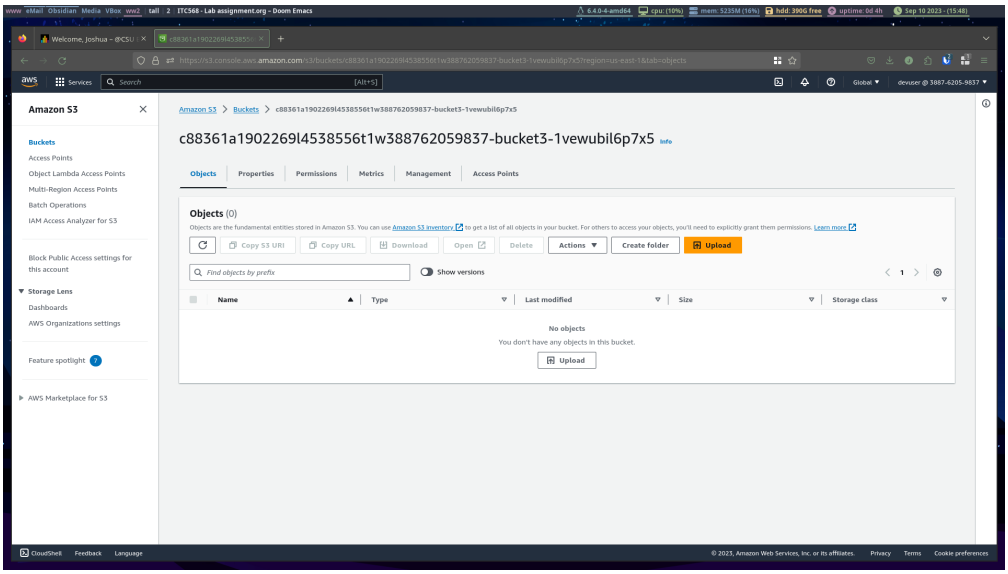


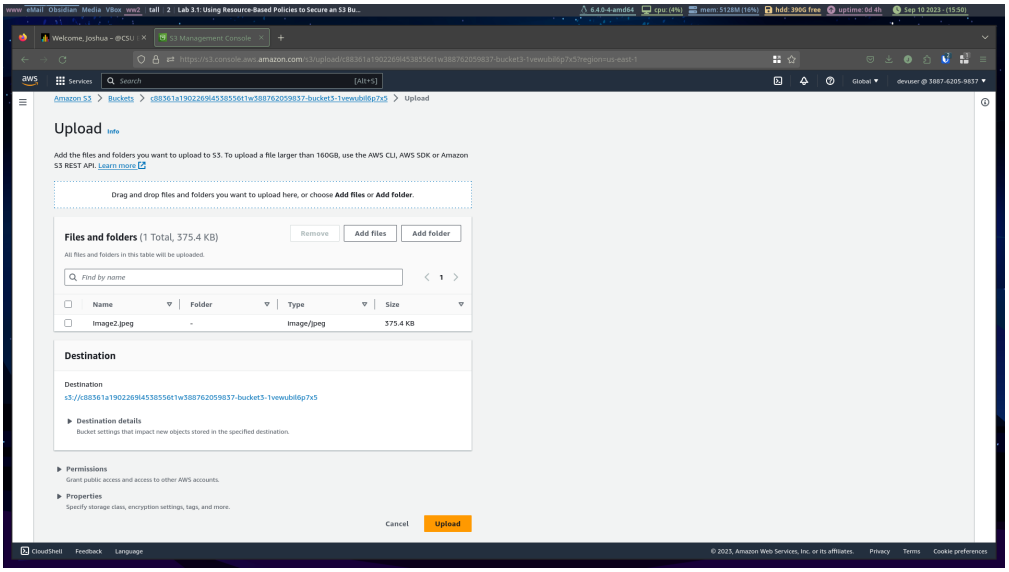
1.6 Task 6: Understanding Resource-based policies

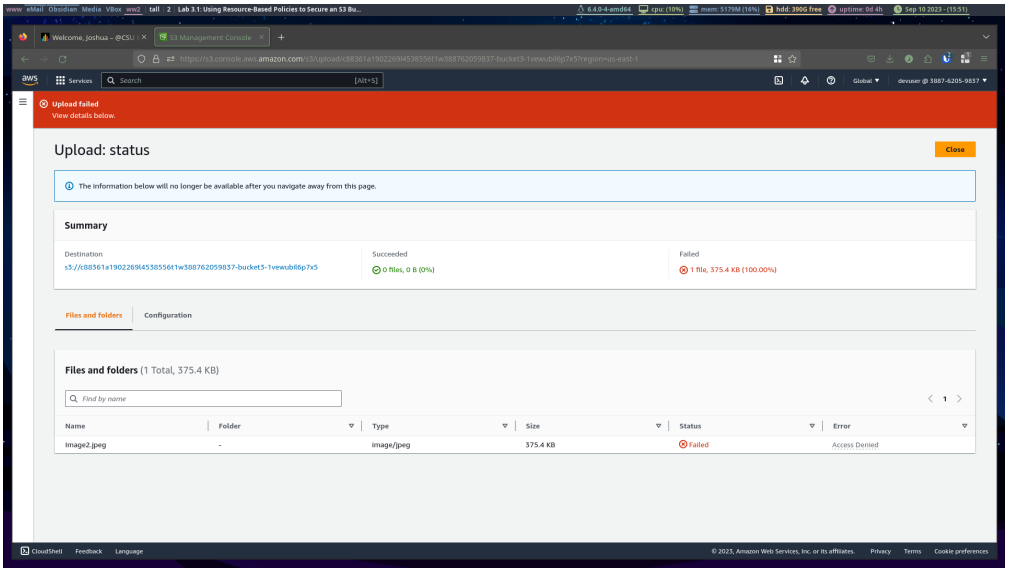


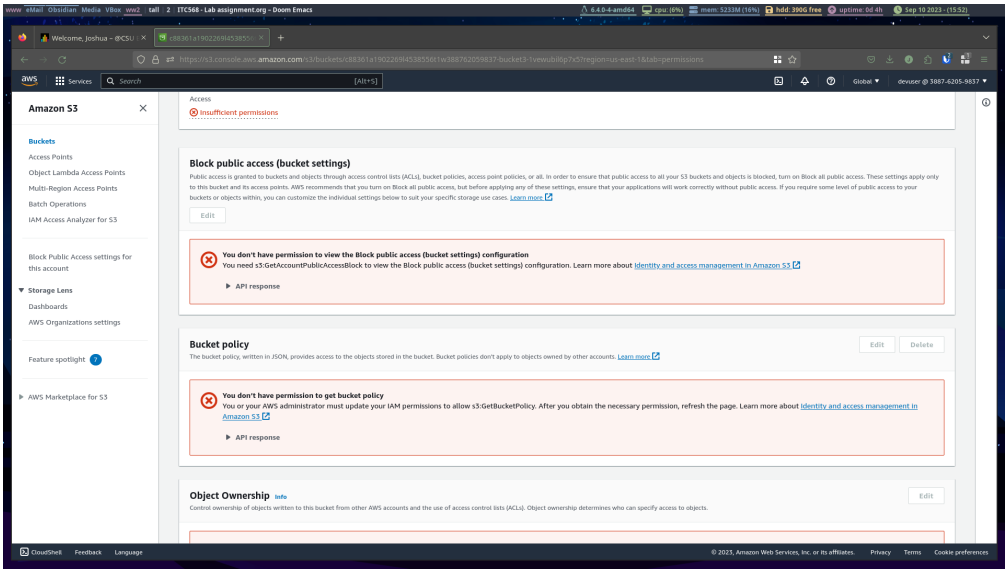


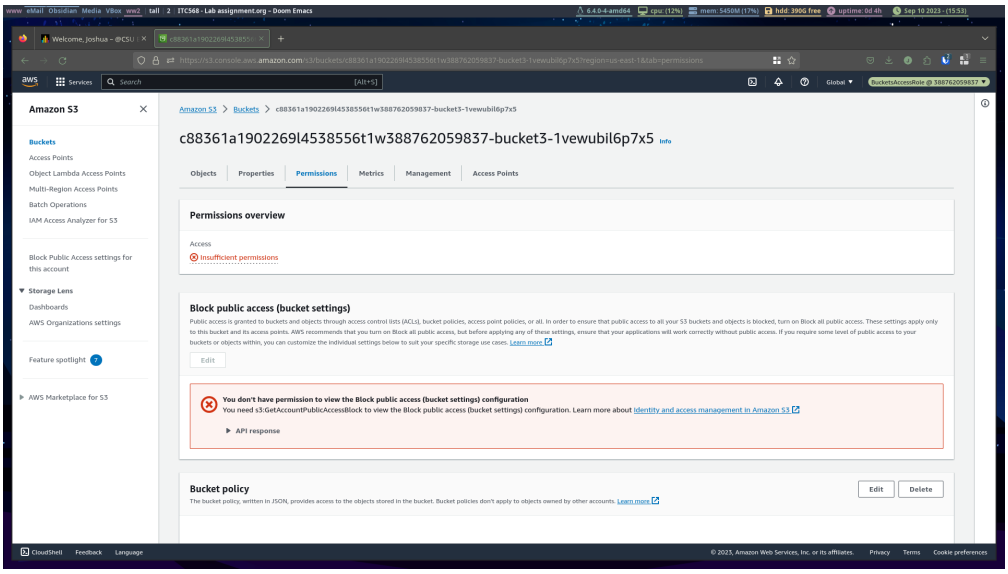
1.7 Challenge Task

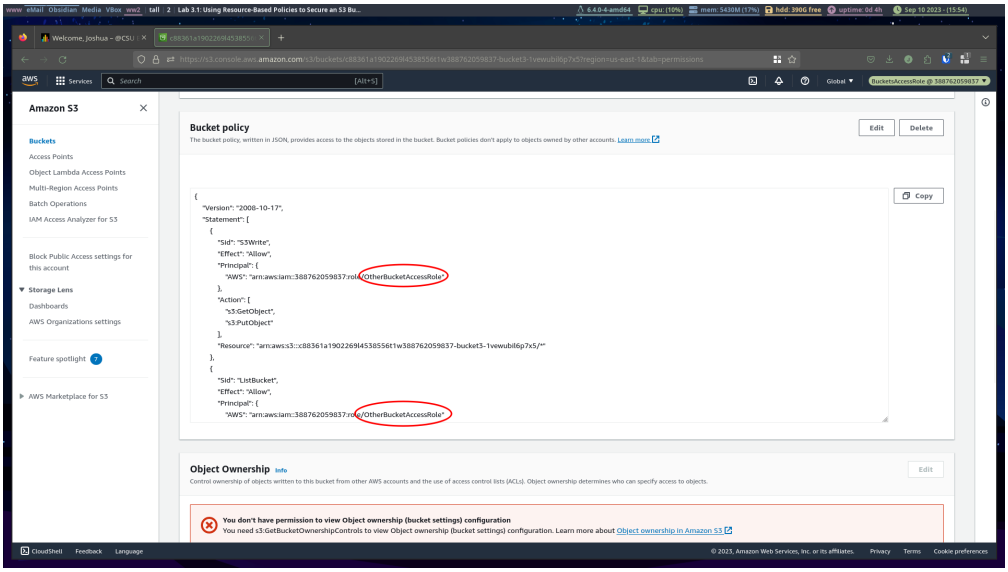



Upload
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 375.4 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
Image2.jpeg
-
image/jpeg
375.4 KB
Destination
Destination
s3://c88361a1902269l45385561w388762059837-bucket3-1vewubil6p7x5
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload

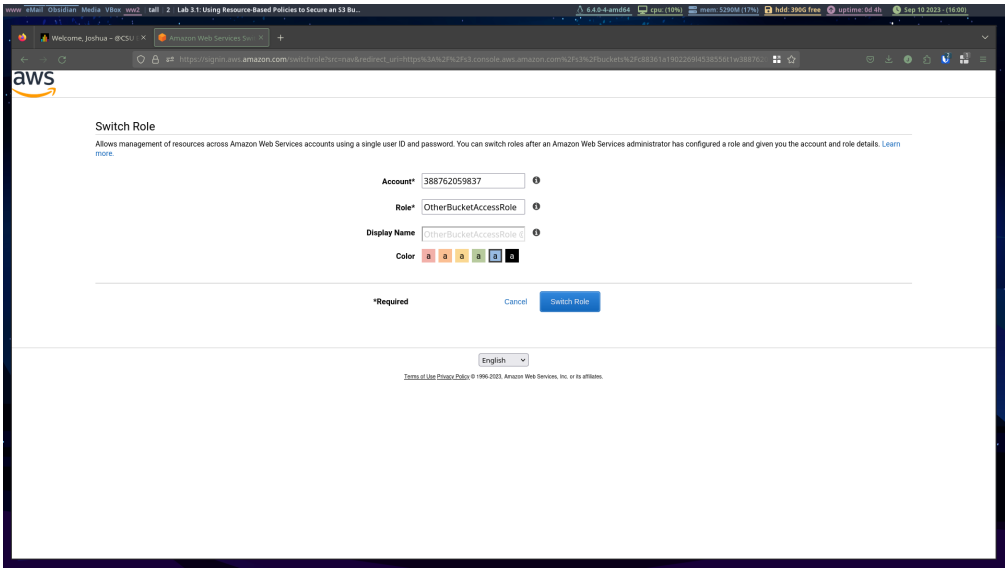

Upload failed
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://c88361a1902269l45385561w388762059837-bucket3-1vewubil6p7x5
Succeeded
0 files, 0 B (0%)
Failed
1 file, 375.4 KB (100.00%)
Files and folders
Configuration
Files and folders (1 Total, 375.4 KB)
Find by name
Name
Folder
Type
Size
Status
Error
Image2.jpeg
-
image/jpeg
375.4 KB
Failed
Access Denied

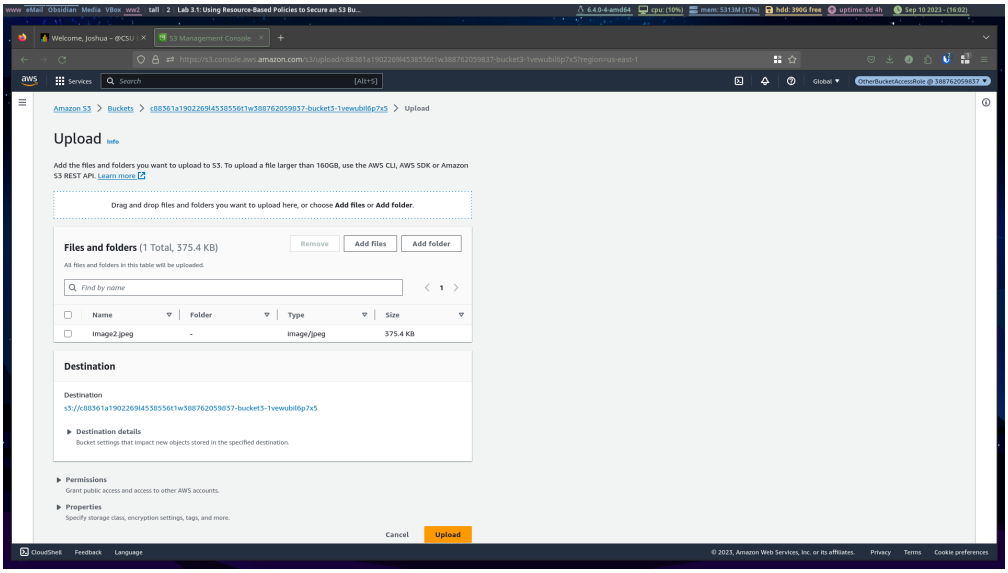

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Access
Insufficient permissions
Block public access (bucket settings)
Edit
You don't have permission to view the Block public access (bucket settings) configuration
You need s3:GetAccountPublicAccessBlock to view the Block public access (bucket settings) configuration. Learn more about Identity and access management in Amazon S3
API response
Bucket policy
Edit
Delete
You don't have permission to get bucket policy
You or your AWS administrator must update your IAM permissions to allow s3:GetBucketPolicy. After you obtain the necessary permission, refresh the page. Learn more about Identity and access management in Amazon S3
API response
Object Ownership
Edit
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences

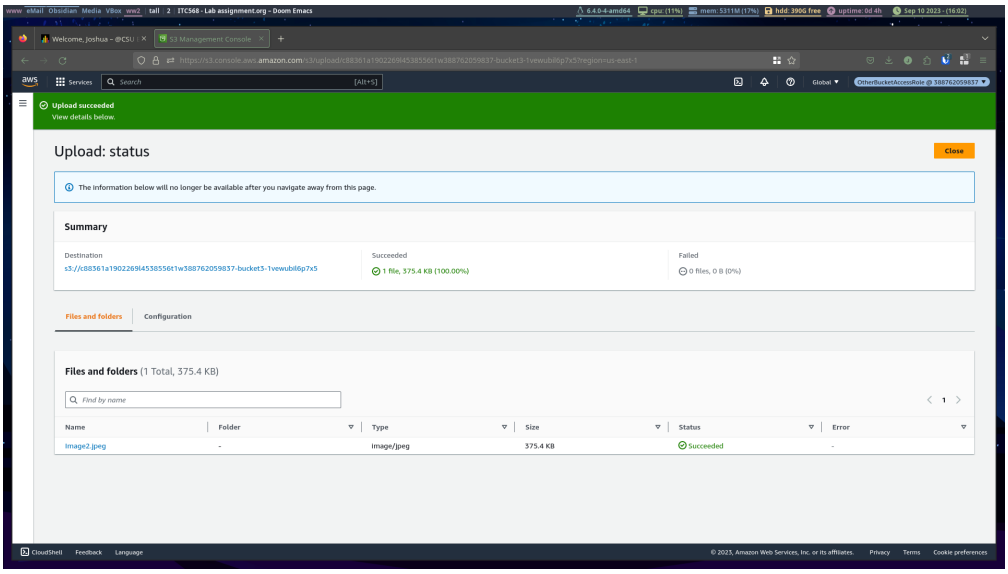

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902269l4538556t1w388762059837-bucket3-1vewubil6p7x5
c88361a1902269l4538556t1w388762059837-bucket3-1vewubil6p7x5
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Insufficient permissions
Block public access (bucket settings)
Edit
You don't have permission to view the Block public access (bucket settings) configuration
You need s3:GetAccountPublicAccessBlock to view the Block public access (bucket settings) configuration. Learn more about Identity and access management in Amazon S3
API response
Bucket policy
Edit
Delete
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences



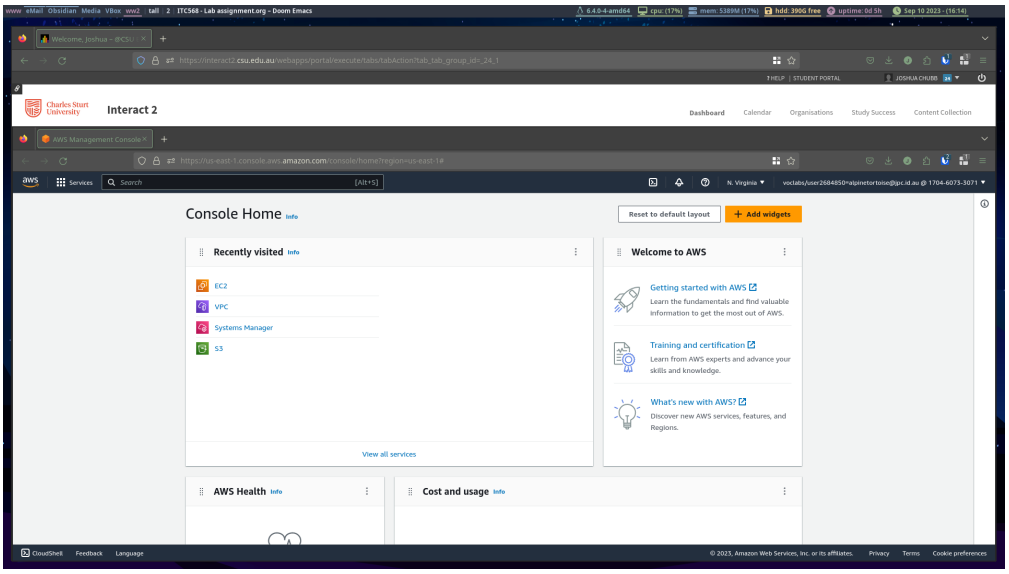
By adopting the OtherBucketAccessRole we should be able to upload.



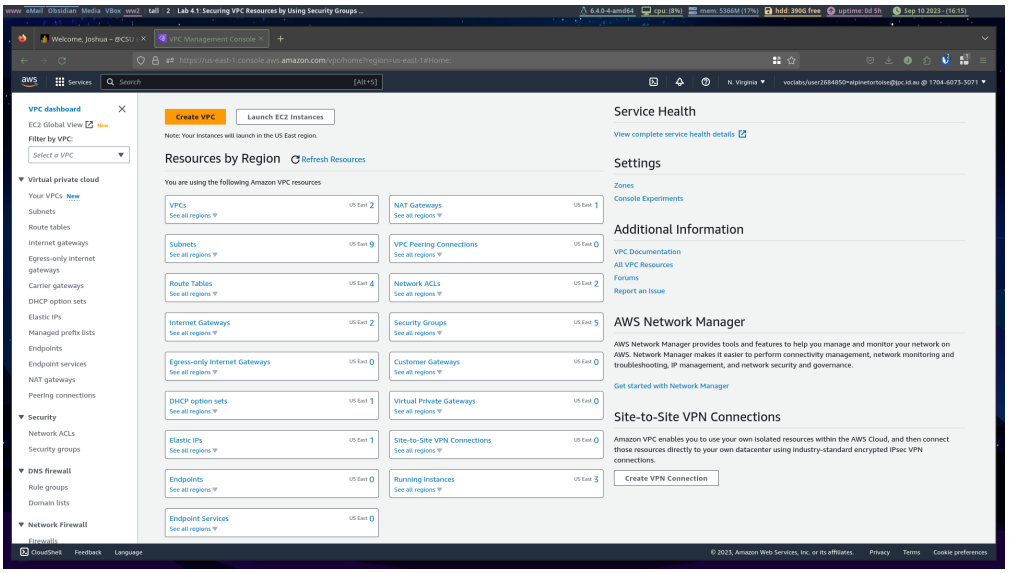

Amazon S3 > Buckets > c88361a1902269l45385561w388762059837-bucket3-1vewubil6p7x5 > Upload
Upload
Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 375.4 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
Image2.jpeg
-
image/jpeg
375.4 KB
Destination
Destination
s3://c88361a1902269l4538556t1w388762059837-bucket3-1vewubil6p7x5
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload

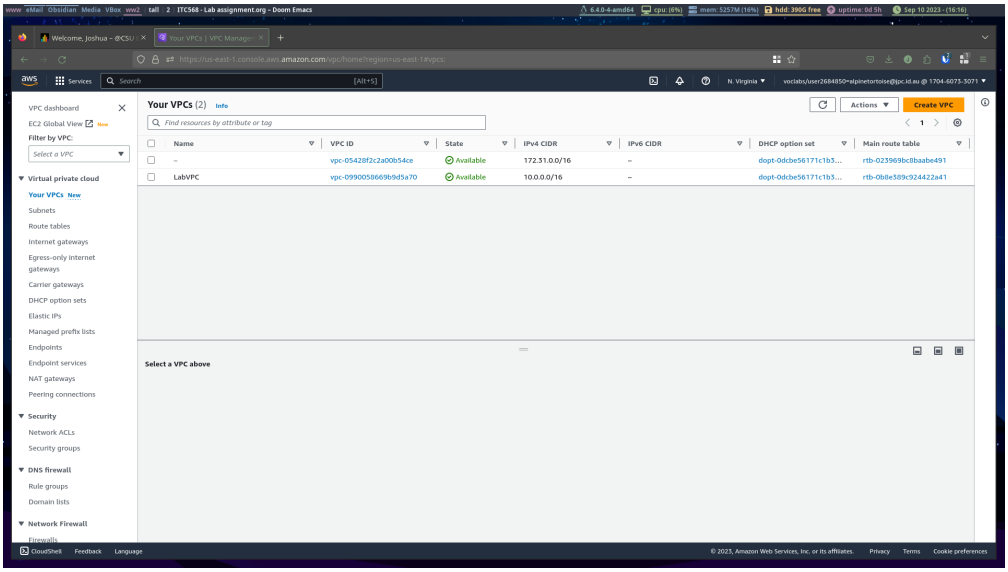

Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://c88361a1902269l4538556t1w388762059837-bucket3-1vewubil6p7x5
Succeeded
1 file, 375.4 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 375.4 KB)
Find by name
Name
Folder
Type
Size
Status
Error
Image2.jpeg
-
image/jpeg
375.4 KB
Succeeded
-

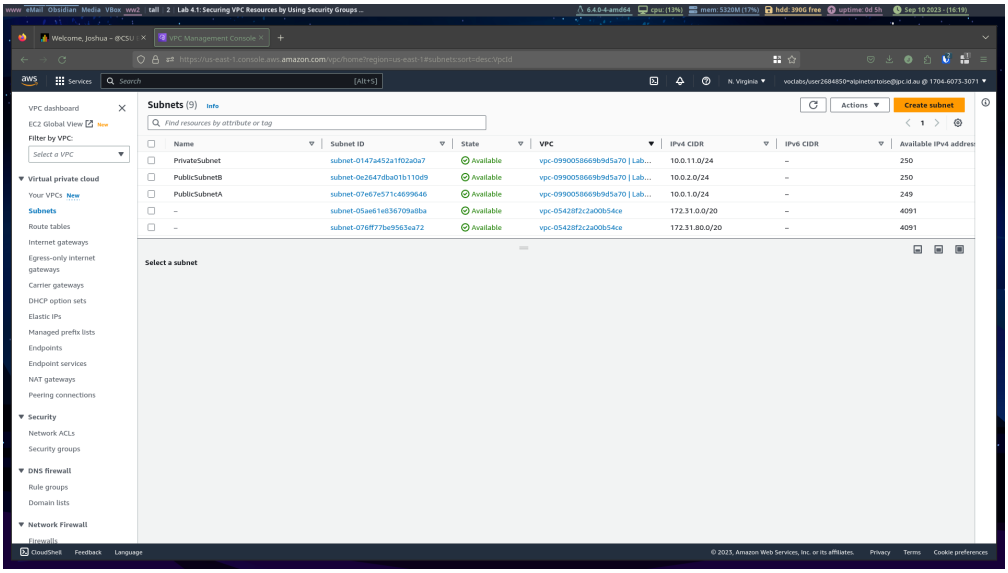
2 Lab 4.1: Securing VPC Resources by Using Security Groups

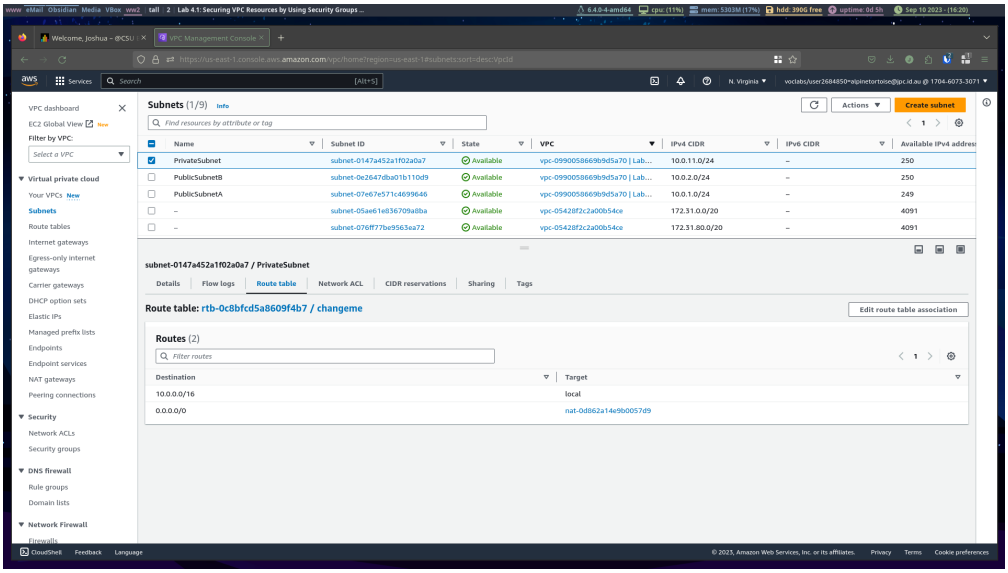


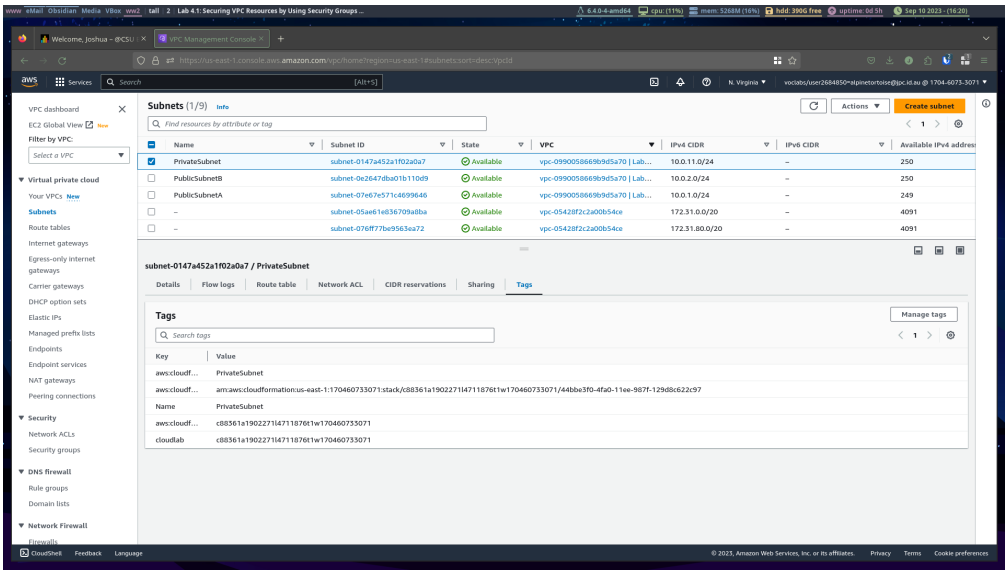
2.1 Task 1: Analyzing the VPC and private subnet resource settings

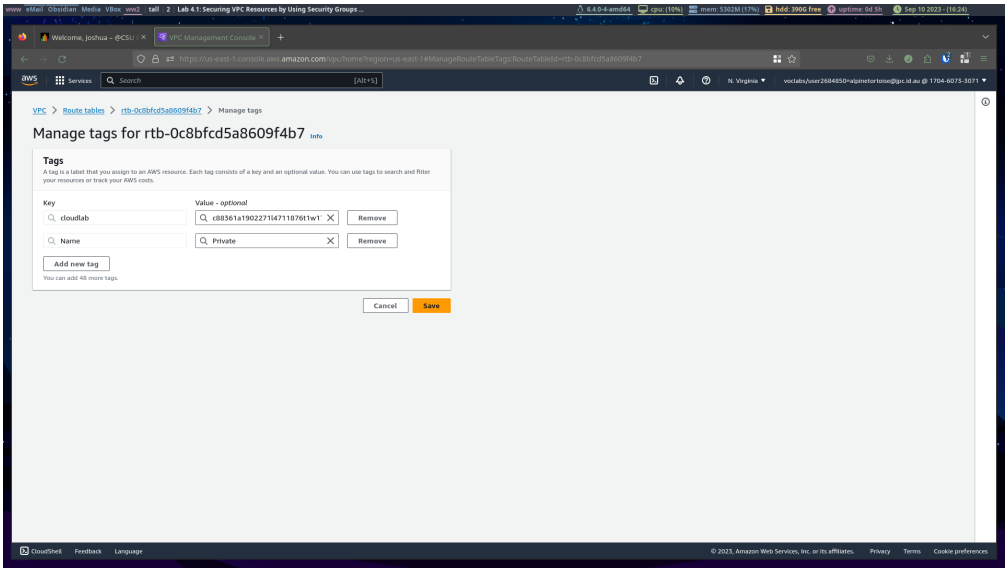


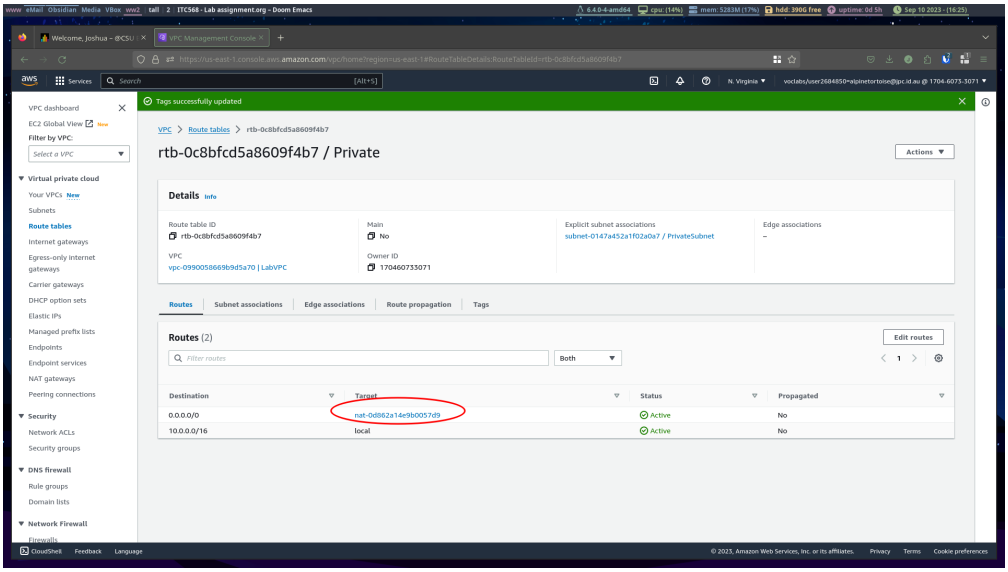

Your VPCs (2) Info
Actions
Create VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
Main route table
vpc-05428f2c2a00b54ce
Available
172.31.0.0/16
dopt-0dcbe56171c1b3...
rtb-023969bc8baabe491
LabVPC
vpc-0990058669b9d5a70
Available
10.0.0.0/16
dopt-0dcbe56171c1b3...
rtb-0b8e389c924422a41
Select a VPC above

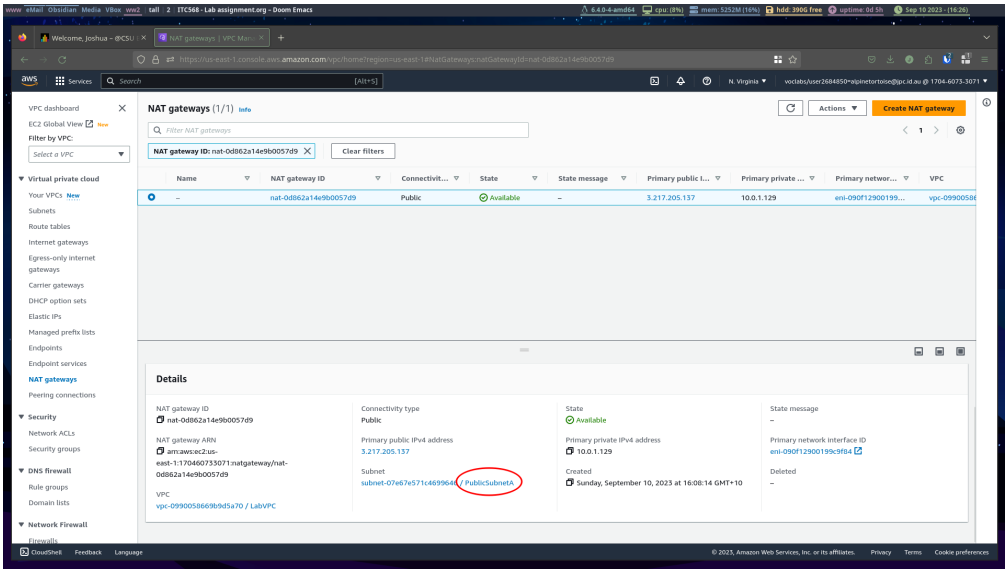

Subnets (9) Info
Actions
Create subnet
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
PrivateSubnet
subnet-0147a452a1f02a0a7
Available
vpc-0990058669b9d5a70 | Lab...
10.0.11.0/24
250
PublicSubnetB
subnet-0e2647dba01b110d9
Available
vpc-0990058669b9d5a70 | Lab...
10.0.2.0/24
250
PublicSubnetA
subnet-07e67e571c4699646
Available
vpc-0990058669b9d5a70 | Lab...
10.0.1.0/24
249
subnet-05ae61e836709a8ba
Available
vpc-05428f2c2a00b54ce
172.31.0.0/20
4091
subnet-076ff77be9563ea72
Available
vpc-05428f2c2a00b54ce
172.31.80.0/20
4091
Select a subnet

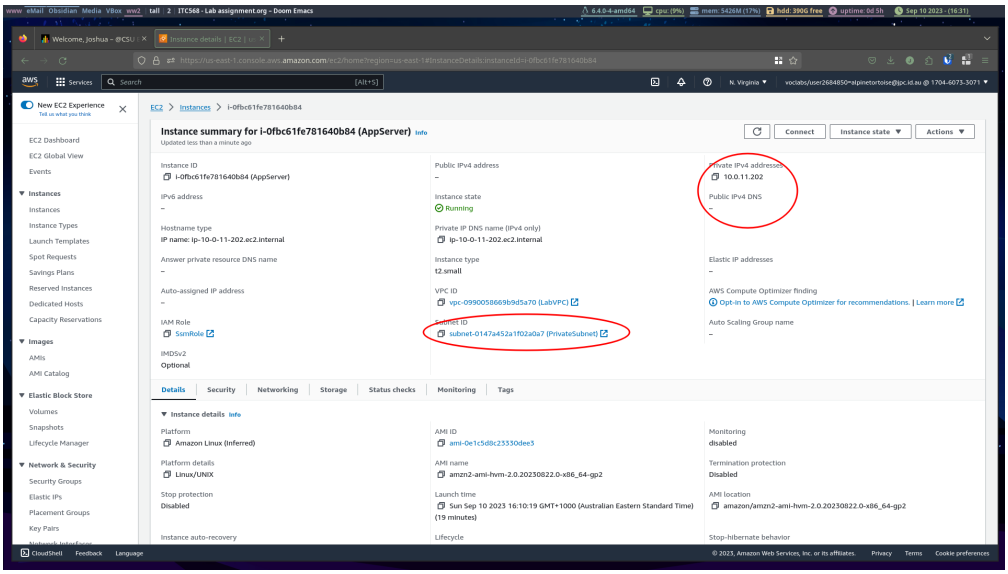

Subnets (1/9) Info
Create subnet
Actions
PrivateSubnet subnet-0147a452a1f02a0a7 Available 10.0.11.0/24
PublicSubnetB subnet-0e2647dba01b110d9 Available 10.0.2.0/24
PublicSubnetA subnet-07e67e571c4699646 Available 10.0.1.0/24
subnet-05ae61e836709a8ba Available 172.31.0.0/20
subnet-076ff77be9563ea72 Available 172.31.80.0/20
subnet-0147a452a1f02a0a7 / PrivateSubnet
Details Flow logs Route table Network ACL CIDR reservations Sharing Tags
Route table: rtb-0c8bfcd5a8609f4b7 / changeme
Edit route table association
Routes (2)
Destination Target
10.0.0.0/16 local
0.0.0.0/0 nat-0d862a14e9b0057d9

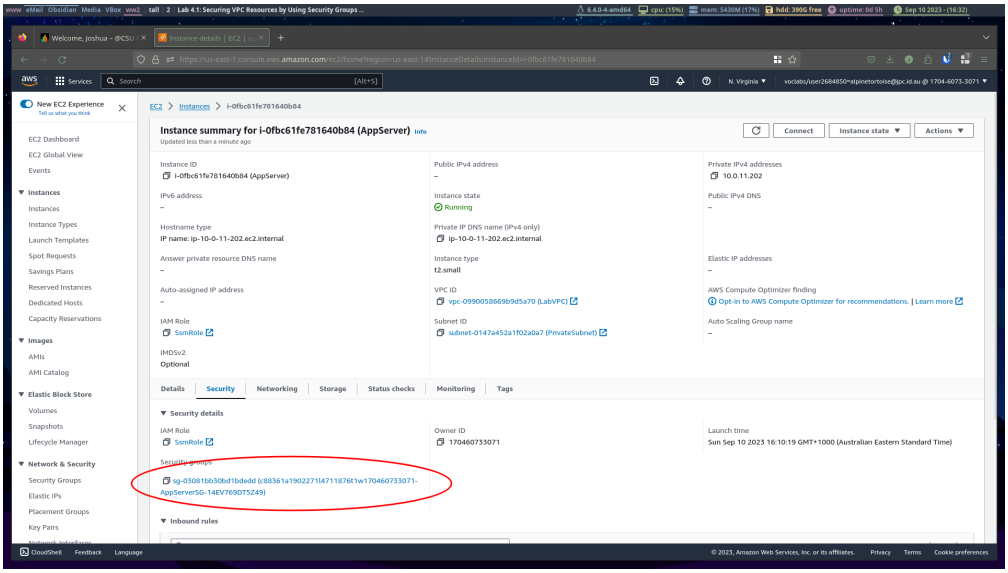

Subnets (1/9) Info
Create subnet
Actions
PrivateSubnet subnet-0147a452a1f02a0a7 Available 10.0.11.0/24
PublicSubnetB subnet-0e2647dba01b110d9 Available 10.0.2.0/24
PublicSubnetA subnet-07e67e571c4699646 Available 10.0.1.0/24
subnet-05ae61e836709a8ba Available 172.31.0.0/20
subnet-076ff77be9563ea72 Available 172.31.80.0/20
subnet-0147a452a1f02a0a7 / PrivateSubnet
Details Flow logs Route table Network ACL CIDR reservations Sharing Tags
Tags
Manage tags
Key Value
aws:cloudf... PrivateSubnet
aws:cloudf... arn:aws:cloudformation:us-east-1:170460733071:stack/c88361a1902271l4711876t1w170460733071/44bbe3f0-4fa0-11ee-987f-129d8c622c97
Name PrivateSubnet
aws:cloudf... c88361a1902271l4711876t1w170460733071
cloudlab c88361a1902271l4711876t1w170460733071

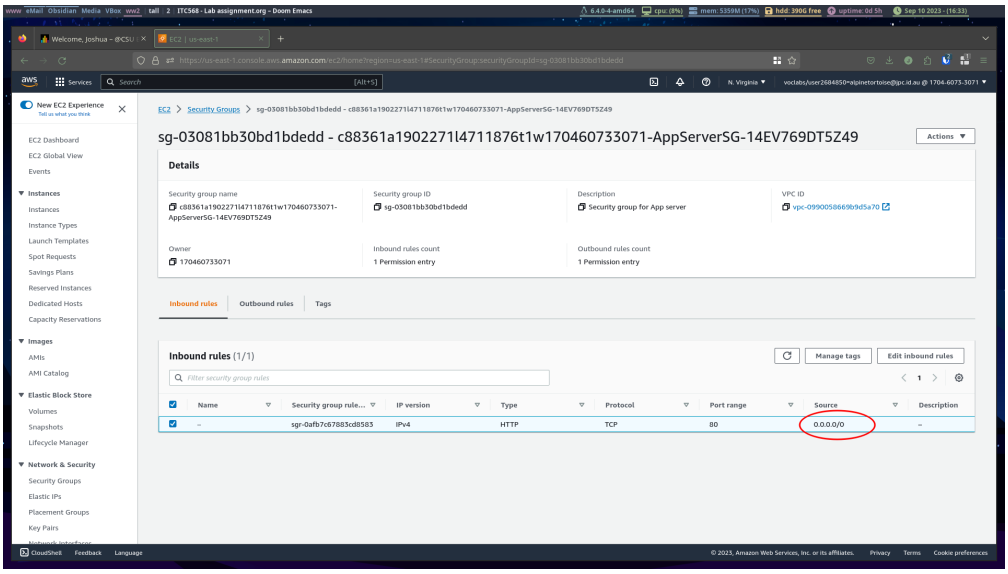

Manage tags for rtb-0c8bfcd5a8609f4b7
Tags
Key
Value - optional
cloudlab
c88361a1902271147118761w1
Remove
Name
Private
Remove
Add new tag
You can add 48 more tags.
Cancel
Save

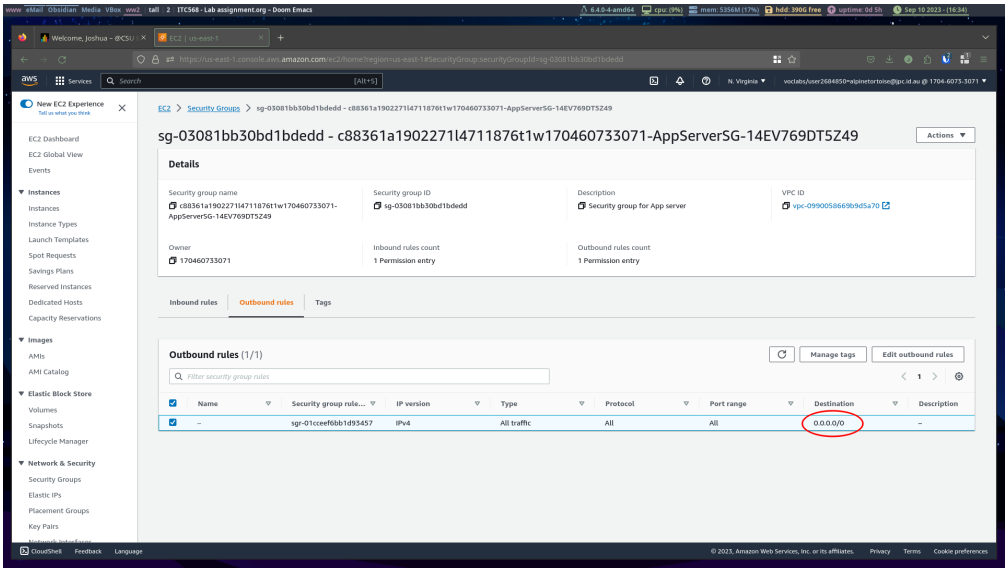

Tags successfully updated
rtb-0c8bfcd5a8609f4b7 / Private
Actions
Details
Route table ID
rtb-0c8bfcd5a8609f4b7
Main
No
Explicit subnet associations
subnet-0147a452a1f02a0a7 / PrivateSubnet
Edge associations
VPC
vpc-0990058669b9d5a70 | LabVPC
Owner ID
170460733071
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Edit routes
Destination
Target
Status
Propagated
0.0.0.0/0
nat-0d862a14e9b0057d9
Active
No
10.0.0.0/16
local
Active
No


NAT gateways (1/1)
Actions
Create NAT gateway
Details
NAT gateway ID
nat-0d862a14e9b0057d9
Connectivity type
Public
State
Available
State message
Primary public IPv4 address
3.217.205.137
Primary private IPv4 address
10.0.1.129
Primary network interface ID
eni-090f12900199c9f84
Subnet
subnet-07e67e571c4699644 / PublicSubnetA
Created
Sunday, September 10, 2023 at 16:08:14 GMT+10
VPC
vpc-0990058669b9d5a70 / LabVPC
Deleted

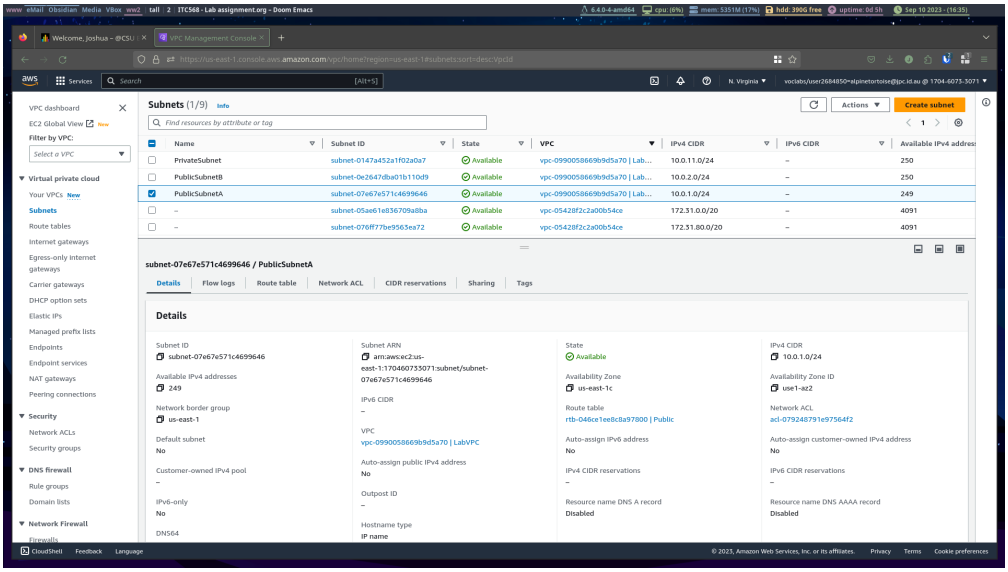

Instance summary for i-0fbc61fe781640b84 (AppServer)
Connect
Instance state
Actions
Instance ID
i-0fbc61fe781640b84 (AppServer)
Public IPv4 address
Private IPv4 addresses
10.0.11.202
IPv6 address
Instance state
Running
Public IPv4 DNS
Hostname type
IP name: ip-10-0-11-202.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-11-202.ec2.internal
Answer private resource DNS name
Instance type
t2.small
Elastic IP addresses
Auto-assigned IP address
VPC ID
vpc-0990058669b9d5a70 (LabVPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. Learn more
IAM Role
SsmRole
Subnet ID
subnet-0147a452a1f02a0a7 (PrivateSubnet)
Auto Scaling Group name
IMDSv2
Optional
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance details
Platform
Amazon Linux (Inferred)
AMI ID
ami-0e1c5d8c23330dee3
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
amzn2-ami-hvm-2.0.20230822.0-x86_64-gp2
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Sep 10 2023 16:10:19 GMT+1000 (Australian Eastern Standard Time) (19 minutes)
AMI location
amazon/amzn2-ami-hvm-2.0.20230822.0-x86_64-gp2
Instance auto-recovery
Lifecycle
Stop-hibernate behavior

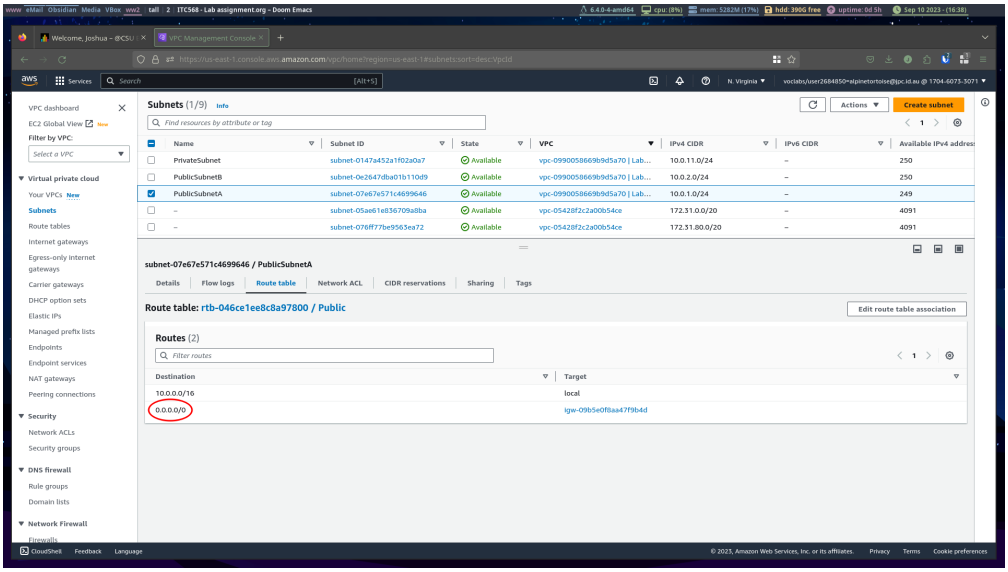

Instance summary for i-0fbc61fe781640b84 (AppServer)
Instance ID
i-0fbc61fe781640b84 (AppServer)
Public IPv4 address
–
Private IPv4 addresses
10.0.11.202
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-10-0-11-202.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-11-202.ec2.internal
Answer private resource DNS name
–
Instance type
t2.small
Elastic IP addresses
–
Auto-assigned IP address
–
VPC ID
vpc-0990058669b9d5a70 (LabVPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
SsmRole
Subnet ID
subnet-0147a452a1f02a0a7 (PrivateSubnet)
Auto Scaling Group name
–
IMDSv2
Optional
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Security details
IAM Role
SsmRole
Owner ID
170460733071
Launch time
Sun Sep 10 2023 16:10:19 GMT+1000 (Australian Eastern Standard Time)
Security groups
sg-03081bb30bd1bdedd (c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49)
Inbound rules

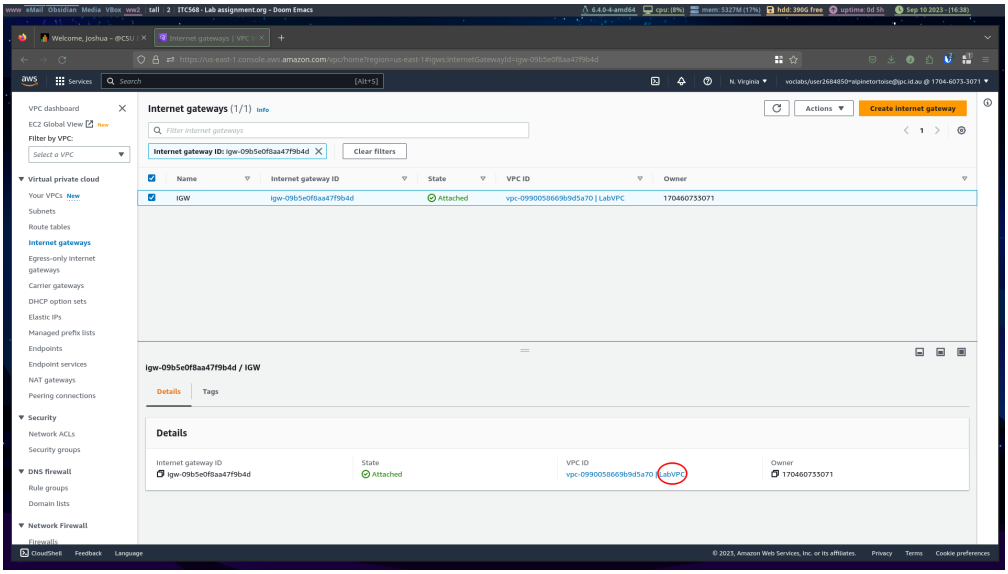

sg-03081bb30bd1bdedd - c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49
Details
Security group name
c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49
Security group ID
sg-03081bb30bd1bdedd
Description
Security group for App server
VPC ID
vpc-0990058669b9d5a70
Owner
170460733071
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (1/1)
Manage tags
Edit inbound rules
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
sgr-0afb7c67883cd8583
IPv4
HTTP
TCP
80
0.0.0.0/0

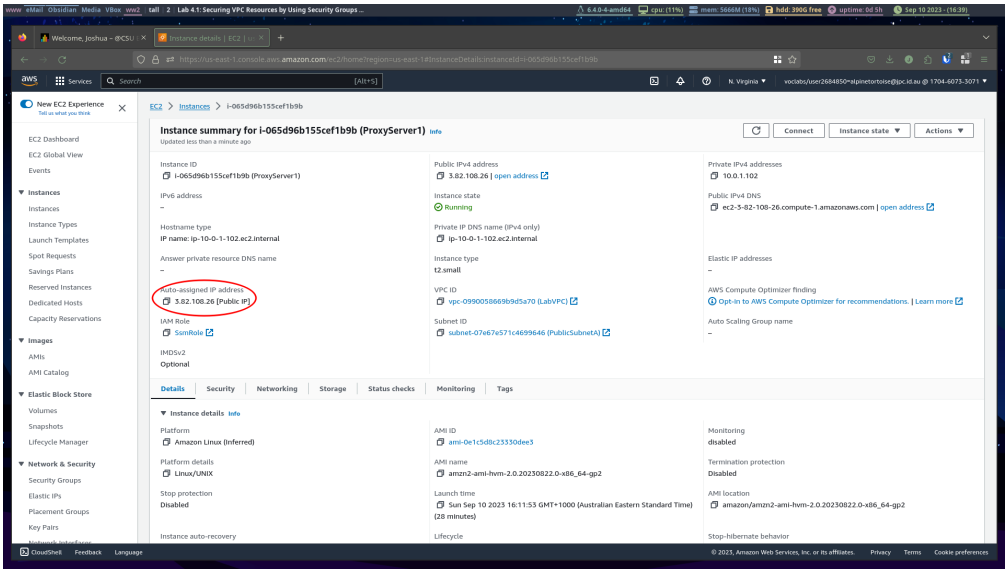


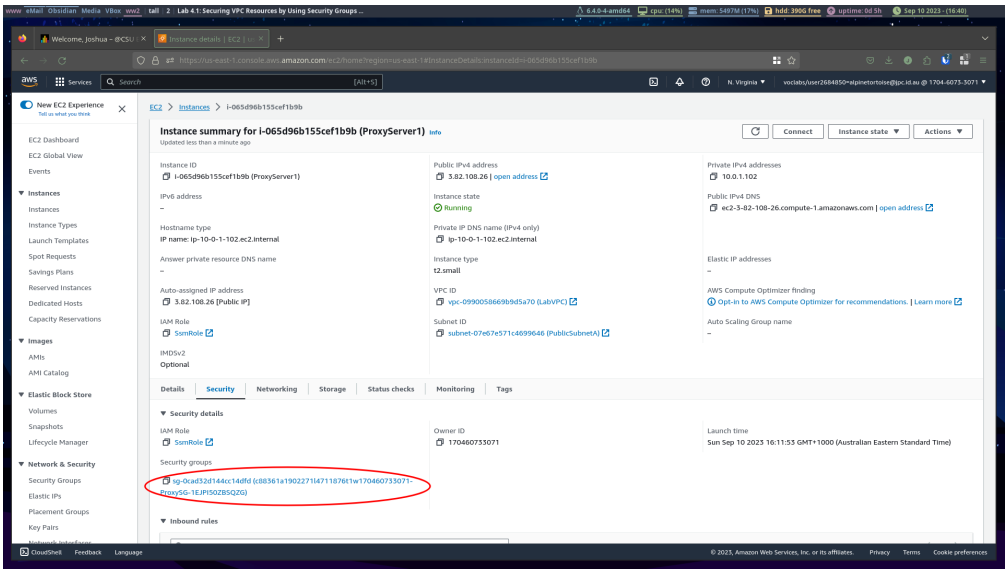
2.2 Task 2: Analyzing the public subnet resource settings

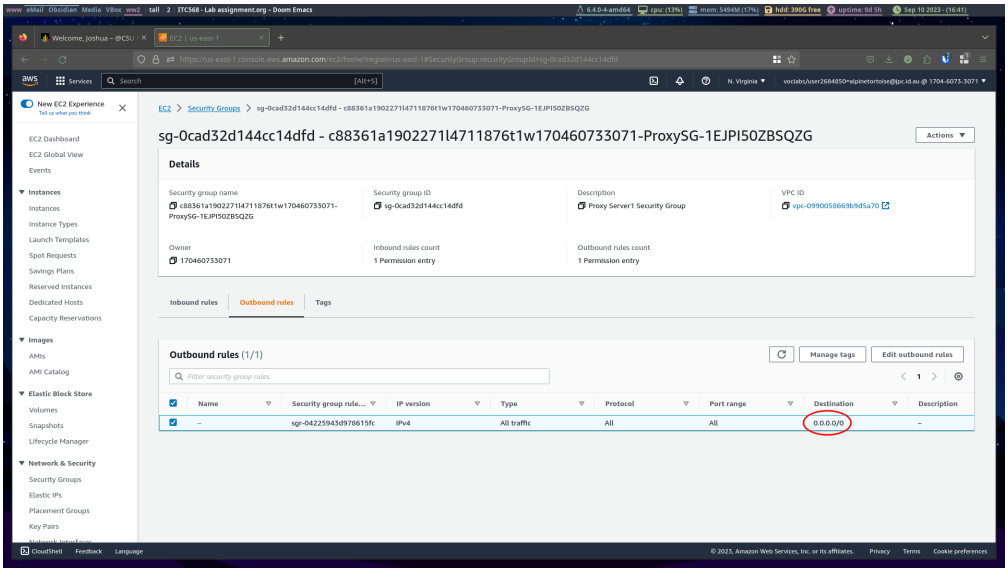


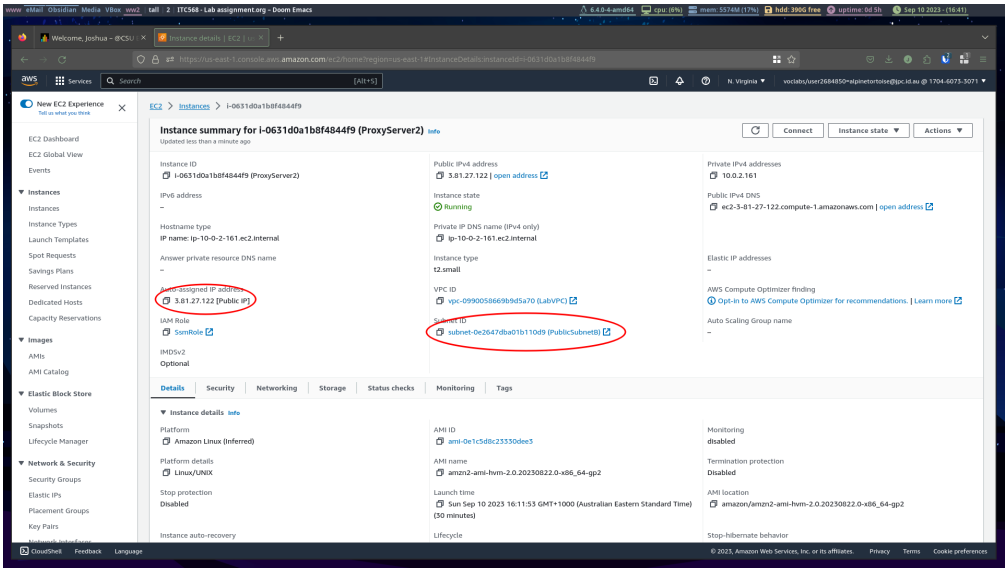

Subnets (1/9)
Create subnet
PrivateSubnet
PublicSubnetB
PublicSubnetA
subnet-07e67e571c4699646 / PublicSubnetA
Route table: rtb-046ce1ee8c8a97800 / Public
Routes (2)
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-09b5e0f8aa47f9b4d

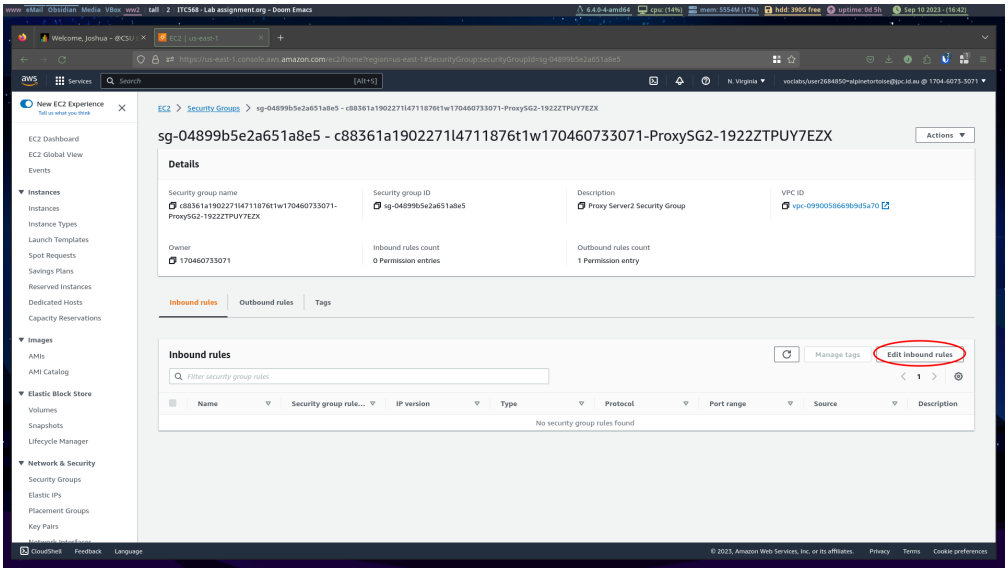

Internet gateways (1/1)
Create internet gateway
IGW
igw-09b5e0f8aa47f9b4d / IGW
Details
Internet gateway ID
igw-09b5e0f8aa47f9b4d
State
Attached
VPC ID
Owner
170460733071

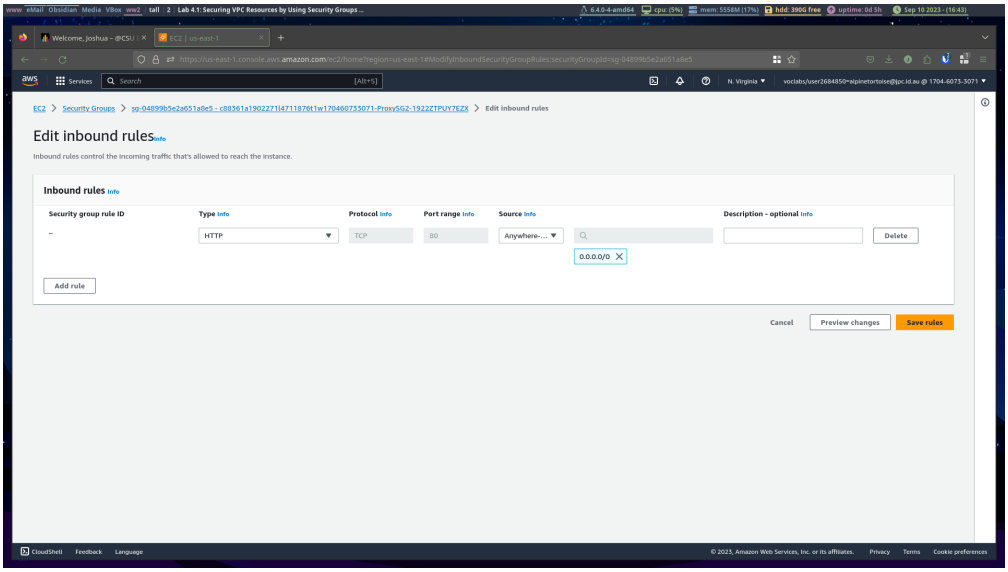

Instance summary for i-065d96b155cef1b9b (ProxyServer1)
Auto-assigned IP address
3.82.108.26 [Public IP]
Details
Security
Networking
Storage
Status checks
Monitoring
Tags

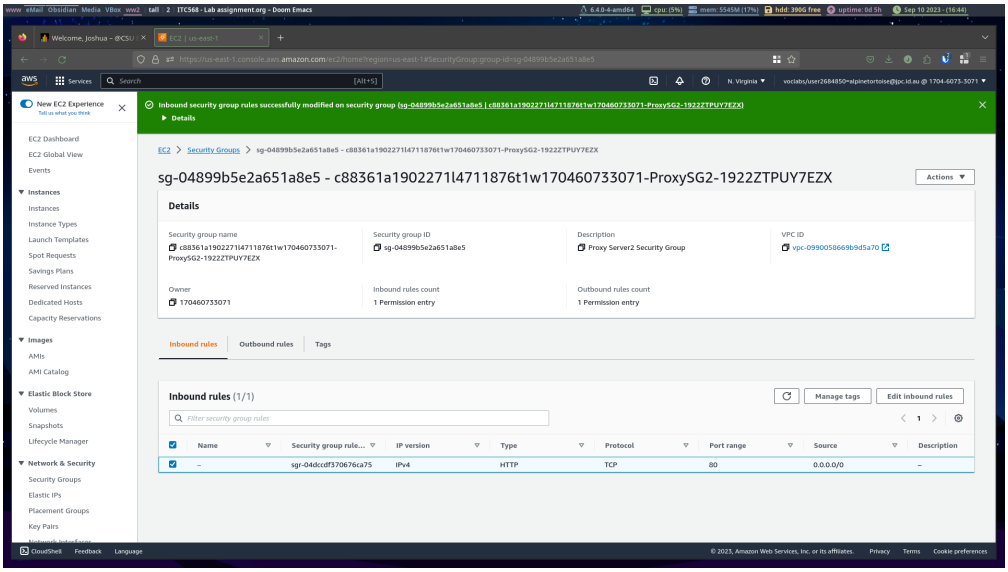

Instance summary for i-065d96b155cef1b9b (ProxyServer1)
Security details
Inbound rules


sg-0cad32d144cc14dfd - c88361a1902271l4711876t1w170460733071-ProxySG-1EJPI50ZBSQZG
Details
Security group name
c88361a1902271l4711876t1w170460733071-ProxySG-1EJPI50ZBSQZG
Security group ID
sg-0cad32d144cc14dfd
Description
Proxy Server1 Security Group
VPC ID
vpc-0990058669b9d5a70
Owner
170460733071
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Outbound rules (1/1)
Manage tags
Edit outbound rules
Name
Security group rule...
IP version
Type
Protocol
Port range
Destination
Description
sgr-04225943d978615fc
IPv4
All traffic
All
All
0.0.0.0/0

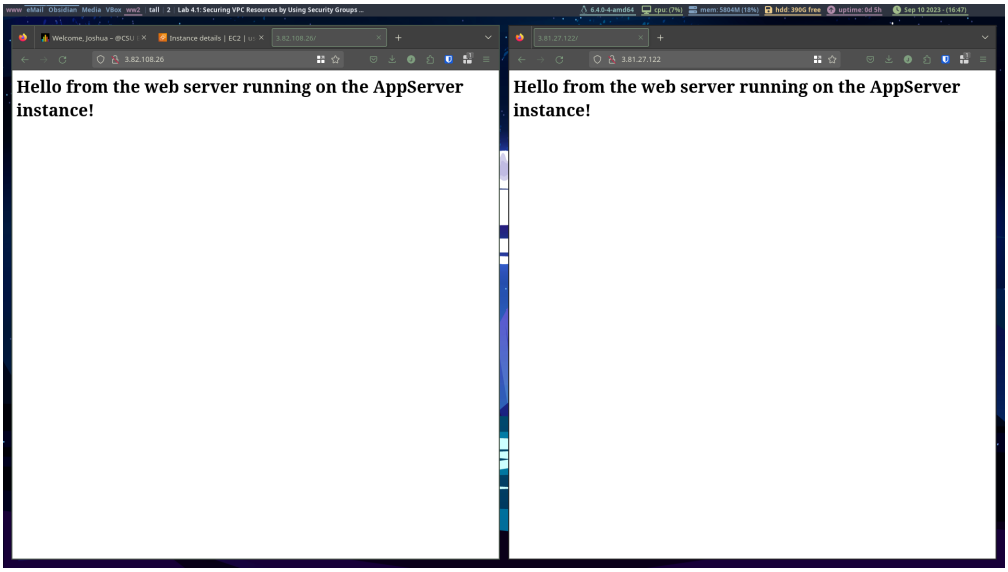

Instance summary for i-0631d0a1b8f4844f9 (ProxyServer2)
Connect
Instance state
Actions
Instance ID
i-0631d0a1b8f4844f9 (ProxyServer2)
Public IPv4 address
3.81.27.122 | open address
Private IPv4 addresses
10.0.2.161
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-3-81-27-122.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-0-2-161.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-2-161.ec2.internal
Answer private resource DNS name
Instance type
t2.small
Elastic IP addresses
Auto-assigned IP address
3.81.27.122 [Public IP]
VPC ID
vpc-0990058669b9d5a70 (LabVPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
SsmRole
Subnet ID
subnet-0e2647dba01b110d9 (PublicSubnet8)
Auto Scaling Group name
IMDSv2
Optional
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance details
Platform
Amazon Linux (Inferred)
AMI ID
ami-0e1c5d8c25550dee3
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
amzn2-ami-hvm-2.0.20230822.0-x86_64-gp2
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Sep 10 2023 16:11:53 GMT+1000 (Australian Eastern Standard Time) (30 minutes)
AMI location
amazon/amzn2-ami-hvm-2.0.20230822.0-x86_64-gp2


sg-04899b5e2a651a8e5 - c88361a1902271l4711876t1w170460733071-ProxySG2-1922ZTPUY7EZX
Actions
Details
Security group name
Security group ID
Description
VPC ID
Owner
Inbound rules count
Outbound rules count
Inbound rules
Outbound rules
Tags
Inbound rules
Manage tags
Edit inbound rules
No security group rules found


Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules
Security group rule ID
Type
Protocol
Port range
Source
Description - optional
HTTP
TCP
80
Anywhere-...
0.0.0.0/0
Delete
Add rule
Cancel
Preview changes
Save rules

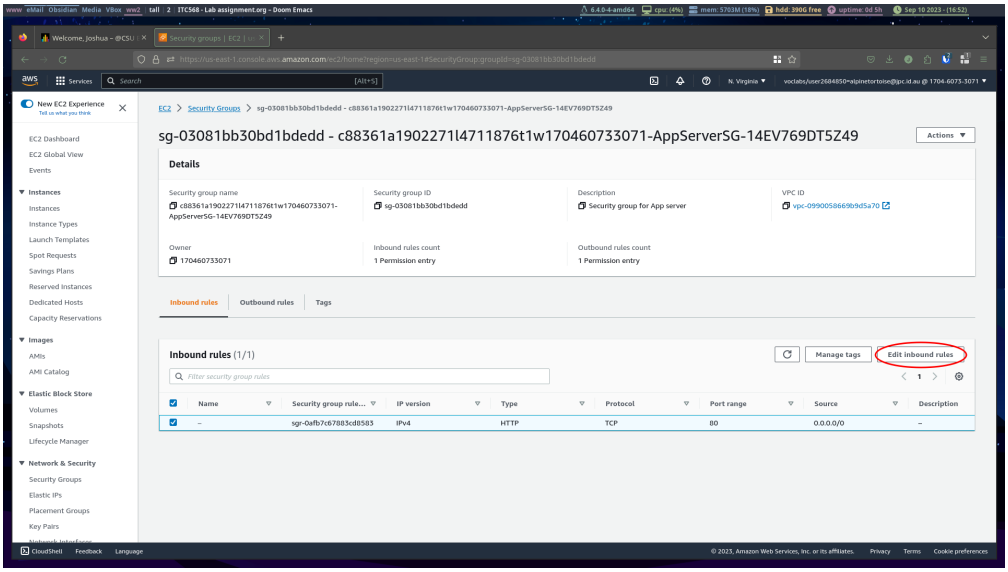


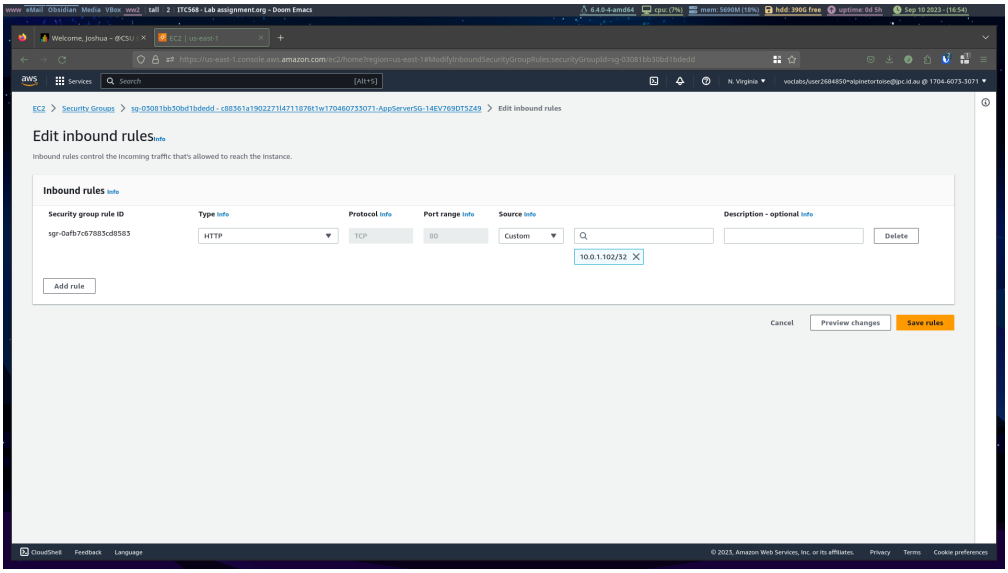
2.3 Task 3: Testing HTTP connectivity from public EC2 instances

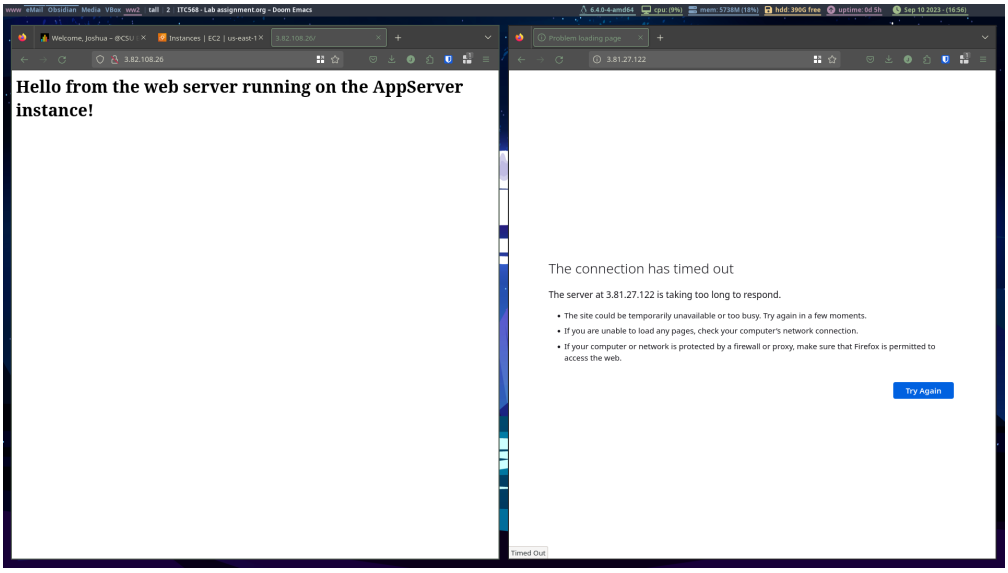


2.4 Task 4: Restricting HTTP access by using an IP address

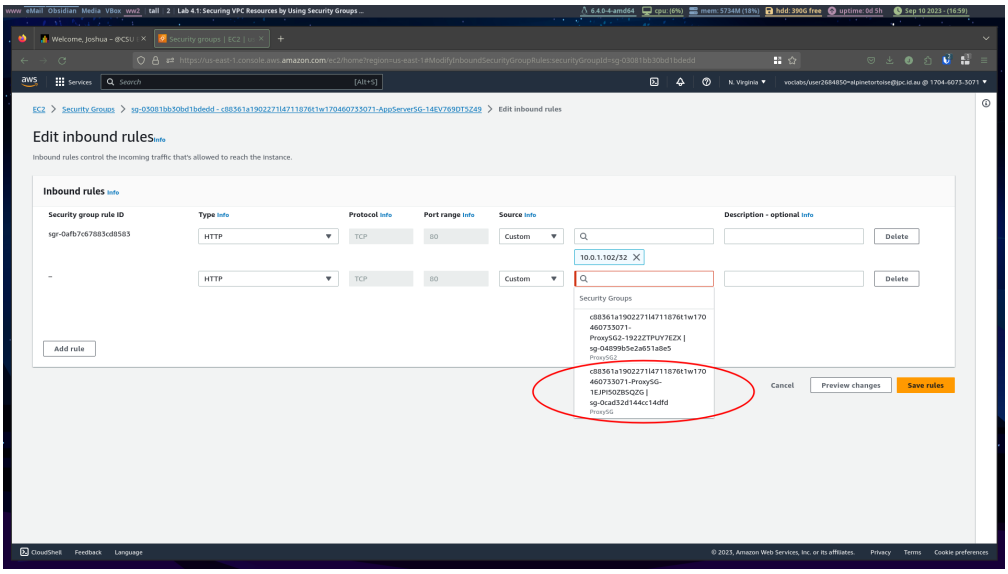
Hostname	Public IP Address	Private IP Address
ProxyServer1	3.82.108.26	10.0.1.102
ProxyServer2	3.81.27.122	10.0.2.161
AppServer	-	10.0.11.202

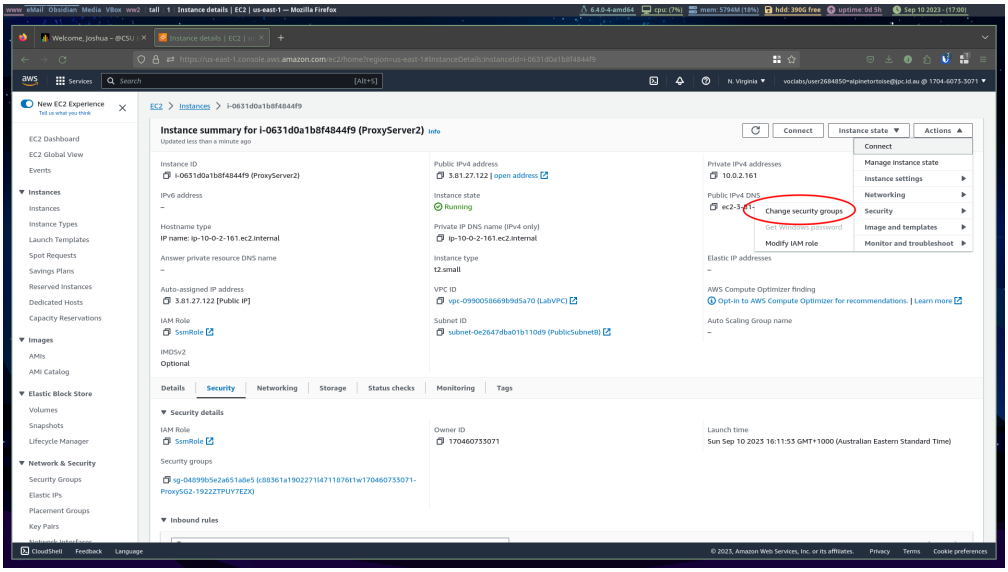

sg-03081bb30bd1bdedd - c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49
Actions
Details
Security group name
c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49
Security group ID
sg-03081bb30bd1bdedd
Description
Security group for App server
VPC ID
vpc-0990058669b9d5a70
Owner
170460733071
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (1/1)
Manage tags
Edit inbound rules
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
sgr-0afb7c67883cd8583
IPv4
HTTP
TCP
80
0.0.0.0/0

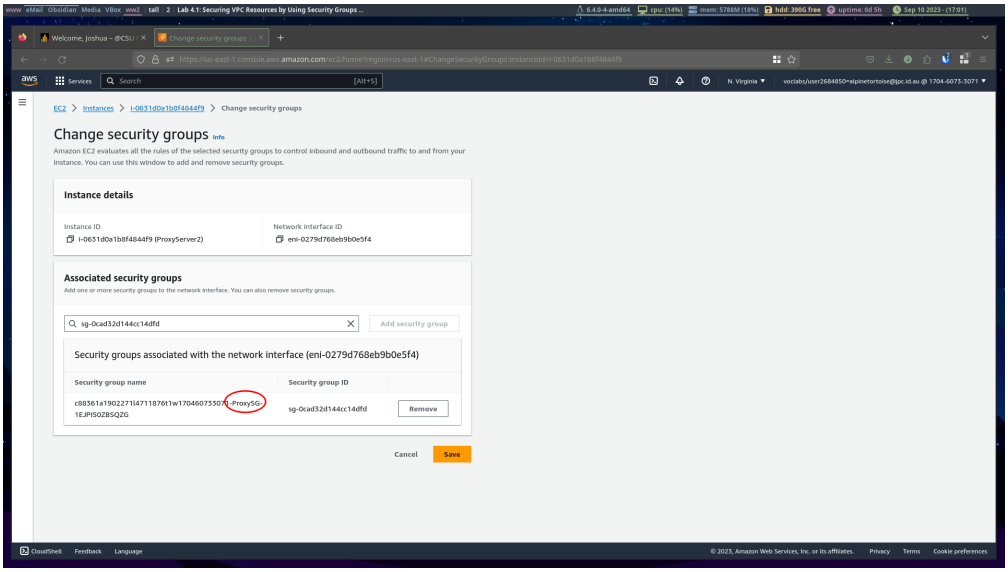

Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules
Security group rule ID
Type
Protocol
Port range
Source
Description - optional
sgr-0afb7c67883cd8583
HTTP
TCP
80
Custom
10.0.1.102/32
Delete
Add rule
Cancel
Preview changes
Save rules

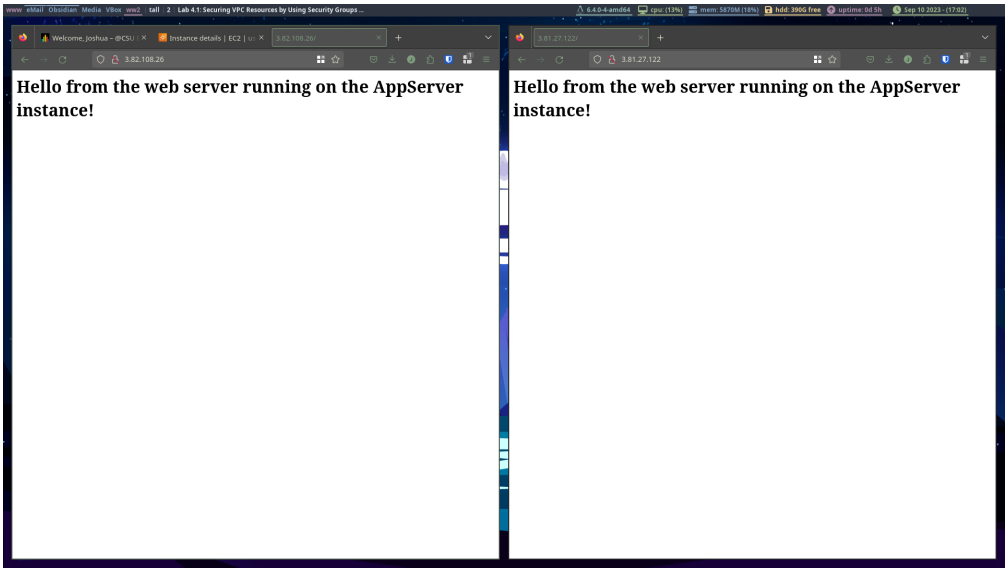


2.5 Task 5: Scaling restricted HTTP access by referencing a security group

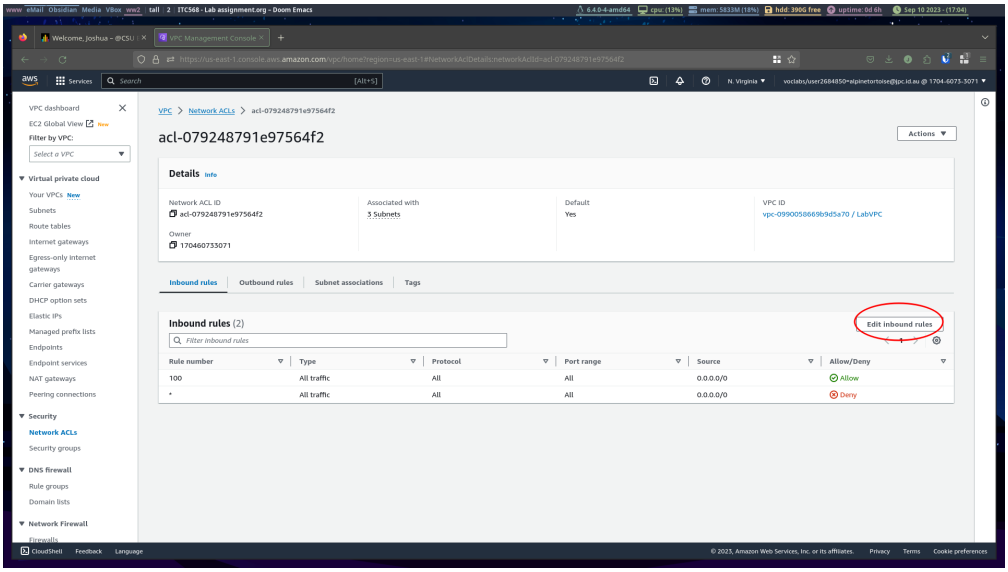


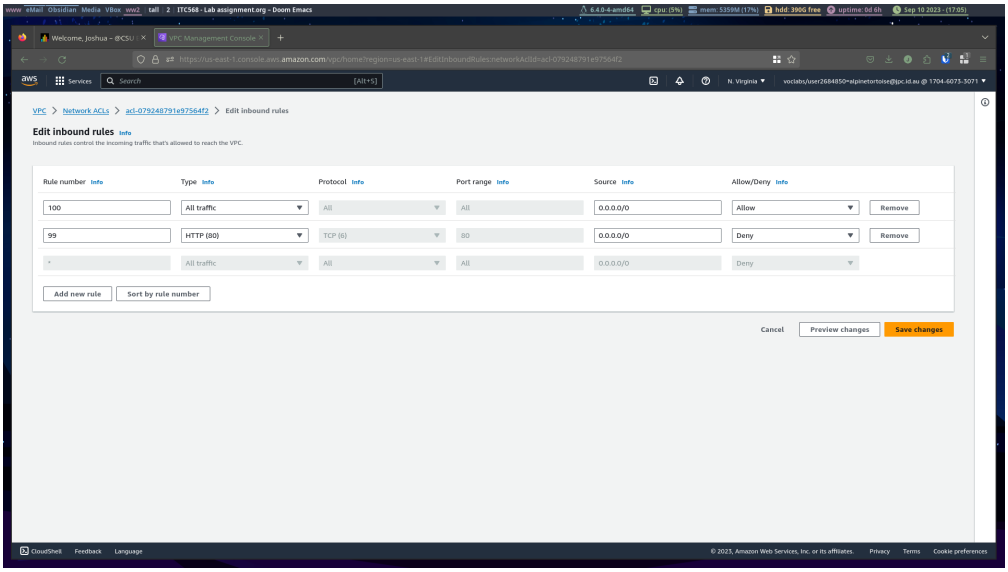

Instance summary for i-0631d0a1b8f4844f9 (ProxyServer2)
Connect
Instance state
Actions
Change security groups
Security details
sg-04899b5e2a651a8e5 (c88361a1902271l47118761w170460733071-ProxySG2-1922ZTPUY7EZX)

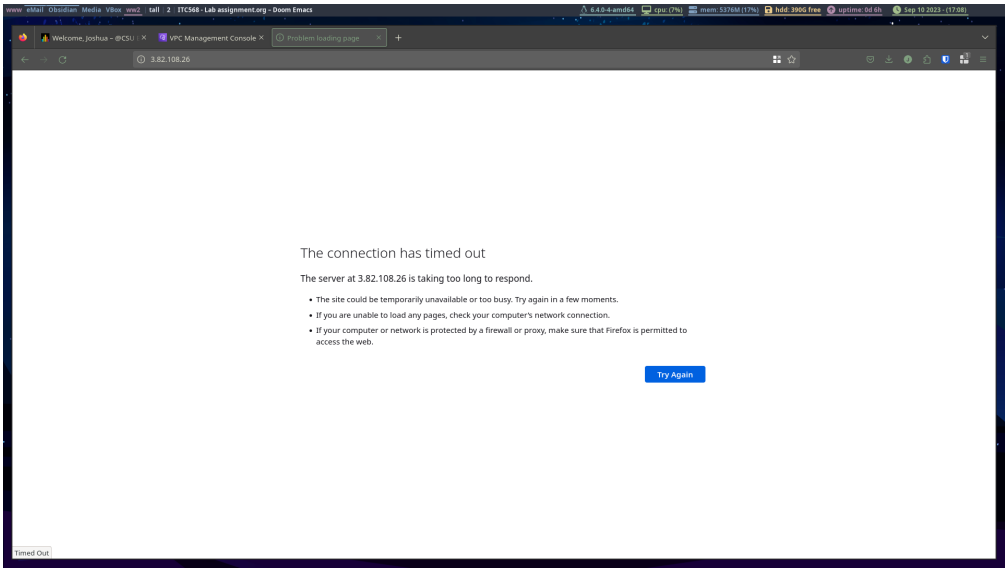

Change security groups
Instance details
Associated security groups
sg-0cad32d144cc14dfd
Security groups associated with the network interface (eni-0279d768eb9b0e5f4)
Security group name
Security group ID
c88361a1902271l47118761w170460733071-ProxySG-1EJPI50Z8SQZG
sg-0cad32d144cc14dfd
Remove
Cancel
Save

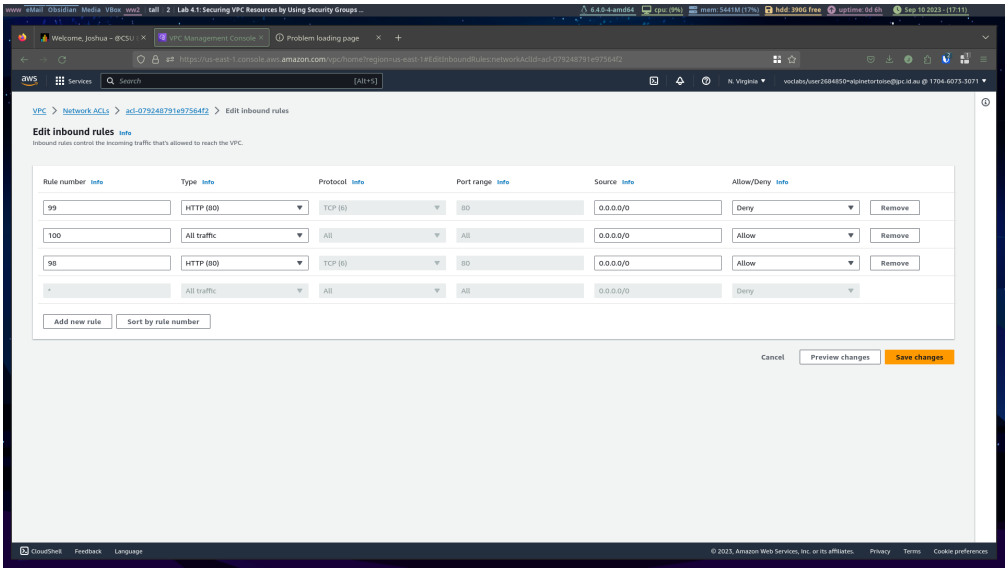


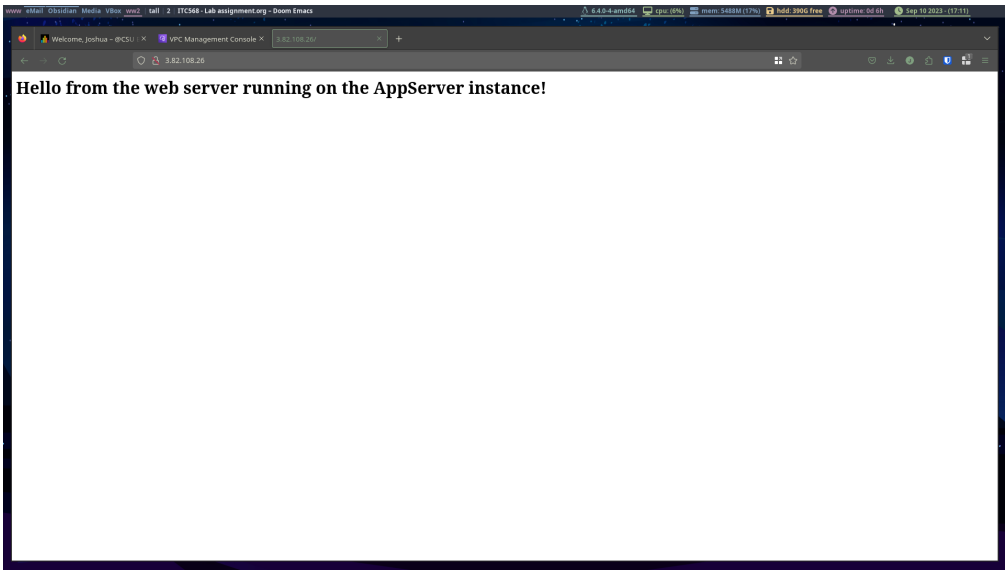
2.6 Task 6: Restricting HTTP access by using a network ACL



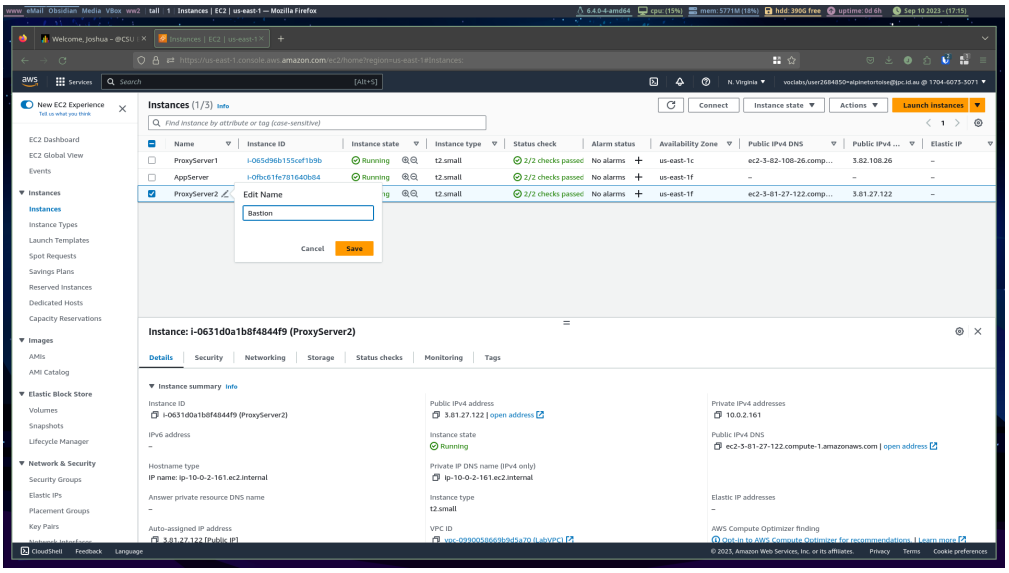

Welcome, Joshua – @CSU
VPC Management Console
https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditInboundRules:networkAclId=acl-079248791e97564f2
Services
Search
[Alt+S]
N. Virginia
VPC > Network ACLs > acl-079248791e97564f2 > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the VPC.
Rule number Info
Type Info
Protocol Info
Port range Info
Source Info
Allow/Deny Info
100
All traffic
All
All
0.0.0.0/0
Allow
Remove
99
HTTP (80)
TCP (6)
80
0.0.0.0/0
Deny
Remove
All traffic
All
All
0.0.0.0/0
Deny
Add new rule
Sort by rule number
Cancel
Preview changes
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

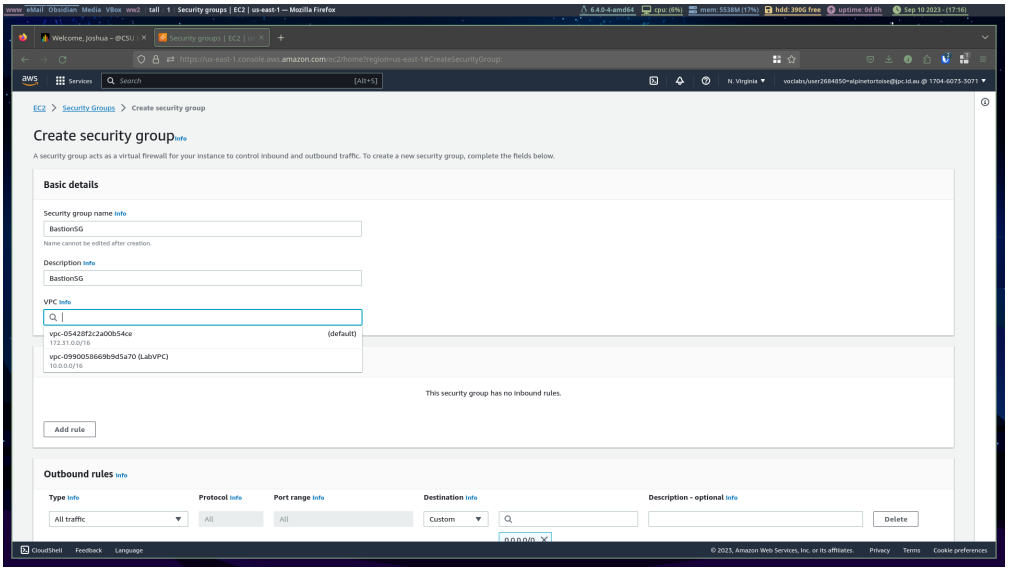

Welcome, Joshua – @CSU
VPC Management Console
Problem loading page
3.82.108.26
The connection has timed out
The server at 3.82.108.26 is taking too long to respond.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.
Try Again
Timed Out

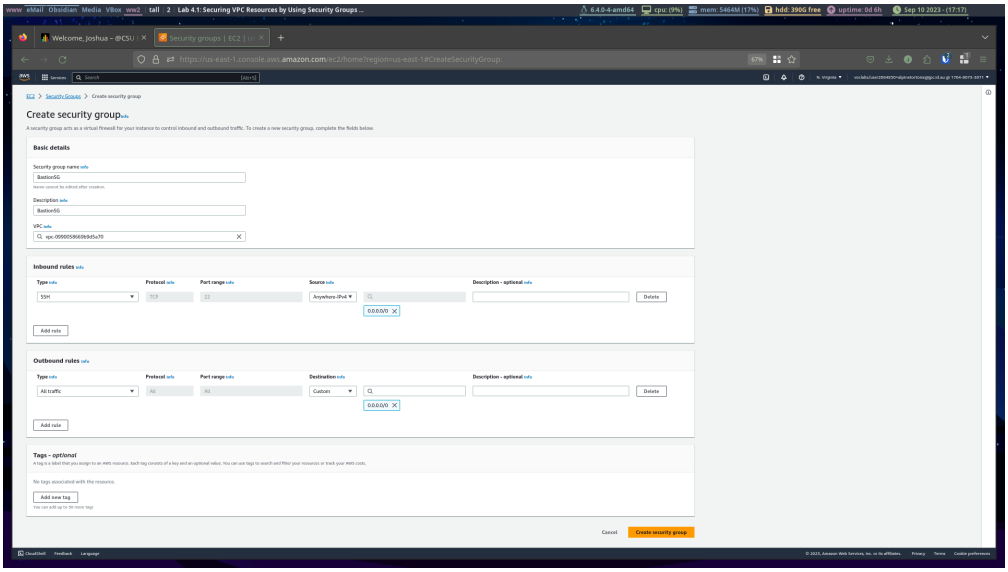

Welcome, Joshua – @CSU
VPC Management Console
Problem loading page
Services
Search
N. Virginia
VPC > Network ACLs > acl-079248791e97564f2 > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the VPC.
Rule number Info
Type Info
Protocol Info
Port range Info
Source Info
Allow/Deny Info
99
HTTP (80)
TCP (6)
80
0.0.0.0/0
Deny
Remove
100
All traffic
All
All
0.0.0.0/0
Allow
Remove
98
HTTP (80)
TCP (6)
80
0.0.0.0/0
Allow
Remove
*
All traffic
All
All
0.0.0.0/0
Deny
Add new rule
Sort by rule number
Cancel
Preview changes
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

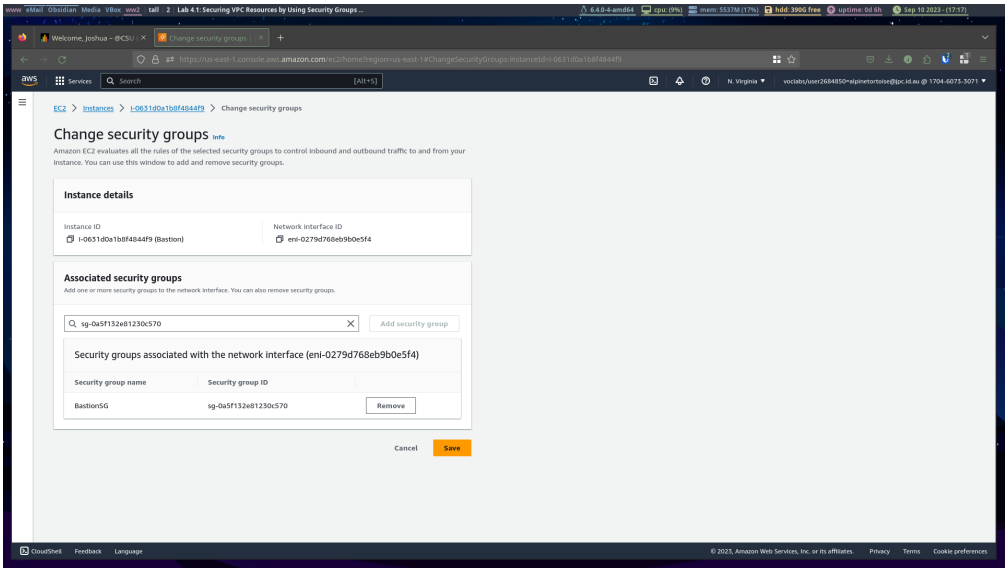

Welcome, Joshua – @CSU
VPC Management Console
3.82.108.26
Hello from the web server running on the AppServer instance!

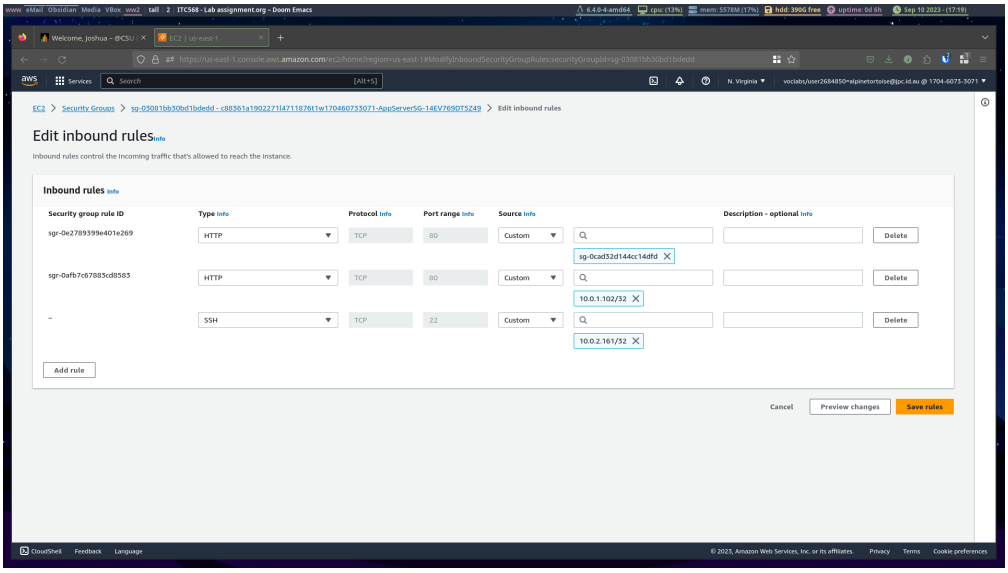
2.7 Task 7: Connecting to the AppServer by using a bastion host and SSH

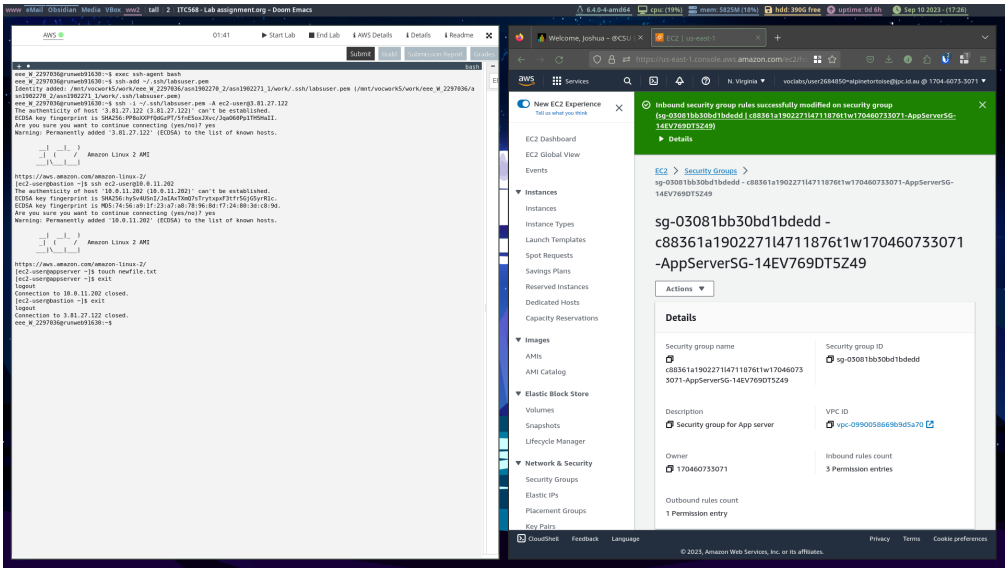




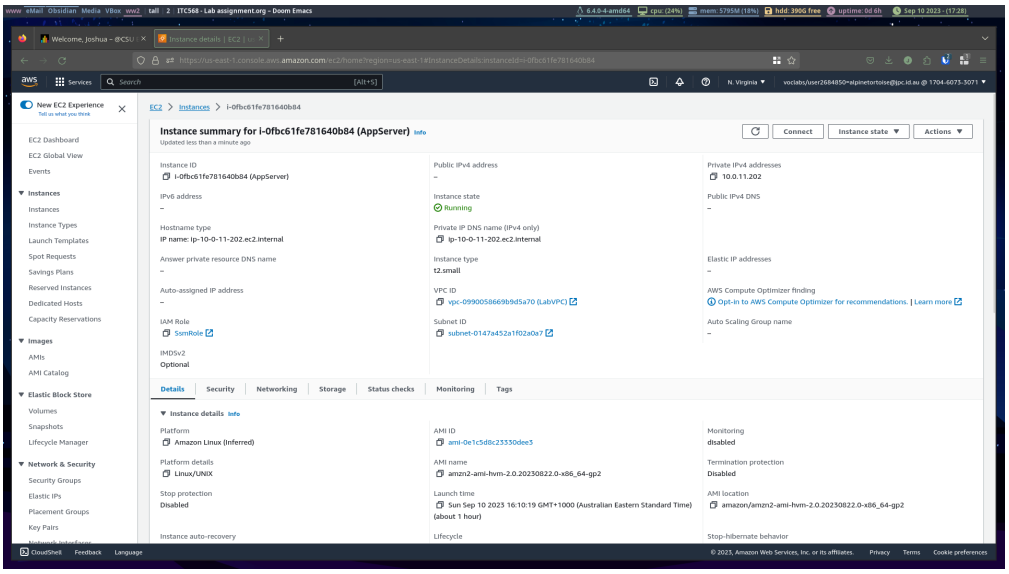

Create security group
Basic details
Security group name info
BastionSG
Description info
BastionSG
VPC info
vpc-0590059f668b8d5a70
Inbound rules info
Type info
Protocol info
Port range info
Source info
Description - optional info
SSH
TCP
22
Anywhere-IPv4
0.0.0.0/0
Delete
Add rule
Outbound rules info
Type info
Protocol info
Port range info
Destination info
Description - optional info
All traffic
All
All
Custom
0.0.0.0/0
Delete
Add rule
Tags - optional
No tags associated with the resource.
Add new tag
Cancel
Create security group

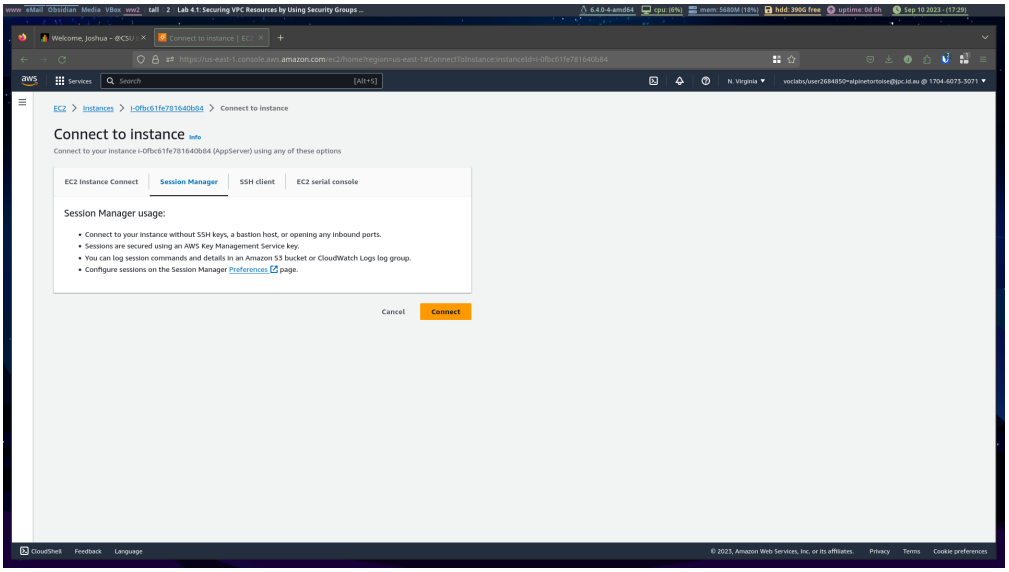

EC2 > Instances > i-0651d0a1b8f4844f9 > Change security groups
Change security groups info
Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.
Instance details
Instance ID
i-0651d0a1b8f4844f9 (Bastion)
Network interface ID
eni-0279d768eb9b0e5f4
Associated security groups
Add one or more security groups to the network interface. You can also remove security groups.
sg-0a5f132e81230c570
Add security group
Security groups associated with the network interface (eni-0279d768eb9b0e5f4)
Security group name
Security group ID
BastionSG
sg-0a5f132e81230c570
Remove
Cancel
Save

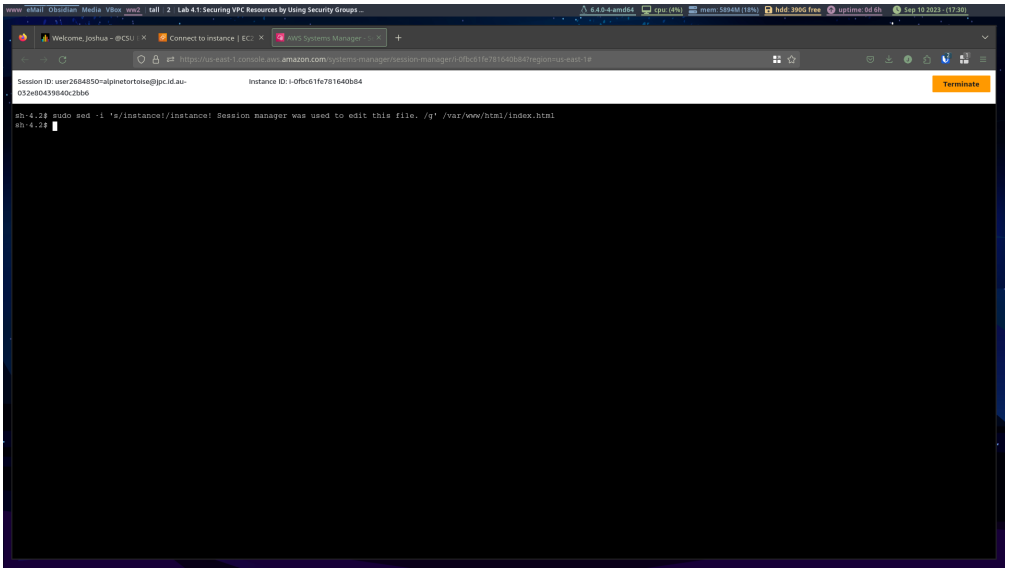

Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules
Security group rule ID
Type
Protocol
Port range
Source
Description - optional
sgr-0e2789399e401e269
HTTP
TCP
80
Custom
sg-0cad32d144cc14dfd
sgr-0afb7c67883cd8583
HTTP
TCP
80
Custom
10.0.1.102/32
SSH
TCP
22
Custom
10.0.2.161/32
Delete
Add rule
Cancel
Preview changes
Save rules

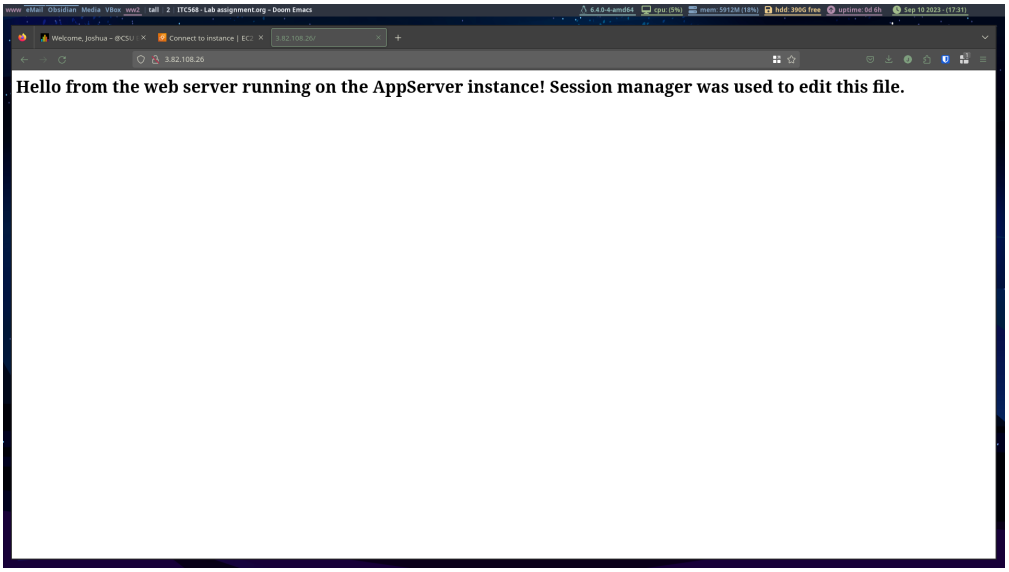

Inbound security group rules successfully modified on security group
sg-03081bb30bd1bdedd - c88361a1902271l4711876t1w170460733071-AppServerSG-14EV769DT5Z49
Details
Security group name
Security group ID
Description
Security group for App server
VPC ID
Owner
170460733071
Inbound rules count
3 Permission entries
Outbound rules count
1 Permission entry

2.8 Task 8: Connecting directly to a host in a private subnet by using Session Manager

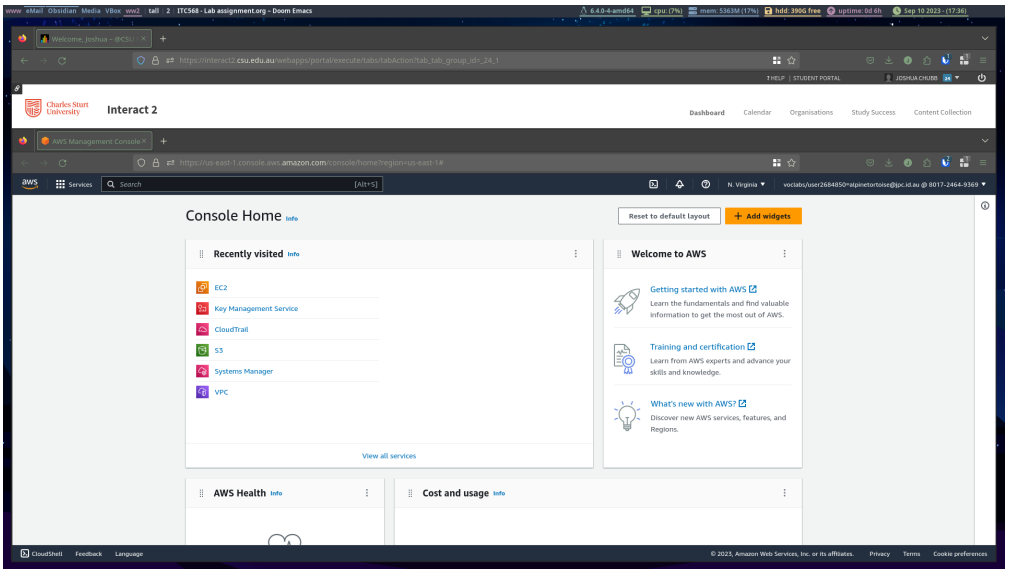




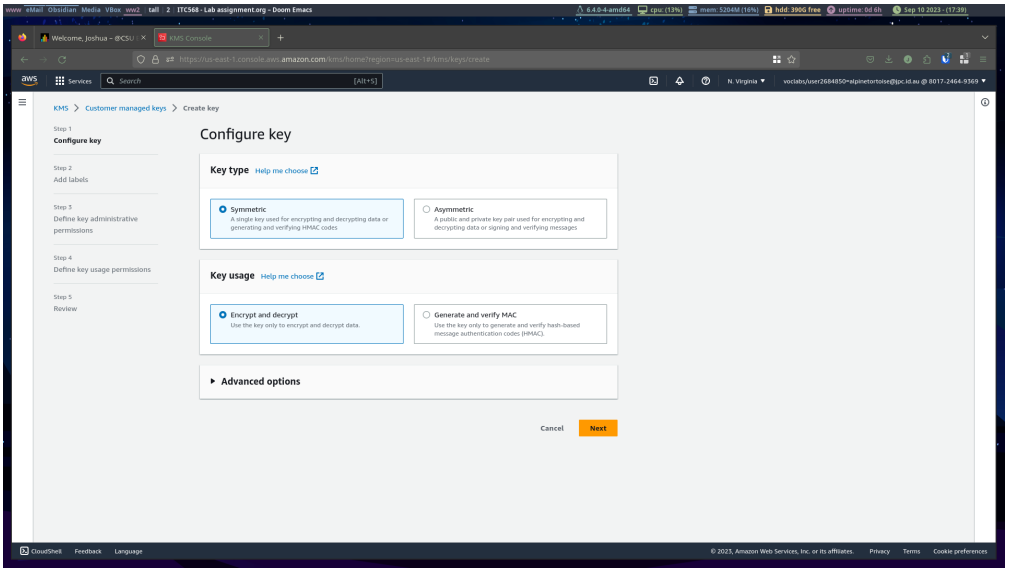

Session ID: user2684850=alpinetortoise@jpc.id.au-052e80439840c2bb6
Instance ID: i-0fbc61fe781640b84
Terminate
sh-4.2$ sudo sed -i 's/instance!/instance! Session manager was used to edit this file. /g' /var/www/html/index.html
sh-4.2$

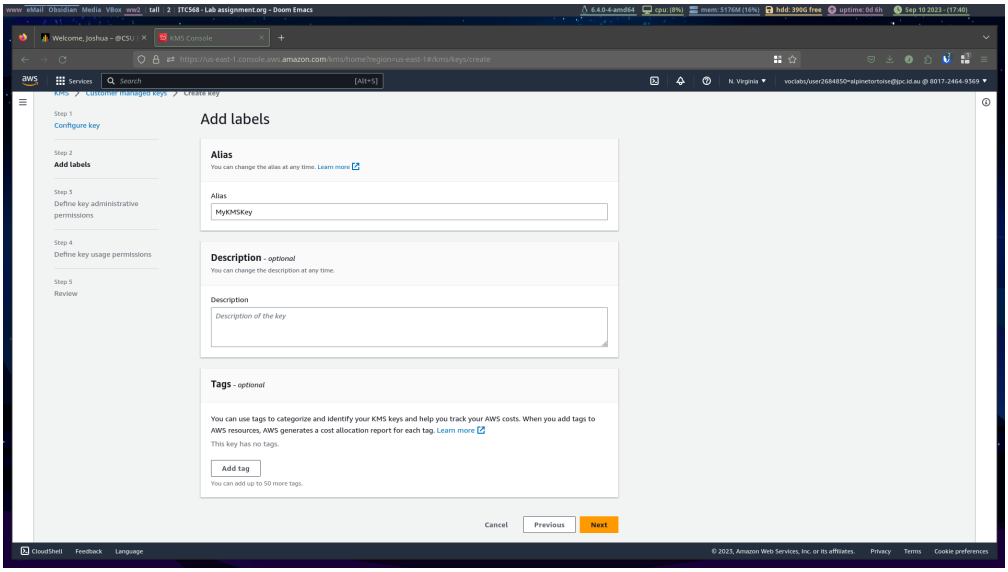

Hello from the web server running on the AppServer instance! Session manager was used to edit this file.

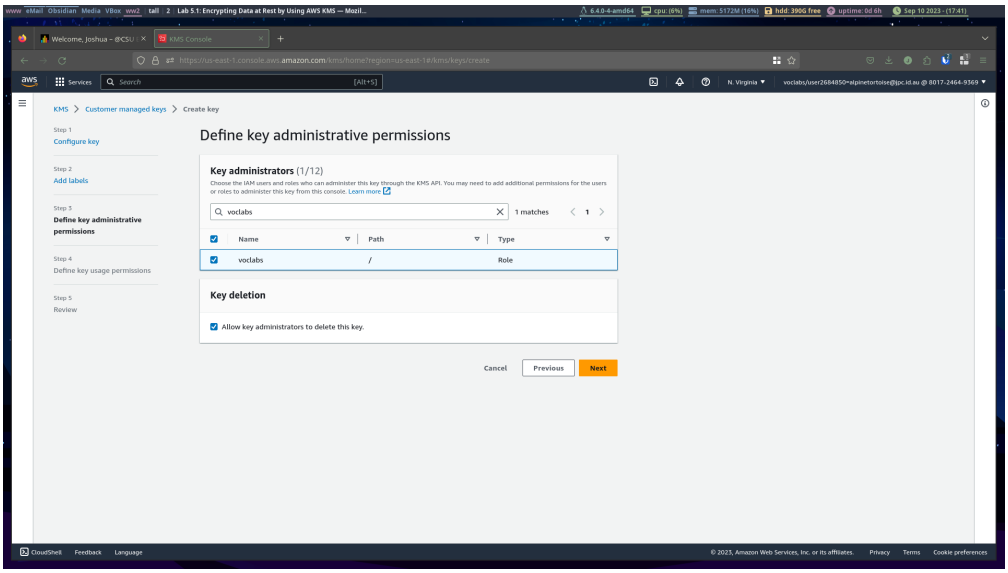
3 Lab 5.1: Encrypting Data at Rest by Using AWS KMS

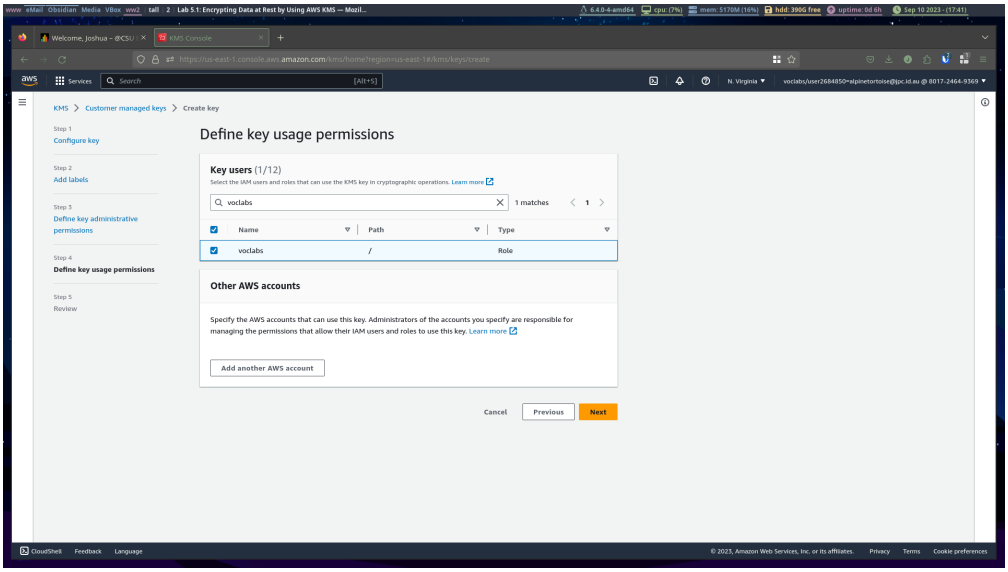


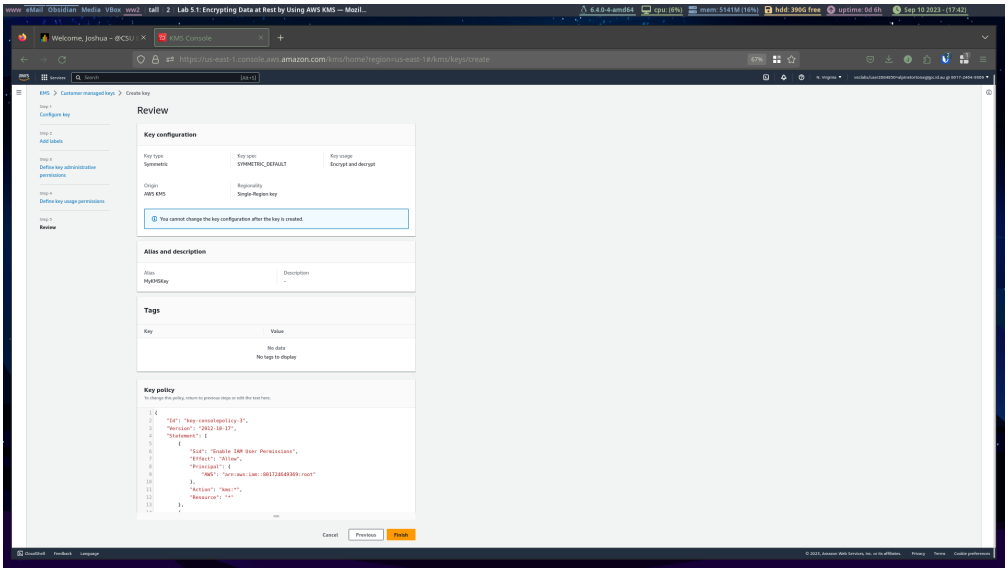
3.1 Task 1: Creating an AWS KMS key



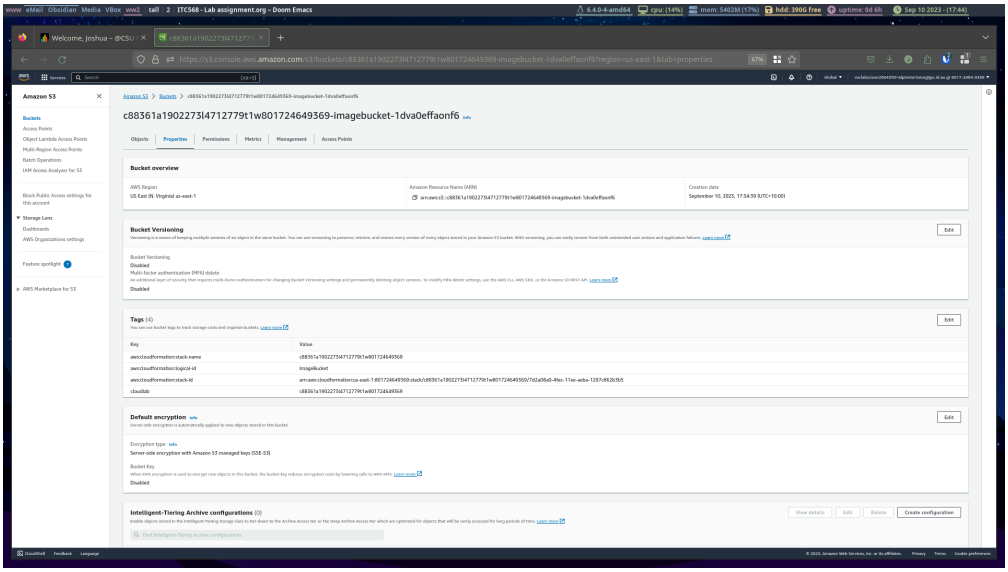

Add labels
Alias
You can change the alias at any time. Learn more
Alias
MyKMSKey
Description - optional
You can change the description at any time.
Description
Description of the key
Tags - optional
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more
This key has no tags.
Add tag
You can add up to 50 more tags.
Cancel
Previous
Next

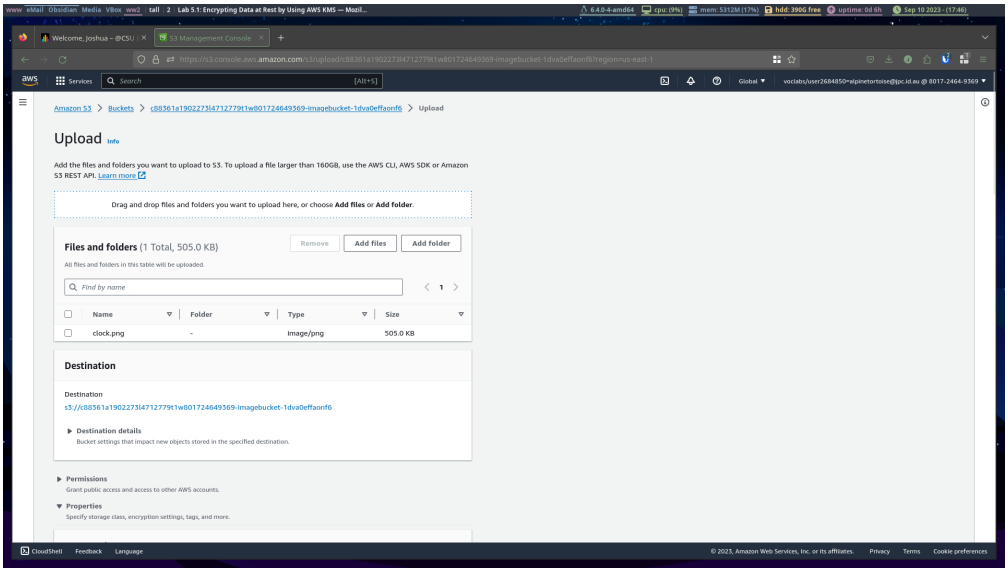

KMS > Customer managed keys > Create key
Define key administrative permissions
Key administrators (1/12)
Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more
voclabs
1 matches
Name
Path
Type
voclabs
/
Role
Key deletion
Allow key administrators to delete this key.
Cancel
Previous
Next

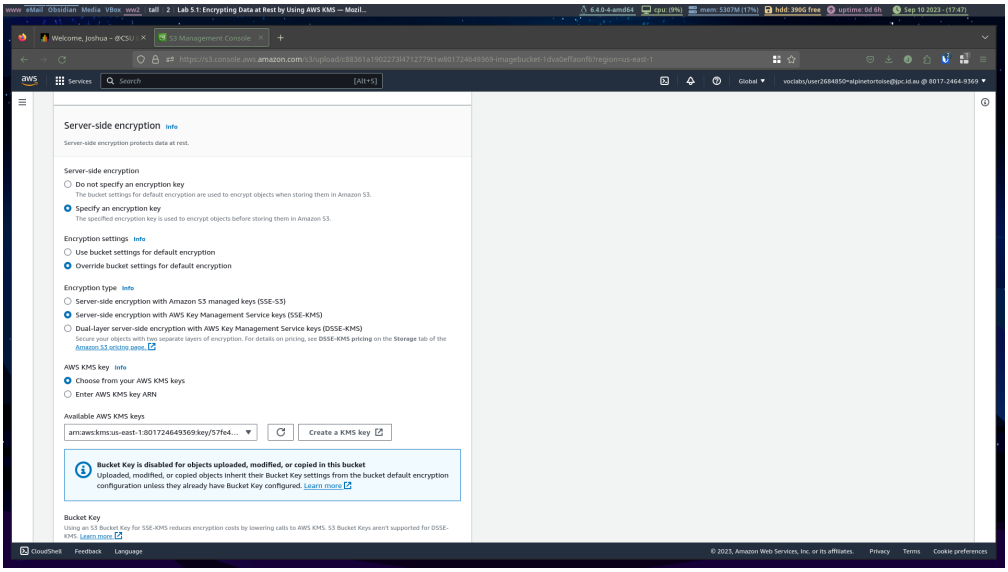

KMS > Customer managed keys > Create key
Define key usage permissions
Key users (1/12)
Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more
voclabs
1 matches
Name
Path
Type
voclabs
/
Role
Other AWS accounts
Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more
Add another AWS account
Cancel
Previous
Next

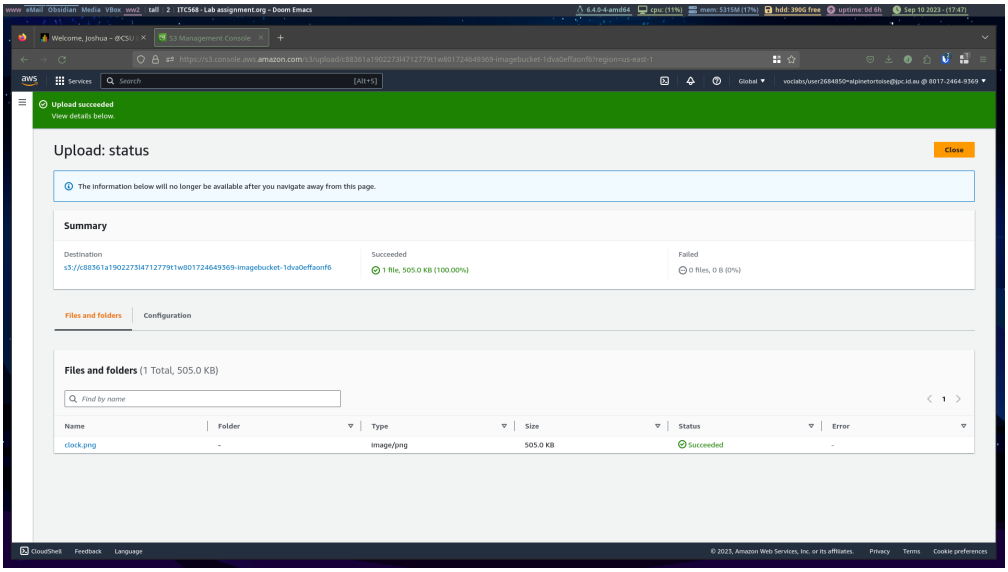

Review
Key configuration
Alias and description
Tags
Key policy
Cancel
Previous
Finish

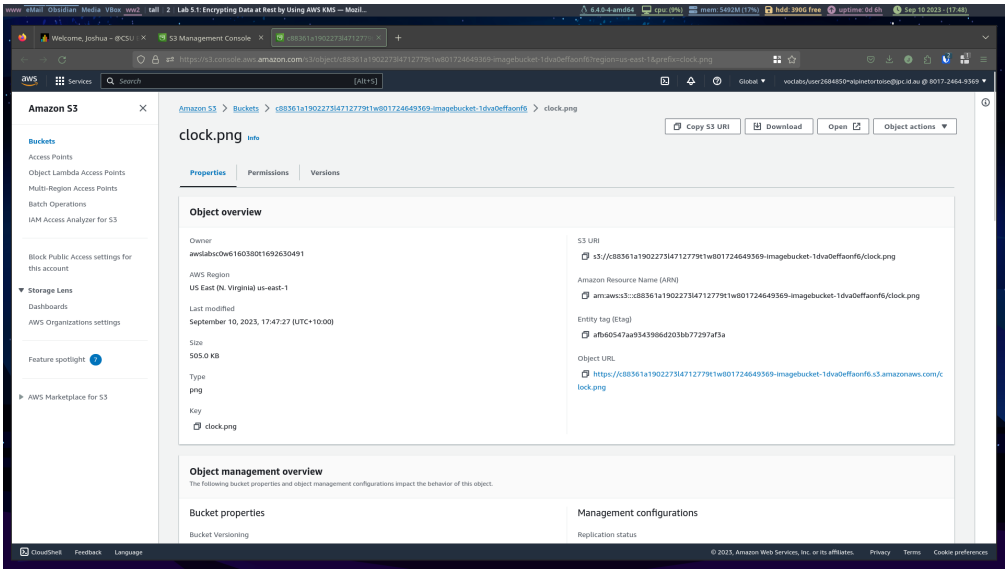
3.2 Task 2: Storing an encrypted object in an S3 bucket

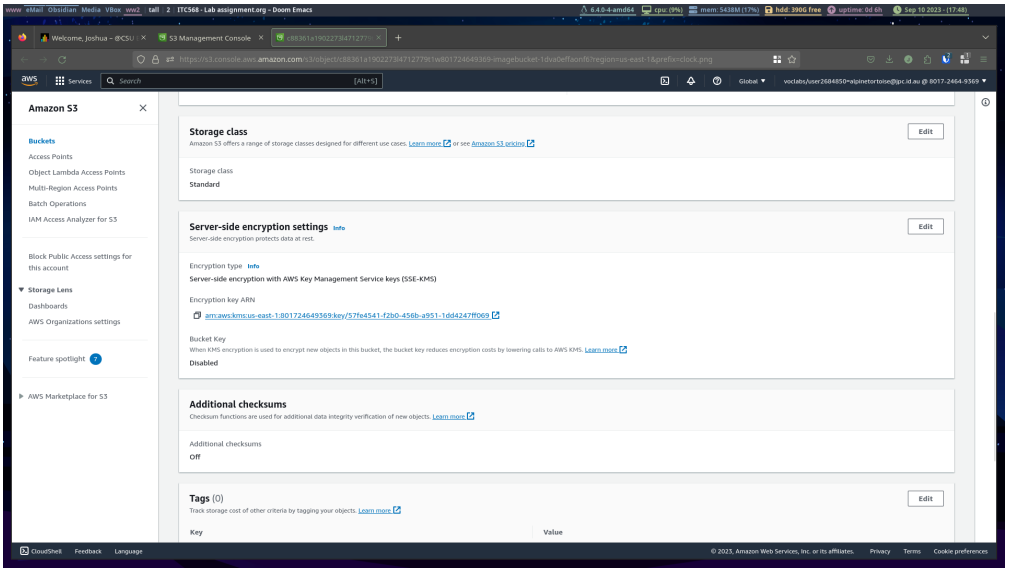



Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 505.0 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
clock.png
-
image/png
505.0 KB
Destination
Destination
s3://c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

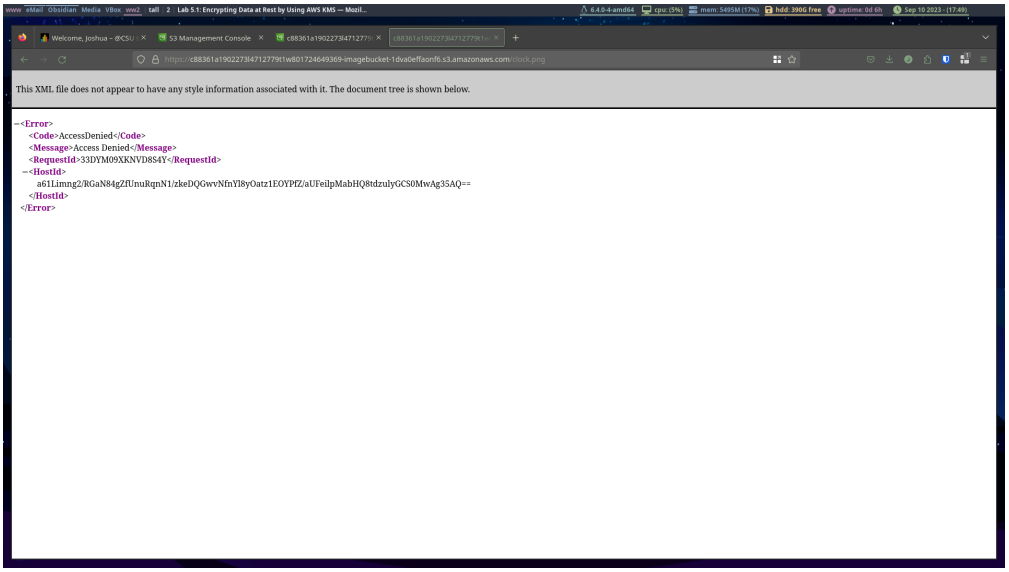

Server-side encryption Info
Server-side encryption protects data at rest.
Server-side encryption
Do not specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.
Encryption settings Info
Use bucket settings for default encryption
Override bucket settings for default encryption
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page
AWS KMS key Info
Choose from your AWS KMS keys
Enter AWS KMS key ARN
Available AWS KMS keys
arn:aws:kms:us-east-1:801724649369:key/57fe4...
Create a KMS key
Bucket Key is disabled for objects uploaded, modified, or copied in this bucket
Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. Learn more
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

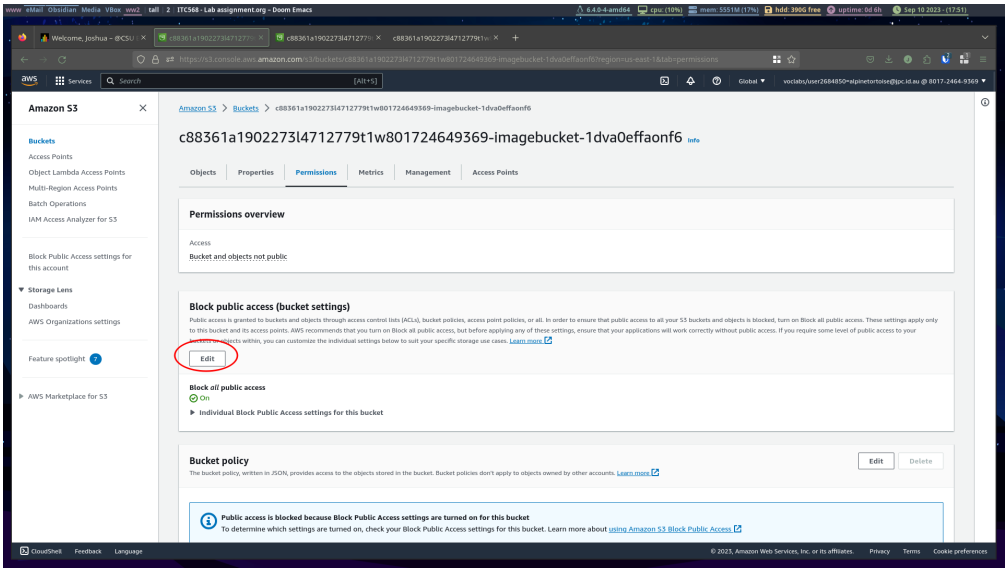

Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6
Succeeded
1 file, 505.0 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 505.0 KB)
Find by name
Name
Folder
Type
Size
Status
Error
clock.png
-
image/png
505.0 KB
Succeeded
-

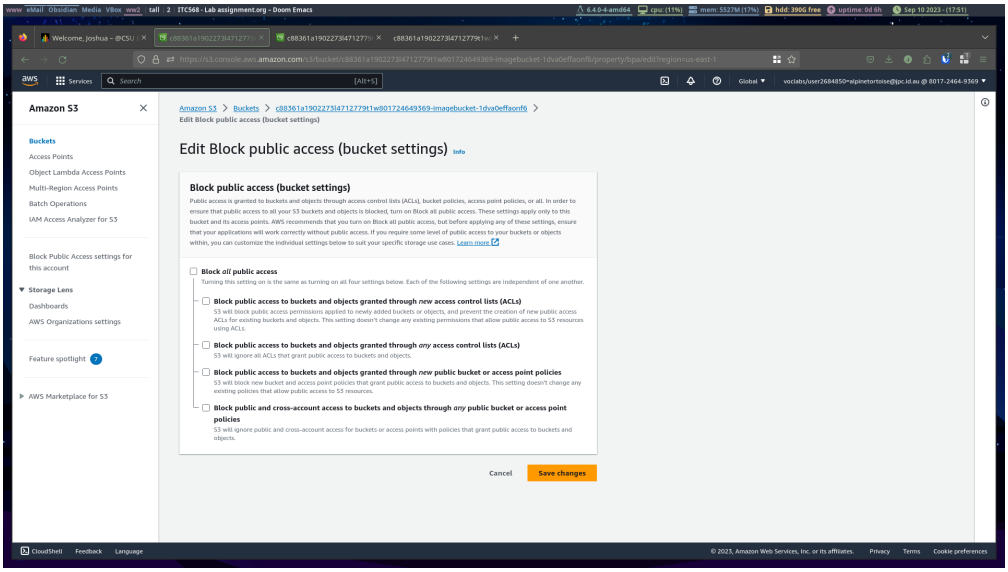

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 > clock.png
clock.png
Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w6160380t1692630491
AWS Region
US East (N. Virginia) us-east-1
Last modified
September 10, 2023, 17:47:27 (UTC+10:00)
Size
505.0 KB
Type
png
Key
clock.png
S3 URI
s3://c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6/clock.png
Amazon Resource Name (ARN)
arn:aws:s3:::c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6/clock.png
Entity tag (Etag)
afb60547aa9343986d203bb77297af3a
Object URL
https://c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6.s3.amazonaws.com/clock.png
Object management overview
The following bucket properties and object management configurations impact the behavior of this object.
Bucket properties
Bucket Versioning
Management configurations
Replication status

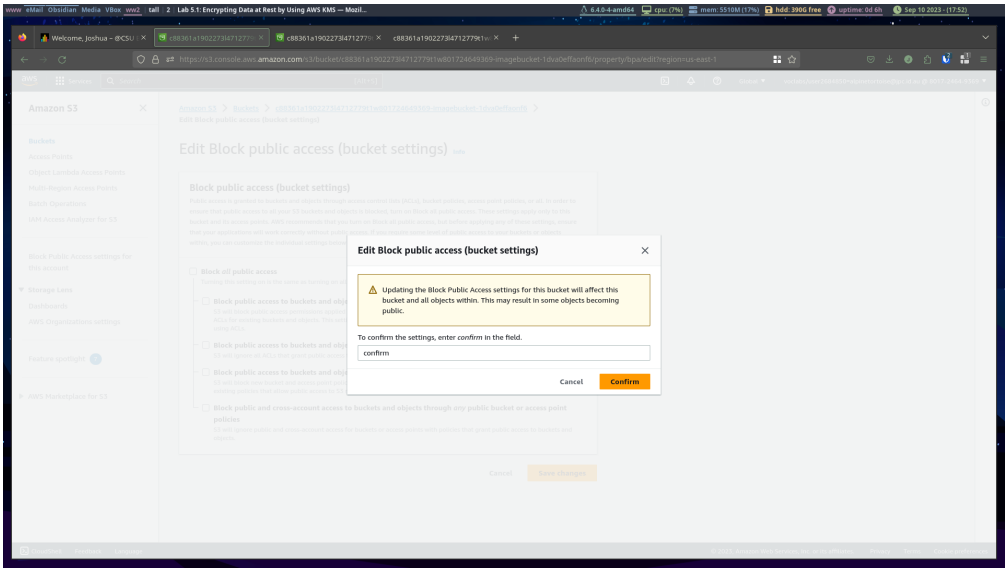


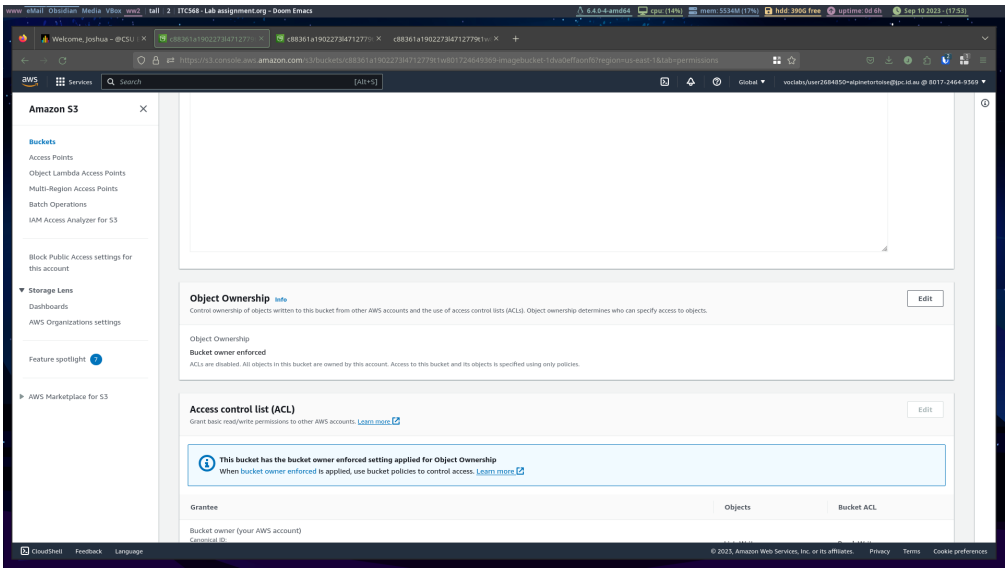
3.3 Task 3: Attempting public access to the encrypted object

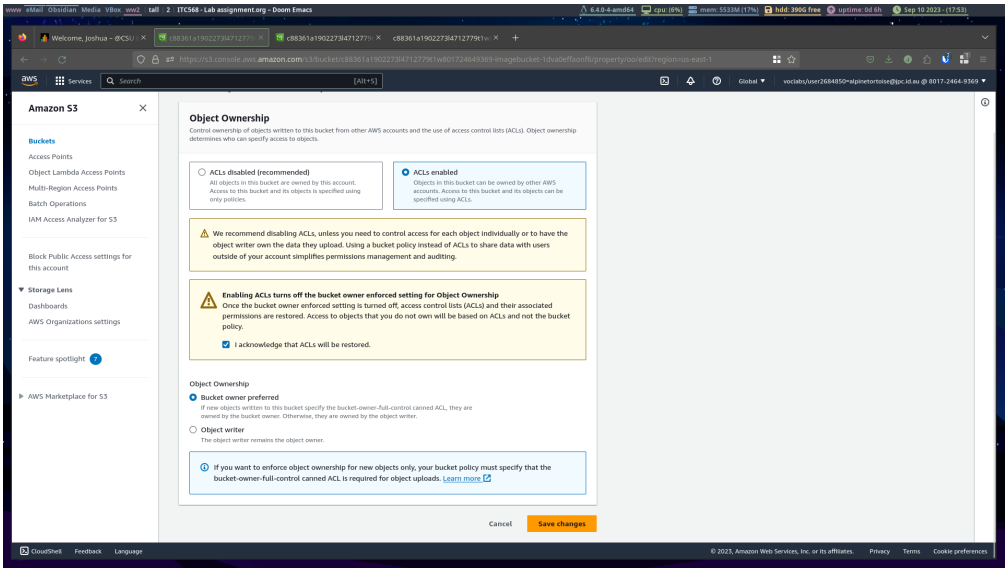


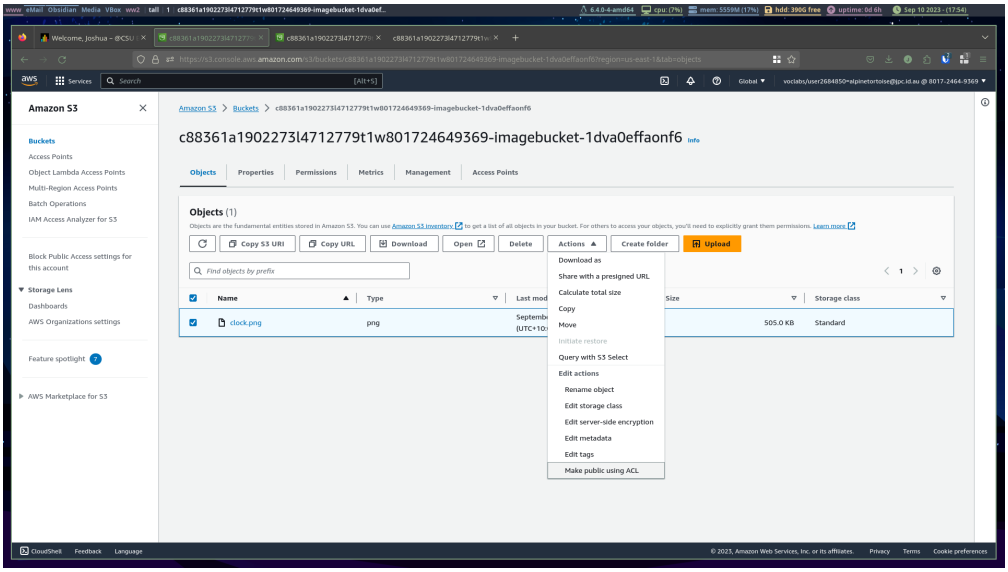

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6
c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Bucket and objects not public
Block public access (bucket settings)
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
Edit
Block all public access
On
Individual Block Public Access settings for this bucket
Bucket policy
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
Edit
Delete
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
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

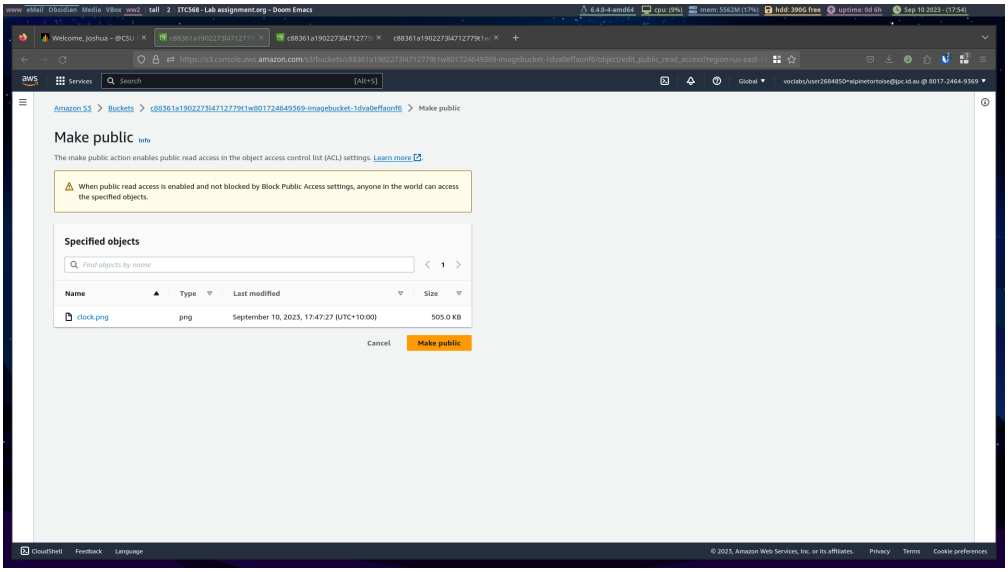

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 >
Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
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
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Cancel
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

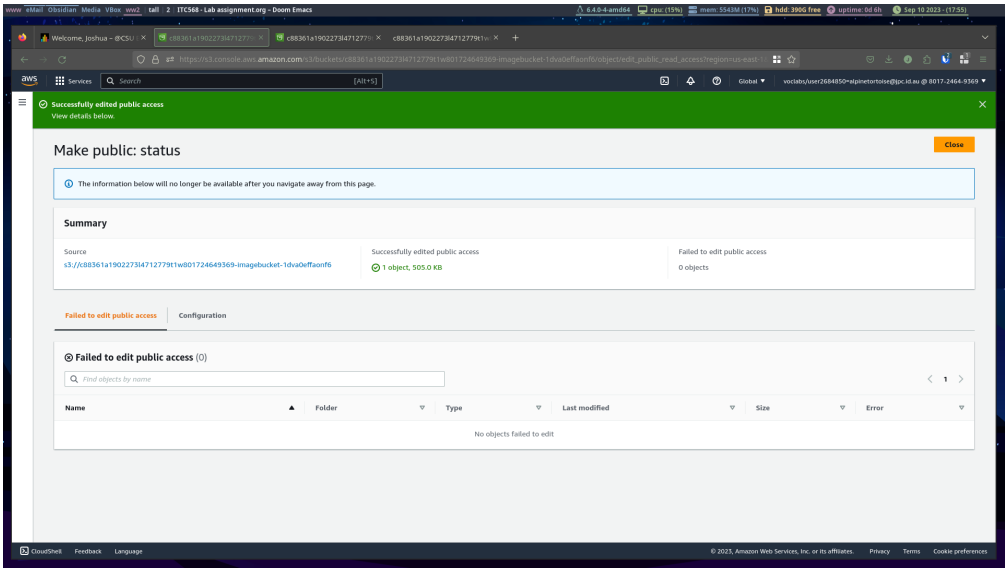

Edit Block public access (bucket settings)
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.
To confirm the settings, enter confirm in the field.
confirm
Cancel
Confirm

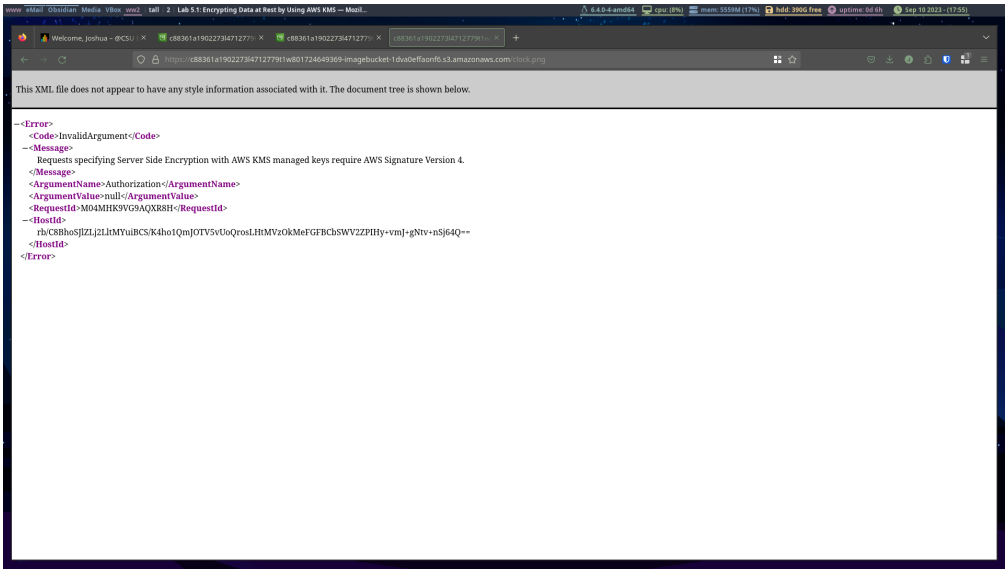

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Edit
Object Ownership
Bucket owner enforced
ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts.
This bucket has the bucket owner enforced setting applied for Object Ownership
When bucket owner enforced is applied, use bucket policies to control access.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.
I acknowledge that ACLs will be restored.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
Cancel
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

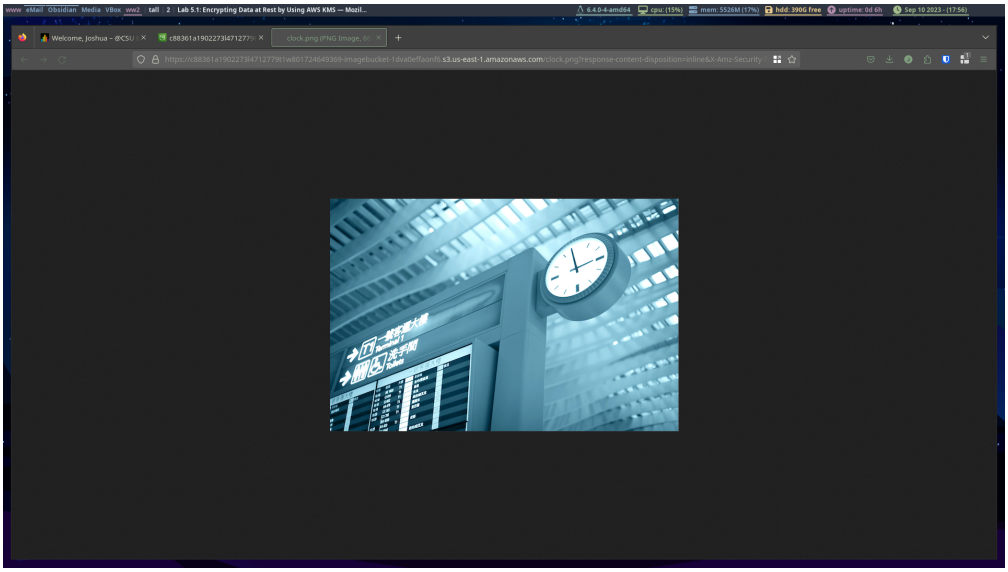

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6
c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Size
Storage class
clock.png
png
505.0 KB
Standard
Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
Edit actions
Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3 > Buckets > c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6 > Make public
Make public Info
The make public action enables public read access in the object access control list (ACL) settings. Learn more
When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.
Specified objects
Find objects by name
Name
Type
Last modified
Size
clock.png
png
September 10, 2023, 17:47:27 (UTC+10:00)
505.0 KB
Cancel
Make public


Successfully edited public access
View details below.
Make public: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Source
s3://c88361a1902273l4712779t1w801724649369-imagebucket-1dva0effaonf6
Successfully edited public access
1 object, 505.0 KB
Failed to edit public access
0 objects
Failed to edit public access
Configuration
Failed to edit public access (0)
Find objects by name
Name
Folder
Type
Last modified
Size
Error
No objects failed to edit



3.4 Task 4: Attempting signed access to the encrypted object

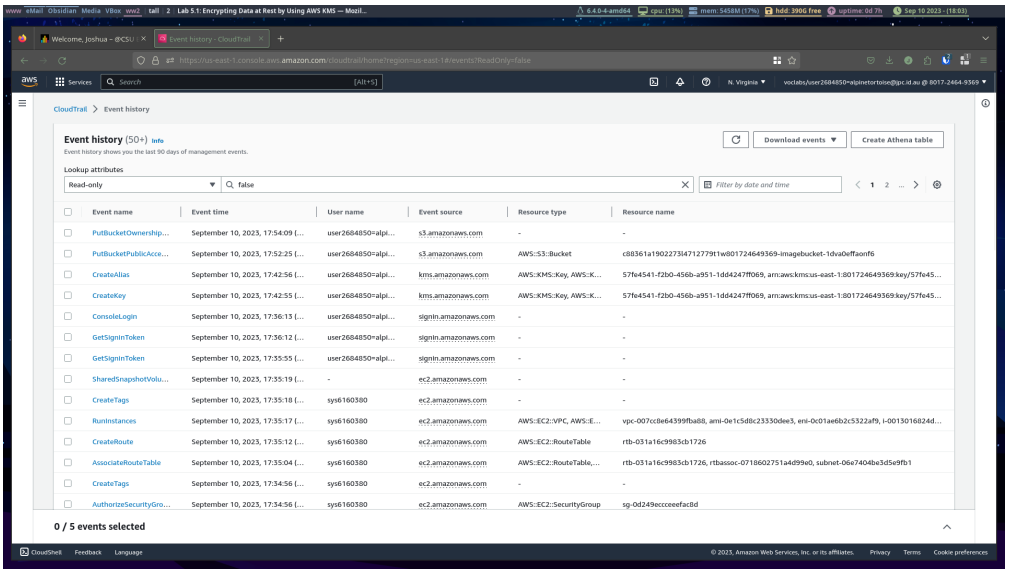


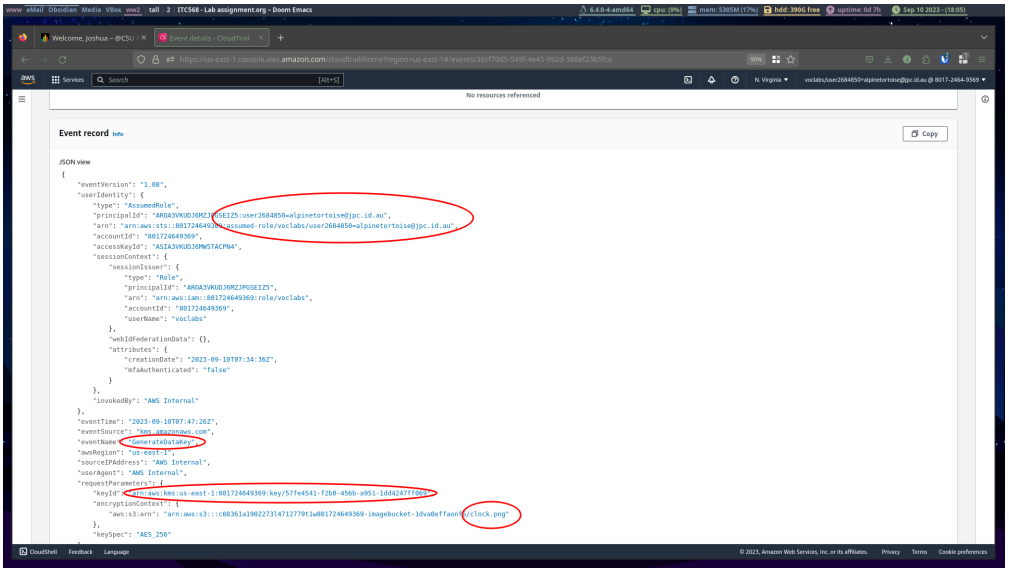
```
https://c88361a190227314712779t1w801724649369-imagebucket-1dva0effaonf6.s3.us-east-1.amazonaws.co
?
response-content-disposition=inline
&
X-Amz-Security-Token=IQoJb3JpZ2luX2VjEPj%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaDmFwLXNvdXRoZWFzdC0yIkcw
&
X-Amz-Algorithm=AWS4-HMAC-SHA256
&
X-Amz-Date=20230910T075639Z
&
```

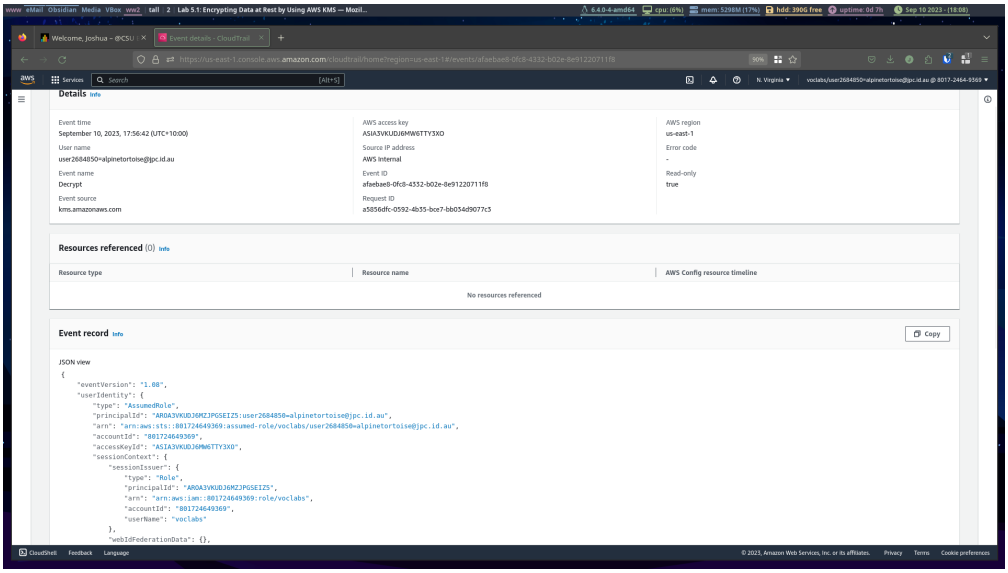
```
X-Amz-SignedHeaders=host
&
X-Amz-Expires=300
&
X-Amz-Credential=ASIA3VKUDJ6M7YLI3NMO%2F20230910%2Fus-east-1%2Fs3%2Faws4_request
&
X-Amz-Signature=608e75471c18549f541fa1578cadcf4868bae9a31c8174783925f89cccd1af23
```

We can see that opening the image file from inside the Amazon S3 console provides a number of arguments to decrypt the image.

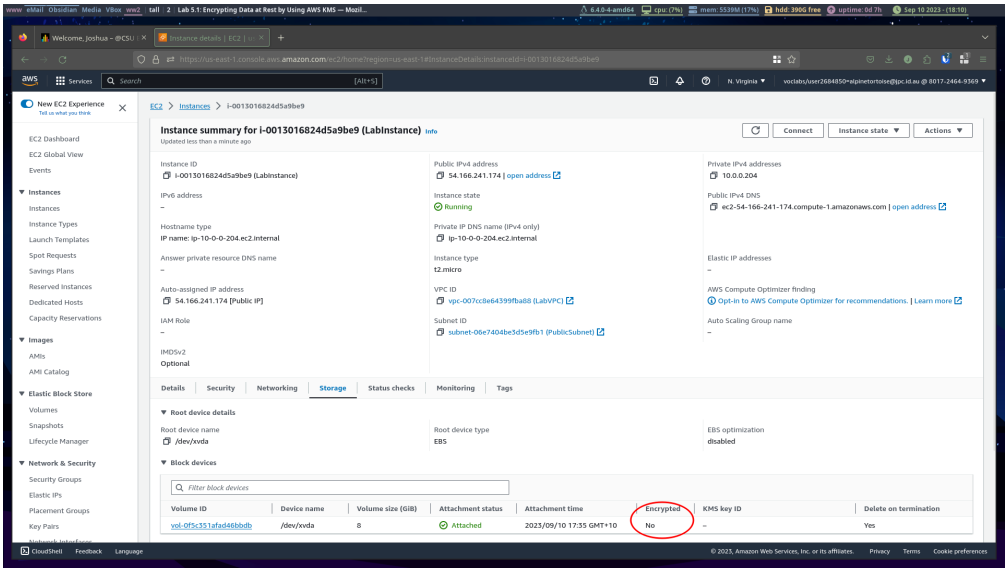
3.5 Task 5: Monitoring AWS KMS activity by using CloudTrail

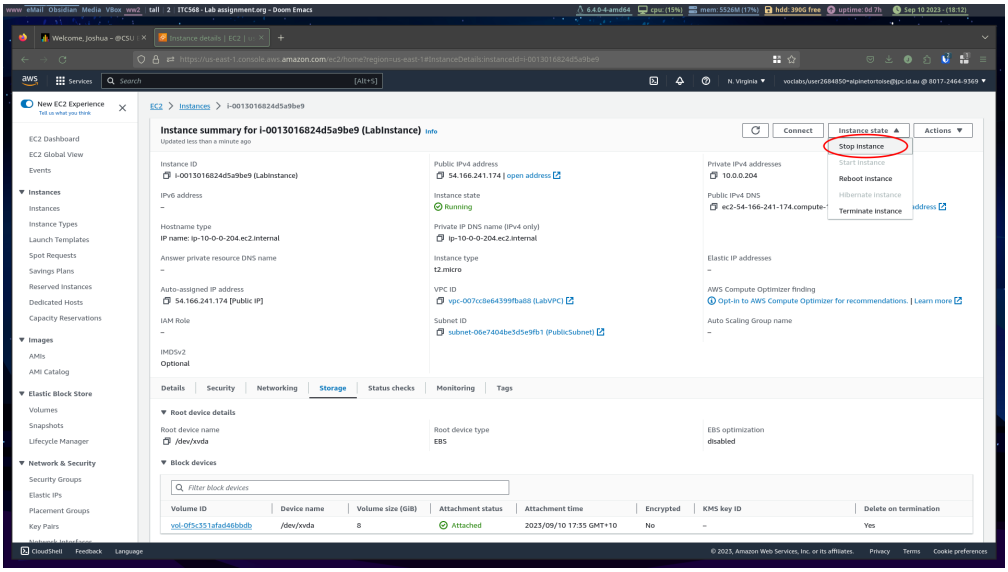


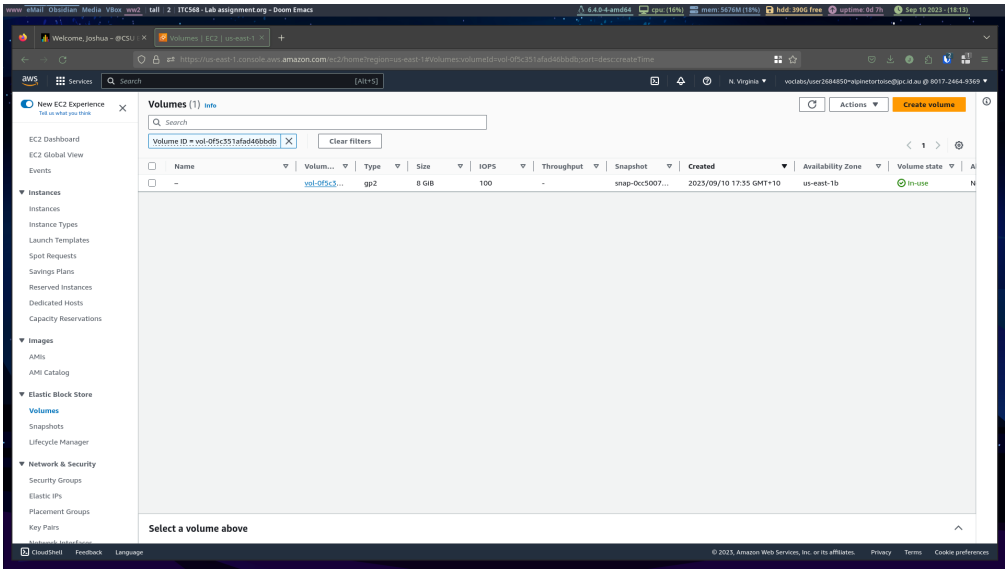




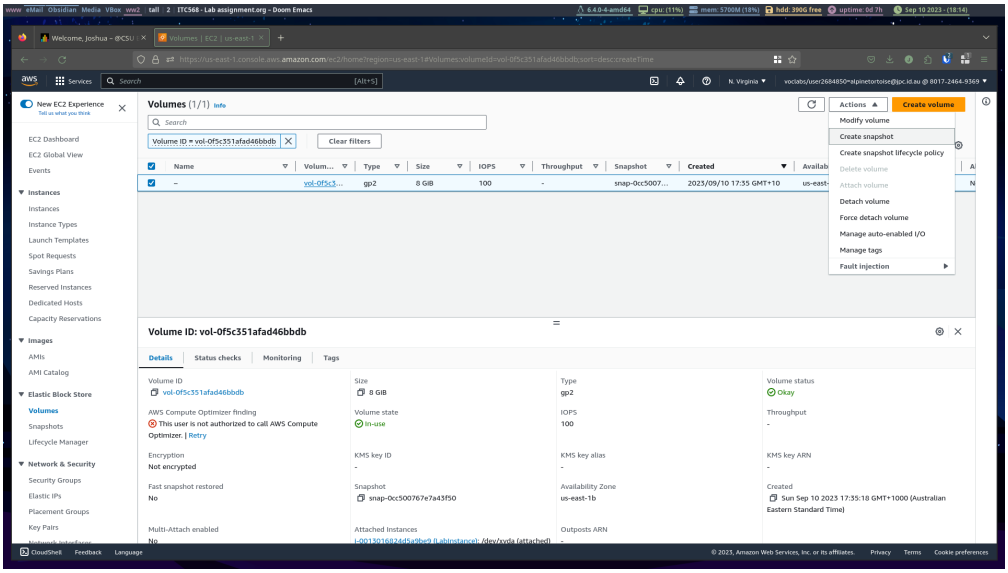
3.6 Task 6: Encrypting the root volume of an existing EC2 instance

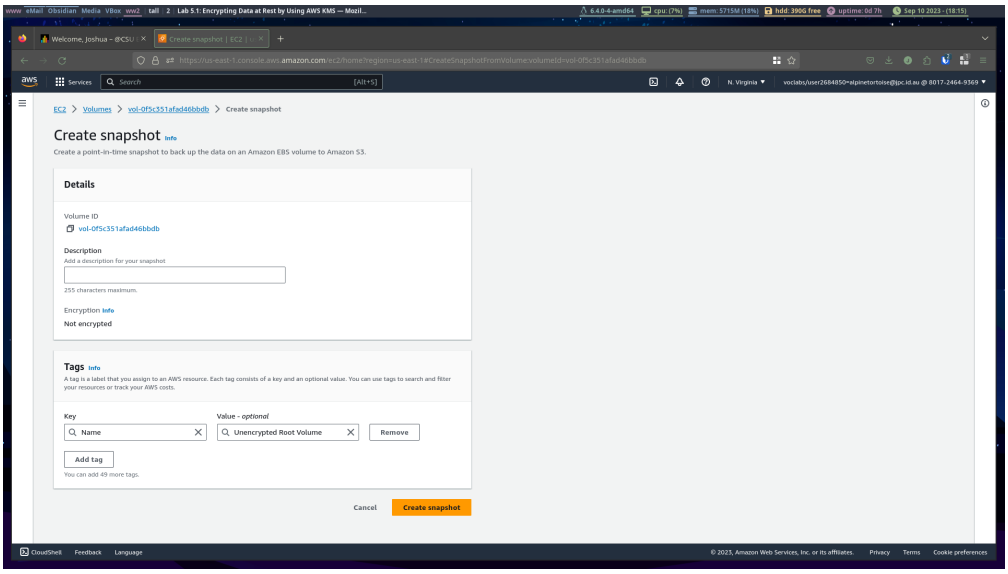


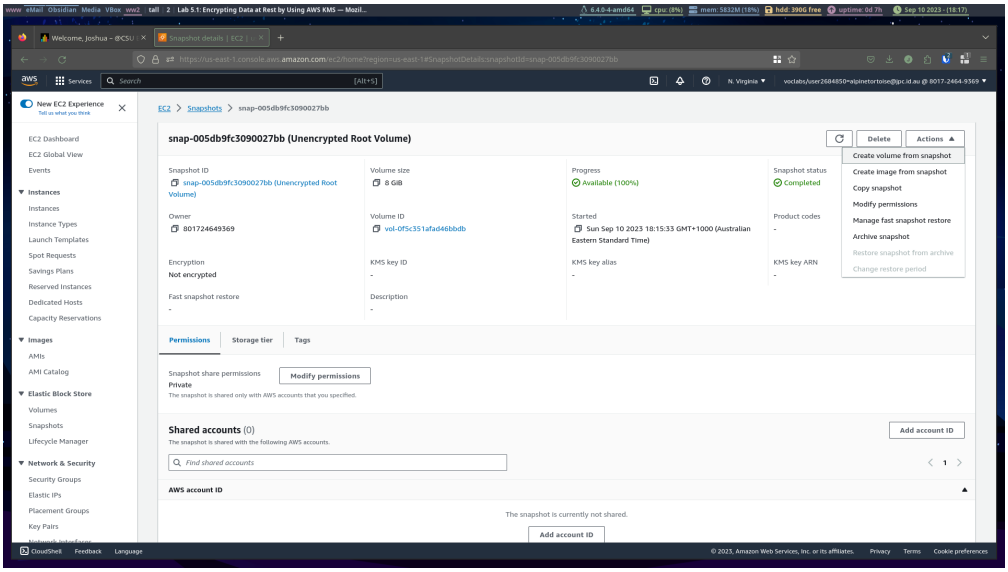


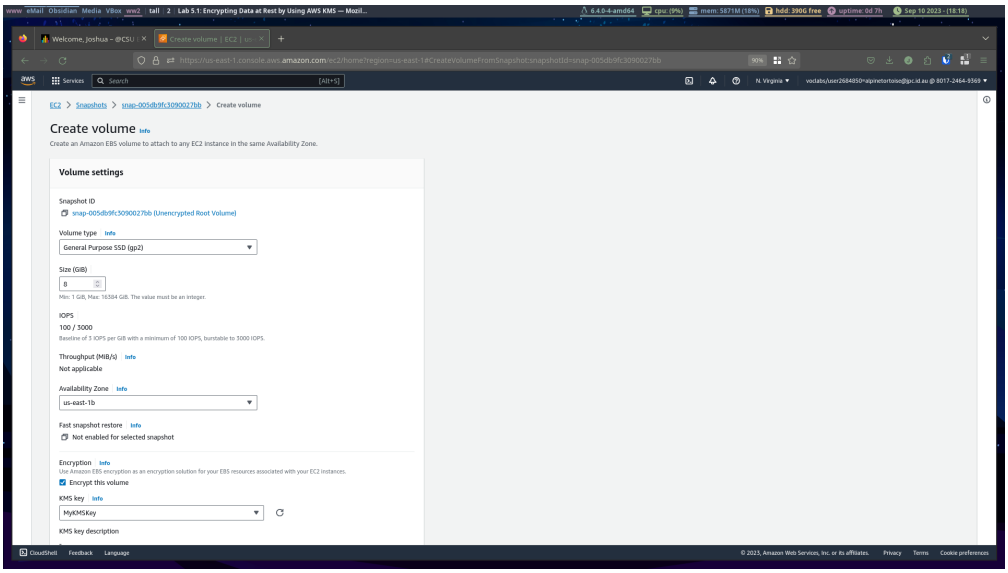


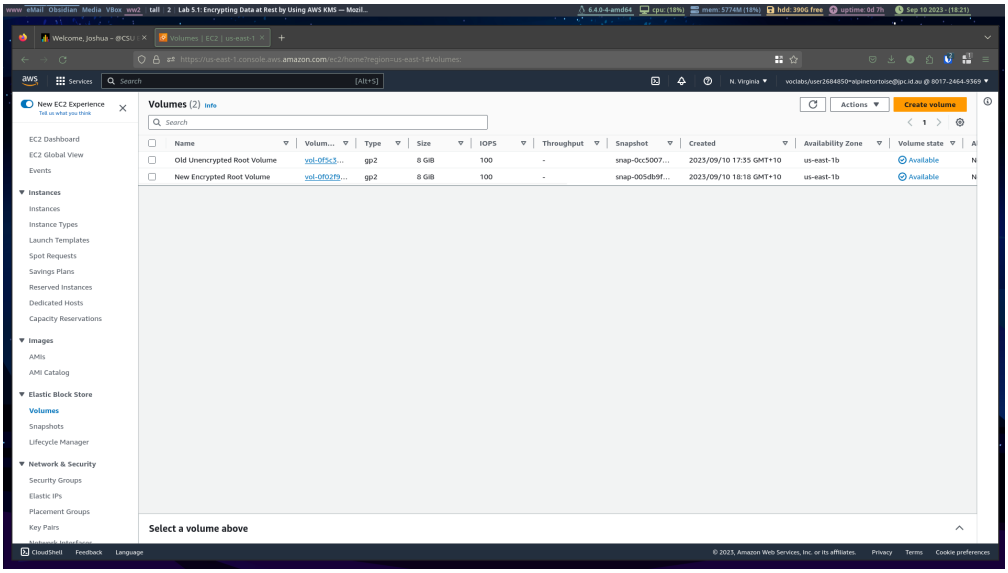
Availability Zone: us-east-1b

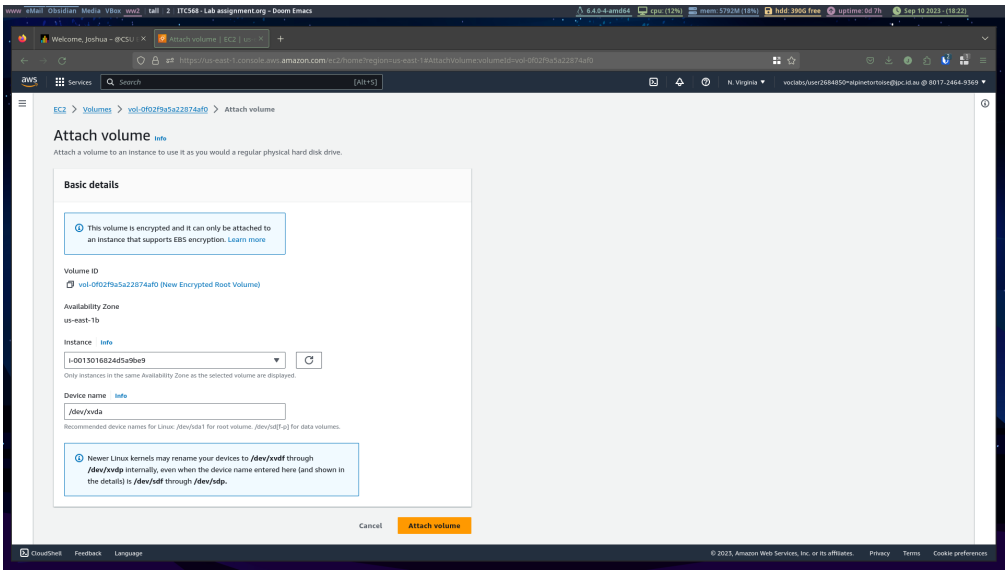

Volumes (1/1) Info
Volume ID = vol-0f5c351afad46bbdb
Clear filters
Actions
Create volume
Modify volume
Create snapshot
Create snapshot lifecycle policy
Delete volume
Attach volume
Detach volume
Force detach volume
Manage auto-enabled I/O
Manage tags
Fault injection
Volume ID: vol-0f5c351afad46bbdb
Details
Status checks
Monitoring
Tags
Volume ID
vol-0f5c351afad46bbdb
Size
8 GiB
Type
gp2
Volume status
Okay
AWS Compute Optimizer finding
This user is not authorized to call AWS Compute Optimizer. | Retry
Volume state
In-use
IOPS
100
Throughput
-
Encryption
Not encrypted
KMS key ID
-
KMS key alias
-
KMS key ARN
-
Fast snapshot restored
No
Snapshot
snap-0cc500767e7a43f50
Availability Zone
us-east-1b
Created
Sun Sep 10 2023 17:35:18 GMT+1000 (Australian Eastern Standard Time)
Multi-Attach enabled
No
Attached Instances
Outposts ARN

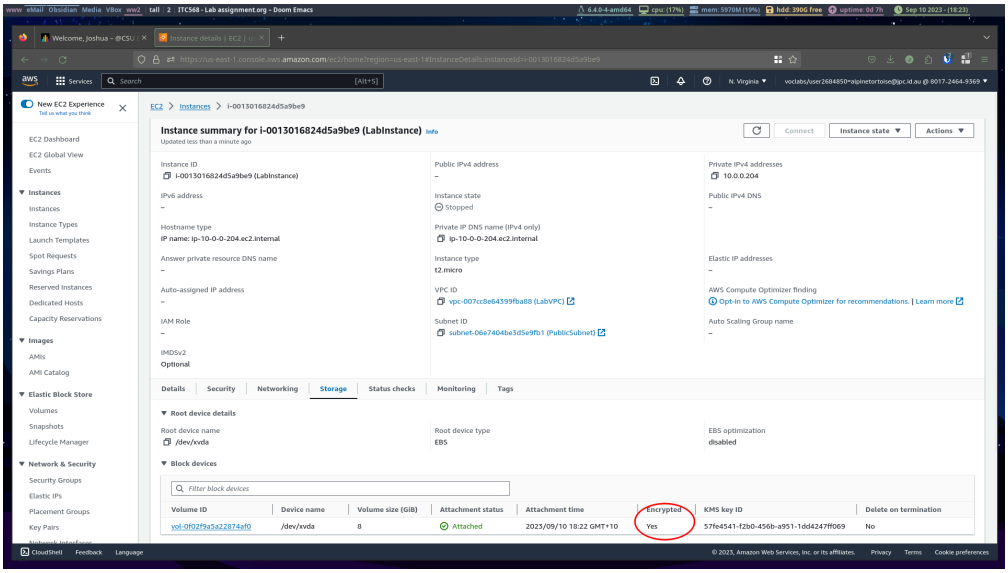

EC2 > Volumes > vol-0f5c351afad46bbdb > Create snapshot
Create snapshot Info
Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.
Details
Volume ID
vol-0f5c351afad46bbdb
Description
Add a description for your snapshot
255 characters maximum.
Encryption Info
Not encrypted
Tags Info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
Unencrypted Root Volume
Remove
Add tag
You can add 49 more tags.
Cancel
Create snapshot


Lab 5.1: Encrypting Data at Rest by Using AWS KMS — Mozil...
Snapshot details | EC2 | us-...
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SnapshotDetails:snapshotId=snap-005db9fc3090027bb
Services
Search
[Alt+S]
N. Virginia
New EC2 Experience
EC2 Dashboard
EC2 Global View
Events
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
EC2 > Snapshots > snap-005db9fc3090027bb
snap-005db9fc3090027bb (Unencrypted Root Volume)
Delete
Actions
Create volume from snapshot
Create image from snapshot
Copy snapshot
Modify permissions
Manage fast snapshot restore
Archive snapshot
Restore snapshot from archive
Change restore period
Snapshot ID
snap-005db9fc3090027bb (Unencrypted Root Volume)
Volume size
8 GiB
Progress
Available (100%)
Snapshot status
Completed
Owner
801724649369
Volume ID
vol-0f5c351afad46bbdb
Started
Sun Sep 10 2023 18:15:33 GMT+1000 (Australian Eastern Standard Time)
Product codes
Encryption
Not encrypted
KMS key ID
KMS key alias
KMS key ARN
Fast snapshot restore
Description
Permissions
Storage tier
Tags
Snapshot share permissions
Private
The snapshot is shared only with AWS accounts that you specified.
Modify permissions
Shared accounts (0)
The snapshot is shared with the following AWS accounts.
Add account ID
Find shared accounts
AWS account ID
The snapshot is currently not shared.
Add account ID
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

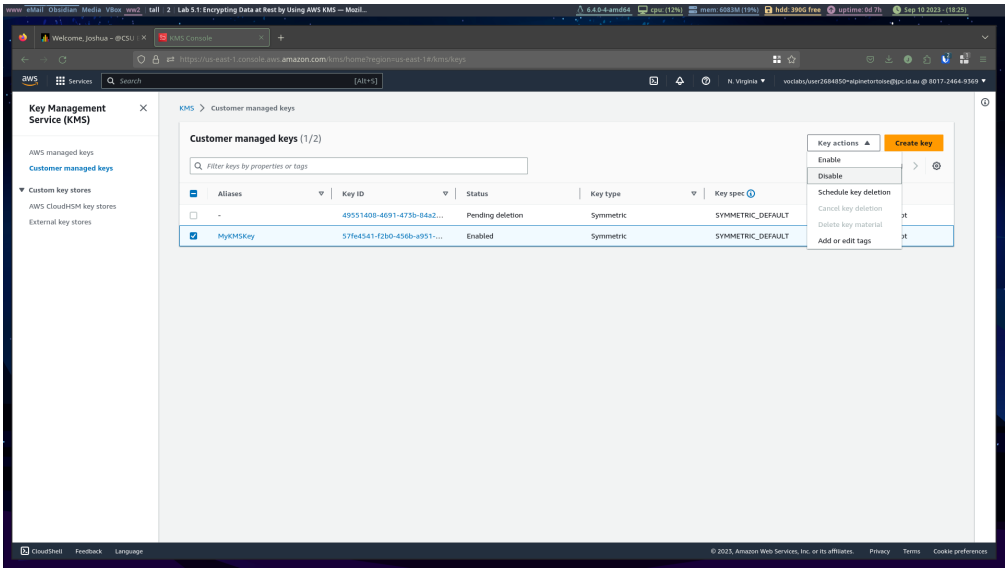

Lab 5.1: Encrypting Data at Rest by Using AWS KMS — Mozil...
Create volume | EC2 | us-...
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateVolumeFromSnapshot:snapshotId=snap-005db9fc3090027bb
Services
Search
[Alt+S]
N. Virginia
EC2 > Snapshots > snap-005db9fc3090027bb > Create volume
Create volume Info
Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.
Volume settings
Snapshot ID
snap-005db9fc3090027bb (Unencrypted Root Volume)
Volume type Info
General Purpose SSD (gp2)
Size (GiB)
8
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.
IOPS
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.
Throughput (MiB/s) Info
Not applicable
Availability Zone Info
us-east-1b
Fast snapshot restore Info
Not enabled for selected snapshot
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
KMS key Info
MyKMSKey
KMS key description
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

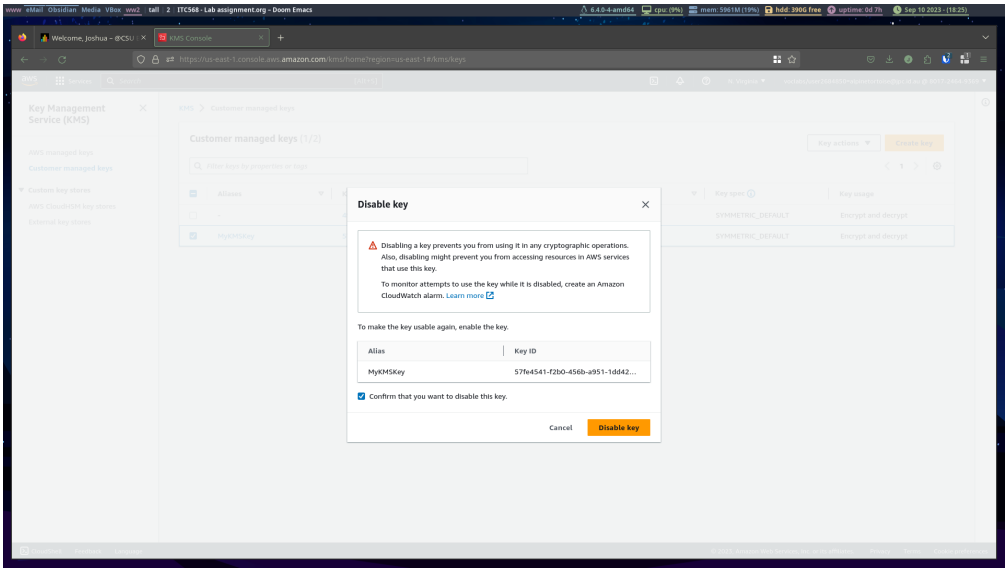

Volumes (2) Info
Actions
Create volume
Name
Volum...
Type
Size
IOPS
Throughput
Snapshot
Created
Availability Zone
Volume state
Old Unencrypted Root Volume
New Encrypted Root Volume
Select a volume above

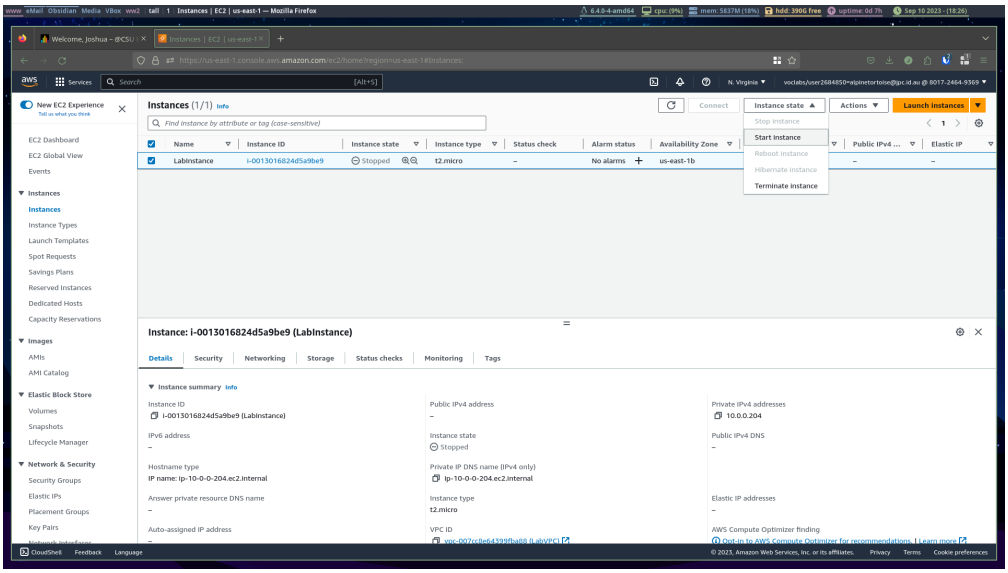

Attach volume Info
Attach a volume to an instance to use it as you would a regular physical hard disk drive.
Basic details
This volume is encrypted and it can only be attached to an instance that supports EBS encryption. Learn more
Volume ID
vol-0f02f9a5a22874af0 (New Encrypted Root Volume)
Availability Zone
us-east-1b
Instance Info
i-0013016824d5a9be9
Device name Info
/dev/xvda
Cancel
Attach volume

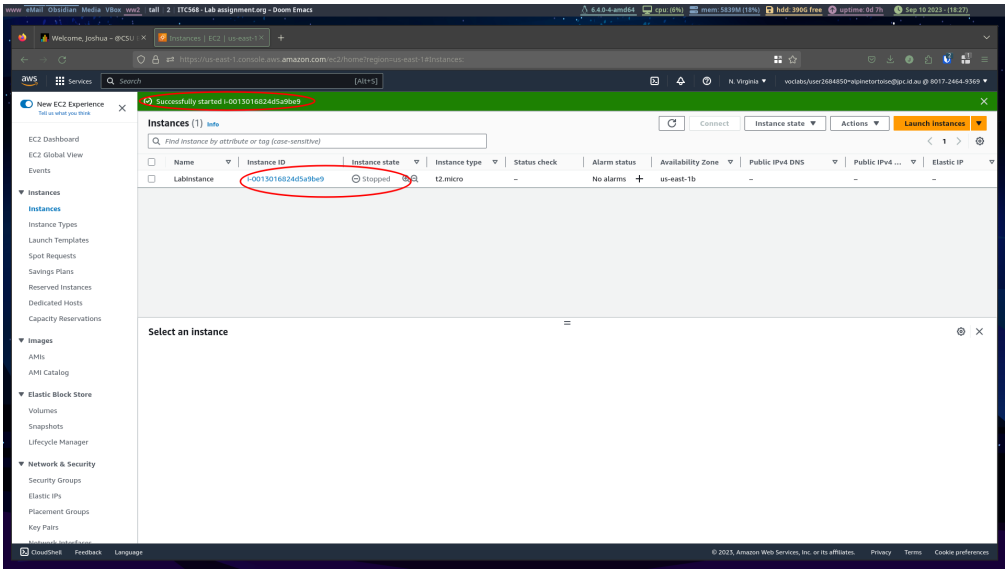


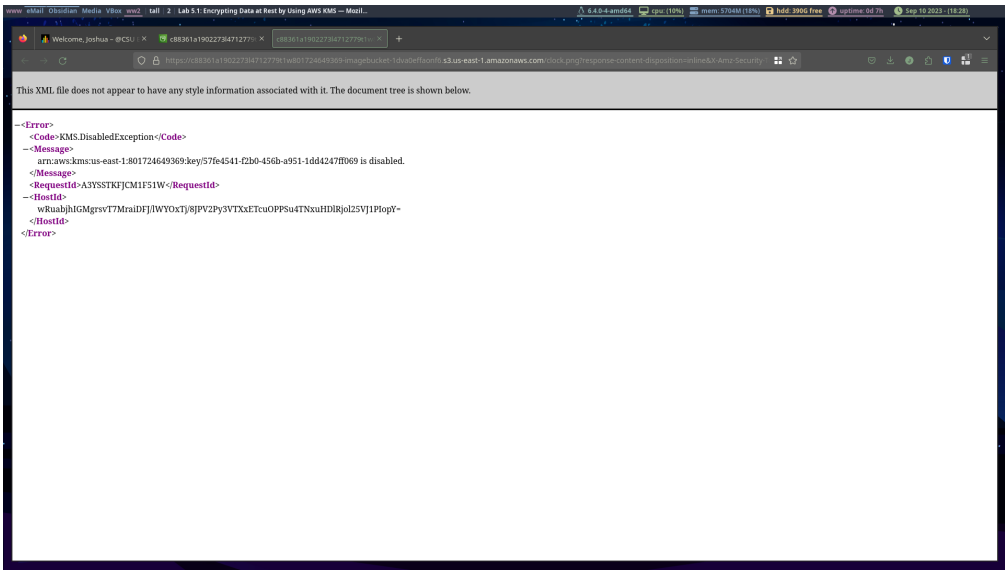
3.7 Task 7: Disabling the encryption key and observing the effects

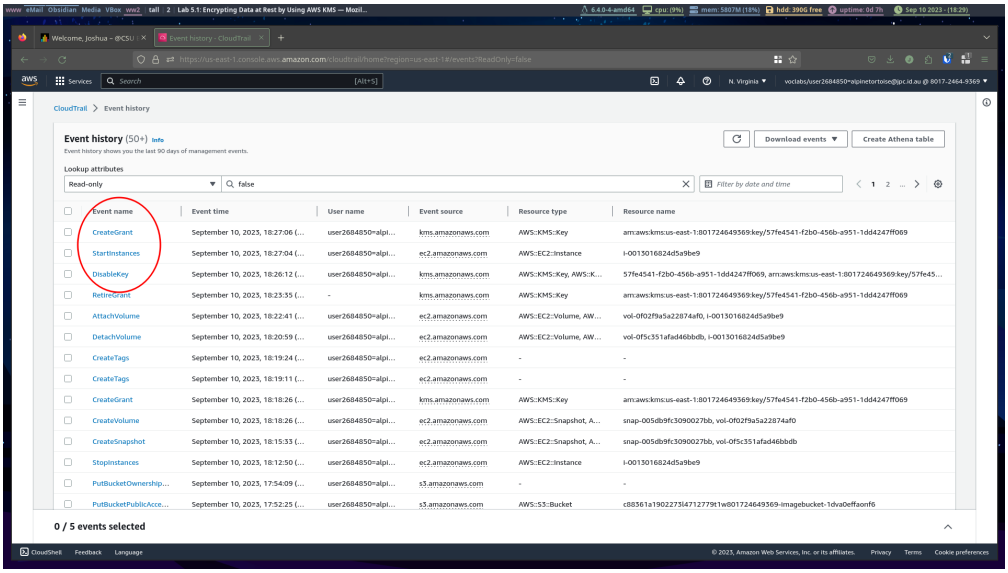



Disable key
Disabling a key prevents you from using it in any cryptographic operations. Also, disabling might prevent you from accessing resources in AWS services that use this key.
To monitor attempts to use the key while it is disabled, create an Amazon CloudWatch alarm. Learn more
To make the key usable again, enable the key.
Alias
Key ID
MyKMSKey
57fe4541-f2b0-456b-a951-1dd42...
Confirm that you want to disable this key.
Cancel
Disable key


Instances (1/1)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
LabInstance
i-0013016824d5a9be9
Stopped
t2.micro
No alarms
us-east-1b
Instance state
Actions
Launch instances
Start instance
Reboot instance
Hibernate instance
Terminate instance
Instance: i-0013016824d5a9be9 (LabInstance)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags


Successfully started i-0013016824d5a9be9
Instances (1)
Connect
Instance state
Actions
Launch instances
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
LabInstance
i-0013016824d5a9be9
Stopped
t2.micro
No alarms
us-east-1b
Select an instance


This XML file does not appear to have any style information associated with it. The document tree is shown below.
<Error>
<Code>KMS.DisabledException</Code>
<Message>
arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069 is disabled.
</Message>
<RequestId>A3YSSTKFJCM1F51W</RequestId>
<HostId>
wRuabjhIGMgrsvT7MraiDFJ/lWYOxTj/8JPV2Py3VTXxETcuOPSu4TNxuHDlRjol25VJ1PIopY=
</HostId>
</Error>



3.7.1 CloudTrail

DisableKey


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA3VKUDJ6MZJPGSEIZ5:user2684850=alpinetortoise@jpc.id.au",
        "arn": "arn:aws:sts::801724649369:assumed-role/voclabs/user2684850=alpinetortoise@jpc.id.
        "accountId": "801724649369",
        "accessKeyId": "ASIA3VKUDJ6MXXYAS74D",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA3VKUDJ6MZJPGSEIZ5",
                "arn": "arn:aws:iam::801724649369:role/voclabs",
                "accountId": "801724649369",
                "userName": "voclabs"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-10T07:34:36Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-10T08:26:12Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisableKey",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "124.183.193.175",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/117.0",
    "requestParameters": {
        "keyId": "57fe4541-f2b0-456b-a951-1dd4247ff069"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069"
    },
    "requestID": "e35eae44-8d56-4f58-af54-7315bf353658",
    "eventID": "31bfd455-eacb-4d90-a677-b285b611c396",
    "readOnly": false,
    "resources": [
        {
            "accountId": "801724649369",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "801724649369",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


StartInstances


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA3VKUDJ6MZJPGSEIZ5:user2684850=alpinetortoise@jpc.id.au",
        "arn": "arn:aws:sts::801724649369:assumed-role/voclabs/user2684850=alpinetortoise@jpc.id.
        "accountId": "801724649369",
        "accessKeyId": "ASIA3VKUDJ6M4NQSD3AI",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA3VKUDJ6MZJPGSEIZ5",
                "arn": "arn:aws:iam::801724649369:role/voclabs",
                "accountId": "801724649369",
                "userName": "voclabs"
            },
            "webIdFederationData": {},
            "attributes": {
```

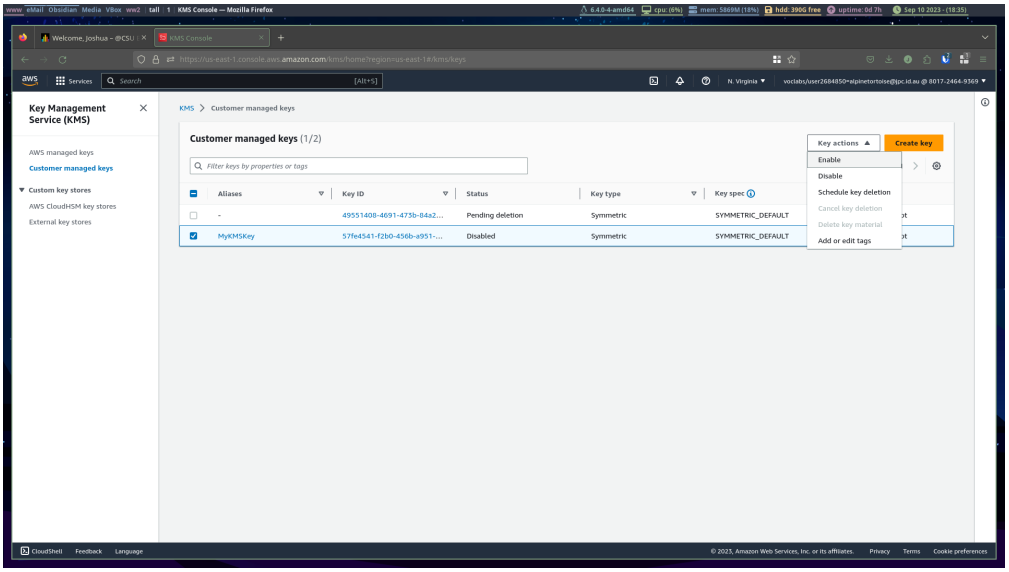
```
                "creationDate": "2023-09-10T07:34:36Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-10T08:27:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "124.183.193.175",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-0013016824d5a9be9"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "3892c780-f10e-4976-ab8a-78033b663a81",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-0013016824d5a9be9",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "3892c780-f10e-4976-ab8a-78033b663a81",
    "eventID": "81018f73-3cf4-4add-bdb7-7ba1e4f2250d",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "801724649369",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

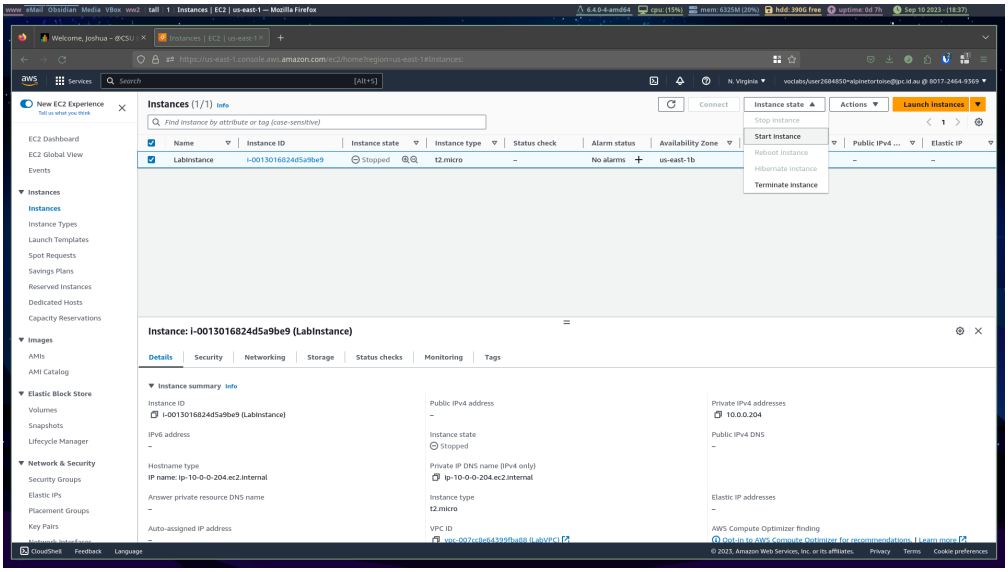

CreateGrant

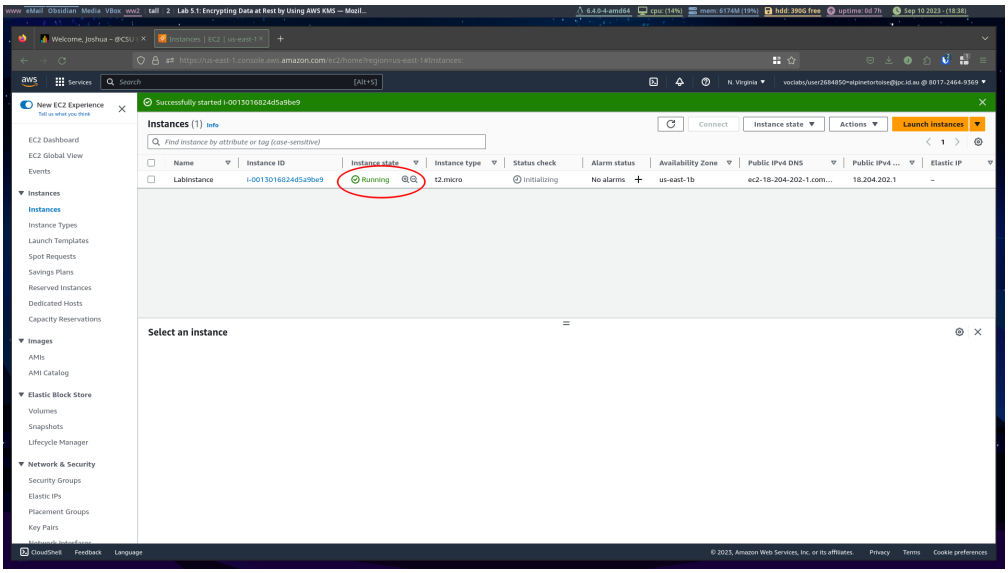
```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA3VKUDJ6MZJPGSEIZ5:user2684850=alpinetortoise@jpc.id.au",
        "arn": "arn:aws:sts::801724649369:assumed-role/voclabs/user2684850=alpinetortoise@jpc.id.
        "accountId": "801724649369",
        "accessKeyId": "ASIA3VKUDJ6MU7RVY4O7",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA3VKUDJ6MZJPGSEIZ5",
                "arn": "arn:aws:iam::801724649369:role/voclabs",
                "accountId": "801724649369",
                "userName": "voclabs"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-10T07:34:36Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "ec2-frontend-api.amazonaws.com"
    },
    "eventTime": "2023-09-10T08:27:06Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "ec2-frontend-api.amazonaws.com",
    "userAgent": "AWS Internal",
    "errorCode": "DisabledException",
    "errorMessage": "arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069
    "requestParameters": {
        "granteePrincipal": "arn:aws:sts::801724649369:assumed-role/aws:ec2-infrastructure/i-0013
        "retiringPrincipal": "ec2.us-east-1.amazonaws.com",
        "keyId": "arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069",
        "constraints": {
            "encryptionContextSubset": {
                "aws:ebs:id": "vol-0f02f9a5a22874af0"
            }
        },
        "operations": [
            "Decrypt"
        ]
    },
    "responseElements": null,
    "requestID": "3892c780-f10e-4976-ab8a-78033b663a81",
    "eventID": "8baca37e-4128-4779-9ea7-6f6780477431",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "801724649369",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:801724649369:key/57fe4541-f2b0-456b-a951-1dd4247ff069"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "801724649369",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

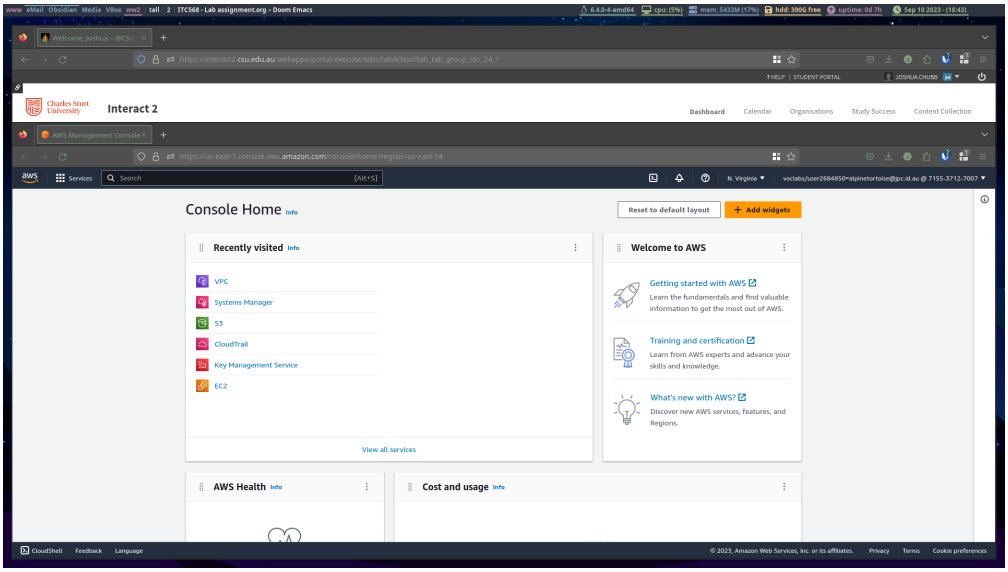

We can see in the CreateGrant event that EC2 attempted to decrypt the new volume for the instance to initialize.



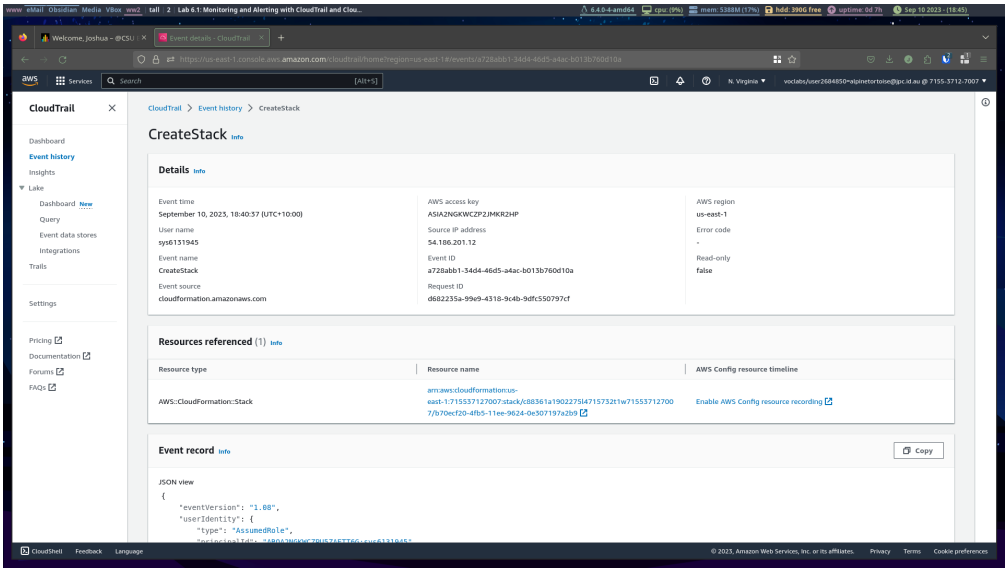

Instances (1/1) Info
Instance state
Actions
Launch instances
Start instance
Stop instance
Reboot instance
Hibernate instance
Terminate instance
Instance: i-0013016824d5a9be9 (LabInstance)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags

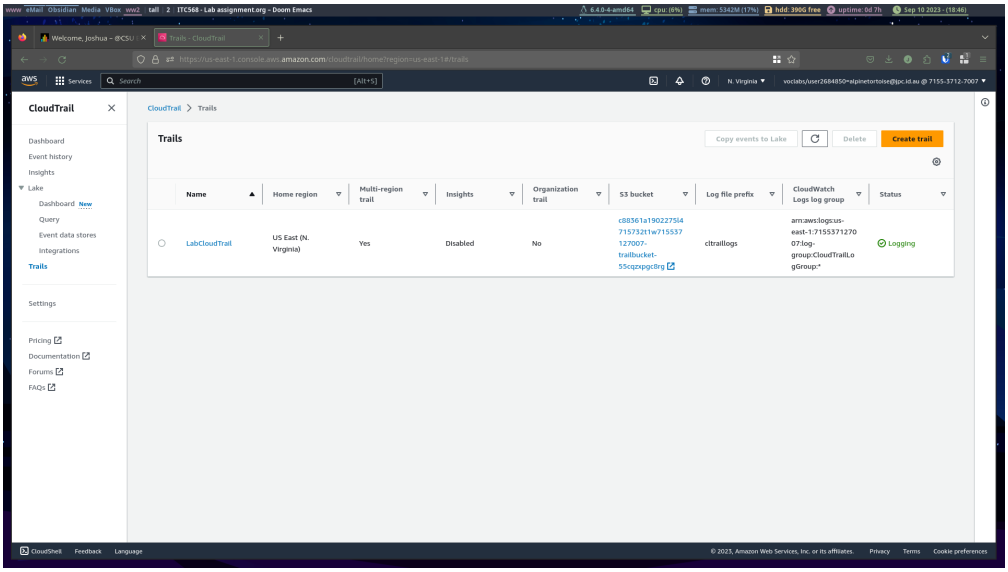

Successfully started i-0013016824d5a9be9
Instances (1) Info
Running
Initializing
Select an instance

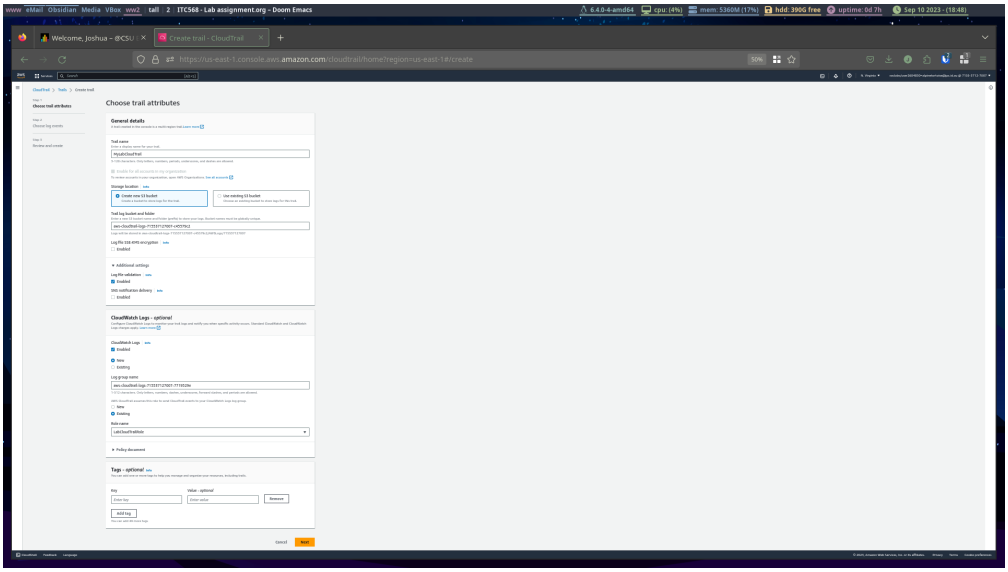
4 Lab 6.1: Monitoring and Alerting with CloudTrail and CloudWatch

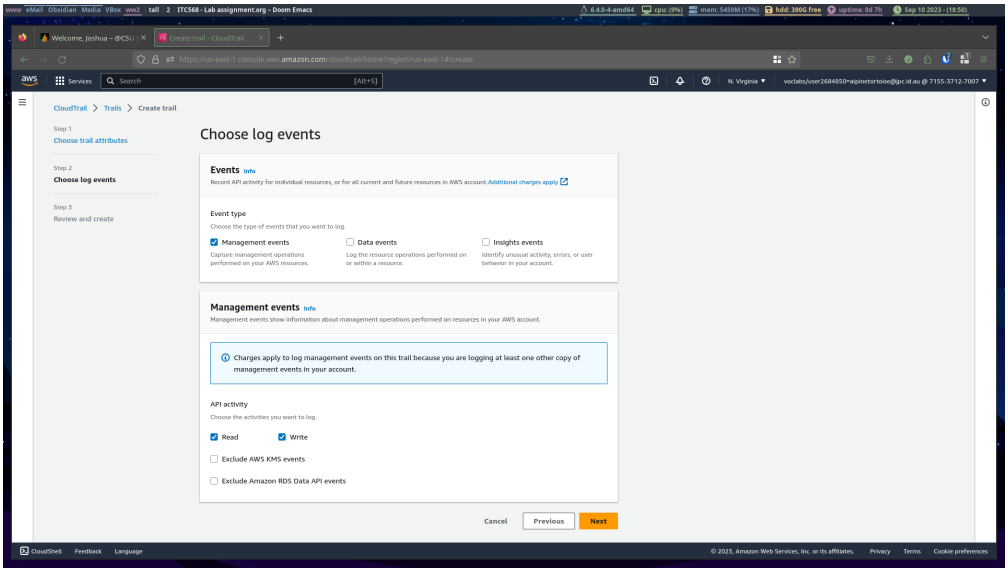


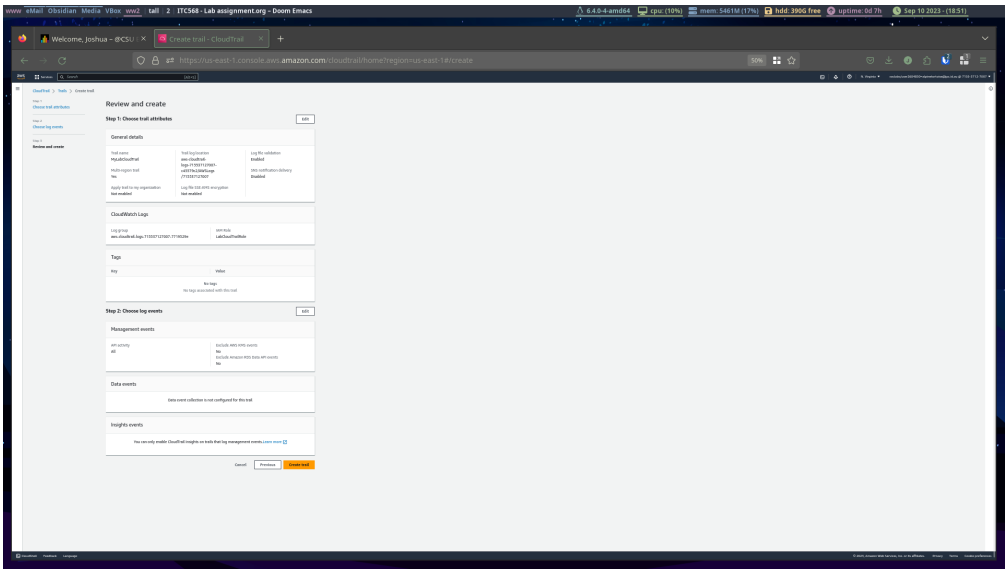
4.1 Task 1: Creating a CloudTrail trail with CloudWatch Logs enabled

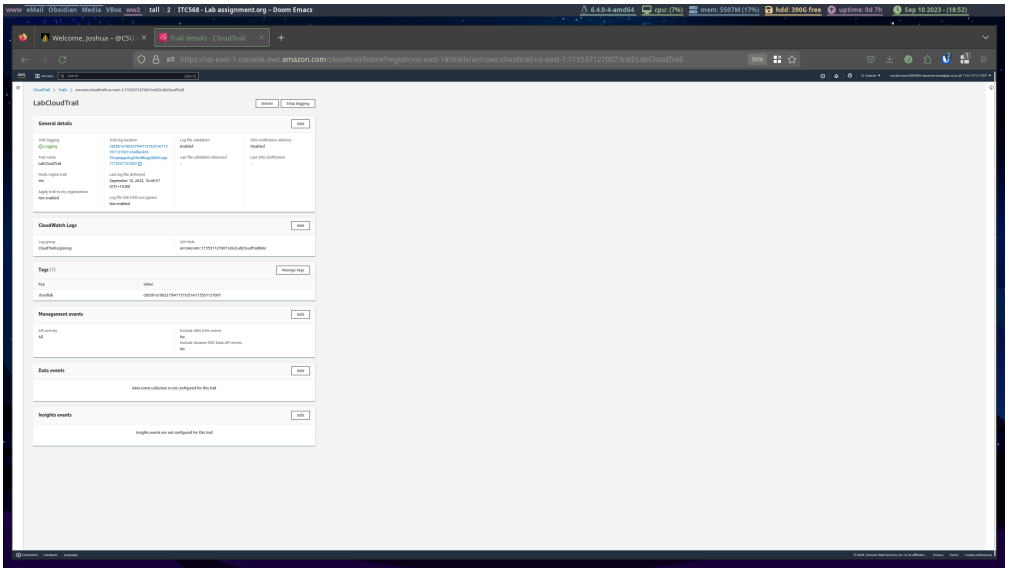



CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Trails
Trails
Copy events to Lake
Delete
Create trail
Name
Home region
Multi-region trail
Insights
Organization trail
S3 bucket
Log file prefix
CloudWatch Logs log group
Status
LabCloudTrail
US East (N. Virginia)
Yes
Disabled
No
c88361a190227514715732t1w715537127007-traillbucket-55cqzxpgc8rg
citraillogs
arn:aws:logs:us-east-1:715537127007:log-group:CloudTrailLogGroup:*
Logging
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

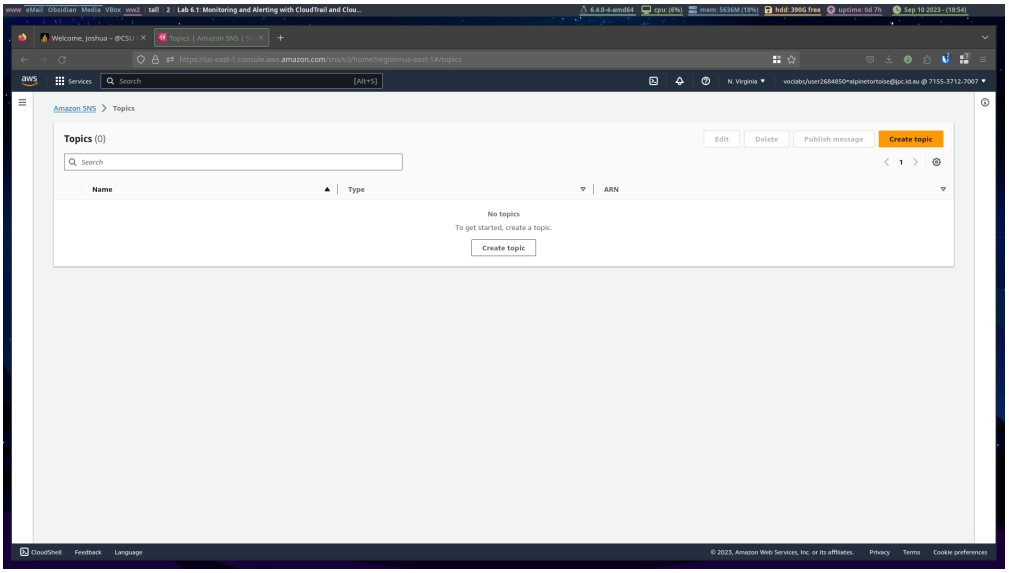

Choose trail attributes
General details
Trail name
MyLabCloudTrail
Storage location
Create new S3 bucket
Use existing S3 bucket
Trail log bucket and folder
aws-cloudtrail-logs-715537127007-e9557f12
Log file SSE-KMS encryption
Enabled
Additional settings
Log file validation
Enabled
SNS notification delivery
Enabled
CloudWatch Logs - optional
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more
CloudWatch Logs
Enabled
New
Existing
Log group name
aws-cloudtrail-logs-715537127007-7f1852ba
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.
AWS CloudTrail automatically creates a new CloudTrail-enable log group.
New
Existing
Role name
LabCloudTrailRole
Policy document
Tags - optional
You can add one or more tags to help you manage and organize your resources, including trails.
Key
Enter Key
Value - optional
Enter value
Remove
Add tag
You can add 50 more tags.
Cancel
Next

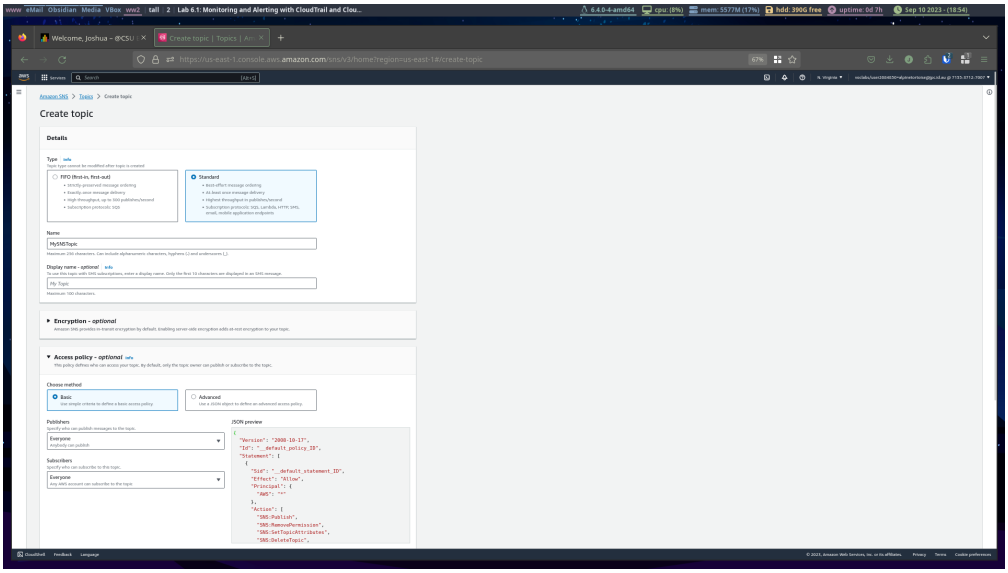

Create trail - CloudTrail
https://us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
CloudTrail > Trails > Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Choose log events
Events Info
Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply
Event type
Choose the type of events that you want to log.
Management events
Capture management operations performed on your AWS resources.
Data events
Log the resource operations performed on or within a resource.
Insights events
Identify unusual activity, errors, or user behavior in your account.
Management events Info
Management events show information about management operations performed on resources in your AWS account.
Charges apply to log management events on this trail because you are logging at least one other copy of management events in your account.
API activity
Choose the activities you want to log.
Read
Write
Exclude AWS KMS events
Exclude Amazon RDS Data API events
Cancel
Previous
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

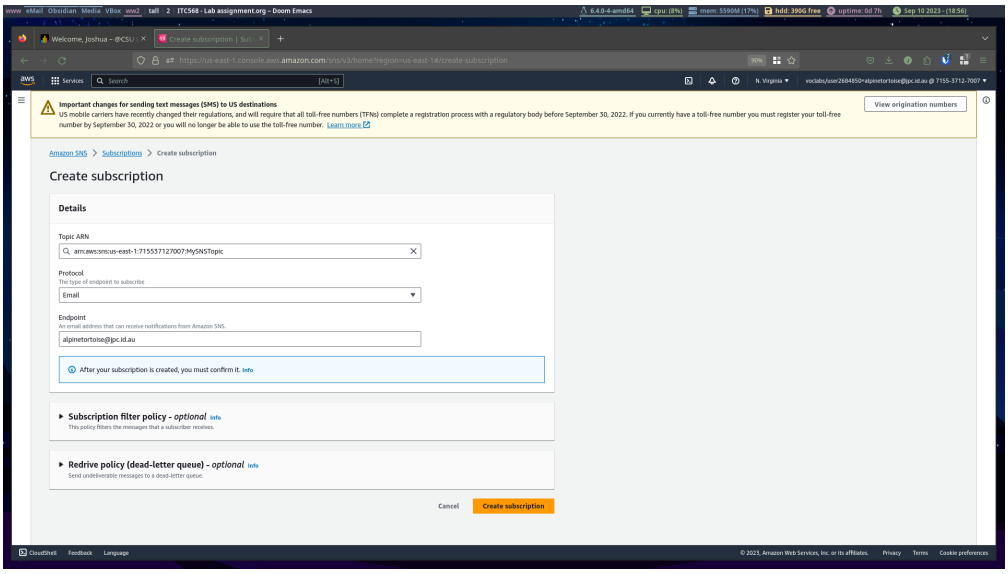

Create trail - CloudTrail
Review and create
Step 1: Choose trail attributes
Edit
General details
CloudWatch Logs
Tags
Step 2: Choose log events
Edit
Management events
Data events
Insights events
Cancel
Previous
Create trail

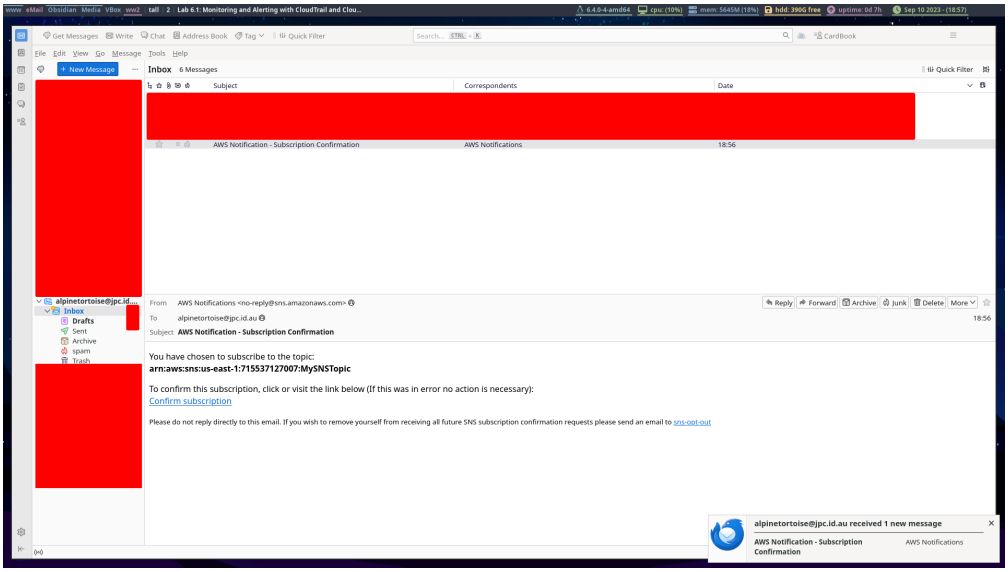


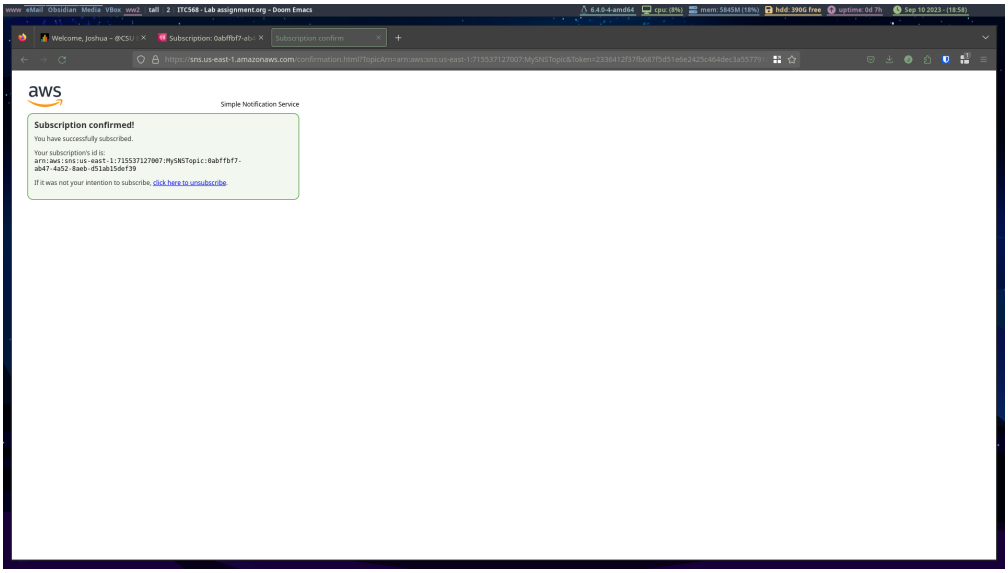
4.2 Task 2: Creating an SNS topic and subscribing to it



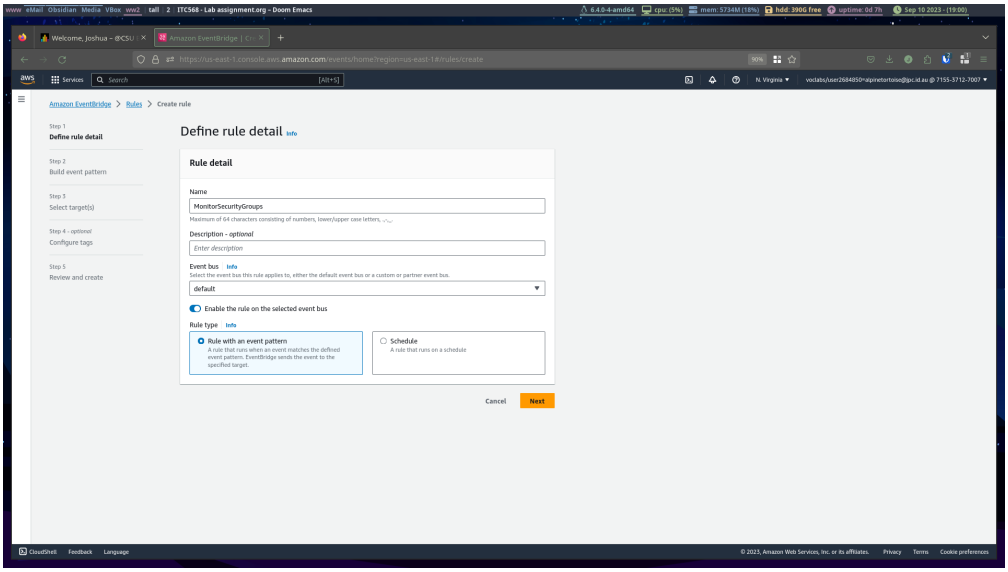

Create topic
Details
Type
FIFO (first-in, first-out)
Standard
Name
MySNSTopic
Display name - optional
My Topic
Encryption - optional
Access policy - optional
Choose method
Basic
Advanced
Publishers
Everyone
Subscribers
Everyone
JSON preview

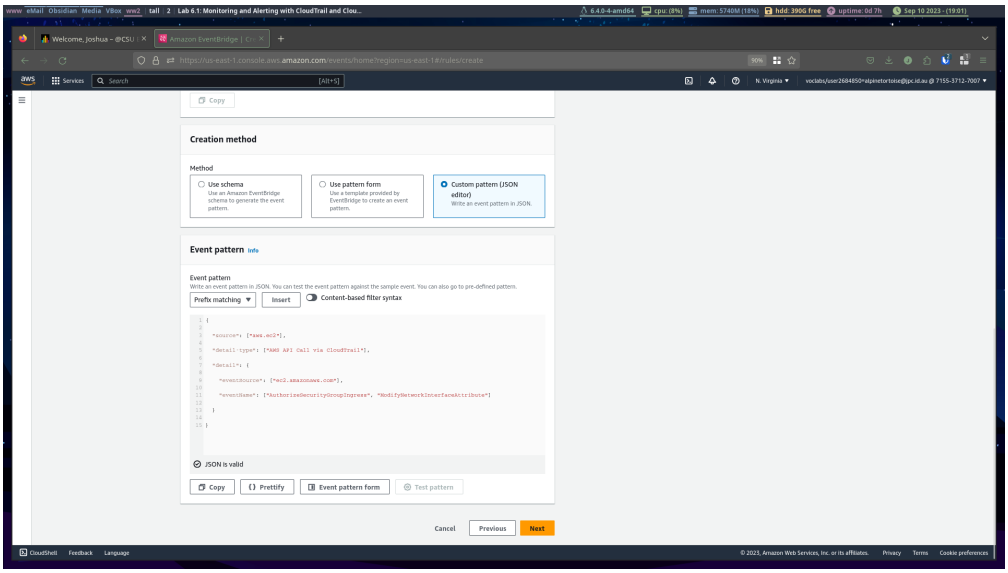

Important changes for sending text messages (SMS) to US destinations
US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. Learn more
View origination numbers
Amazon SNS > Subscriptions > Create subscription
Create subscription
Details
Topic ARN
arn:aws:sns:us-east-1:715557127007:MySNSTopic
Protocol
The type of endpoint to subscribe
Email
Endpoint
An email address that can receive notifications from Amazon SNS.
alpinetortoise@jpc.id.au
After your subscription is created, you must confirm it. Info
Subscription filter policy - optional Info
This policy filters the messages that a subscriber receives.
Redrive policy (dead-letter queue) - optional Info
Send undeliverable messages to a dead-letter queue.
Cancel
Create subscription

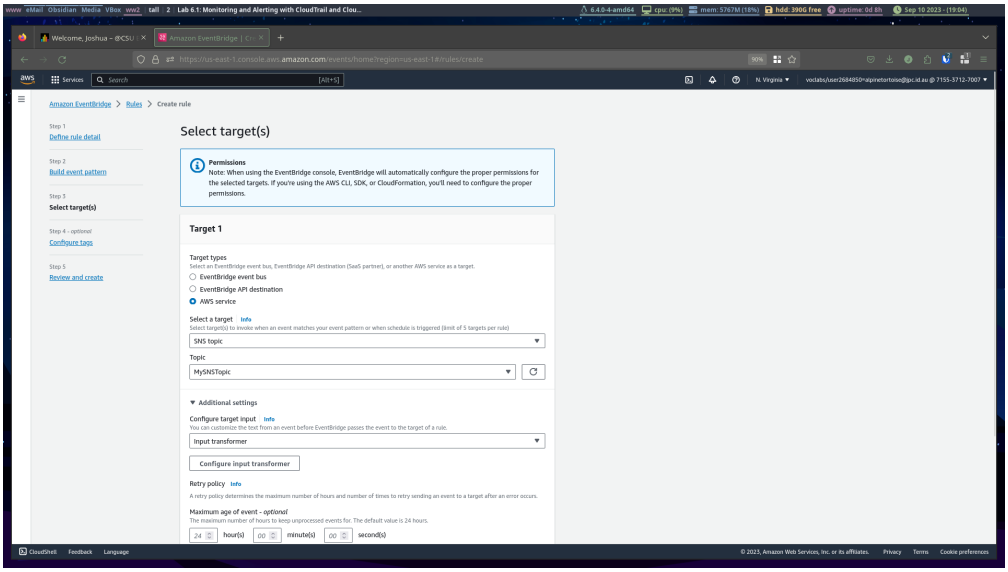

Inbox 6 Messages
Subject
Correspondents
Date
AWS Notification - Subscription Confirmation
AWS Notifications
18:56
From AWS Notifications <no-reply@sns.amazonaws.com>
To alpinetortoise@jpc.id.au
Subject AWS Notification - Subscription Confirmation
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:715537127007:MySNSTopic
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out
alpinetortoise@jpc.id.au received 1 new message
AWS Notification - Subscription Confirmation
AWS Notifications

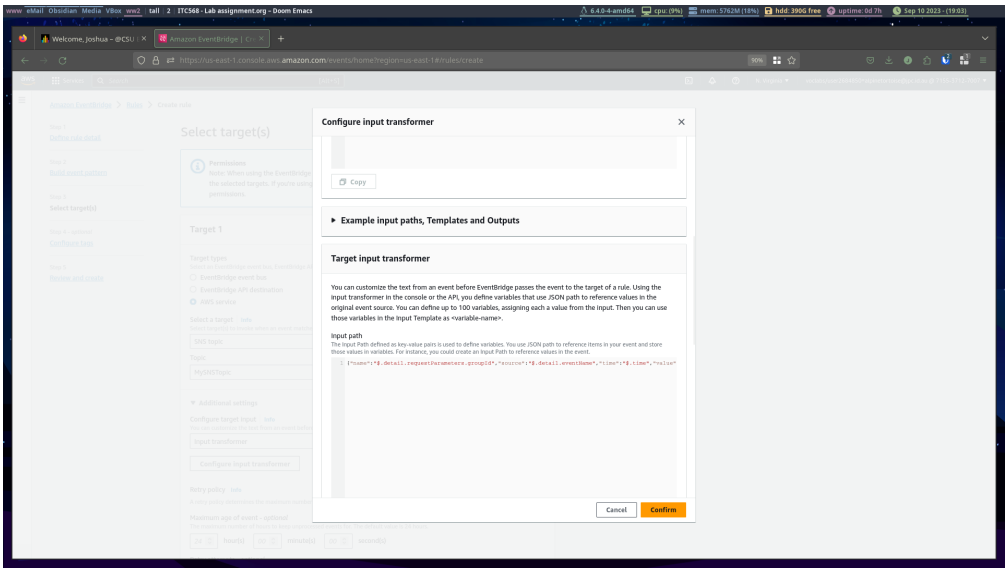

aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:us-east-1:715537127007:MySNSTopic:0abffbf7-ab47-4a52-8aeb-d51ab15def39
If it was not your intention to subscribe, click here to unsubscribe.

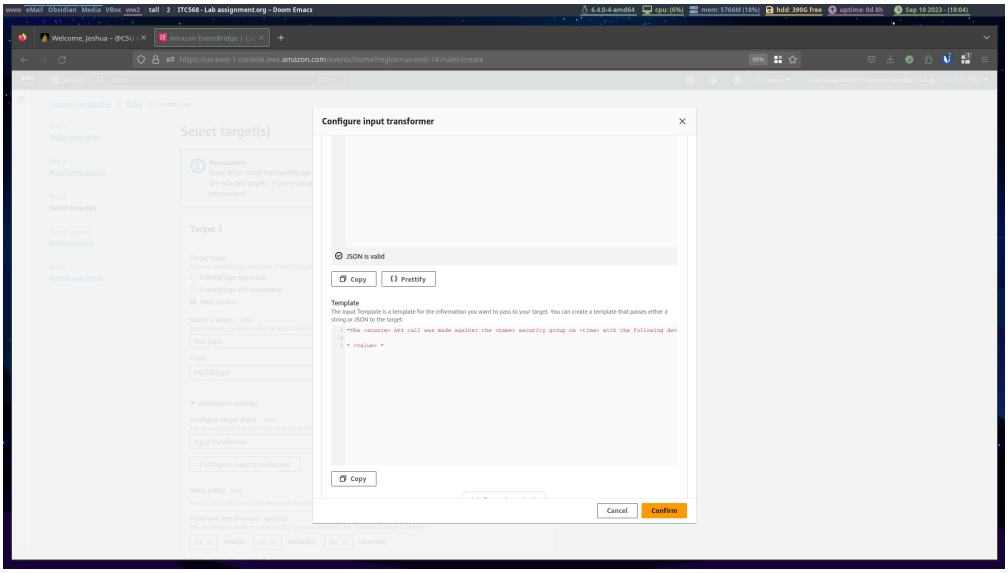
4.3 Task 3: Creating an EventBridge rule to monitor security groups

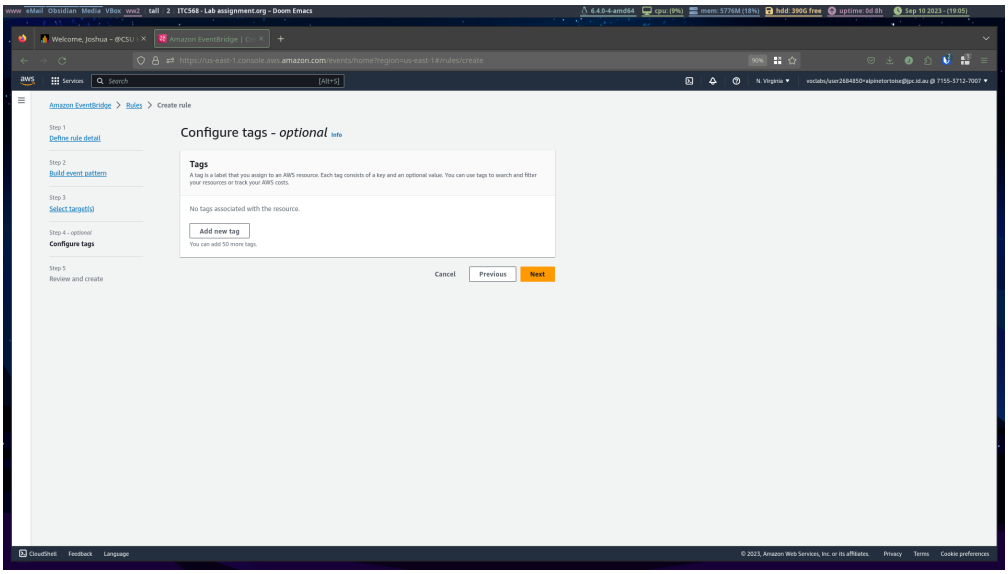


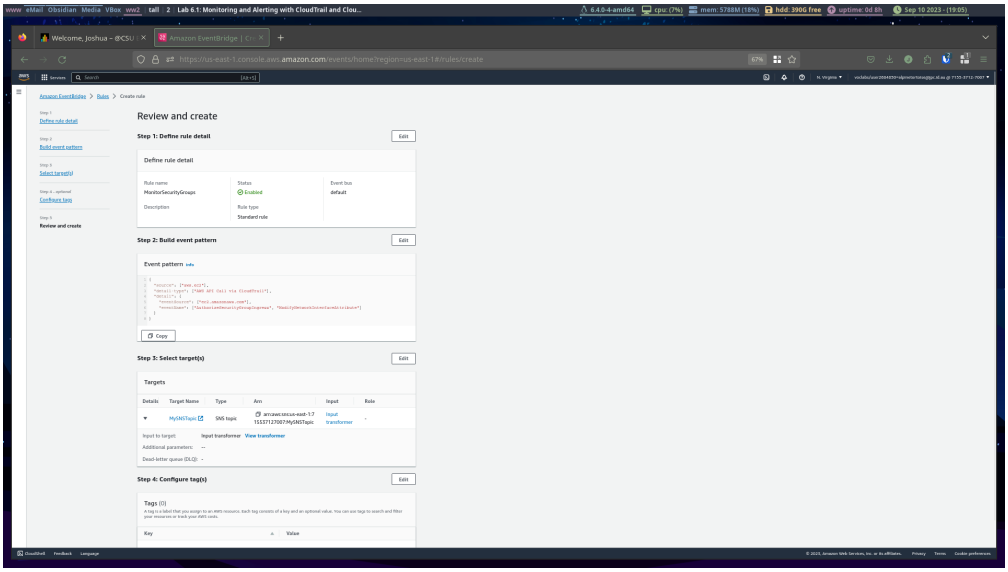


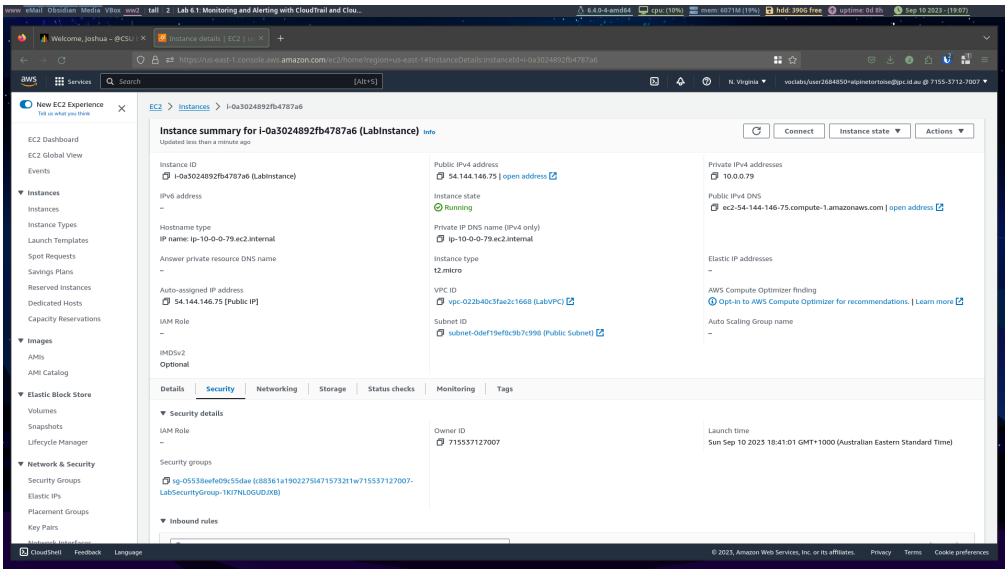

Amazon EventBridge > Rules > Create rule
Select target(s)
Permissions
Target 1
Target types
EventBridge event bus
EventBridge API destination
AWS service
Select a target
SNS topic
Topic
MySNSTopic
Additional settings
Configure target input
Input transformer
Configure input transformer
Retry policy
Maximum age of event - optional
24 hour(s) 00 minute(s) 00 second(s)

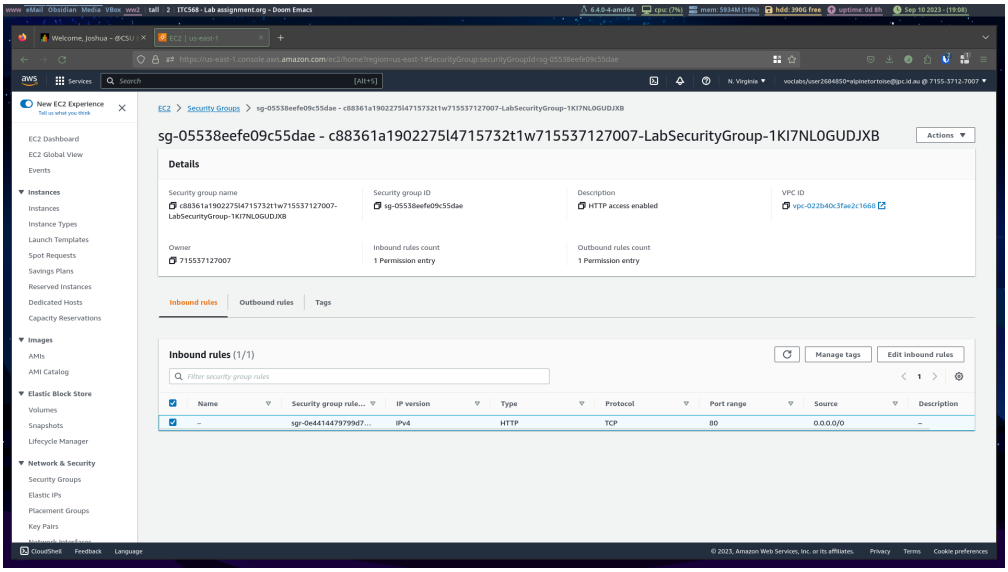

Configure input transformer
Copy
Example input paths, Templates and Outputs
Target input transformer
You can customize the text from an event before EventBridge passes the event to the target of a rule. Using the input transformer in the console or the API, you define variables that use JSON path to reference values in the original event source. You can define up to 100 variables, assigning each a value from the input. Then you can use those variables in the Input Template as <variable-name>.
Input path
The input Path defined as key-value pairs is used to define variables. You use JSON path to reference items in your event and store those values in variables. For instance, you could create an Input Path to reference values in the event.
Cancel
Confirm

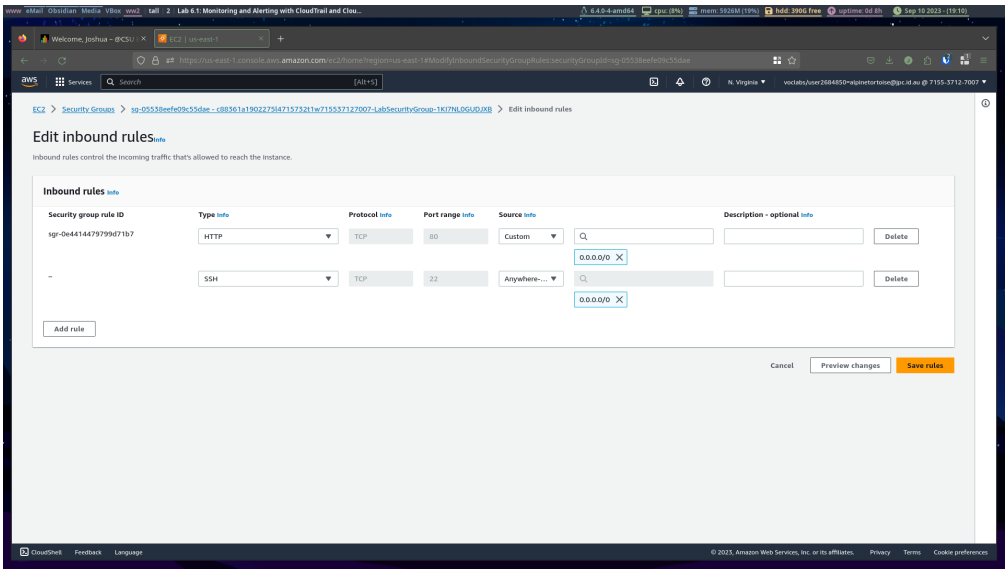

Configure input transformer
JSON is valid
Copy
Prettify
Template
Copy
Cancel
Confirm

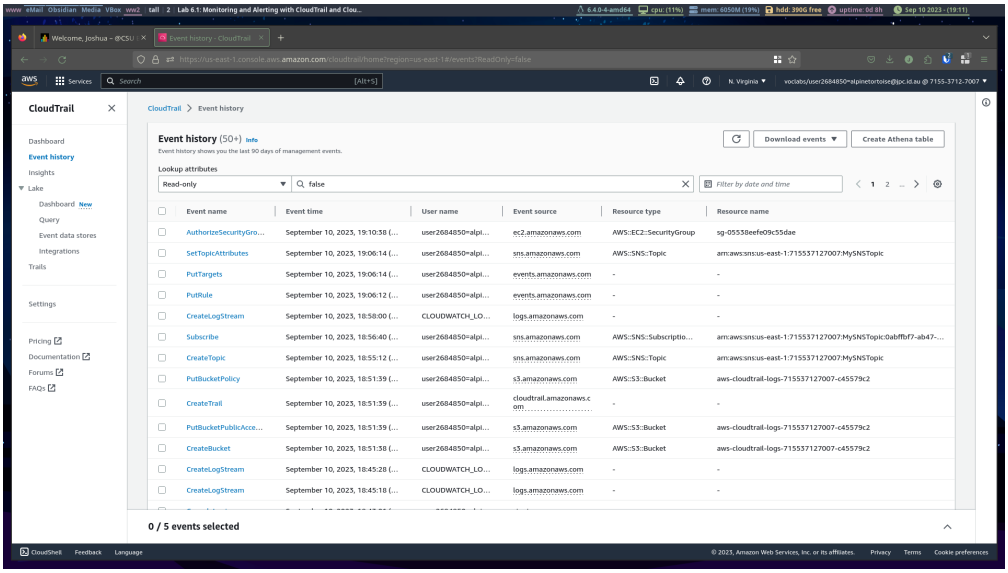

Amazon EventBridge
Rules
Create rule
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Configure tags - optional
Info
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.
Add new tag
You can add 50 more tags.
Cancel
Previous
Next

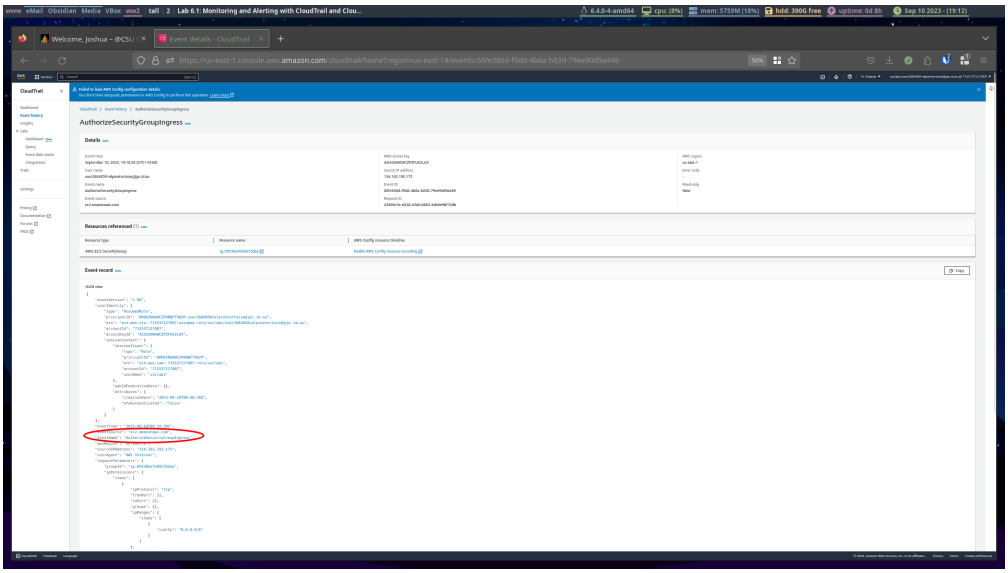

Review and create
Step 1: Define rule detail
Edit
Define rule detail
Step 2: Build event pattern
Edit
Event pattern
Copy
Step 3: Select target(s)
Edit
Targets
Step 4: Configure tag(s)
Edit
Tags (0)

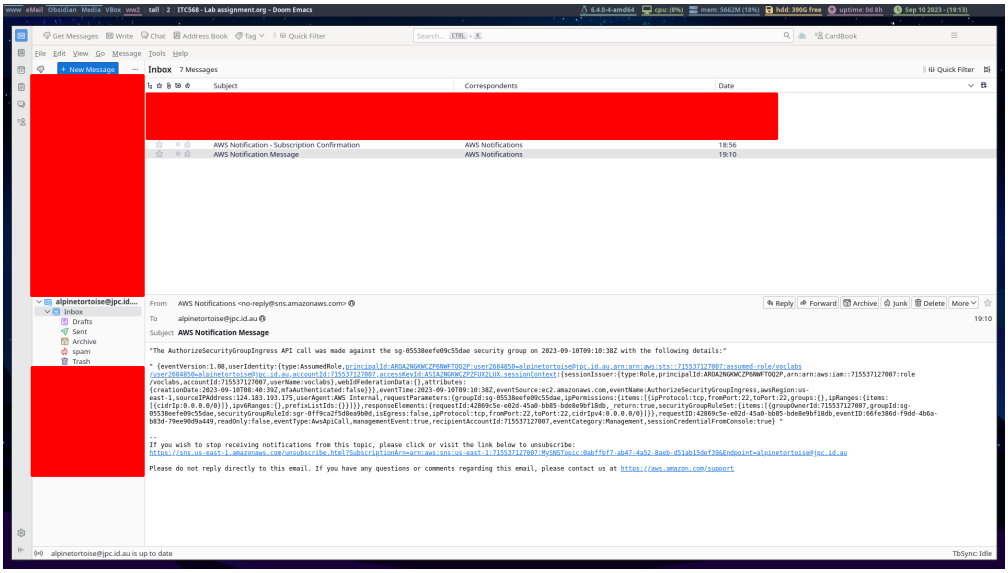

Instance summary for i-0a3024892fb4787a6 (LabInstance)
Connect
Instance state
Actions
Instance ID
i-0a3024892fb4787a6 (LabInstance)
Public IPv4 address
54.144.146.75 | open address
Private IPv4 addresses
10.0.0.79
Instance state
Running
Public IPv4 DNS
ec2-54-144-146-75.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-0-0-79.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-0-79.ec2.internal
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
54.144.146.75 [Public IP]
VPC ID
vpc-022b40c3fae2c1668 (LabVPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
Subnet ID
subnet-0def19ef8c9b7c998 (Public Subnet)
Auto Scaling Group name
IMDSv2
Optional
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Security details
IAM Role
Owner ID
715537127007
Launch time
Sun Sep 10 2023 18:41:01 GMT+1000 (Australian Eastern Standard Time)
Security groups
Inbound rules


sg-05538eefe09c55dae - c88361a1902275l4715732t1w715537127007-LabSecurityGroup-1KI7NL0GUDJXB
Actions
Details
Security group name
c88361a1902275l4715732t1w715537127007-LabSecurityGroup-1KI7NL0GUDJXB
Security group ID
sg-05538eefe09c55dae
Description
HTTP access enabled
VPC ID
vpc-022b40c3fae2c1666
Owner
715537127007
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (1/1)
Manage tags
Edit inbound rules
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
sgr-0e4414479799d7...
IPv4
HTTP
TCP
80
0.0.0.0/0

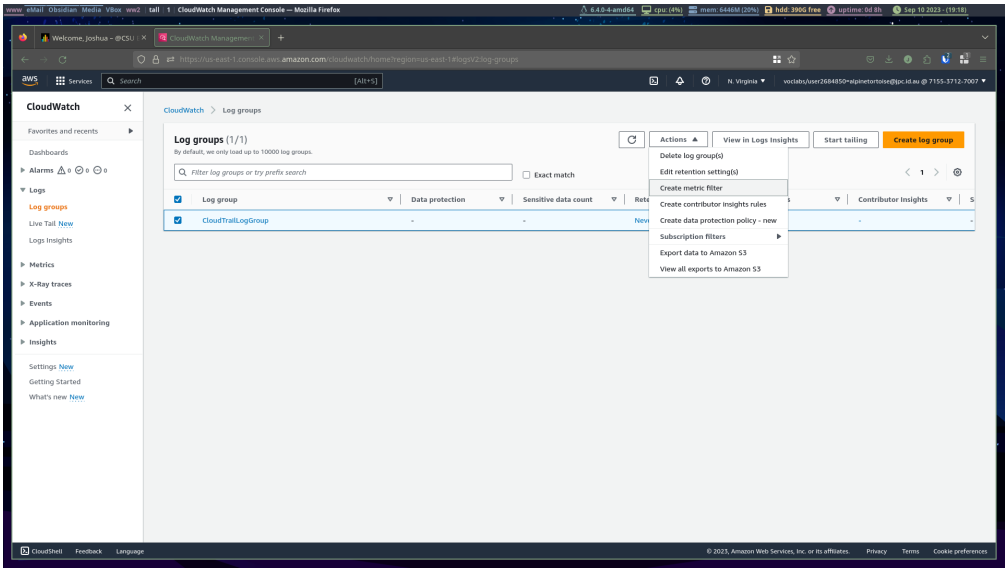

Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules
Security group rule ID
Type
Protocol
Port range
Source
Description - optional
sgr-0e4414479799d71b7
HTTP
TCP
80
Custom
0.0.0.0/0
Delete
SSH
22
Anywhere-...
Add rule
Cancel
Preview changes
Save rules

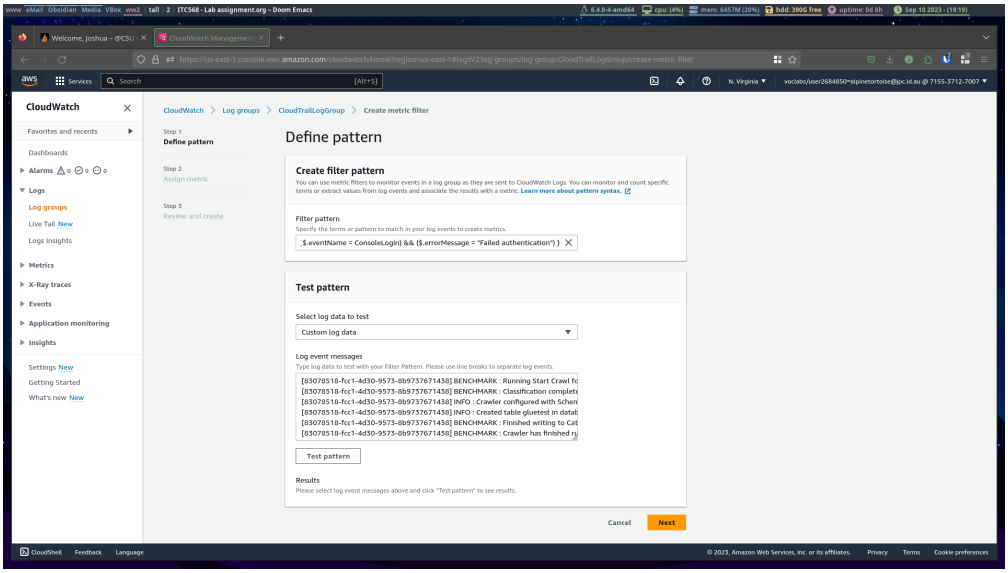

CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Event history
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Create Athena table
Lookup attributes
Read-only
false
Filter by date and time
Event name
Event time
User name
Event source
Resource type
Resource name
AuthorizeSecurityGro...
September 10, 2023, 19:10:58 (...
user2684850=alpi...
ec2.amazonaws.com
AWS::EC2::SecurityGroup
sg-05538eefe09c55dae
SetTopicAttributes
September 10, 2023, 19:06:14 (...
sns.amazonaws.com
AWS::SNS::Topic
arn:aws:sns:us-east-1:715537127007:MySNSTopic
PutTargets
September 10, 2023, 19:06:14 (...
events.amazonaws.com
PutRule
September 10, 2023, 19:06:12 (...
CreateLogStream
September 10, 2023, 18:58:00 (...
CLOUDWATCH_LO...
logs.amazonaws.com
Subscribe
September 10, 2023, 18:56:40 (...
AWS::SNS::Subscriptio...
arn:aws:sns:us-east-1:715537127007:MySNSTopic:0abffbf7-ab47-...
CreateTopic
September 10, 2023, 18:55:12 (...
PutBucketPolicy
September 10, 2023, 18:51:39 (...
s3.amazonaws.com
AWS::S3::Bucket
aws-cloudtrail-logs-715537127007-c45579c2
CreateTrail
cloudtrail.amazonaws.com
PutBucketPublicAcce...
CreateBucket
September 10, 2023, 18:51:38 (...
CreateLogStream
September 10, 2023, 18:45:28 (...
CreateLogStream
September 10, 2023, 18:45:18 (...
0 / 5 events selected
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

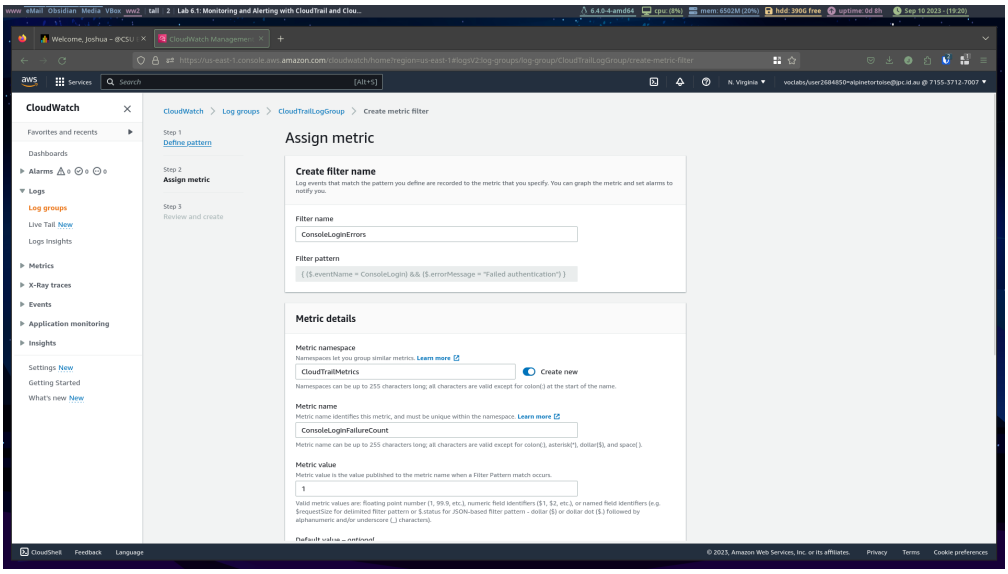

AuthorizeSecurityGroupIngress
Details
Resources referenced
Event record

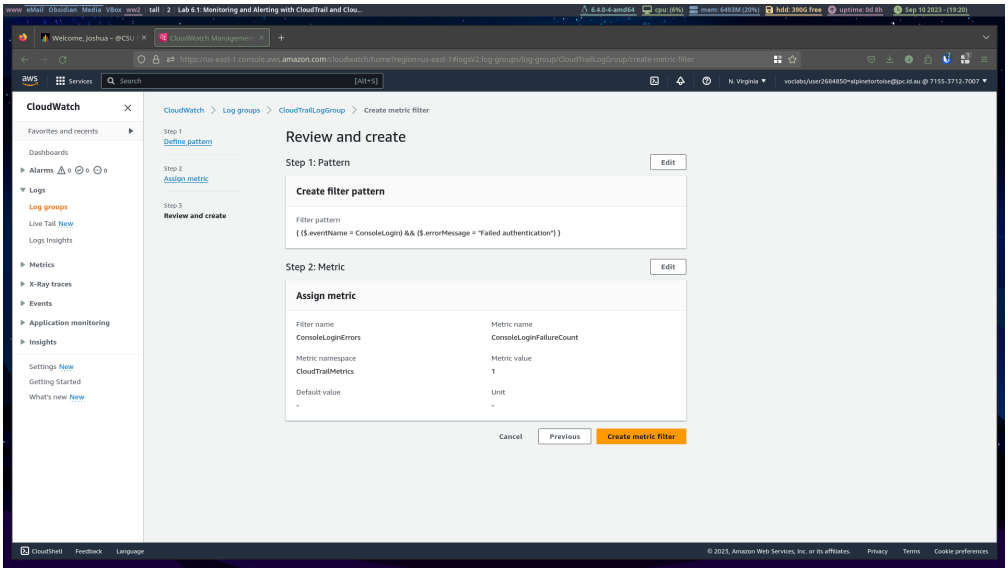


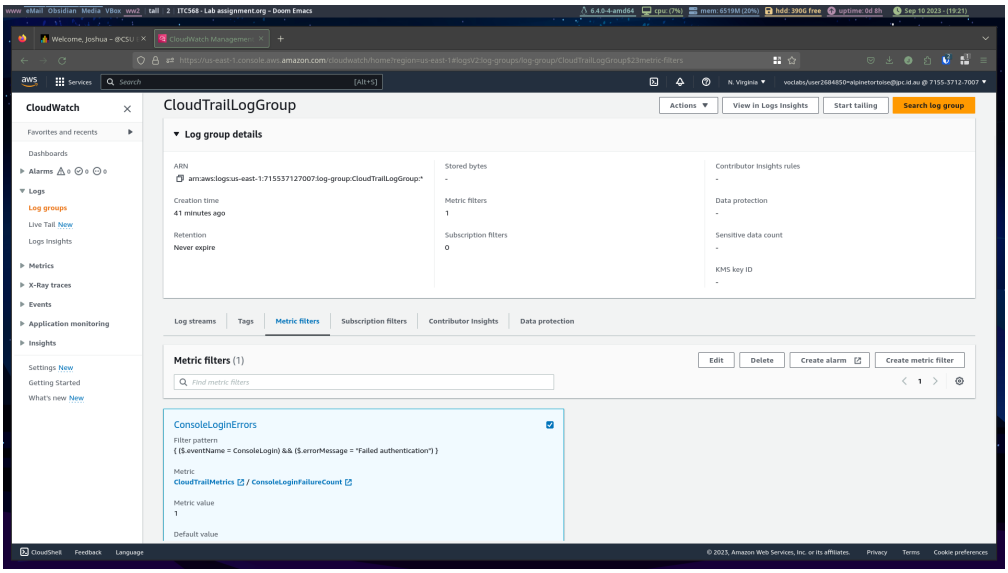
4.4 Task 4: Creating a CloudWatch alarm based on a metrics filter

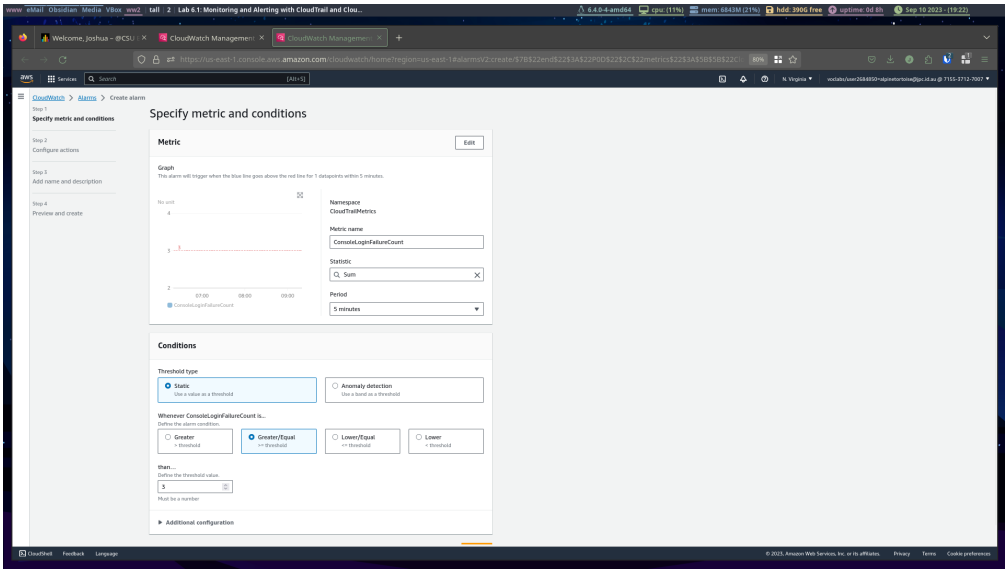


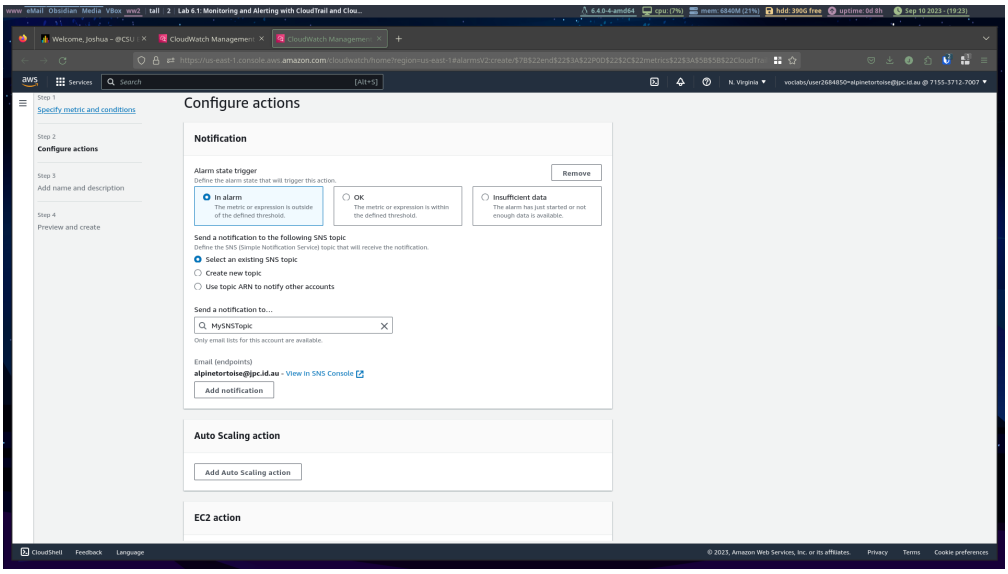

CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Live Tail New
Logs Insights
Metrics
X-Ray traces
Events
Application monitoring
Insights
Settings New
Getting Started
What's new New
CloudWatch > Log groups > CloudTrailLogGroup > Create metric filter
Step 1
Define pattern
Step 2
Assign metric
Step 3
Review and create
Define pattern
Create filter pattern
You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. Learn more about pattern syntax.
Filter pattern
Specify the terms or pattern to match in your log events to create metrics.
{ $.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Test pattern
Select log data to test
Custom log data
Log event messages
Type log data to test with your Filter Pattern. Please use line breaks to separate log events.
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Running Start Crawl fo
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Classification complete
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Crawler configured with Schem
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Created table gluetest in datab
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Finished writing to Cat
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Crawler has finished ru
Test pattern
Results
Please select log event messages above and click "Test pattern" to see results.
Cancel
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

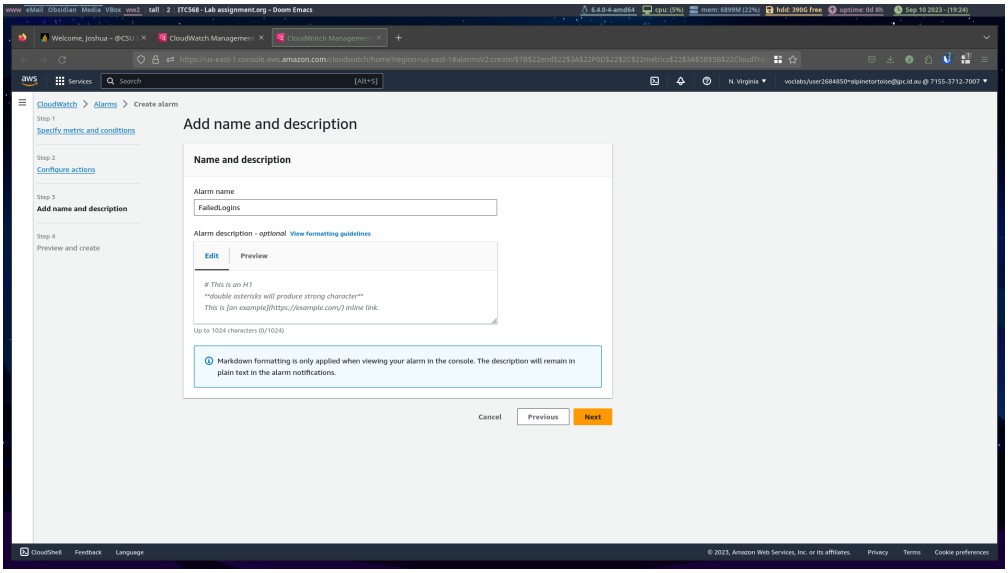

CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Live Tail New
Logs Insights
Metrics
X-Ray traces
Events
Application monitoring
Insights
Settings New
Getting Started
What's new New
CloudWatch > Log groups > CloudTrailLogGroup > Create metric filter
Step 1
Define pattern
Step 2
Assign metric
Step 3
Review and create
Assign metric
Create filter name
Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.
Filter name
ConsoleLoginErrors
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Metric details
Metric namespace
Namespaces let you group similar metrics. Learn more
CloudTrailMetrics
Create new
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.
Metric name
Metric name identifies this metric, and must be unique within the namespace. Learn more
ConsoleLoginFailureCount
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).
Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.
1
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers ($1, $2, etc.), or named field identifiers (e.g. $requestSize for delimited filter pattern or $.status for JSON-based filter pattern - dollar ($) or dollar dot ($.) followed by alphanumeric and/or underscore (_) characters).
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

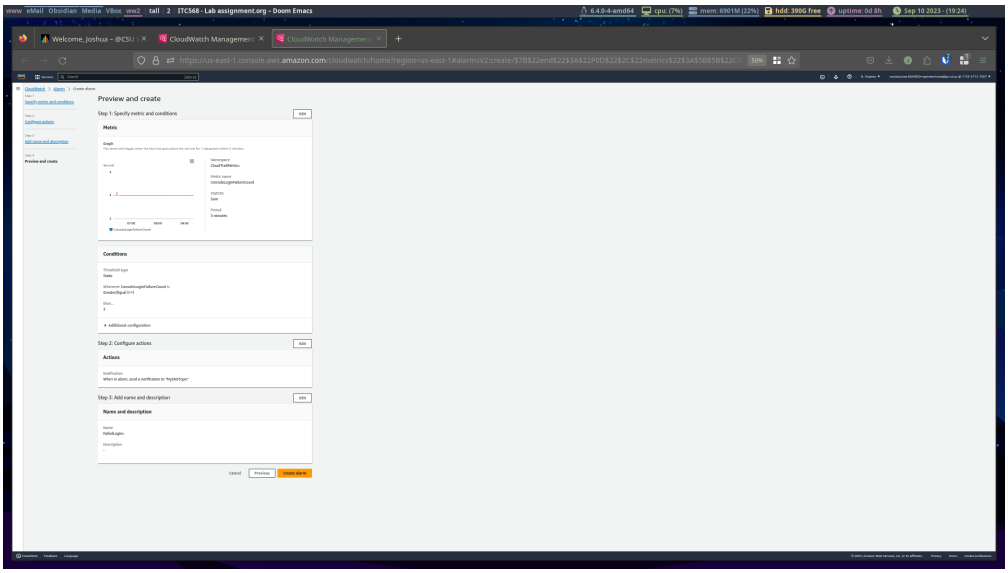

CloudWatch
Log groups > CloudTrailLogGroup > Create metric filter
Step 1 Define pattern
Step 2 Assign metric
Step 3 Review and create
Review and create
Step 1: Pattern
Edit
Create filter pattern
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Step 2: Metric
Edit
Assign metric
Filter name
ConsoleLoginErrors
Metric name
ConsoleLoginFailureCount
Metric namespace
CloudTrailMetrics
Metric value
1
Default value
-
Unit
-
Cancel
Previous
Create metric filter

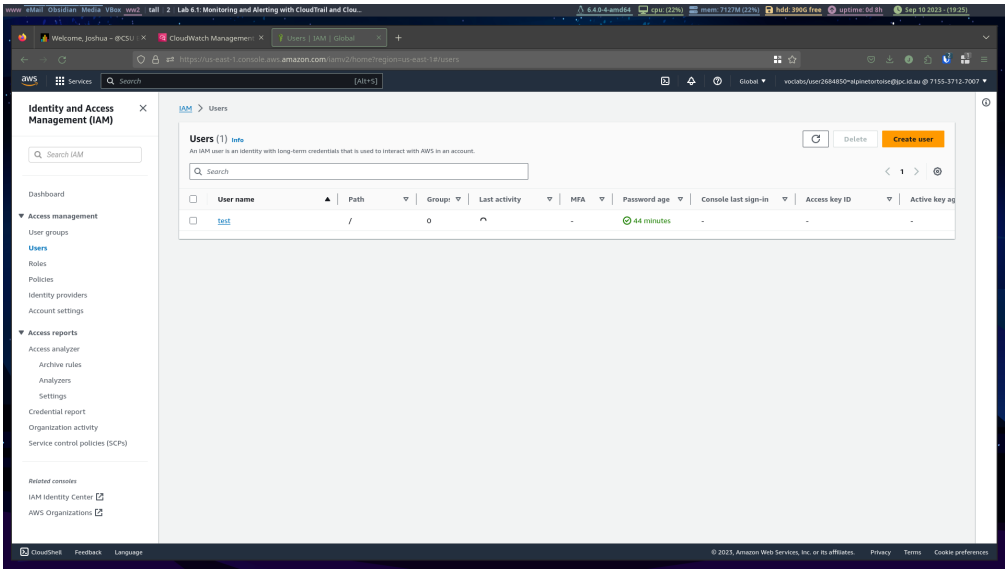

CloudWatch
CloudTrailLogGroup
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
ARN
arn:aws:logs:us-east-1:715537127007:log-group:CloudTrailLogGroup:*
Creation time
41 minutes ago
Retention
Never expire
Stored bytes
-
Metric filters
1
Subscription filters
0
Contributor Insights rules
-
Data protection
-
Sensitive data count
-
KMS key ID
-
Log streams
Tags
Metric filters
Subscription filters
Contributor Insights
Data protection
Metric filters (1)
Edit
Delete
Create alarm
Create metric filter
ConsoleLoginErrors
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Metric
CloudTrailMetrics / ConsoleLoginFailureCount
Metric value
1
Default value

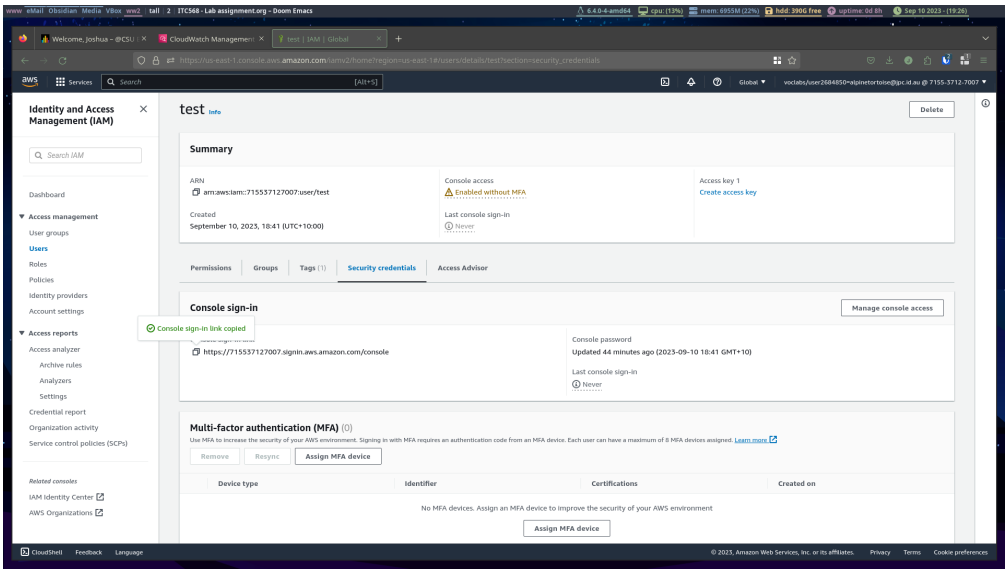

Specify metric and conditions
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
Namespace
CloudTrailMetrics
Metric name
ConsoleLoginFailureCount
Statistic
Sum
Period
5 minutes
Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever ConsoleLoginFailureCount is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
3
Must be a number
Additional configuration

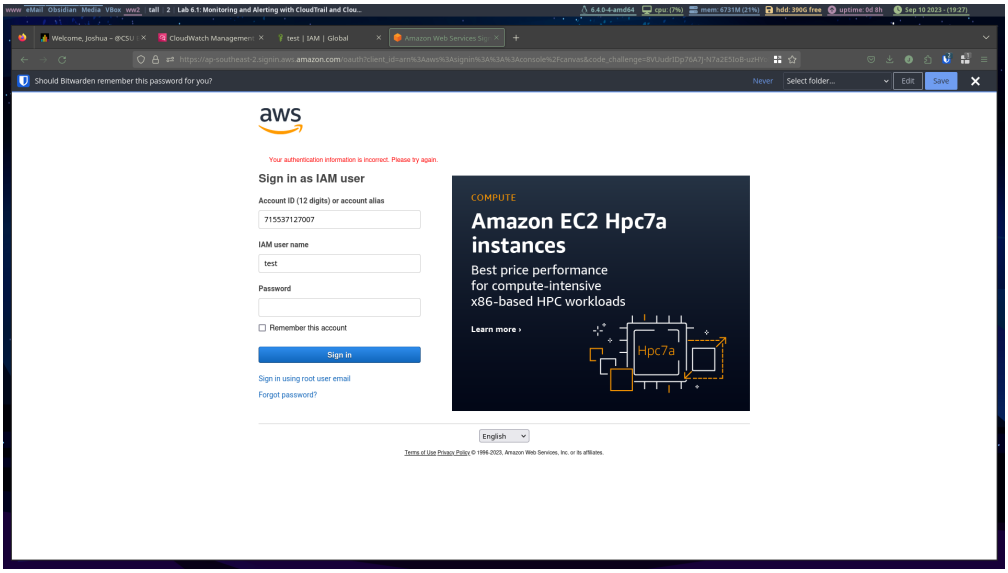

Configure actions
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Notification
Remove
Alarm state trigger
Define the alarm state that will trigger this action.
In alarm
The metric or expression is outside of the defined threshold.
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...
MySNSTopic
Only email lists for this account are available.
Email (endpoints)
alpinetortoise@jpc.id.au - View in SNS Console
Add notification
Auto Scaling action
Add Auto Scaling action
EC2 action

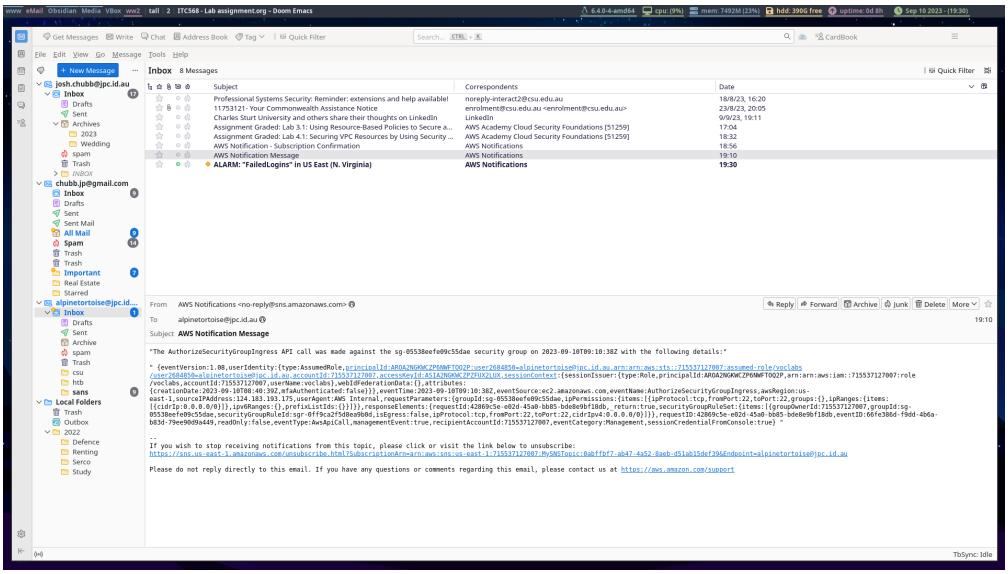

CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Add name and description
Name and description
Alarm name
FailedLogins
Alarm description - optional View formatting guidelines
Edit
Preview
This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.
Up to 1024 characters (0/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
Cancel
Previous
Next

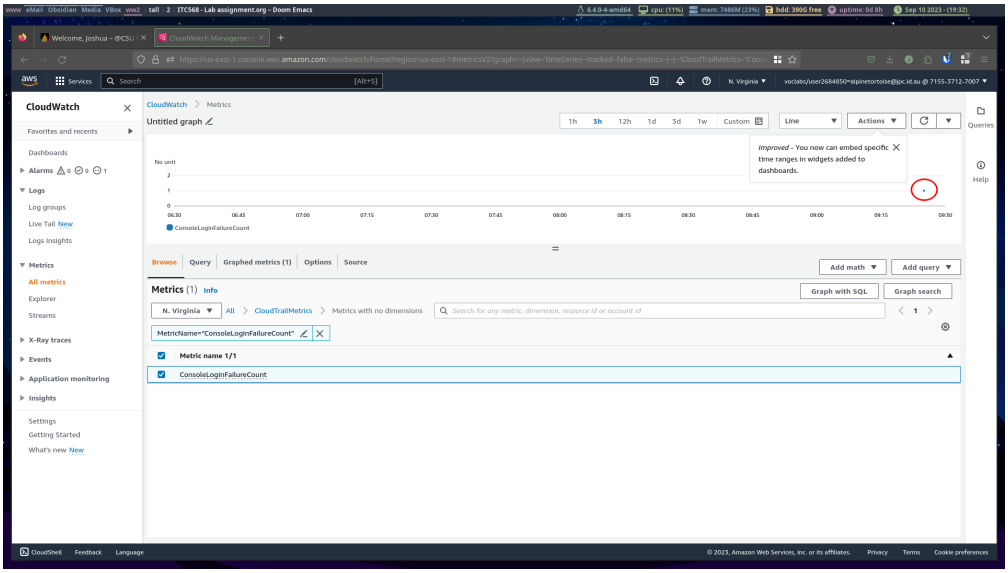

Preview and create

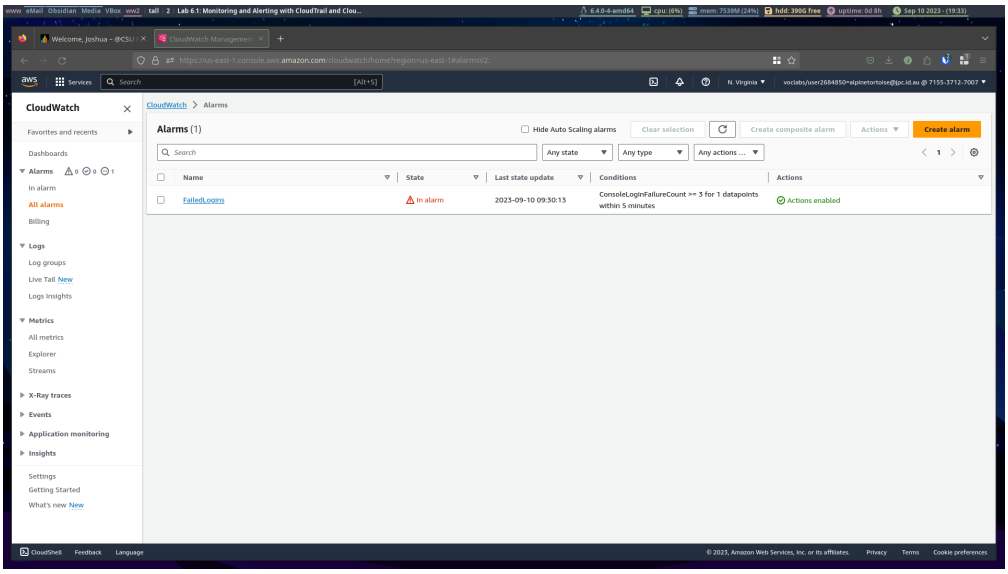

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
IAM Identity Center
AWS Organizations
IAM > Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
Delete
Create user
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key ag
test
/
0
-
44 minutes
-
-
-
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

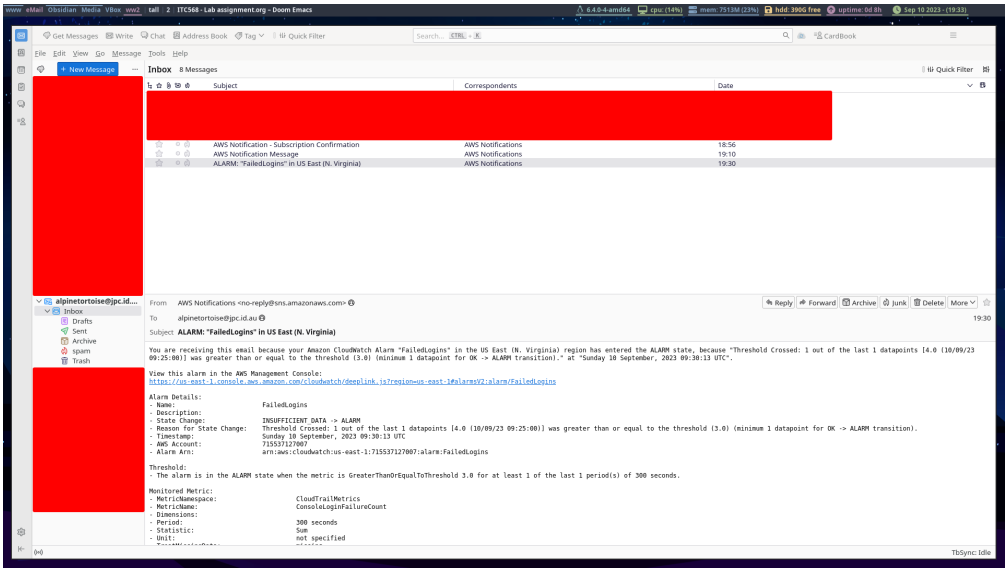

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
IAM Identity Center
AWS Organizations
Console sign-in link copied
test Info
Delete
Summary
ARN
arn:aws:iam::715537127007:user/test
Console access
Enabled without MFA
Access key 1
Create access key
Created
September 10, 2023, 18:41 (UTC+10:00)
Last console sign-in
Never
Permissions
Groups
Tags (1)
Security credentials
Access Advisor
Console sign-in
Manage console access
https://715537127007.signin.aws.amazon.com/console
Console password
Updated 44 minutes ago (2023-09-10 18:41 GMT+10)
Last console sign-in
Never
Multi-factor authentication (MFA) (0)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Remove
Resync
Assign MFA device
Device type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Your authentication information is incorrect. Please try again.
Sign in as IAM user
Account ID (12 digits) or account alias
715537127007
IAM user name
test
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
COMPUTE
Amazon EC2 Hpc7a instances
Best price performance for compute-intensive x86-based HPC workloads
Learn more ›
Hpc7a
English
Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.


Inbox 8 Messages
Subject
Correspondents
Date
Professional Systems Security: Reminder: extensions and help available!
noreply-interact2@csu.edu.au
18/8/23, 16:20
11753121- Your Commonwealth Assistance Notice
enrolment@csu.edu.au <enrolment@csu.edu.au>
23/9/23, 20:05
Charles Sturt University and others share their thoughts on LinkedIn
LinkedIn
9/9/23, 19:11
Assignment Graded: Lab 3.1: Using Resource-Based Policies to Secure a...
AWS Academy Cloud Security Foundations [51259]
17:04
Assignment Graded: Lab 4.1: Securing VPC Resources by Using Security ...
AWS Academy Cloud Security Foundations [51259]
18:32
AWS Notification - Subscription Confirmation
AWS Notifications
18:56
AWS Notification Message
AWS Notifications
19:10
ALARM: "FailedLogins" in US East (N. Virginia)
AWS Notifications
19:30
From AWS Notifications <no-reply@sns.amazonaws.com>
To alpinetortoise@jpc.id.au
19:10
Subject AWS Notification Message
"The AuthorizeSecurityGroupIngress API call was made against the sg-05538eefe09c55dae security group on 2023-09-10T09:10:38Z with the following details:"
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support


CloudWatch
Metrics
Untitled graph
Actions
Graphed metrics (1)
Options
Source
Add math
Add query
Graph with SQL
Graph search
N. Virginia
CloudTrailMetrics
MetricName="ConsoleLoginFailureCount"
Metric name 1/1
ConsoleLoginFailureCount


CloudWatch
Alarms (1)
Hide Auto Scaling alarms
Create alarm
Name
State
Last state update
Conditions
Actions
FailedLogins
In alarm
2023-09-10 09:30:13
ConsoleLoginFailureCount >= 5 for 1 datapoints within 5 minutes
Actions enabled



4.5 Task 5: Querying CloudTrail logs by using CloudWatch Logs Insights