AWS Projects Group 4

Names:

- هاجر سعيد السيد علي
- اسامة جمال عبدالعزيز
- محمد احمد محمود
- محمد سعد محمد علي

Project 6 : Exploring AWS Identity and Access Management (IAM)

Open the Environment on CLI

we are using the AWS CLI in a terminal environment. Make

sure the AWS CLI is installed and configured with AWS credentials and region.

- Open Terminal
- Configure AWS CLI

* Provide the necessary inputs for:

- AWS Access Key ID

- AWS Secret Access Key

- Default region name (e.g., us-east-1)

-Default output format (e.g., json)

Task 1: Explore Users

and Groups Step 1: List

IAM Users

List all the IAM users to get an overview of pre-created users.

```
C:\Users\Hagar>aws configure
AWS Access Key ID [****************DPS5]:
AWS Secret Access Key [****************CZsZ]:
Default region name [us-east-1]:
Default output format [json]:

C:\Users\Hagar>aws iam list-users
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA5GVR5MOQNA56TN2X4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA5GVR5MOQLLO2LE6L4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA5GVR5MOQA6RJ6ZRWG",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
```

Step 2: List IAM Groups

Retrieve a list of all IAM groups

```
C:\Users\Hagar>aws iam list-groups
{
    "Groups": [
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Admin",
            "GroupId": "AGPA5GVR5MOQOMLH4ID5L",
            "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Support",
            "GroupId": "AGPA5GVR5MOQMWZ7F632E",
            "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "S3-Support",
            "GroupId": "AGPA5GVR5MOQCSTASWKGX",
            "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ]
}


C:\Users\Hagar>
C:\Users\Hagar>
```

Step 3: View User Details

To inspect a specific user, use the following command by replacing <user_name>with the

actual username.

comand : aws iam get-user --user-name <user_name>

```
C:\Users\Hagar>aws iam get-user --user-name user-1
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDA5GVR5MOQNA56TN2X4",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
        ]
    }
}


C:\Users\Hagar>aws iam get-user --user-name user-2
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDA5GVR5MOQLLO2LE6L4",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
        ]
    }
}


C:\Users\Hagar>aws iam get-user --user-name user-3
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDA5GVR5MOQA6RJ6ZRWG",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
```

Step 4: List Users in a Specific Group

To get a list of all users that belong to a specific group,

comand : aws iam get-group --group-name <group_name>

```
C:\Users\Hagar>
C:\Users\Hagar>aws iam get-group --group-name EC2-Admin
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA5GVR5MOQOMLH4ID5L",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}


C:\Users\Hagar>aws iam get-group --group-name EC2-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA5GVR5MOQMWZ7F632E",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}


C:\Users\Hagar>aws iam get-group --group-name S3-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA5GVR5MOQCSTASWKGX",
        "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}
```

Task 2: Inspect IAM Policies

Step 1: List Attached Policies for a Group

```
C:\Users\Hagar>aws iam list-attached-group-policies --group-name EC2-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}


C:\Users\Hagar>aws iam list-attached-group-policies --group-name S3-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}


C:\Users\Hagar>aws iam list-attached-group-policies --group-name EC2-Admin
{
    "AttachedPolicies": []
}


C:\Users\Hagar>
```

Step 2: View Policy Details

To view the details of a specific policy attached to the group, use the policy's ARN(Amazon Resource Name) from the previous command's output

```
C:\Users\Hagar>aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}


C:\Users\Hagar>aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}


C:\Users\Hagar>
```

Task 3: Add Users to Groups

add users to specific groups according to their role requirements.

Step 1: Add User-1 to S3-Support Group

Grant User-1 read-only access to S3 by adding them to the S3-Support group.

Step 2: Add User-2 to EC2-Support Group

assign User-2 permissions to read-only access to EC2 resources.

Step 3: Add User-3 to EC2-Admin Group

Assign User-3 permissions to view, start, and stop EC2 instances byadding them to the EC2-Admin group.

```
C:\Users\Hagar>aws iam add-user-to-group --group-name S3-Support --user-name User-1

C:\Users\Hagar>aws iam add-user-to-group --group-name EC2-Support --user-name User-2

C:\Users\Hagar>
C:\Users\Hagar>aws iam add-user-to-group --group-name EC2-Admin --user-name User-3

C:\Users\Hagar>
C:\Users\Hagar>
```

Step 4: Verify Users are Added to Groups

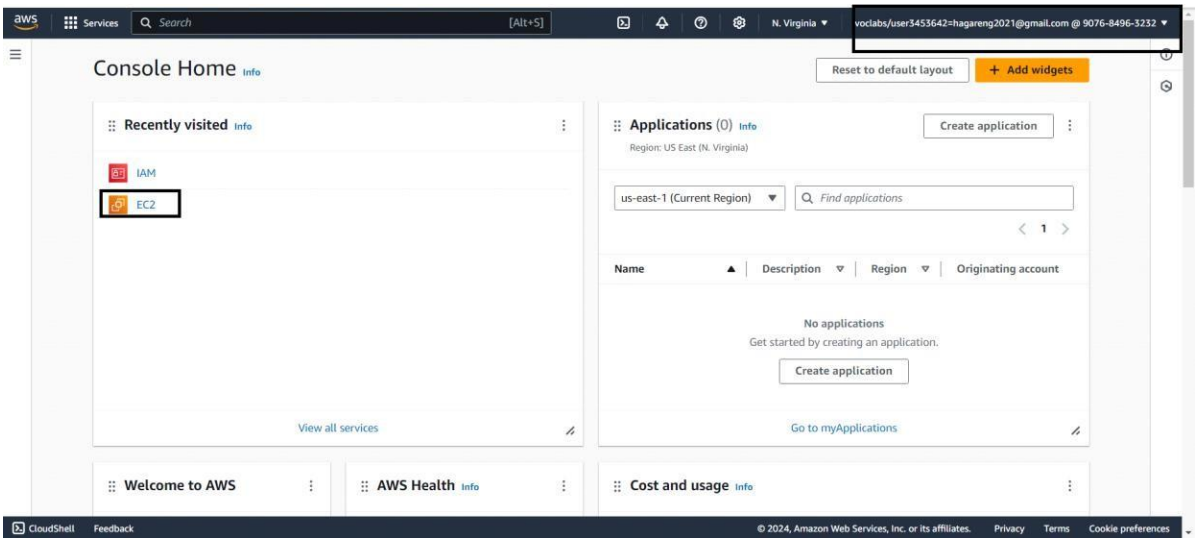
Verify that the users are properly added to the groups by listing users within each group

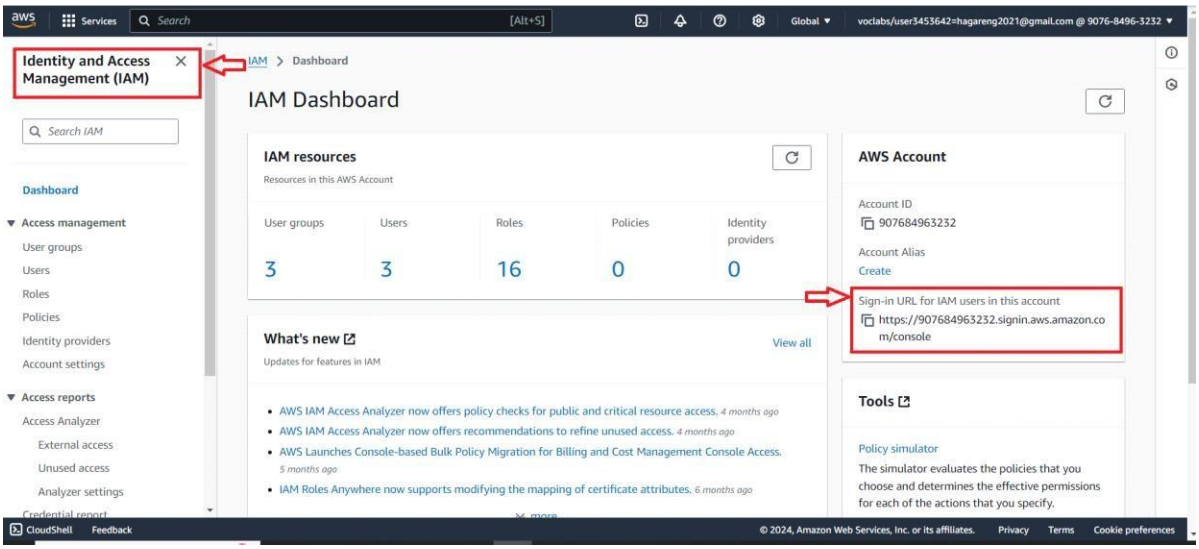
```
C:\Users\Hagar>aws iam get-group --group-name S3-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA5GVR5MOQNA56TN2X4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA5GVR5MOQCSTASWKGX",
        "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}


C:\Users\Hagar>aws iam get-group --group-name EC2-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA5GVR5MOQA6RJ6ZRWG",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA5GVR5MOQLLO2LE6L4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA5GVR5MOQMWZ7F632E",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}
```

```
C:\Users\Hagar>aws iam get-group --group-name EC2-Admin
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA5GVR5MOQA6RJ6ZRWG",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA5GVR5MOQOMLH4ID5L",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}


C:\Users\Hagar>
```

Task 4: Test Permissions

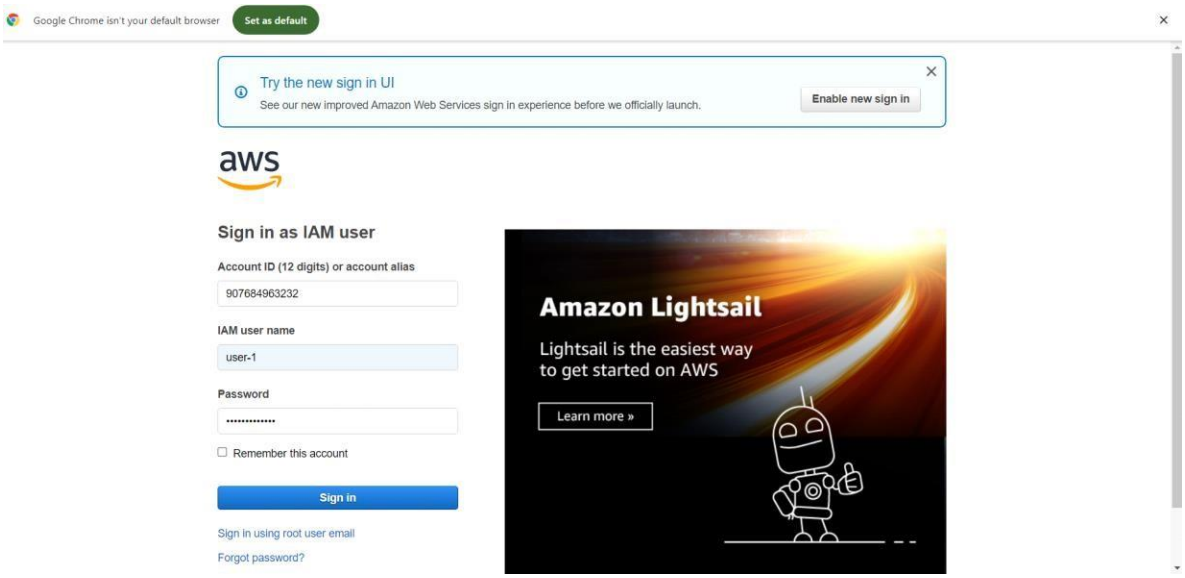
Step 1: Get the console sign-in URL

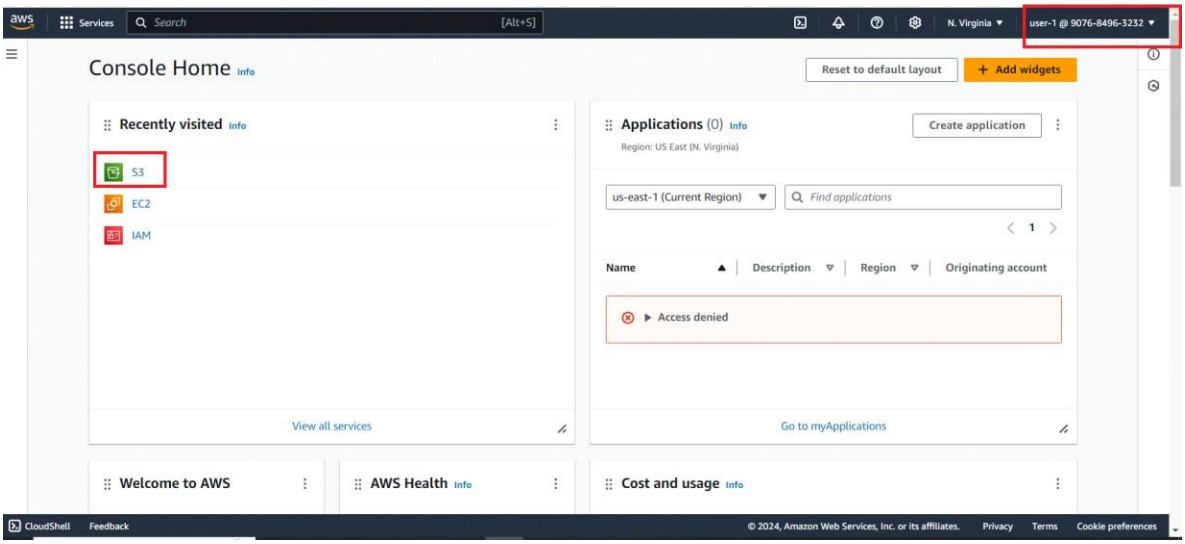


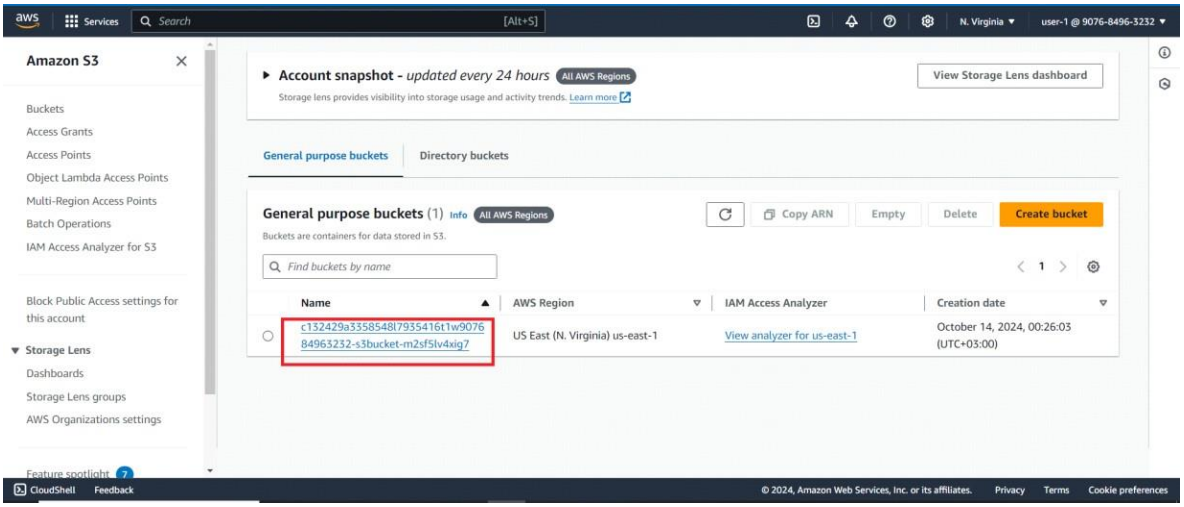


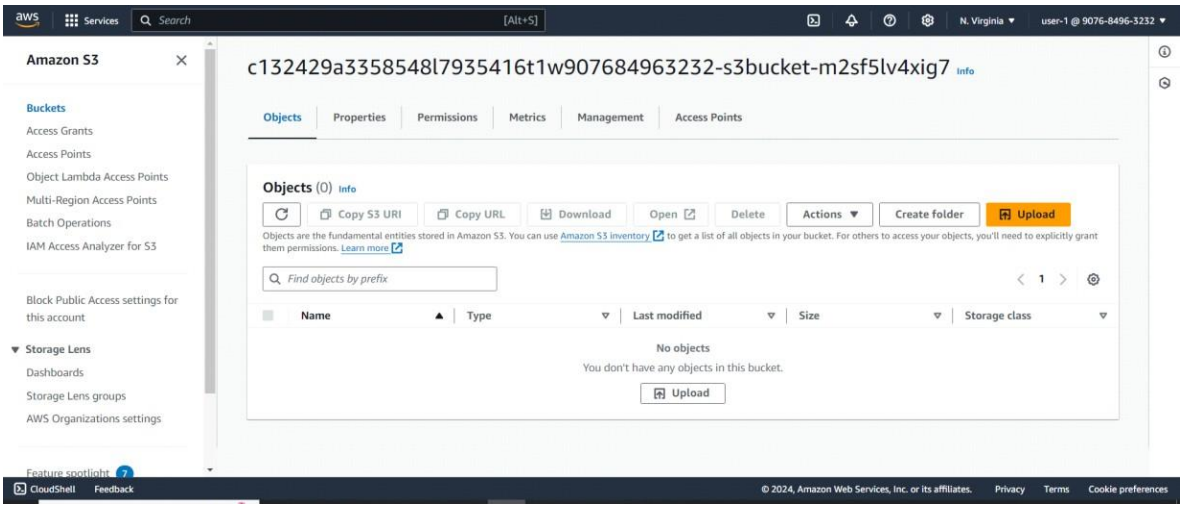
Step 2: User-1 Test S3 Read-only Access:

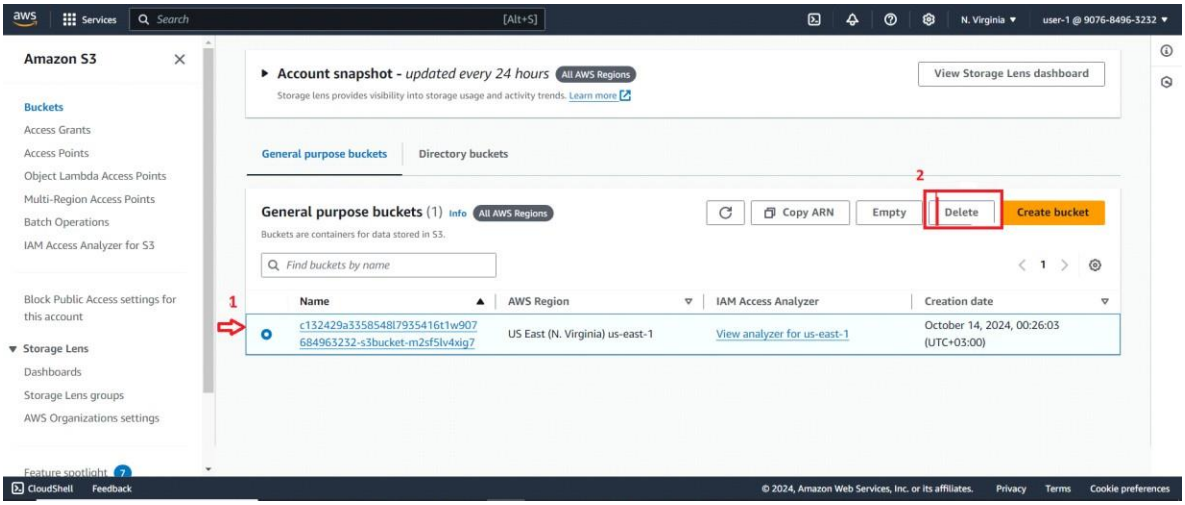
- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.
- Navigate to the S3 service and try to list buckets.
- Try to perform any write operations (like deleting bucket), which should fail due to read-only access

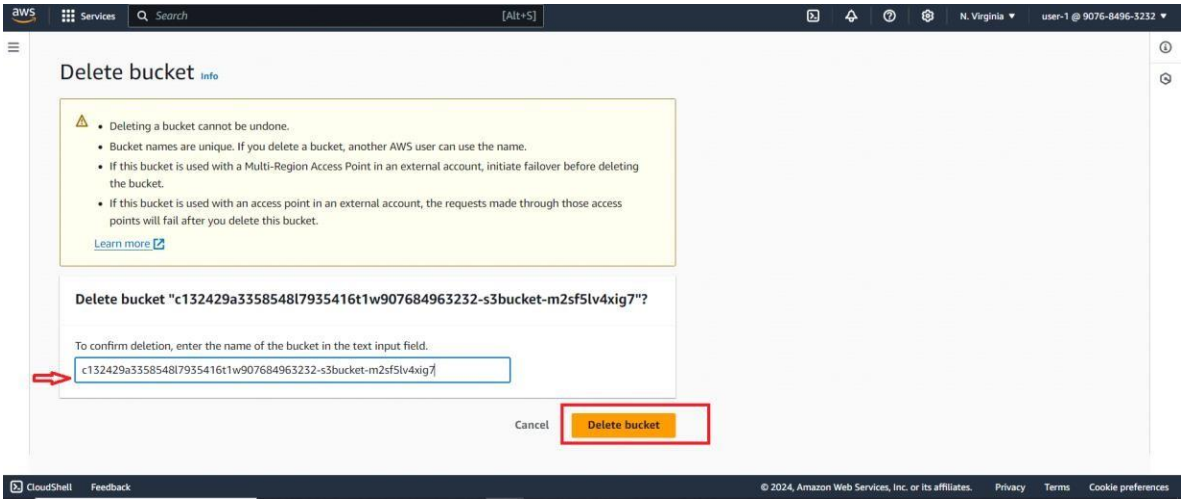


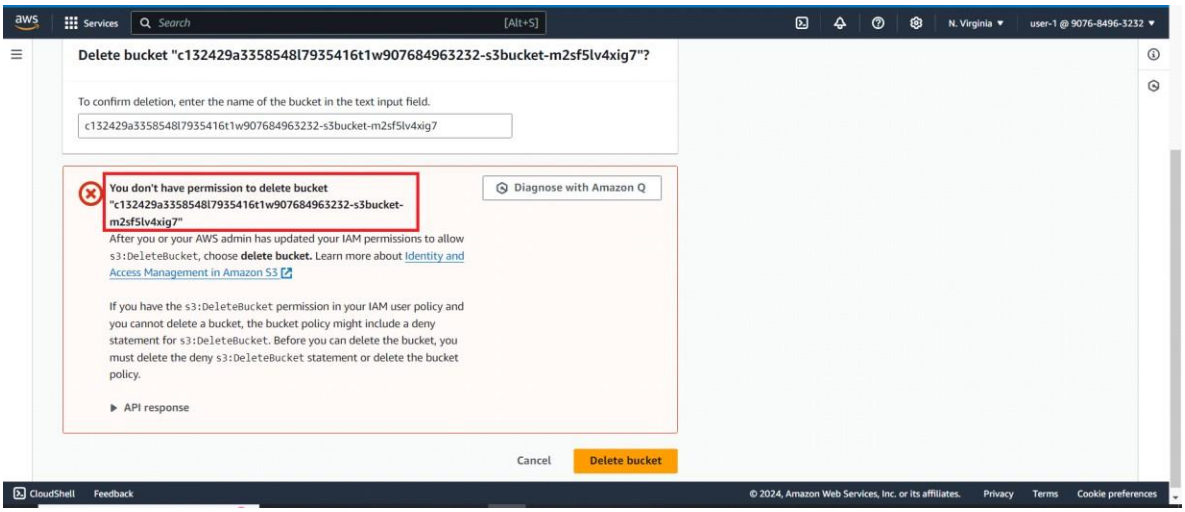

Services
Search
[Alt+S]
N. Virginia
user-1 @ 9076-8496-3232
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
S3
EC2
IAM
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-1 @ 9076-8496-3232
Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
Feature spotlight
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 14, 2024, 00:26:03 (UTC+03:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

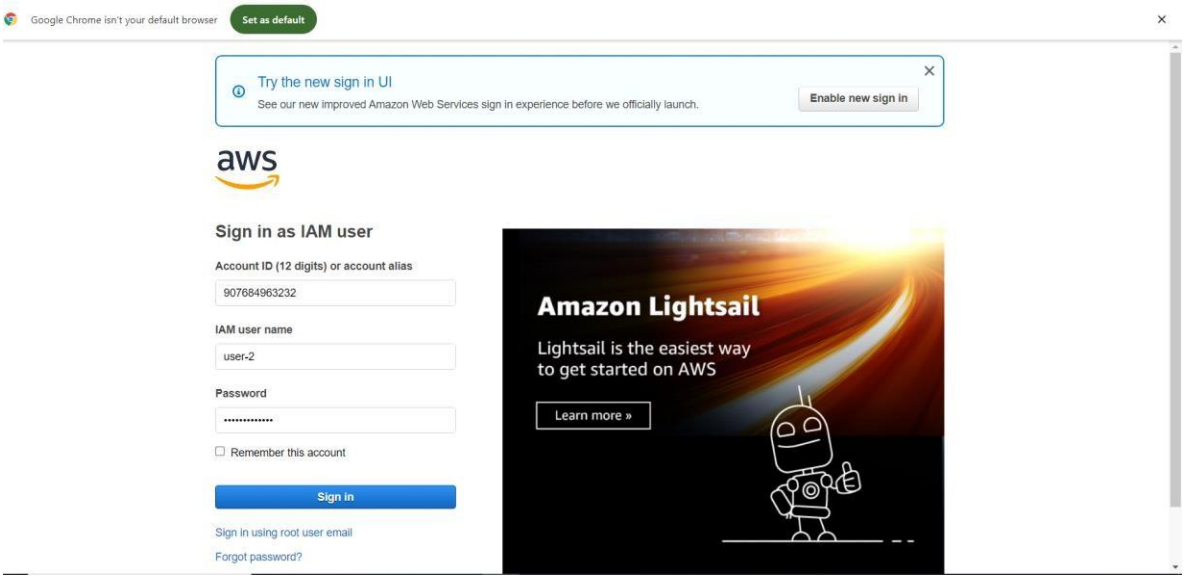

Amazon S3
Account snapshot - updated every 24 hours
All AWS Regions
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 14, 2024, 00:26:03 (UTC+03:00)
1
2

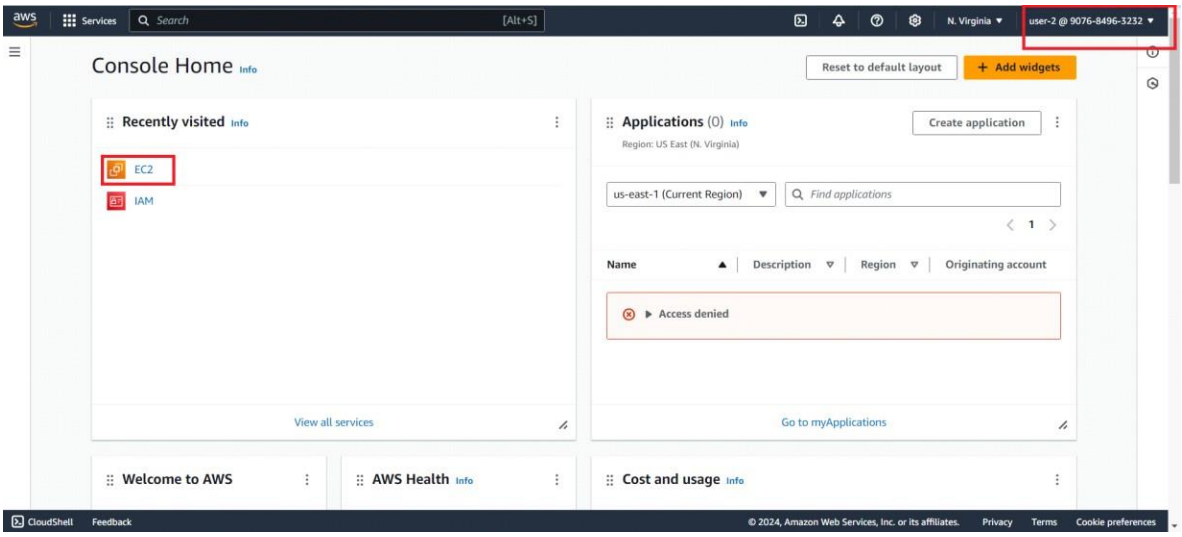

Delete bucket Info
Deleting a bucket cannot be undone.
Bucket names are unique. If you delete a bucket, another AWS user can use the name.
If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
Learn more
Delete bucket "c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7"?
To confirm deletion, enter the name of the bucket in the text input field.
c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7
Cancel
Delete bucket

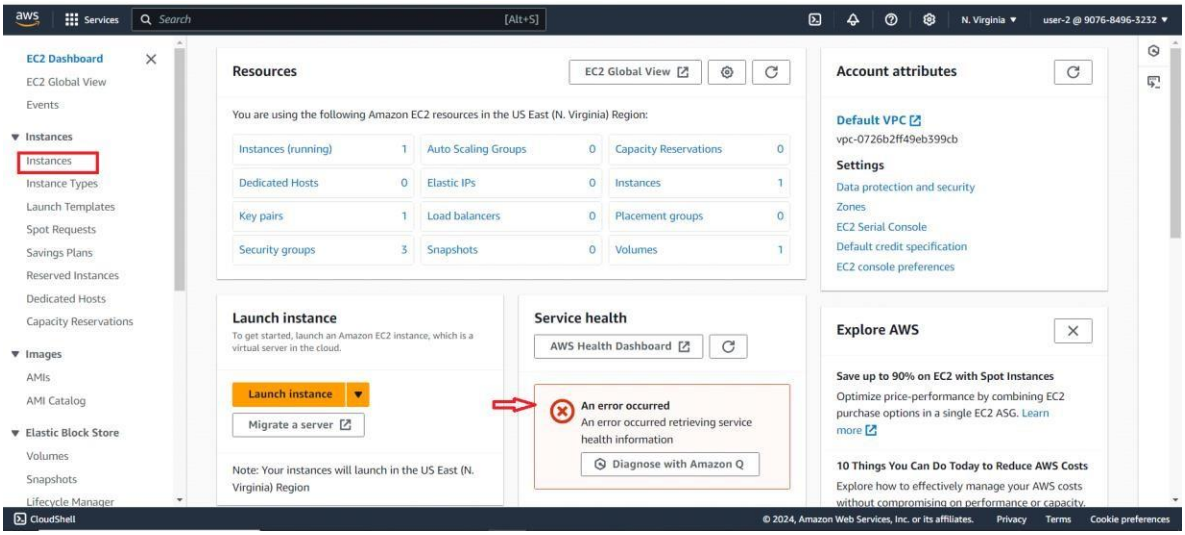


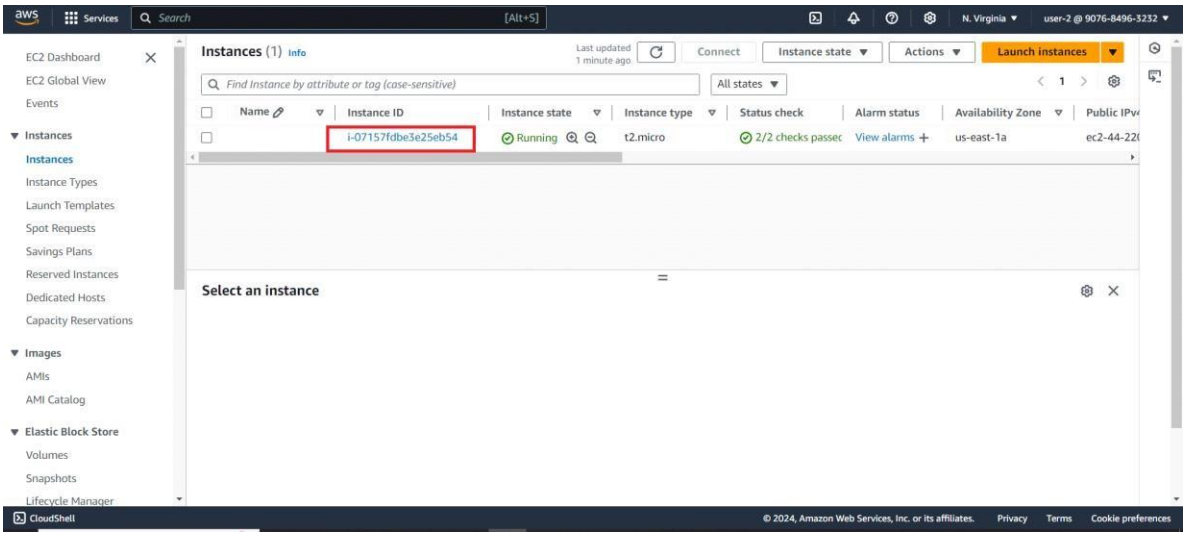
Step 3: User-2 Test EC2 Read-only Access:

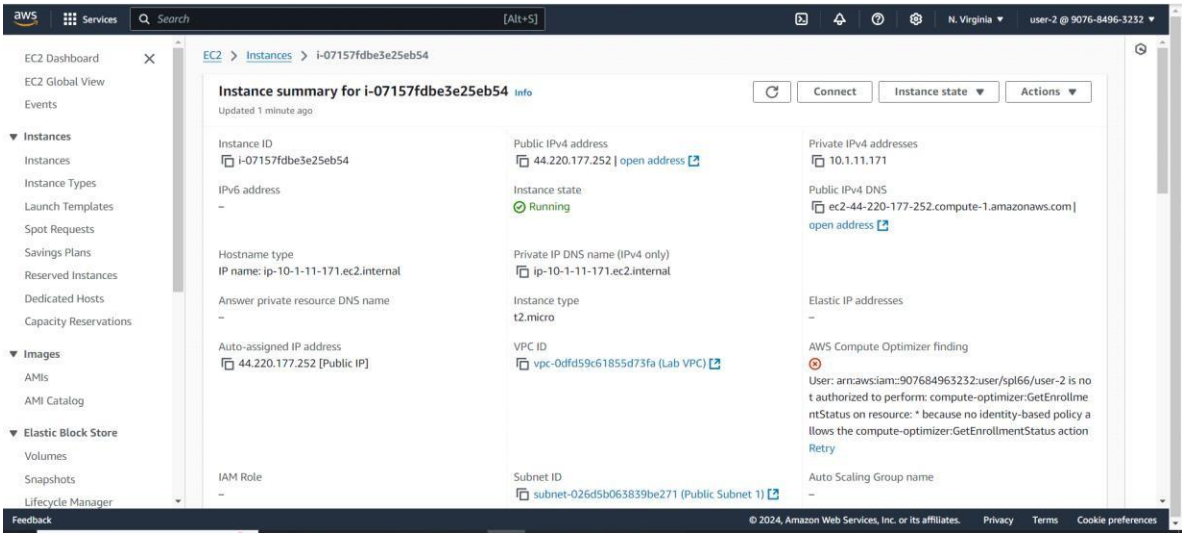
- Sign in as User-2.
- Navigate to the EC2 dashboard.
- Check if User-2 can view instances but cannot modify (start/stop) them

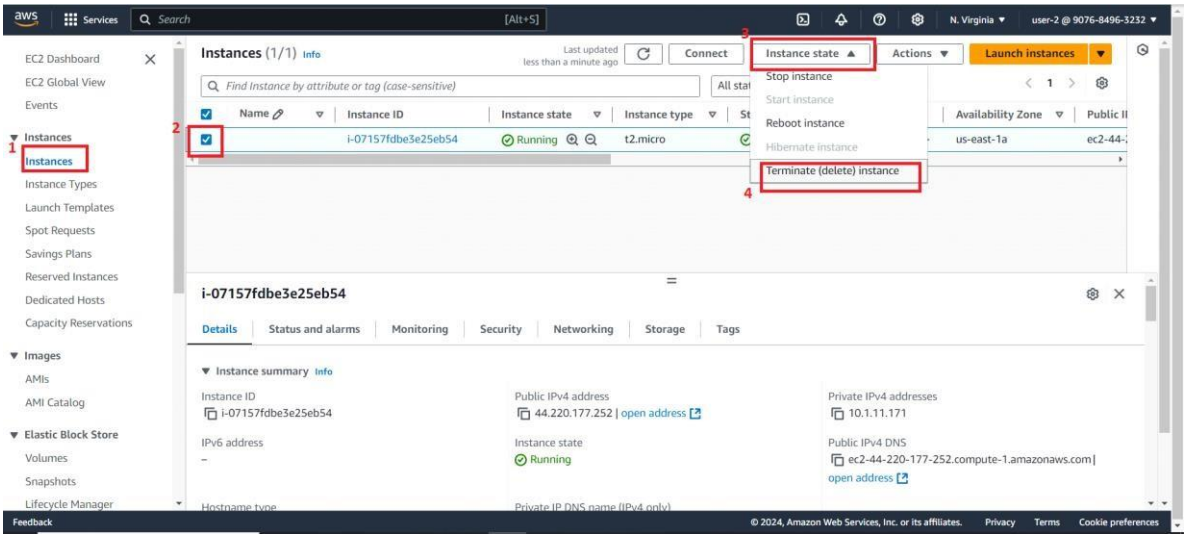

Google Chrome isn't your default browser
Set as default
Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
Enable new sign in
aws
Sign in as IAM user
Account ID (12 digits) or account alias
907684963232
IAM user name
user-2
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

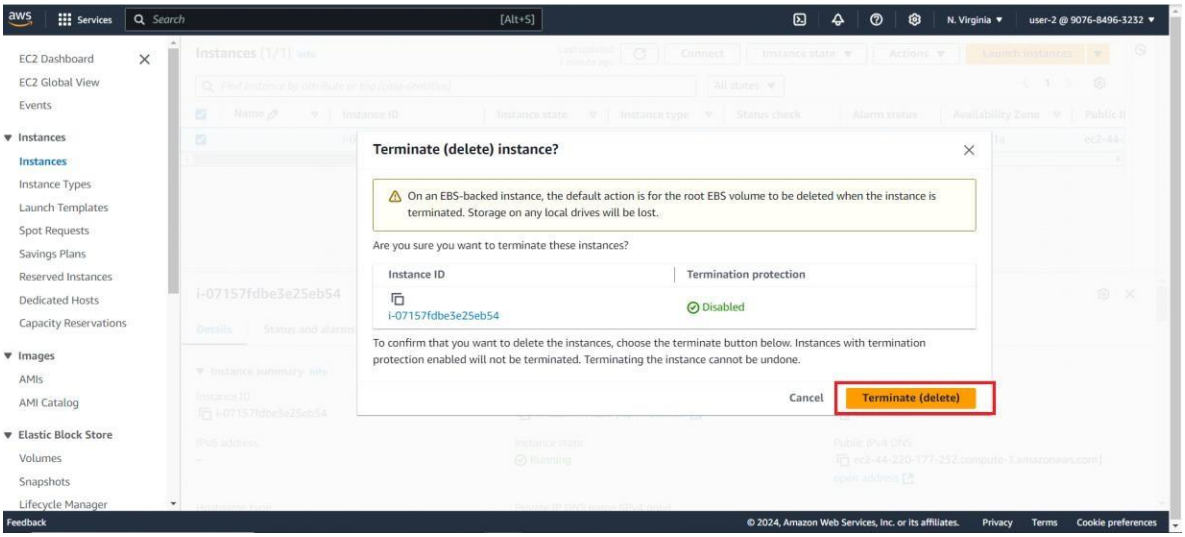

Services
Search
[Alt+S]
N. Virginia
user-2 @ 9076-8496-3232
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
EC2
IAM
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

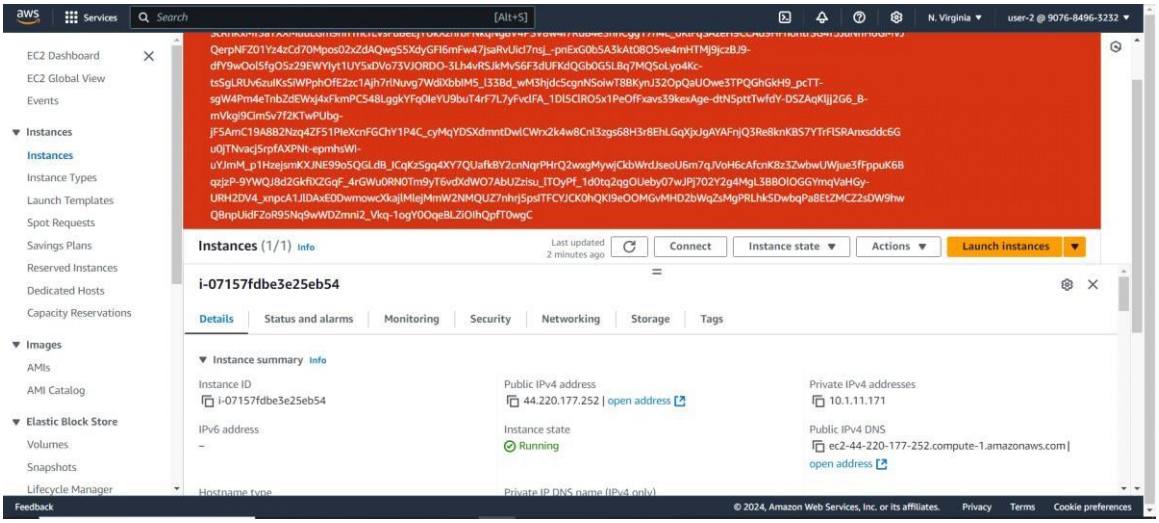

Services
Search
[Alt+S]
N. Virginia
user-2 @ 9076-8496-3232
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 1
Auto Scaling Groups 0
Capacity Reservations 0
Dedicated Hosts 0
Elastic IPs 0
Instances 1
Key pairs 1
Load balancers 0
Placement groups 0
Security groups 3
Snapshots 0
Volumes 1
Account attributes
Default VPC
vpc-0726b2ff49eb399cb
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
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 US East (N. Virginia) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Explore AWS
Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more
10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity.
CloudShell
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-2 @ 9076-8496-3232
EC2 Dashboard
EC2 Global View
Events
Instances
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
Instances (1) Info
Last updated 1 minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv
i-07157fdbe3e25eb54
Running
t2.micro
2/2 checks passec
View alarms
us-east-1a
ec2-44-22
Select an instance
CloudShell
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-2 @ 9076-8496-3232
EC2 Dashboard
EC2 Global View
Events
Instances
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
EC2 > Instances > i-07157fdbe3e25eb54
Instance summary for i-07157fdbe3e25eb54 Info
Updated 1 minute ago
Connect
Instance state
Actions
Instance ID
i-07157fdbe3e25eb54
Public IPv4 address
44.220.177.252 | open address
Private IPv4 addresses
10.1.11.171
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-44-220-177-252.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-171.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-171.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
44.220.177.252 [Public IP]
VPC ID
vpc-0dfd59c61855d73fa (Lab VPC)
AWS Compute Optimizer finding
User: arn:aws:iam::907684963232:user/spl66/user-2 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Retry
IAM Role
–
Subnet ID
subnet-026d5b063839be271 (Public Subnet 1)
Auto Scaling Group name
–
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

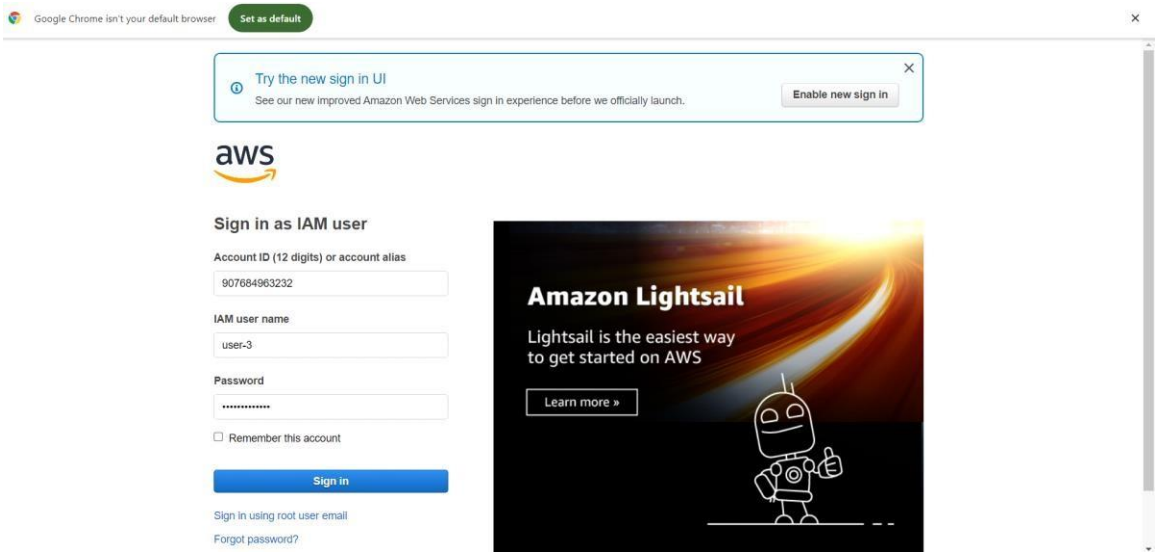

Services
Search
[Alt+S]
N. Virginia
user-2 @ 9076-8496-3232
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Availability Zone
i-07157fdbe3e25eb54
Running
t2.micro
us-east-1a
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
1
2
3
4
i-07157fdbe3e25eb54
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-07157fdbe3e25eb54
Public IPv4 address
44.220.177.252 | open address
Private IPv4 addresses
10.1.11.171
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-44-220-177-252.compute-1.amazonaws.com | open address
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

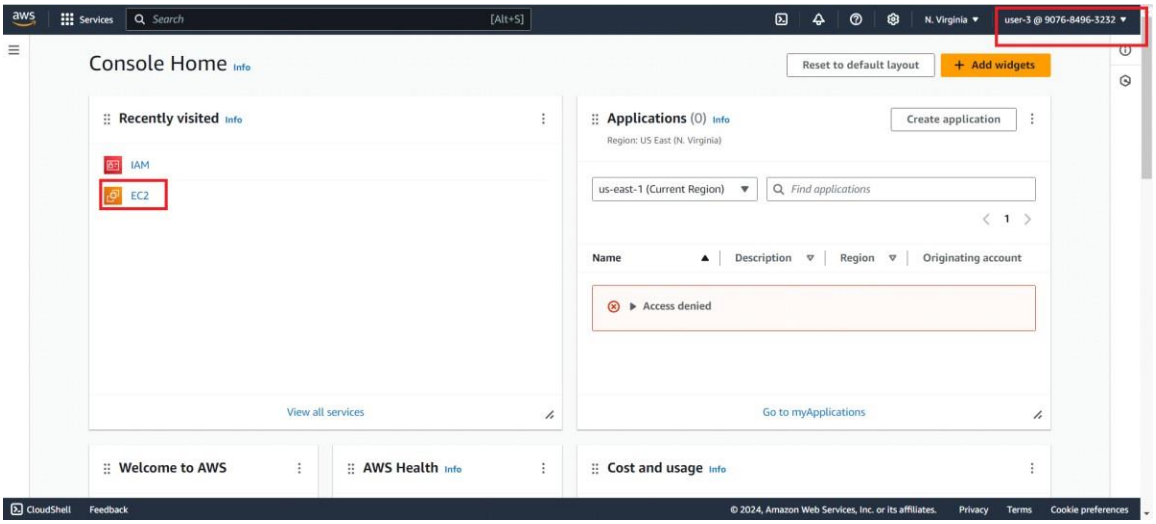

Terminate (delete) instance?
On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.
Are you sure you want to terminate these instances?
Instance ID
Termination protection
i-07157fdbe3e25eb54
Disabled
To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.
Cancel
Terminate (delete)

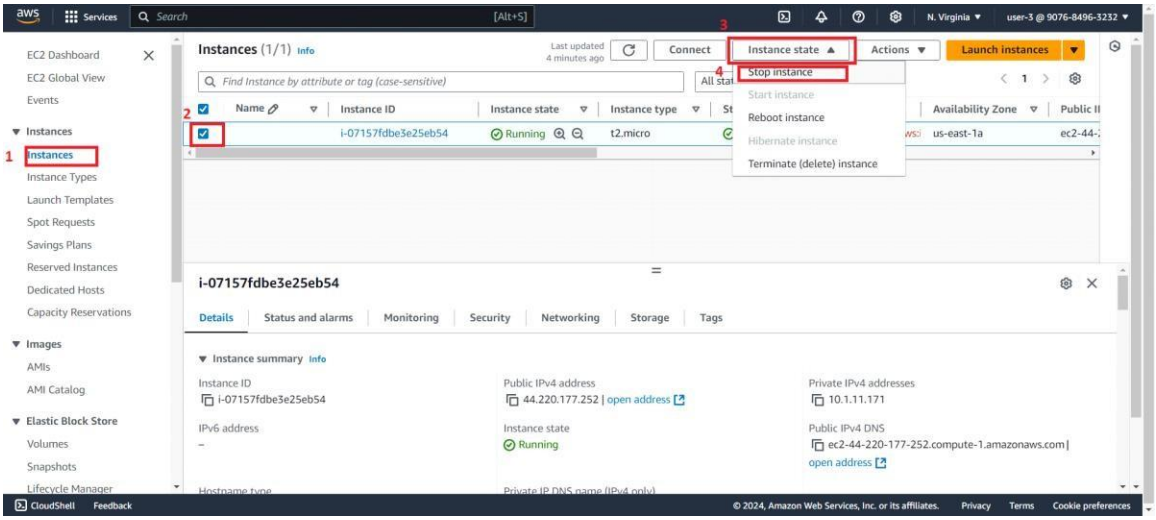


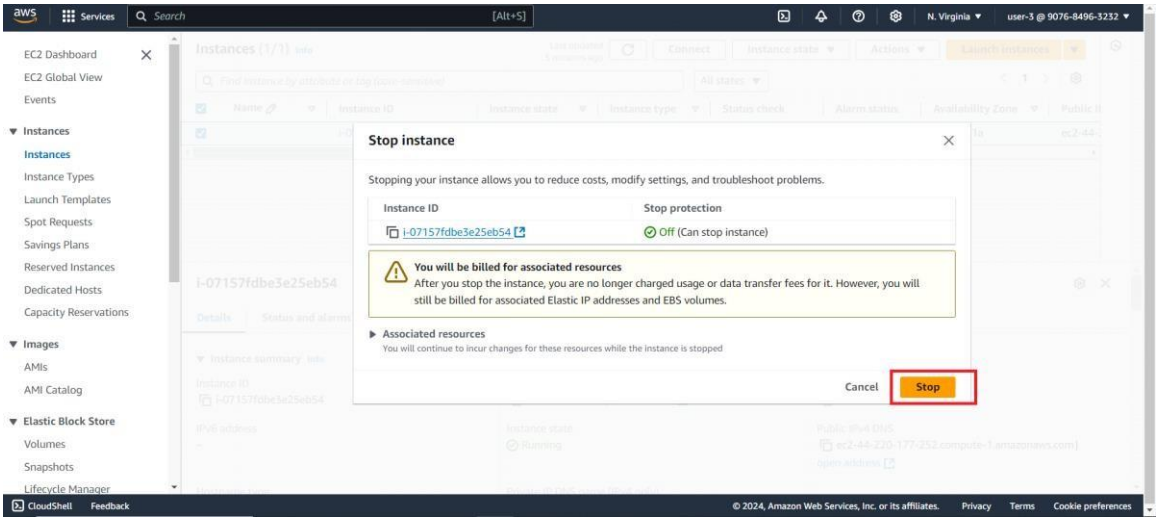
Step 4: User-3 Test EC2 Admin Access:

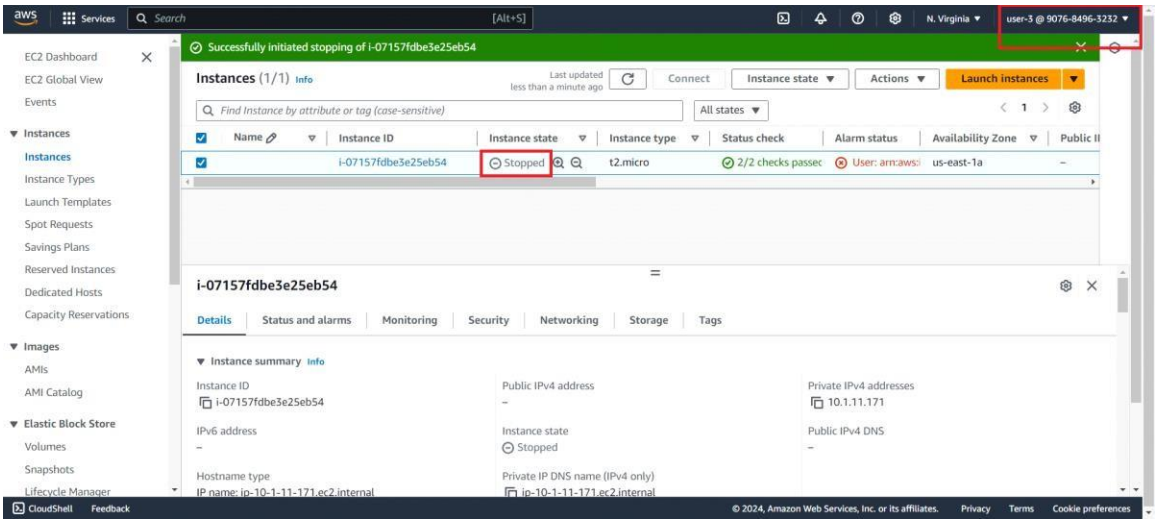
- Sign in as User-3.
- Navigate to the EC2 dashboard.
- Verify that User-3 can view, start, and stop EC2 instances

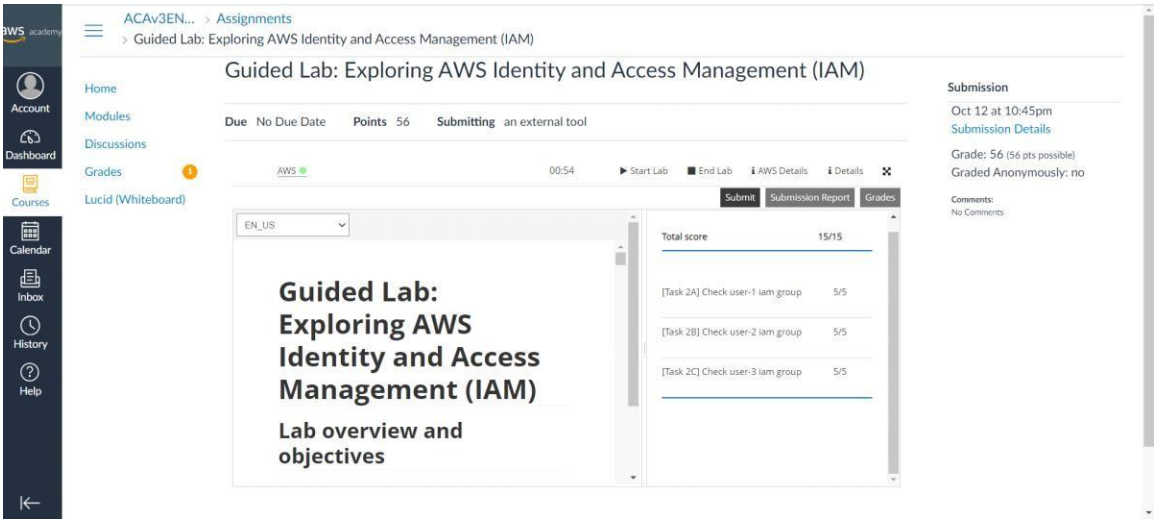



Services
Search
[Alt+S]
N. Virginia
user-3 @ 9076-8496-3232
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
IAM
EC2
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
View all services
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


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
Instances (1/1) Info
Last updated 4 minutes ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Availability Zone
i-07157fdbe3e25eb54
Running
t2.micro
us-east-1a
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
1
2
3
4
i-07157fdbe3e25eb54
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-07157fdbe3e25eb54
Public IPv4 address
44.220.177.252 | open address
Private IPv4 addresses
10.1.11.171
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-44-220-177-252.compute-1.amazonaws.com | open address
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Stop instance
Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.
Instance ID
i-07157fdbe3e25eb54
Stop protection
Off (Can stop instance)
You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.
Associated resources
You will continue to incur charges for these resources while the instance is stopped
Cancel
Stop


Successfully initiated stopping of i-07157fdbe3e25eb54
Instances (1/1)
Connect
Instance state
Actions
Launch instances
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
i-07157fdbe3e25eb54
Stopped
t2.micro
2/2 checks passed
us-east-1a
i-07157fdbe3e25eb54
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary
Instance ID
i-07157fdbe3e25eb54
Public IPv4 address
Private IPv4 addresses
10.1.11.171
IPv6 address
Instance state
Stopped
Public IPv4 DNS
Hostname type
Private IP DNS name (IPv4 only)
ip-10-1-11-171.ec2.internal


ACAv3EN... › Assignments
› Guided Lab: Exploring AWS Identity and Access Management (IAM)
Account
Dashboard
Courses
Calendar
Inbox
History
Help
Home
Modules
Discussions
Grades
Lucid (Whiteboard)
Guided Lab: Exploring AWS Identity and Access Management (IAM)
Due No Due Date Points 56 Submitting an external tool
AWS
00:54
Start Lab
End Lab
AWS Details
Details
Submit
Submission Report
Grades
EN_US
Guided Lab: Exploring AWS Identity and Access Management (IAM)
Lab overview and objectives
Total score 15/15
[Task 2A] Check user-1 iam group 5/5
[Task 2B] Check user-2 iam group 5/5
[Task 2C] Check user-3 iam group 5/5
Submission
Oct 12 at 10:45pm
Submission Details
Grade: 56 (56 pts possible)
Graded Anonymously: no
Comments:
No Comments

Project 6 :Identity and Access Management (IAM) lab

1. Open the Environment on CLI

Start by ensuring you are using the AWS CLI in a terminal environment. Make sure the AWS CLI is installed and properly configured with the correct AWS credentials and region.

- Open Terminal
- Configure AWS CLI
  - Provide the necessary inputs for:
  - AWS Access Key ID
  - AWS Secret Access Key
  - Default region name (e.g., us-east-1)
  - Default output format (e.g., json)

2. Task 1: Explore Users and Groups Step 1: List IAM Users

List all the IAM users to get an overview of pre-created users.

Step 2: List IAM Groups

Retrieve a list of all IAM groups.

Step 3: View User Details

To inspect a specific user, use the following command by replacing <user_name> with the actual username.

aws iam get-user --user-name <user_name>

```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-1

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-2

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDA2CTFHBEV6W4MDCTIL",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-3

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDA2CTFHBEV3D3PPDNGT",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

Step 4: List Users in a Specific Group

To get a list of all users that belong to a specific group, replace <group_name> with the group name.

aws iam get-group --group-name <group_name>

```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name S3-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA2CTFHBEV7R2X36ALH",
        "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Admin

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

3. Task 2: Inspect IAM Policies

Step 1: List Attached Policies for a Group

This command lists all policies attached to a specific group.

```
┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name S3-Support

{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}

┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Support

{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}

┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Admin

{
    "AttachedPolicies": []
}
```

Step 2: View Policy Details

To view the details of a specific policy attached to the group, use the policy's ARN (Amazon Resource Name) from the previous command's output.

```
┌──(root㉿kali)-[~]
└─# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}
```

```
┌──(root㉿kali)-[~]
└─# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}
```

4. Task 3: Add Users to Groups

Now, add users to specific groups according to their role requirements.

Step 1: Add User-1 to S3-Support Group

Grant User-1 read-only access to S3 by adding them to the S3-Support group.

```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-1 --group-name S3-Support
```

Step 2: Add User-2 to EC2-Support Group

Give User-2 read-only access to EC2 resources.

```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-2 --group-name EC2-Support
```

Step 3: Add User-3 to EC2-Admin Group

Assign User-3 permissions to view, start, and stop EC2 instances by adding them to the EC2-Admin group.

```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-3 --group-name EC2-Admin
```

Step 4: Verify Users are Added to Groups

Verify that the users are properly added to the respective groups by listing users within each group.

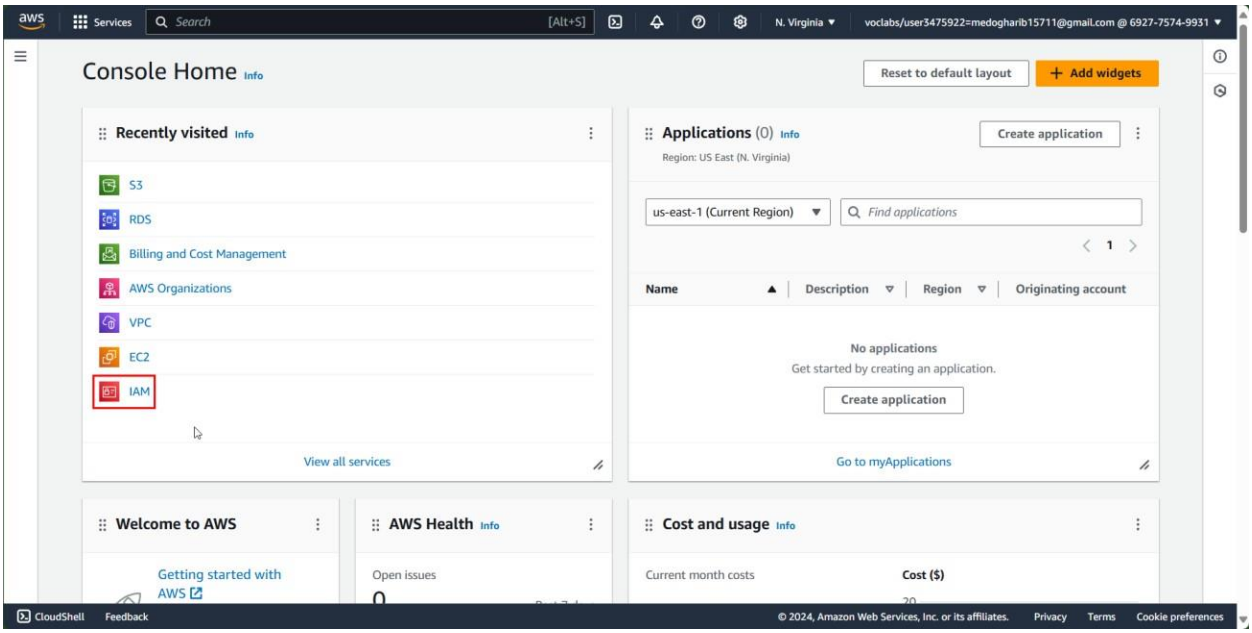
```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name S3-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA2CTFHBEV7R2X36ALH",
        "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

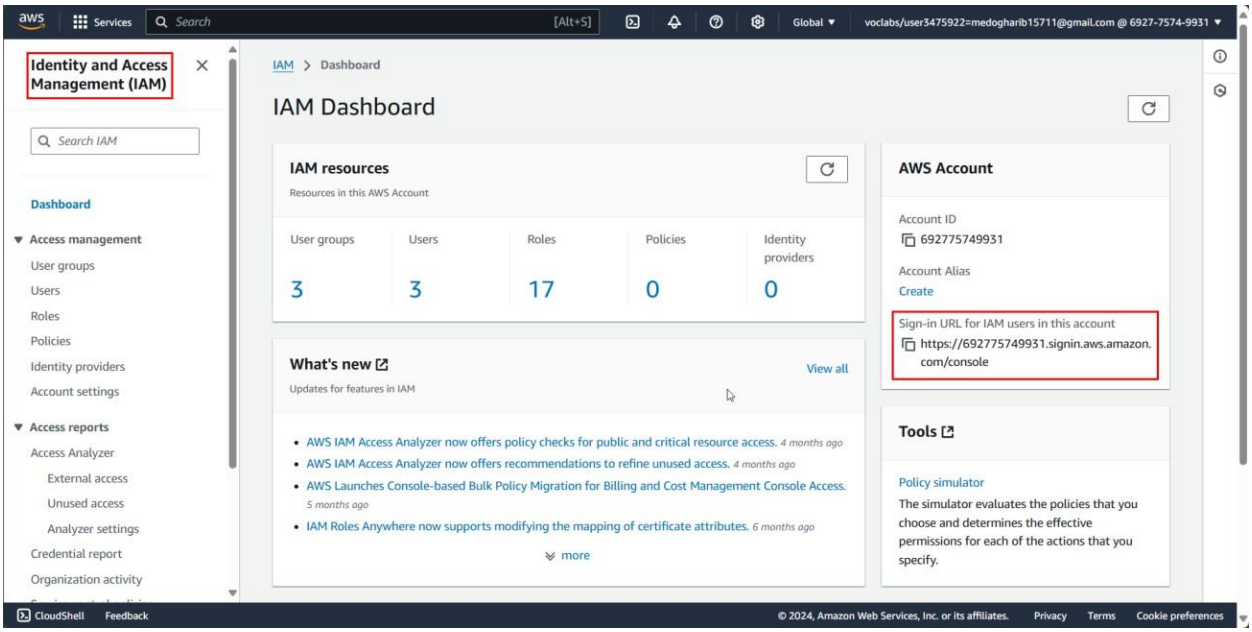
```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Support

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA2CTFHBEV6W4MDCTIL",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Admin

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA2CTFHBEV3D3PPDNGT",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

5. Task 4: Test Permissions

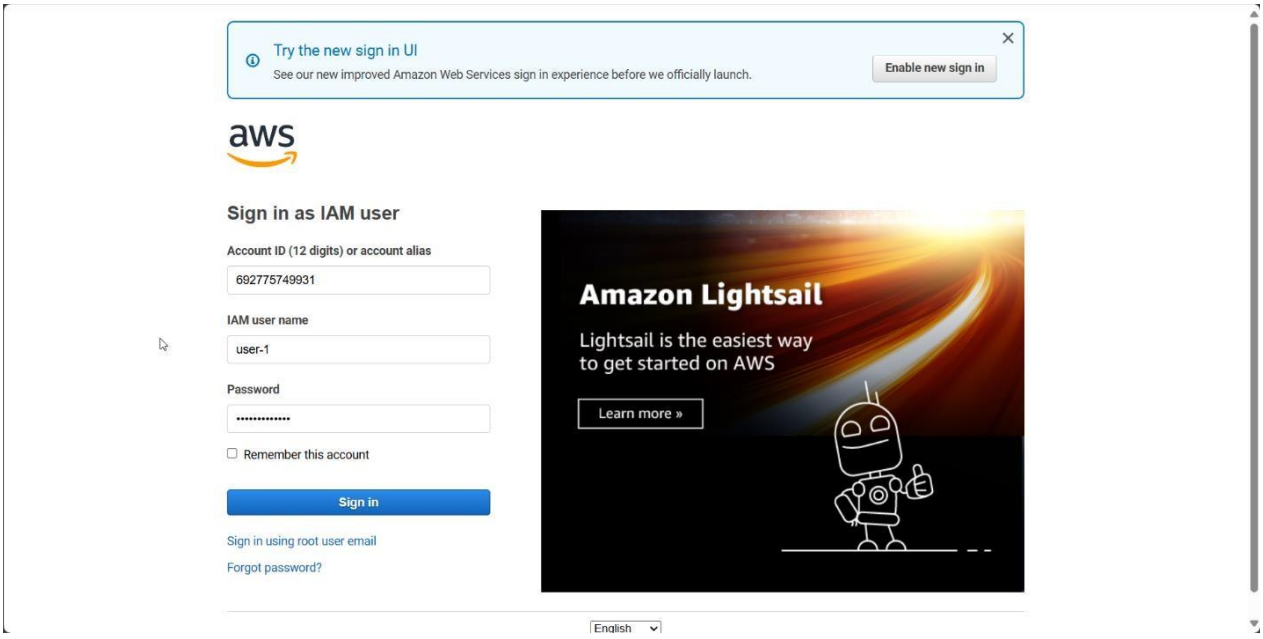
Step 1: Get the console sign-in URL

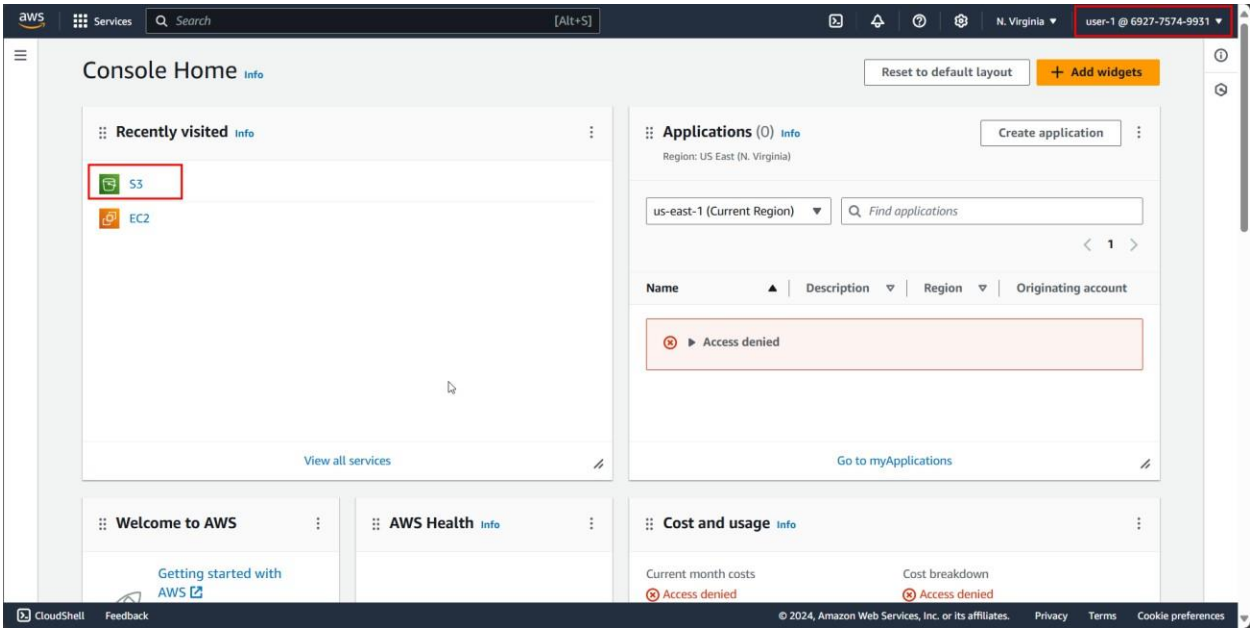


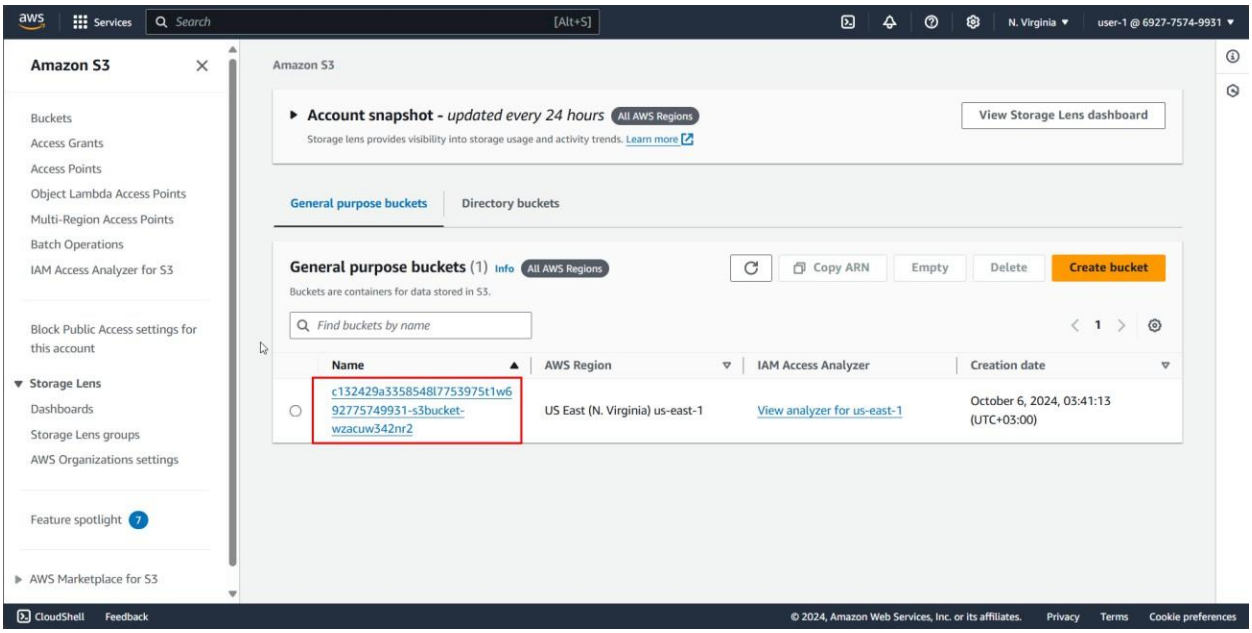


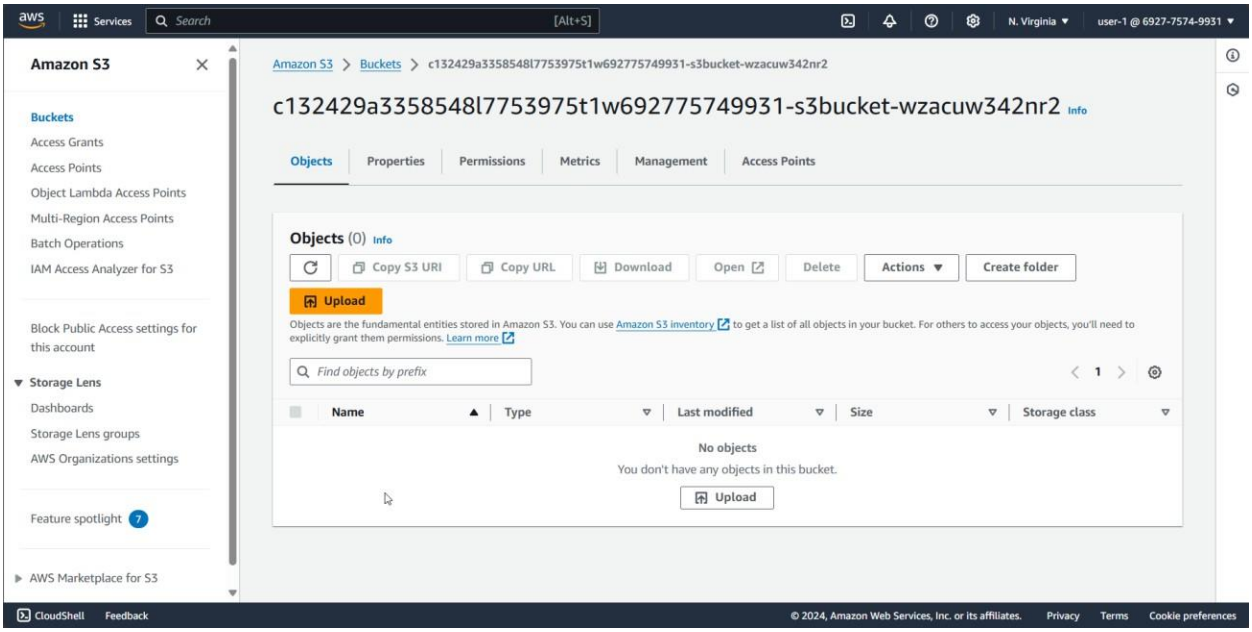
Step 2: User-1 Test S3 Read-only Access:

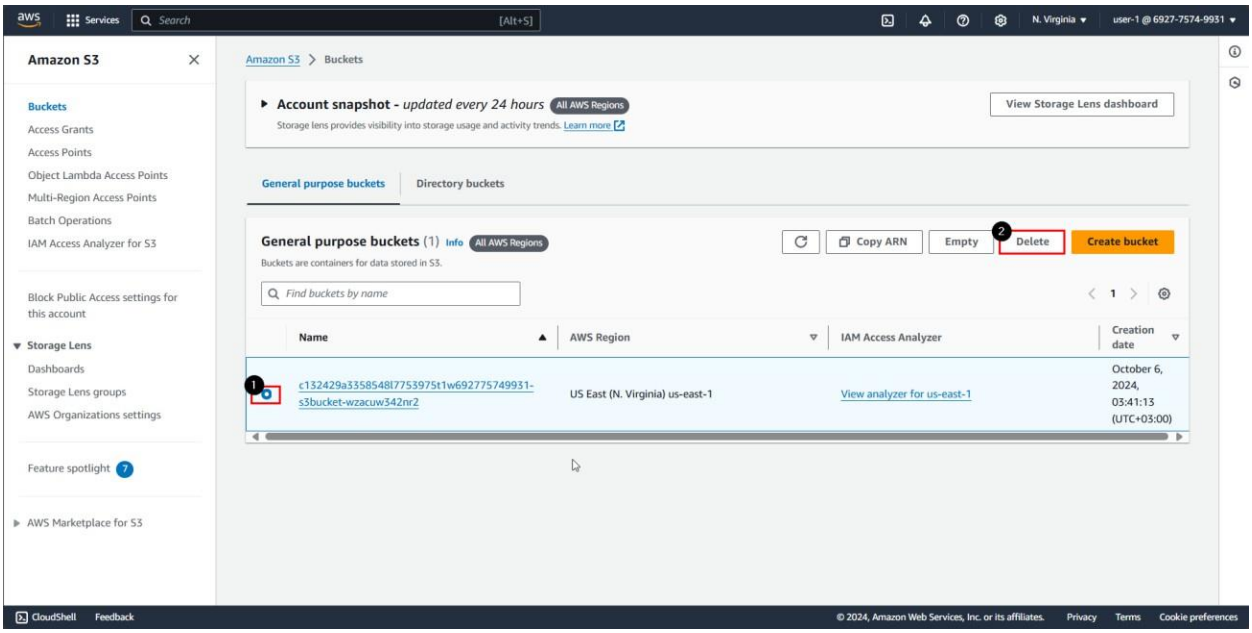
- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.
- Navigate to the S3 service and try to list buckets.
- Try to perform any write operations (like deleting bucket), which should fail due to read-only access.

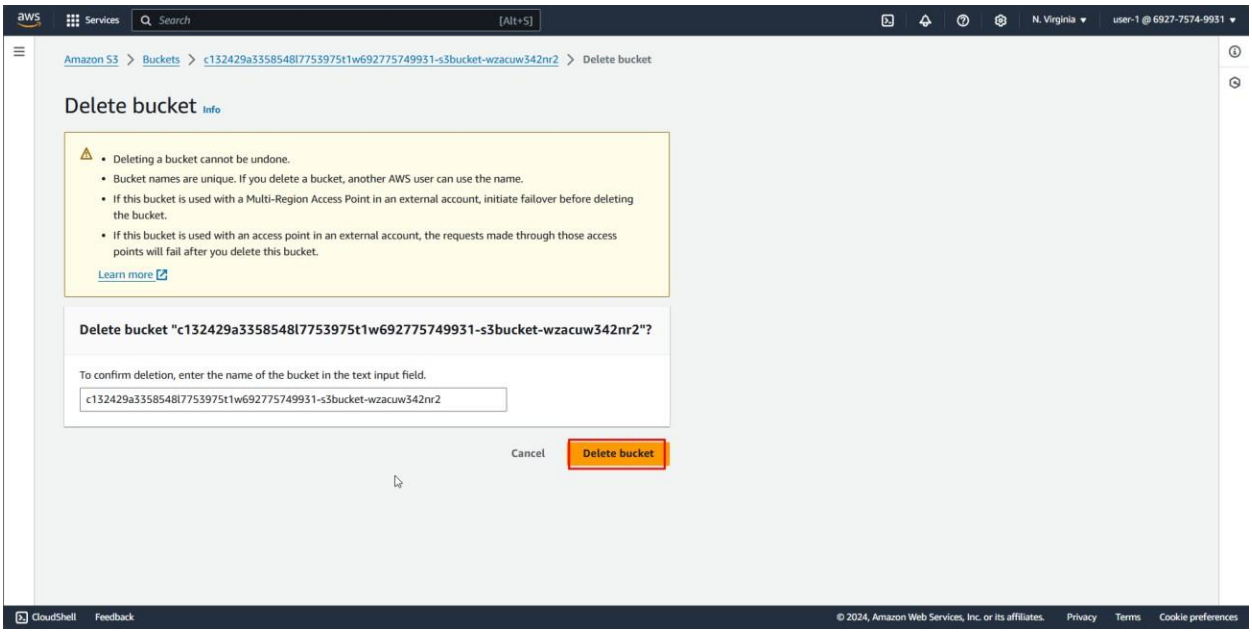


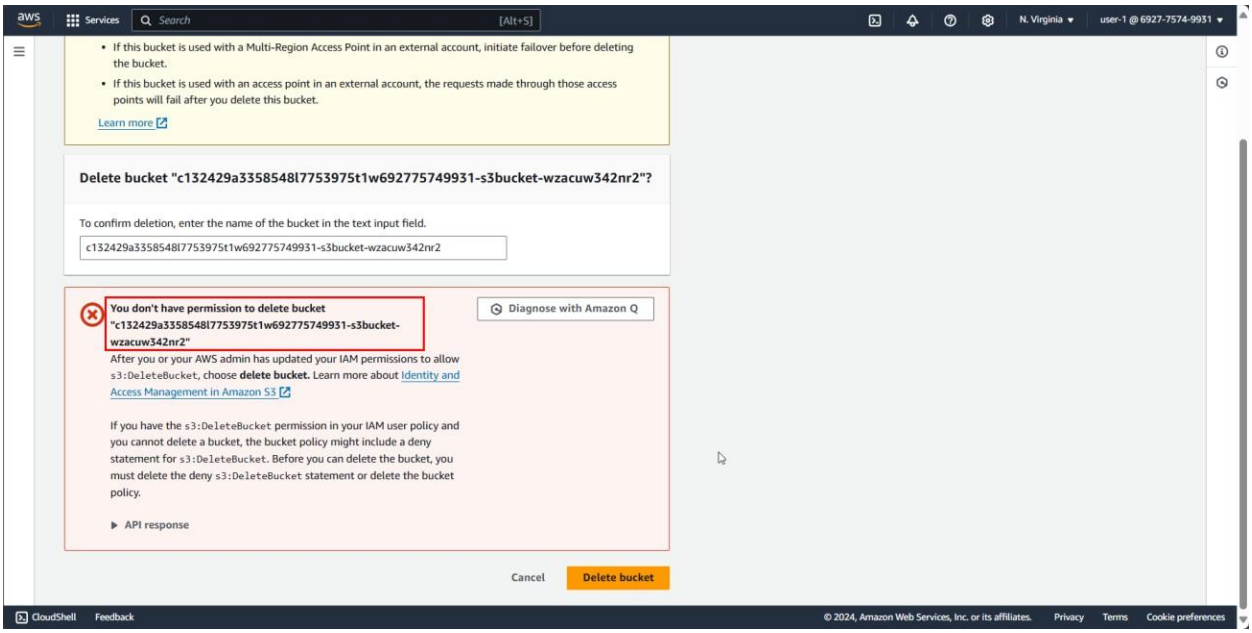



aws
Services
Search
[Alt+S]
N. Virginia
user-1 @ 6927-7574-9931
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 6, 2024, 03:41:13 (UTC+03:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
user-1 @ 6927-7574-9931
Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets > c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
Find objects by prefix
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

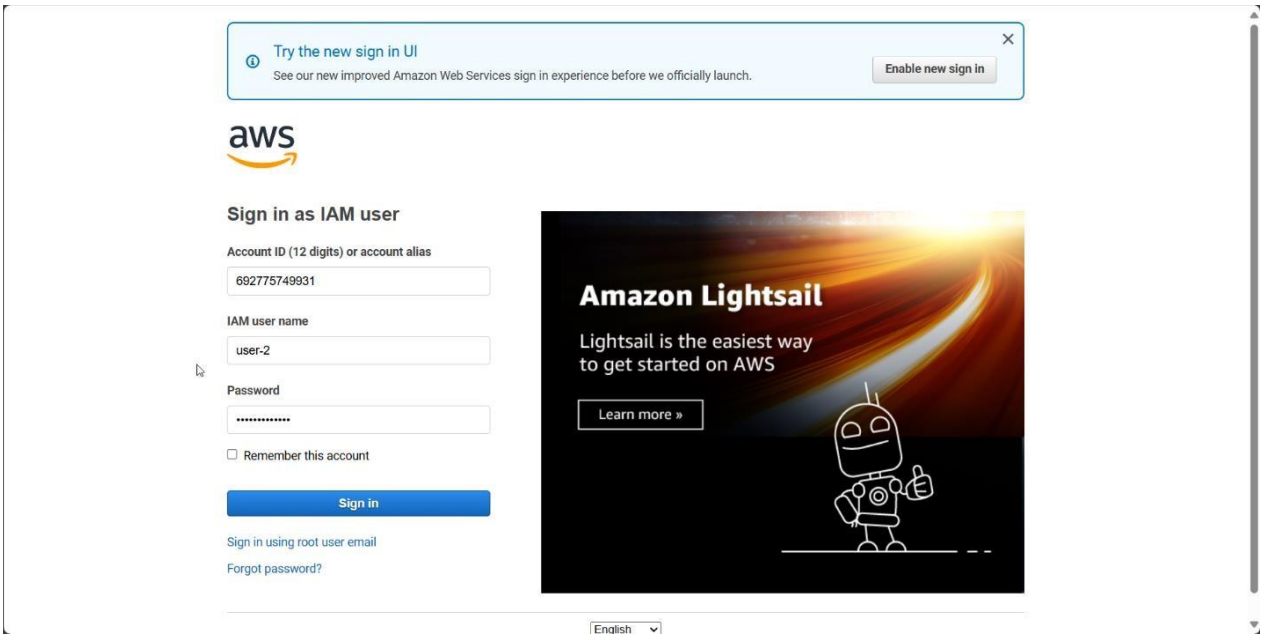

Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 6, 2024, 03:41:13 (UTC+03:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

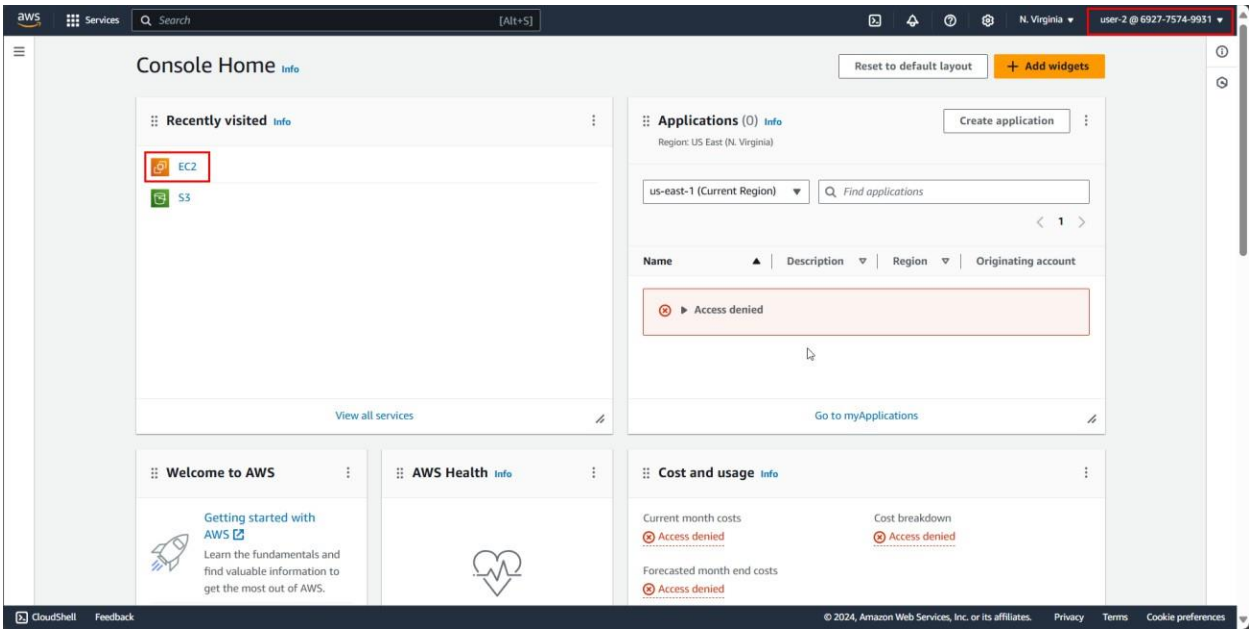

Amazon S3 > Buckets > c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2 > Delete bucket
Delete bucket Info
Deleting a bucket cannot be undone.
Bucket names are unique. If you delete a bucket, another AWS user can use the name.
If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
Learn more
Delete bucket "c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2"?
To confirm deletion, enter the name of the bucket in the text input field.
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2
Cancel
Delete bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

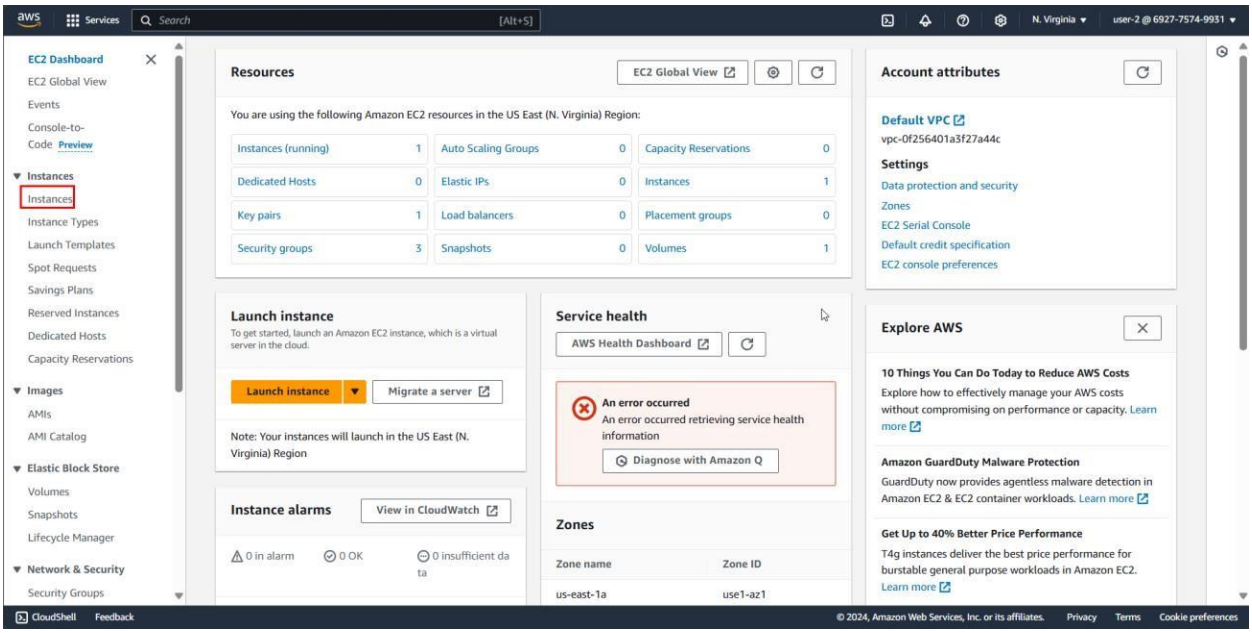

aws
Services
Search
[Alt+S]
N. Virginia
user-1 @ 6927-7574-9931
If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
Learn more
Delete bucket "c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2"?
To confirm deletion, enter the name of the bucket in the text input field.
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2
You don't have permission to delete bucket "c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2"
Diagnose with Amazon Q
After you or your AWS admin has updated your IAM permissions to allow s3:DeleteBucket, choose delete bucket. Learn more about Identity and Access Management in Amazon S3
If you have the s3:DeleteBucket permission in your IAM user policy and you cannot delete a bucket, the bucket policy might include a deny statement for s3:DeleteBucket. Before you can delete the bucket, you must delete the deny s3:DeleteBucket statement or delete the bucket policy.
API response
Cancel
Delete bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

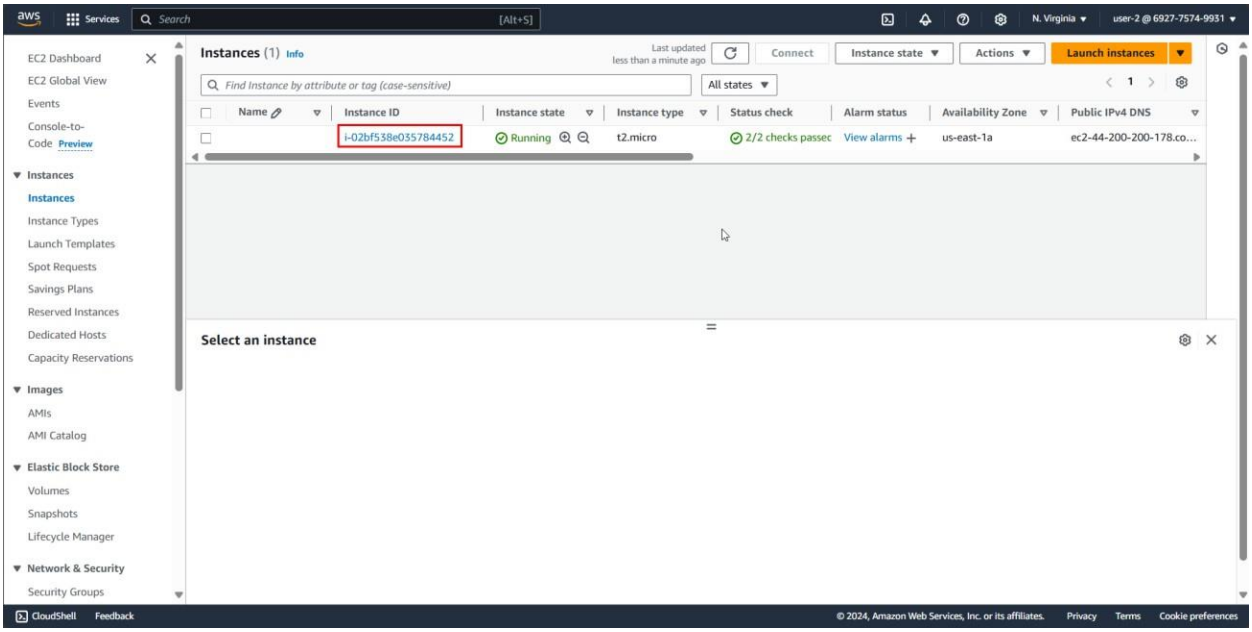
Step 3: User-2 Test EC2 Read-only Access:

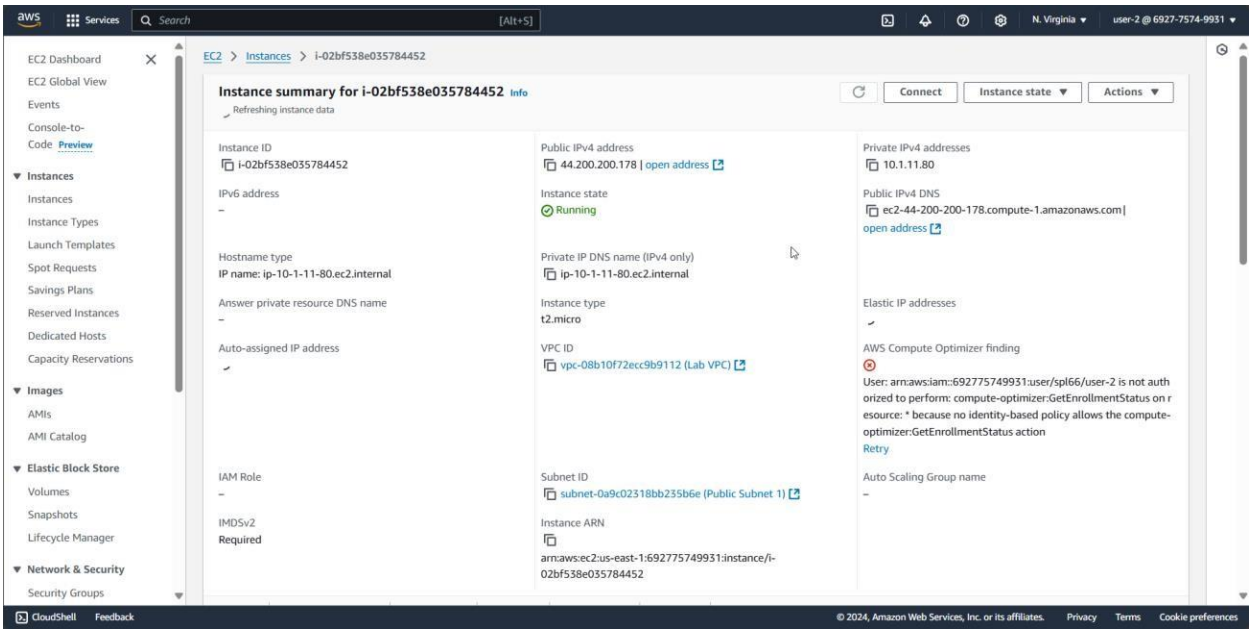
- **Sign in as User-2.**
- **Navigate to the EC2 dashboard.**
- **Check if User-2 can view instances but cannot modify (start/stop) them.**

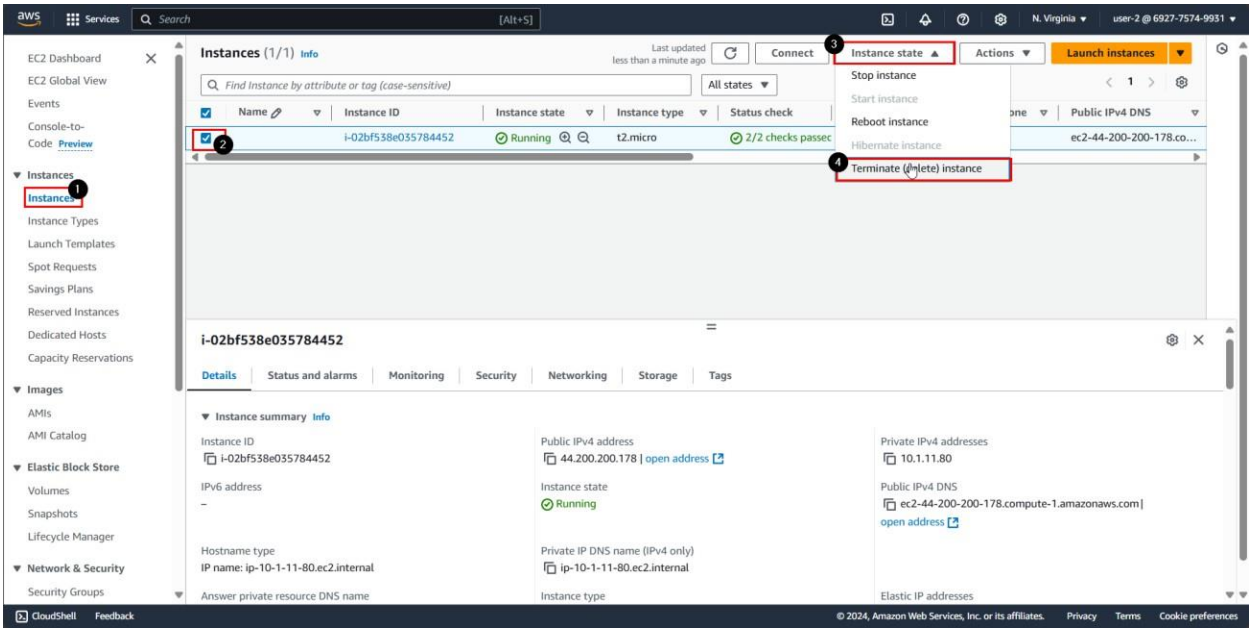


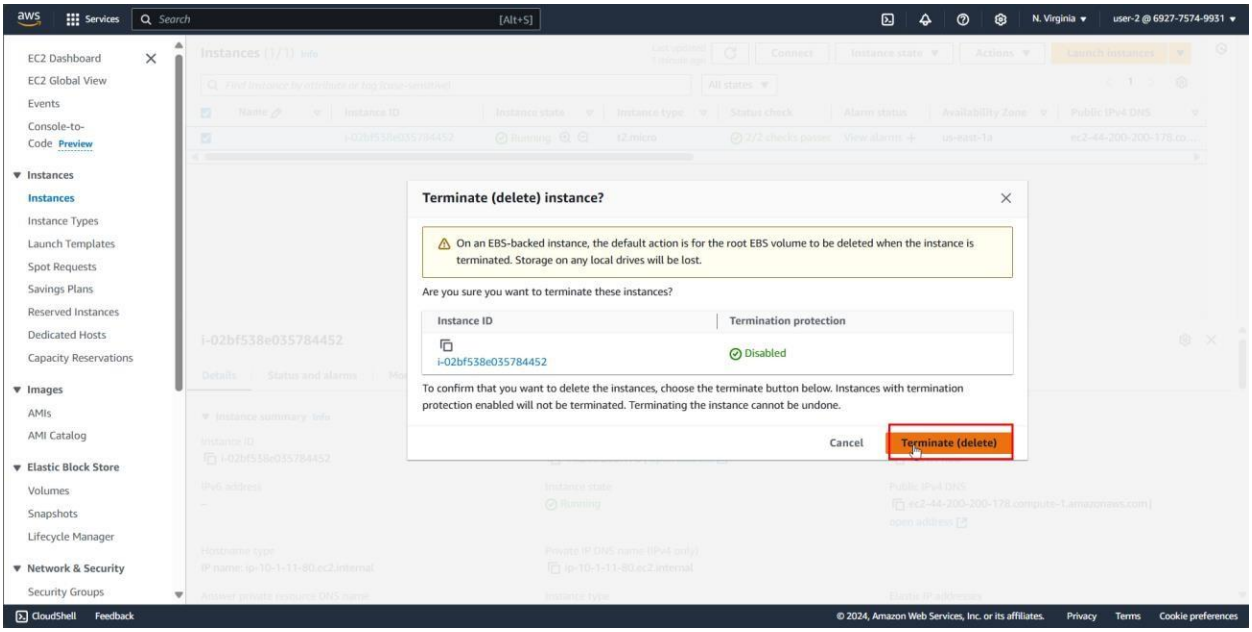


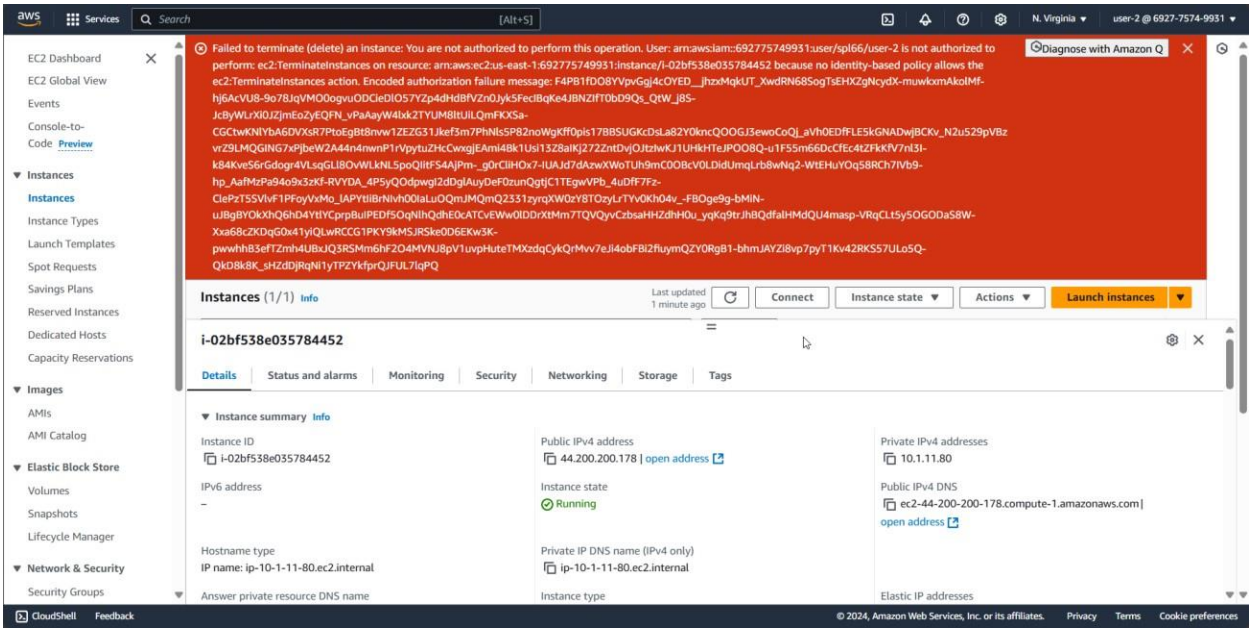

Services
Search
[Alt+S]
N. Virginia
user-2 @ 6927-7574-9931
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 1
Auto Scaling Groups 0
Capacity Reservations 0
Dedicated Hosts 0
Elastic IPs 0
Instances 1
Key pairs 1
Load balancers 0
Placement groups 0
Security groups 3
Snapshots 0
Volumes 1
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 US East (N. Virginia) Region
Instance alarms
View in CloudWatch
0 in alarm
0 OK
0 insufficient data
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Zones
Zone name
Zone ID
us-east-1a
use1-az1
Account attributes
Default VPC
vpc-0f256401a3f27a44c
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
Explore AWS
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
Get Up to 40% Better Price Performance
T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-2 @ 6927-7574-9931
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
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
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
i-02bf538e035784452
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-44-200-200-178.co...
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-2 @ 6927-7574-9931
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
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
EC2 > Instances > i-02bf538e035784452
Instance summary for i-02bf538e035784452 Info
Refreshing instance data
Connect
Instance state
Actions
Instance ID
i-02bf538e035784452
Public IPv4 address
44.200.200.178 | open address
Private IPv4 addresses
10.1.11.80
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-44-200-200-178.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-80.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-80.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
VPC ID
vpc-08b10f72ecc9b9112 (Lab VPC)
AWS Compute Optimizer finding
User: arn:aws:iam::692775749931:user/spl66/user-2 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Retry
IAM Role
–
Subnet ID
subnet-0a9c02318bb235b6e (Public Subnet 1)
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:us-east-1:692775749931:instance/i-02bf538e035784452
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

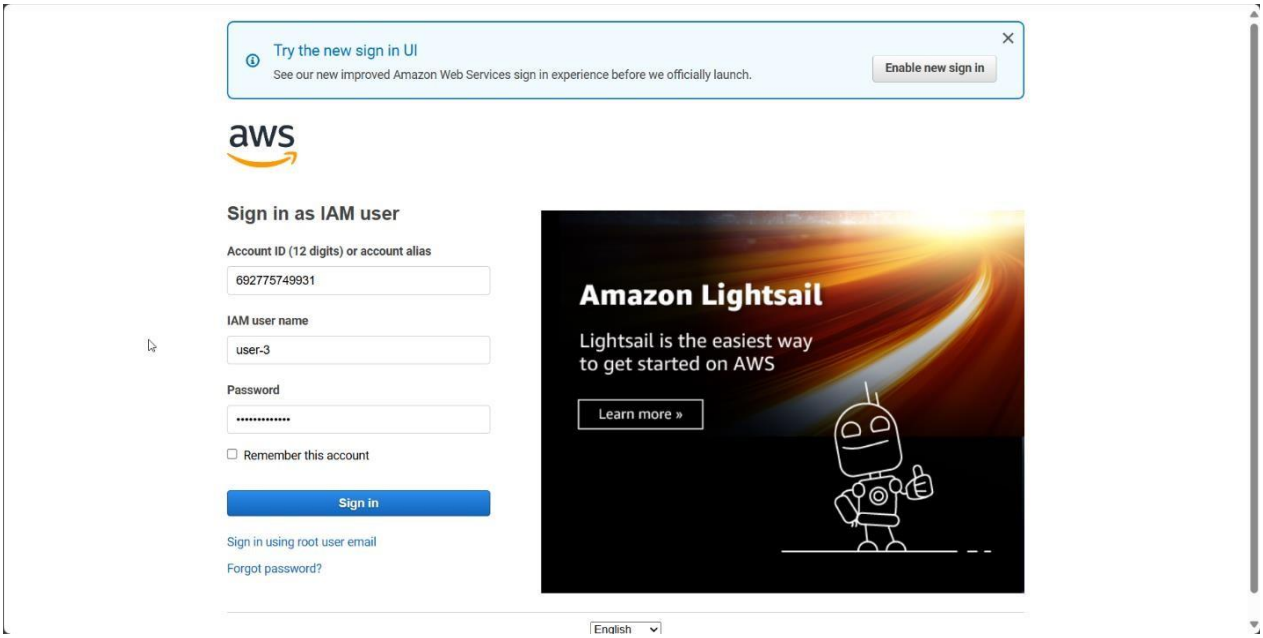

Services
Search
[Alt+S]
N. Virginia
user-2 @ 6927-7574-9931
Instances (1/1) Info
Last updated less than a minute ago
Connect
3
Instance state
Actions
Launch instances
Stop instance
Start instance
Reboot instance
Hibernate instance
4
Terminate (delete) instance
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Public IPv4 DNS
i-02bf538e035784452
Running
t2.micro
2/2 checks passed
ec2-44-200-200-178.co...
2
1
Instances
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
i-02bf538e035784452
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-02bf538e035784452
Public IPv4 address
44.200.200.178 | open address
Private IPv4 addresses
10.1.11.80
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-44-200-200-178.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-80.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-80.ec2.internal
Answer private resource DNS name
Instance type
Elastic IP addresses
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

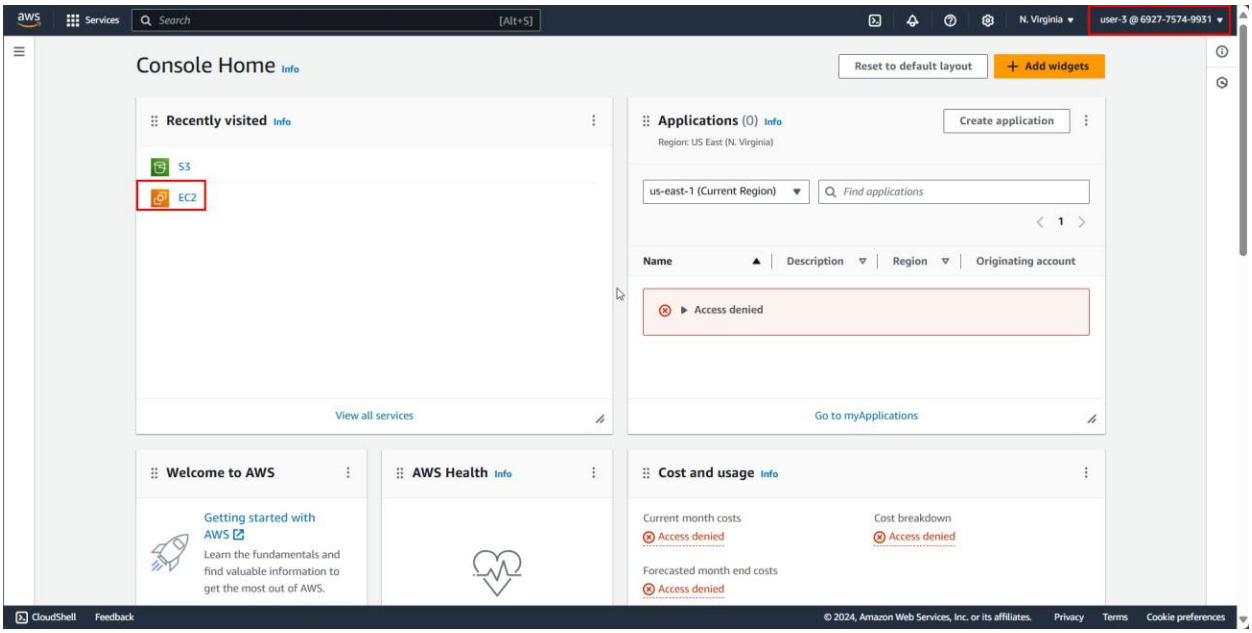

Terminate (delete) instance?
On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.
Are you sure you want to terminate these instances?
Instance ID
Termination protection
i-02bf538e035784452
Disabled
To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.
Cancel
Terminate (delete)

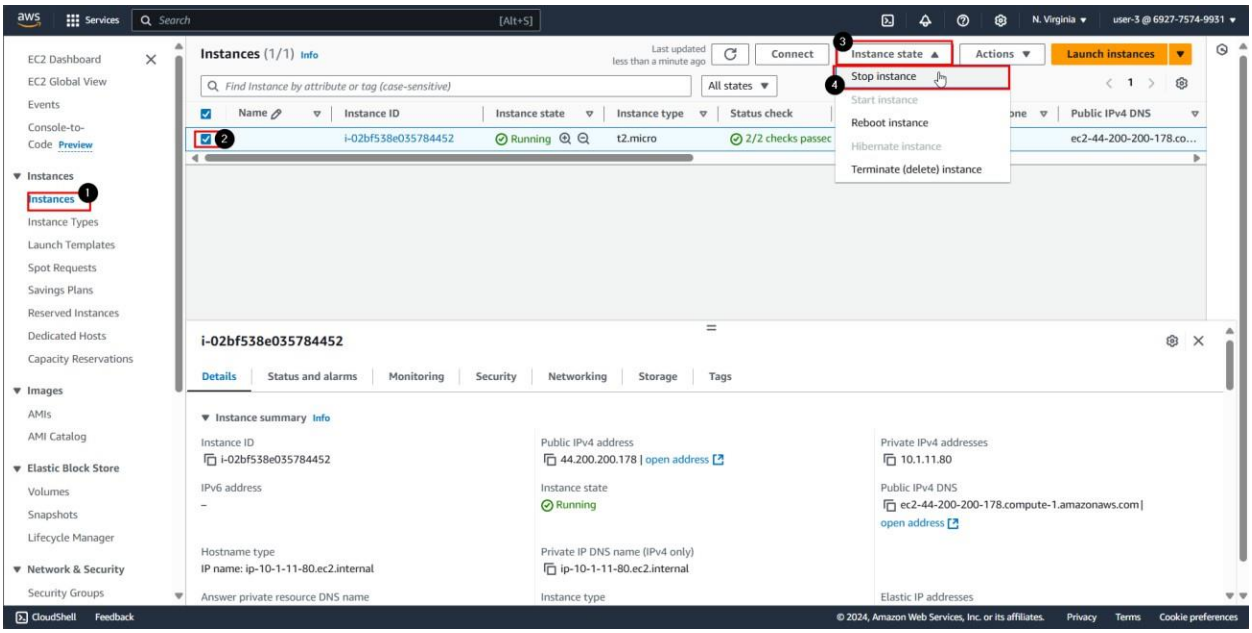

Failed to terminate (delete) an instance: You are not authorized to perform this operation.
Diagnose with Amazon Q
Instances (1/1)
Connect
Instance state
Actions
Launch instances
i-02bf538e035784452
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary
Instance ID
i-02bf538e035784452
Public IPv4 address
44.200.200.178 | open address
Private IPv4 addresses
10.1.11.80
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-44-200-200-178.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-80.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-80.ec2.internal

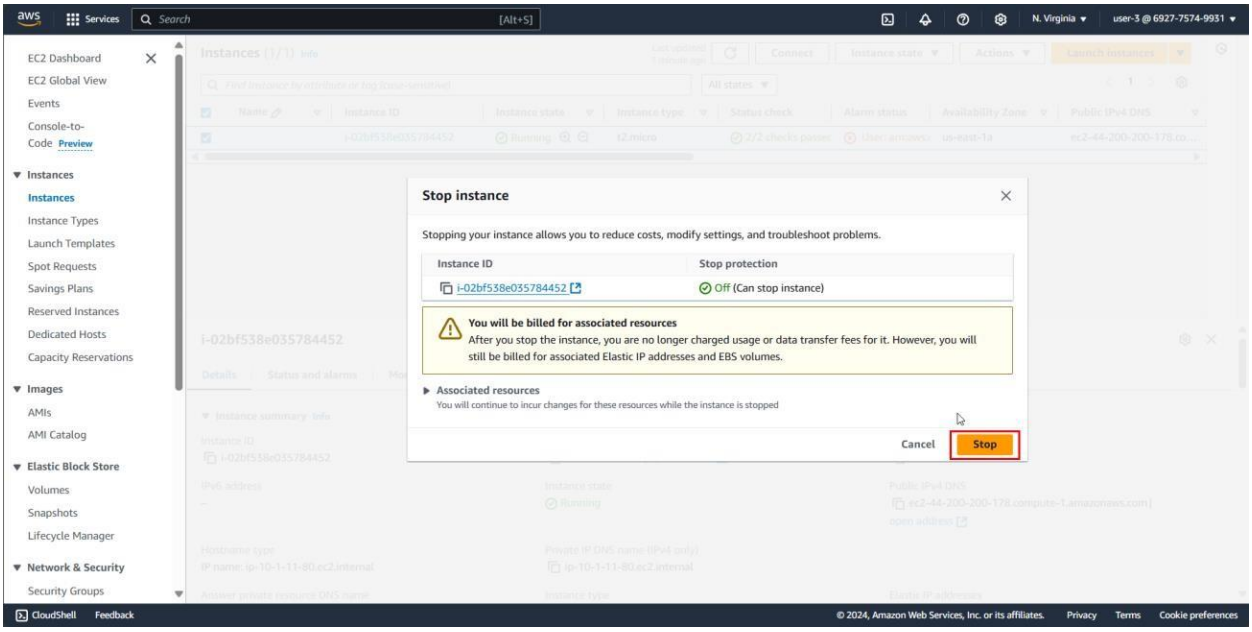
Step 4: User-3 Test EC2 Admin Access:

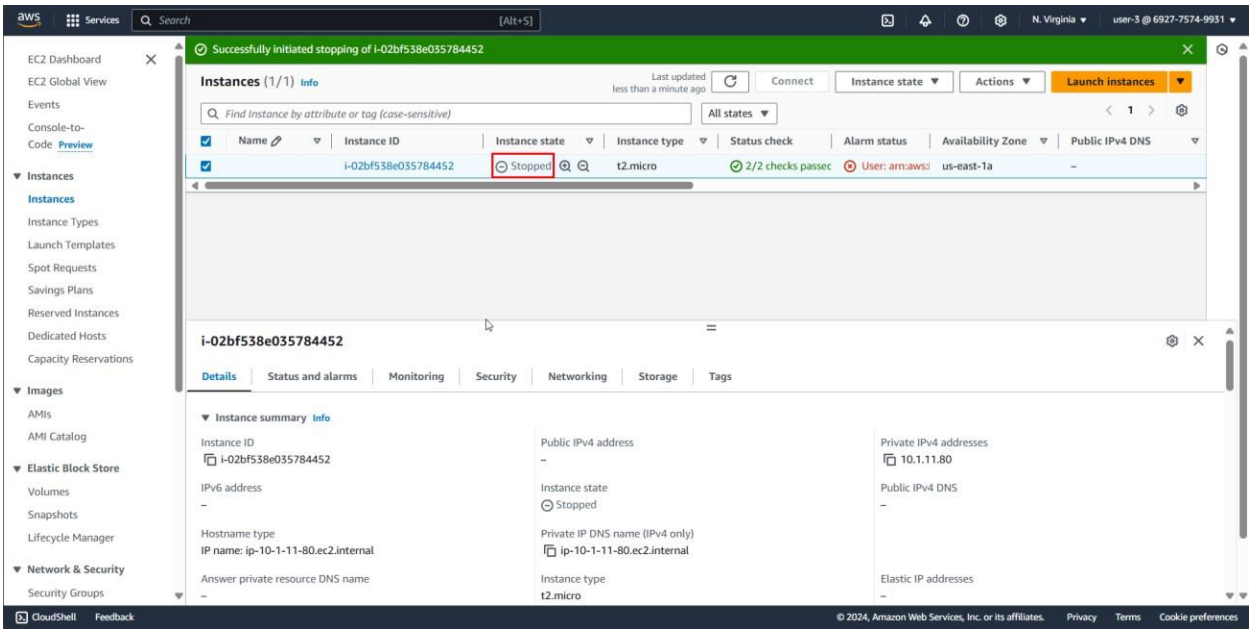
- **Sign in as User-3.**
- **Navigate to the EC2 dashboard.**
- **Verify that User-3 can view, start, and stop EC2 instances.**






Services
Search
[Alt+S]
N. Virginia
user-3 @ 6927-7574-9931
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
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
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
Name
Instance ID
Instance state
Instance type
Status check
Public IPv4 DNS
i-02bf538e035784452
Running
t2.micro
2/2 checks passed
ec2-44-200-200-178.co...
i-02bf538e035784452
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-02bf538e035784452
Public IPv4 address
44.200.200.178 | open address
Private IPv4 addresses
10.1.11.80
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-44-200-200-178.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-80.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-80.ec2.internal
Answer private resource DNS name
Instance type
Elastic IP addresses
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-3 @ 6927-7574-9931
Stop instance
Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.
Instance ID
Stop protection
i-02bf538e035784452
Off (Can stop instance)
You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.
Associated resources
You will continue to incur charges for these resources while the instance is stopped
Cancel
Stop
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Successfully initiated stopping of i-02bf538e035784452
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
i-02bf538e035784452
Stopped
t2.micro
2/2 checks passec
User: arn:aws:
us-east-1a
i-02bf538e035784452
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-02bf538e035784452
Public IPv4 address
Private IPv4 addresses
10.1.11.80
IPv6 address
Instance state
Stopped
Public IPv4 DNS
Hostname type
IP name: ip-10-1-11-80.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-80.ec2.internal
Answer private resource DNS name
Instance type
t2.micro
Elastic IP addresses
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Due No Due Date **Points** 56 **Submitting** an external tool

Guided Lab: Exploring AWS Identity and Access Management (IAM) Lab Assignments	Sep 27 at 5:18pm	56 / 56

Project 9 : Creating an Amazon virtual private cloud (VPC)

Access and

Configure AWS CLI

Step 1: Open the

Lab Environment

- **Start your lab**

session as directed. Step 2: Run the Lab

- **Initiate the lab session by**

clicking the "Run Lab" button. Step 3: Access AWS CLI

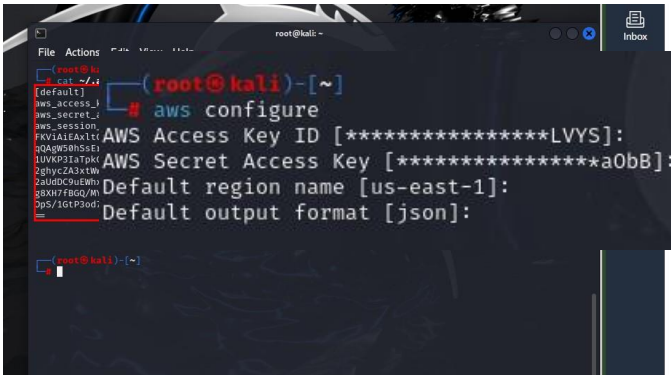
- **Navigate to the AWS Details panel.**
- **Locate the AWS CLI section and click**

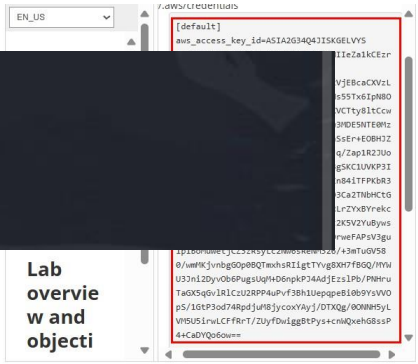
"Show" to reveal the CLI credentials. Step 4: Configure AWS CLI

- **Open Command Prompt (cmd) on your Windows machine.**
- **Enter the following command to start the configuration process: When prompted, input the AWS credentials provided:**

“aws configure”

- **AWS Access Key ID: [Enter your aws_access_key_id]**
- **AWS Secret Access Key: [Enter your aws_secret_access_key]**
- **Default region name: [Enter the desired AWS region, e.g., us-west-2]**
- **Default output format: [Enter your preferred output format, e.g., json]**


root@kali: ~
File Actions
Inbox
(root㉿kali)-[~]
aws configure
AWS Access Key ID [****************LVYS]:
AWS Secret Access Key [****************aObB]:
Default region name [us-east-1]:
Default output format [json]:


EN_US
Lab overview and objecti
[default]
aws_access_key_id=ASIA2G34Q4JISKGELVYS

Task 1: Creating a VPC

1. Create the VPC:

```
┌──(root㉿kali)-[~]
└─# aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications 'ResourceType=vpc,Tags=[{Key=
Name,Value=Lab VPC}]'

{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-07314e6443821a60c",
        "State": "pending",
        "VpcId": "vpc-0c3d8065af0fccdba",
        "OwnerId": "701951435345",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-07b8d3a6d54b43723",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "Lab VPC"
            }
        ]
    }
}
```

2. Enable DNS hostnames for the VPC: First, get the VPC ID:

3. Use the VPC ID to enable DNS hostnames:

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# aws ec2 describe-vpcs --filters "Name=cidr-block,Values=10.0.0.0/16" --query 'Vpcs[0].VpcId' --outp
ut text

vpc-01dcc1827af9ef5af

┌──(root㉿kali)-[~]
└─# aws ec2 modify-vpc-attribute --vpc-id vpc-01dcc1827af9ef5af --enable-dns-hostnames "{\"Value\":true
}"
```

Task 2: Creating Subnets

Task 2.1: Creating a Public Subnet

1. Create the Public Subnet:

```
┌──(root㉿kali)-[~]
└─# aws ec2 create-subnet --vpc-id vpc-01dcc1827af9ef5af --cidr-block 10.0.0.0/24 --availability-zone u
s-east-1a --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public Subnet}]'

{
    "Subnet": {
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "AvailableIpAddressCount": 251,
        "CidrBlock": "10.0.0.0/24",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-094f06a9e81c23778",
        "VpcId": "vpc-01dcc1827af9ef5af",
        "OwnerId": "701951435345",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Public Subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:701951435345:subnet/subnet-094f06a9e81c23778",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        }
    }
}
```

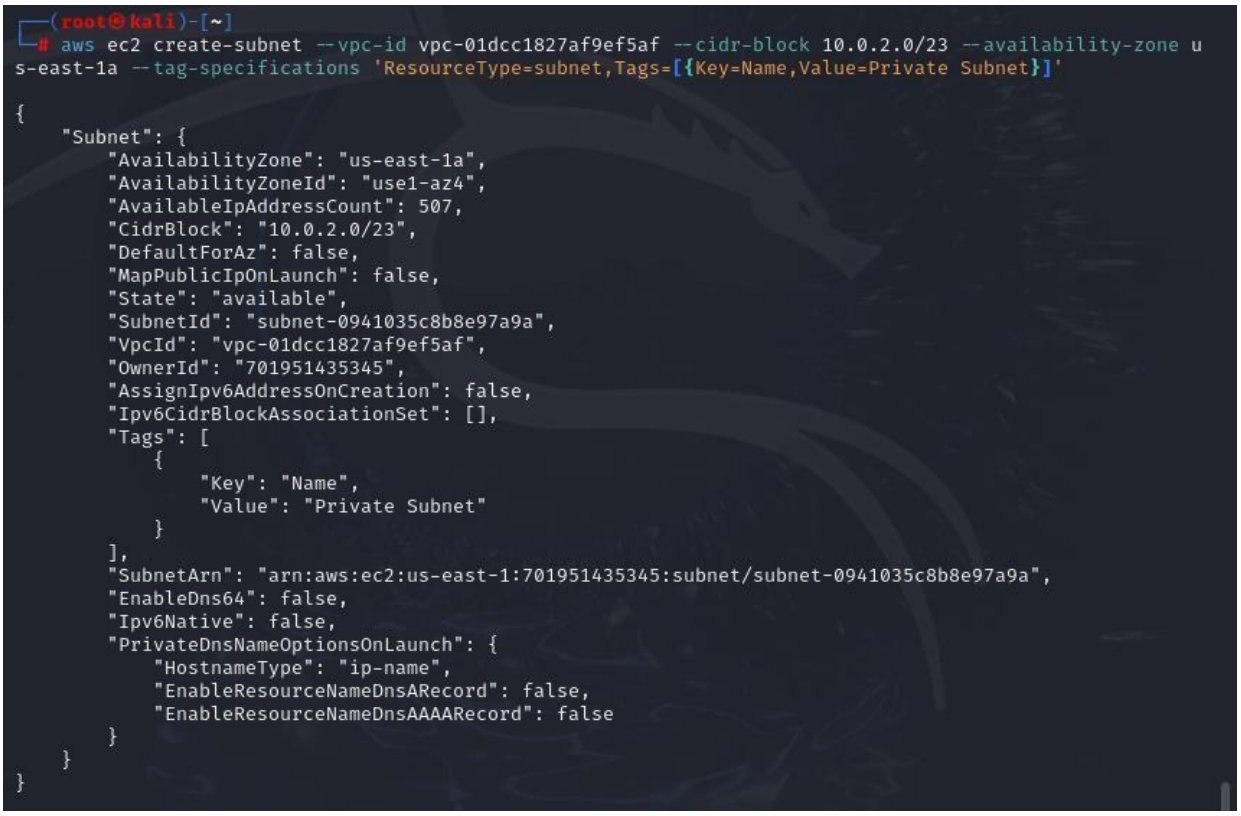
2. Enable Auto-assign Public IP for Public Subnet: Get the subnet ID for the public subnet:

3. Enable auto-assign public IPv4:

```
┌──(root㉿kali)-[~]
└─# aws ec2 describe-subnets --filters "Name=cidr-block,Values=10.0.0.0/24" --query 'Subnets[0].SubnetI
d' --output text

subnet-094f06a9e81c23778

┌──(root㉿kali)-[~]
└─# aws ec2 modify-subnet-attribute --subnet-id subnet-094f06a9e81c23778 --map-public-ip-on-launch
```

Task 2.2: Creating a Private Subnet

1. Create the Private Subnet:



Task 3: Creating an Internet Gateway

1. Create the Internet Gateway:

```
┌──(root㉿kali)-[~]
└─# aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name
,Value=Lab IGW}]'

{
    "InternetGateway": {
        "Attachments": [],
        "InternetGatewayId": "igw-03222a7d8b12fd926",
        "OwnerId": "701951435345",
        "Tags": [
            {
                "Key": "Name",
                "Value": "Lab IGW"
            }
        ]
    }
}
```

2. Attach the Internet Gateway to the VPC: Get the Internet Gateway ID:

3. Attach the Internet Gateway to the VPC:

```
┌──(root㉿kali)-[~]
└─# aws ec2 describe-internet-gateways --filters "Name=tag:Name,Values=Lab IGW" --query 'InternetGatewa
ys[0].InternetGatewayId' --output text

igw-03222a7d8b12fd926

┌──(root㉿kali)-[~]
└─# aws ec2 attach-internet-gateway --vpc-id vpc-01dcc1827af9ef5af --internet-gateway-id igw-03222a7d8b
12fd926
```

Task 4: Configuring Route Tables

1. Create a Public Route Table:

```
┌──(root㉿kali)-[~]
└─# aws ec2 create-route-table --vpc-id vpc-01dcc1827af9ef5af --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public Route Table}]'

{
    "RouteTable": {
        "Associations": [],
        "PropagatingVgws": [],
        "RouteTableId": "rtb-05a5135d3a02ed2af",
        "Routes": [
            {
                "DestinationCidrBlock": "10.0.0.0/16",
                "GatewayId": "local",
                "Origin": "CreateRouteTable",
                "State": "active"
            }
        ],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Public Route Table"
            }
        ],
        "VpcId": "vpc-01dcc1827af9ef5af",
        "OwnerId": "701951435345"
    },
    "ClientToken": "132b3571-6c76-45f6-bfcc-8c0935e61bb0"
}
```

2. Add Route to Internet Gateway: Get the Route Table ID:

```
┌──(root㉿kali)-[~]
└─# aws ec2 describe-route-tables --filters "Name=tag:Name,Values=Public Route Table" --query 'RouteTables[0].RouteTableId' --output text

rtb-05a5135d3a02ed2af

┌──(root㉿kali)-[~]
└─# aws ec2 create-route --route-table-id rtb-05a5135d3a02ed2af --destination-cidr-block 0.0.0.0/0 --gateway-id igw-03222a7d8b12fd926

{
    "Return": true
}
```

3. Add a route to the Internet Gateway:

4. Associate Public Subnet with Public Route Table:
Associate the public subnet to the route table:


(root㉿kali)-[~]
aws ec2 associate-route-table --route-table-id rtb-05a5135d3a02ed2af --subnet-id subnet-094f06a9e81
c23778
{
"AssociationId": "rtbassoc-09576b1b8fa4f852b",
"AssociationState": {
"State": "associated"
}
}

Task 5: Creating a Security Group for the Application Server

1. Create a Security Group:

```
┌──(root㉿kali)-[~]
└─# aws ec2 create-security-group --group-name App-SG --description "Allow HTTP traffic" --vpc-id vpc-0
1dcc1827af9ef5af

{
    "GroupId": "sg-0ad65ec95b3c3e833"
}
```

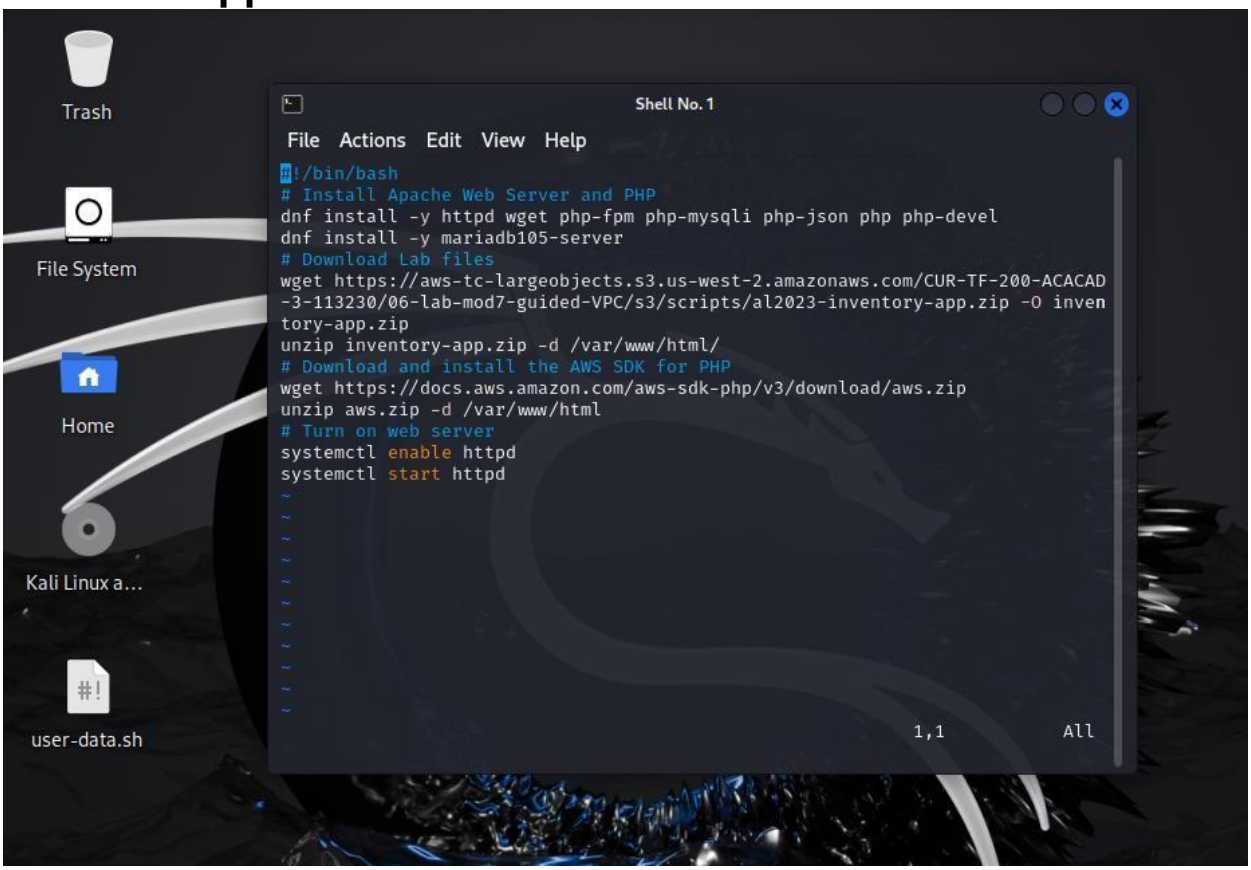
2. Allow HTTP (port 80) traffic: Get the Security Group ID:

3. Add the inbound rule for HTTP:

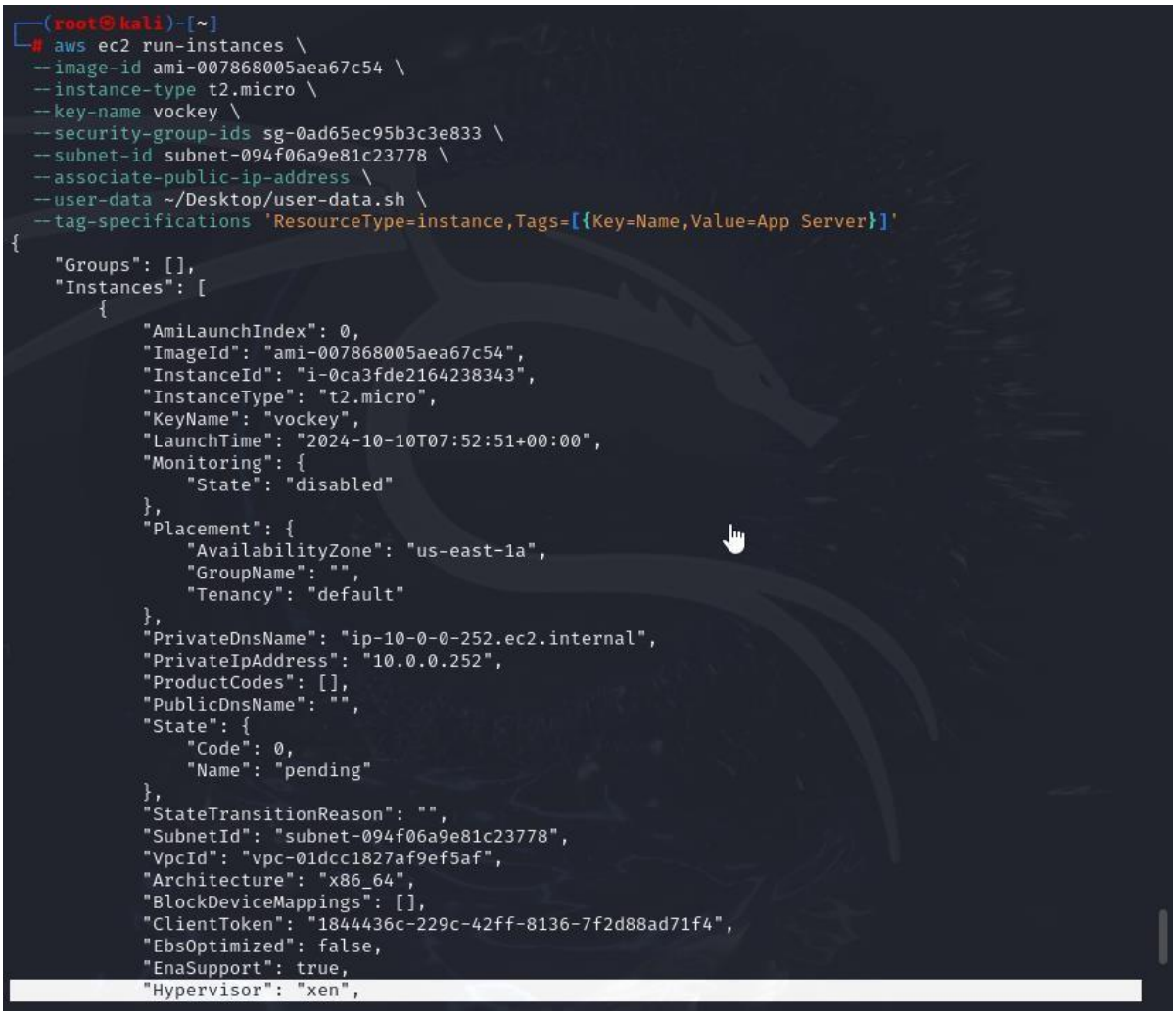
```
┌──(root㉿kali)-[~]
└─# aws ec2 describe-security-groups --filters "Name=group-name,Values=App-SG" --query 'SecurityGroups[
0].GroupId' --output text

sg-0ad65ec95b3c3e833

┌──(root㉿kali)-[~]
└─# aws ec2 authorize-security-group-ingress --group-id sg-0ad65ec95b3c3e833 --protocol tcp --port 80 -
-cidr 0.0.0.0/0

{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0d4e66c3cdd468003",
            "GroupId": "sg-0ad65ec95b3c3e833",
            "GroupOwnerId": "701951435345",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "CidrIpv4": "0.0.0.0/0"
        }
    ]
}
```

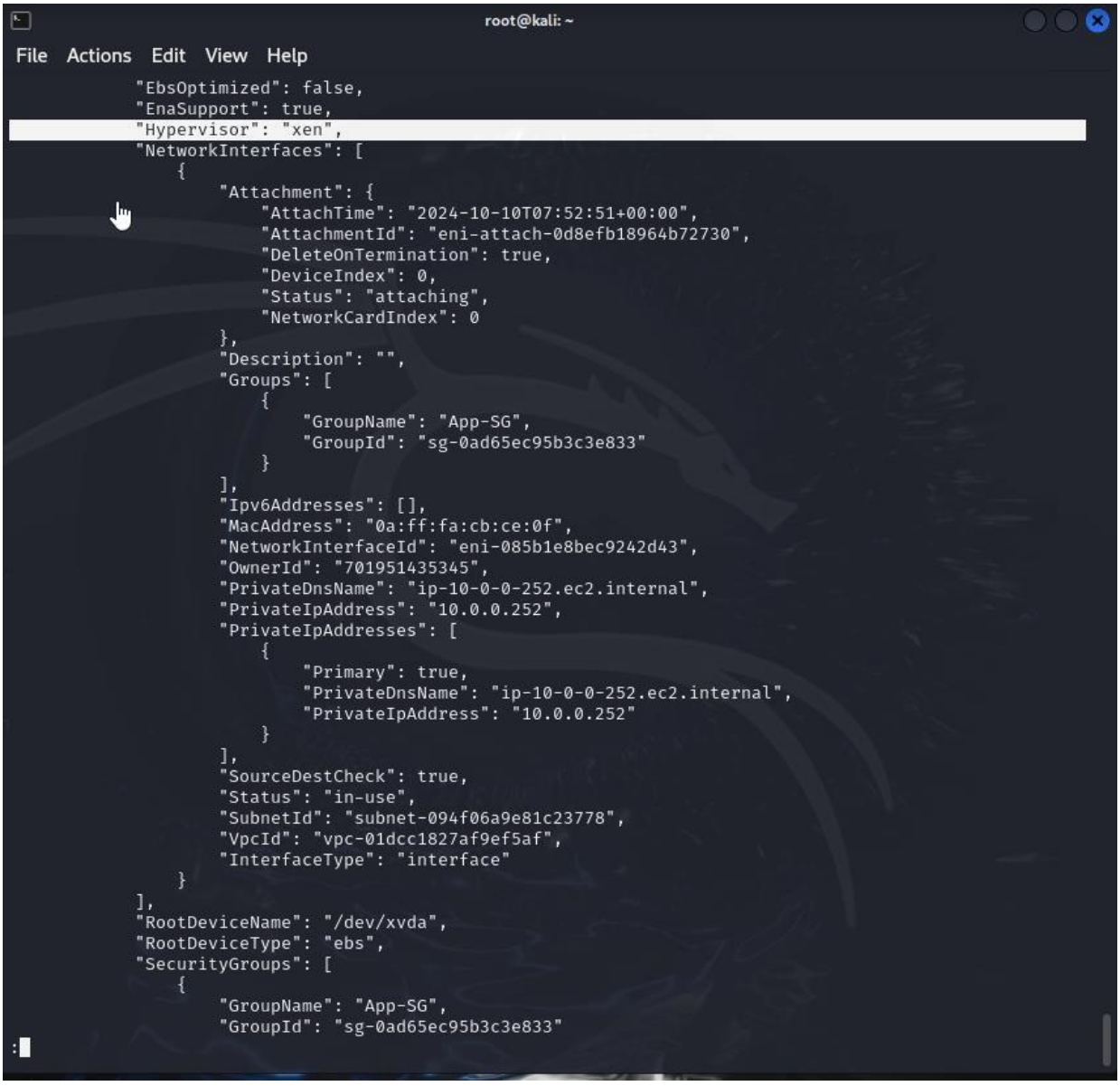
Task 6: Launching an Application Server in the Public Subnet

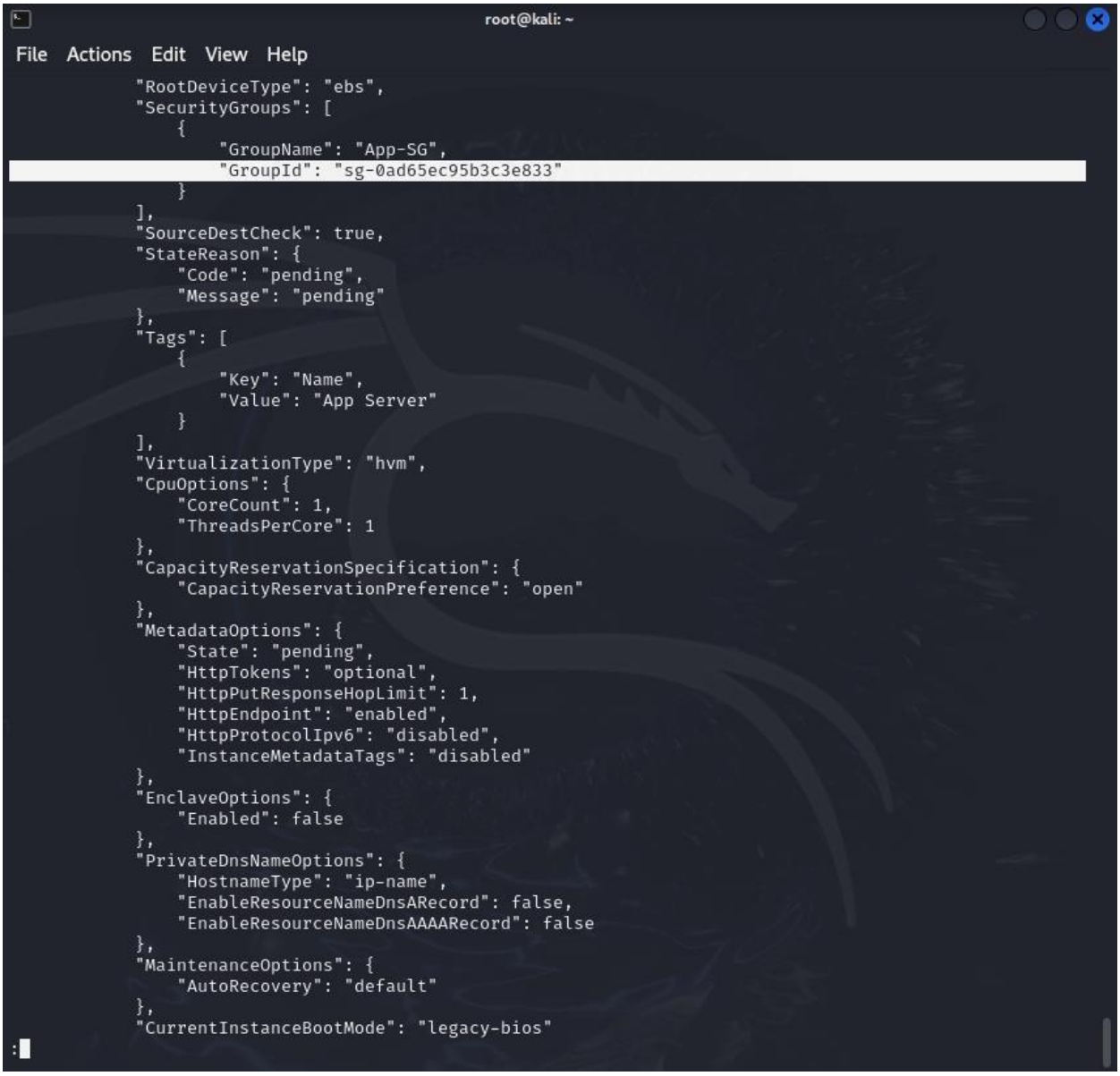
1. **Prepare User Data Script: Create a user-data.sh file that contains the script to install and configure the web application**

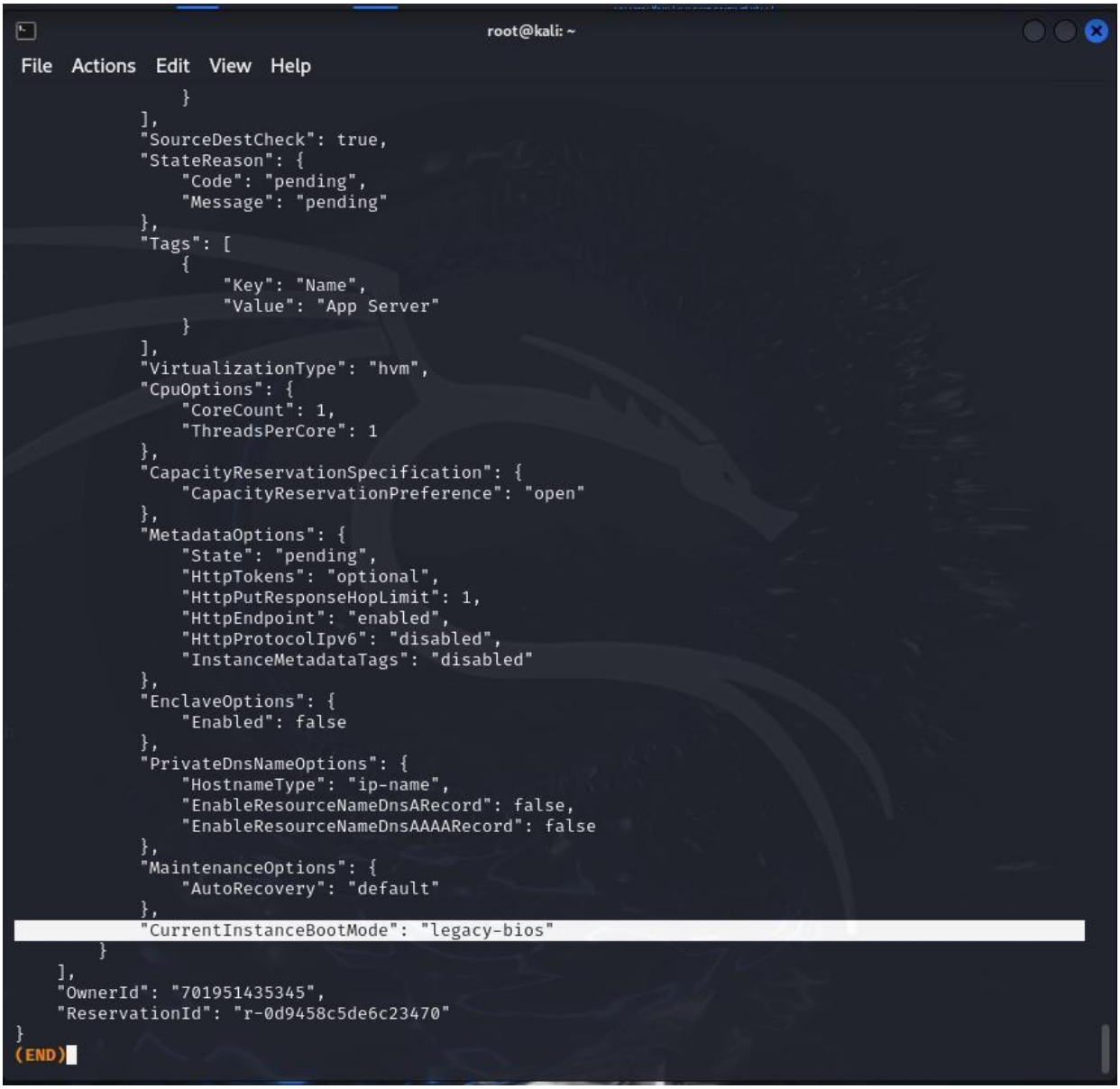


2. Launch EC2 Instance:

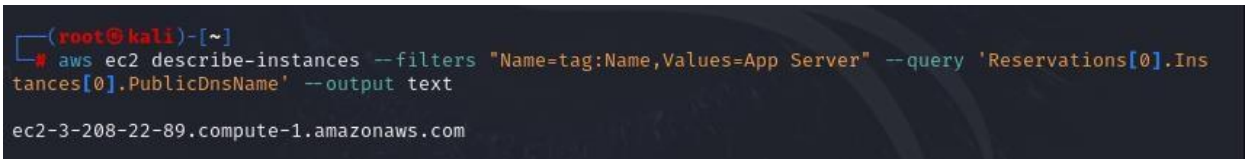



root@kali: ~
File Actions Edit View Help
"EbsOptimized": false,
"EnaSupport": true,
"Hypervisor": "xen",
"NetworkInterfaces": [
{
"Attachment": {
"AttachTime": "2024-10-10T07:52:51+00:00",
"AttachmentId": "eni-attach-0d8efb18964b72730",
"DeleteOnTermination": true,
"DeviceIndex": 0,
"Status": "attaching",
"NetworkCardIndex": 0
},
"Description": "",
"Groups": [
{
"GroupName": "App-SG",
"GroupId": "sg-0ad65ec95b3c3e833"
}
],
"Ipv6Addresses": [],
"MacAddress": "0a:ff:fa:cb:ce:0f",
"NetworkInterfaceId": "eni-085b1e8bec9242d43",
"OwnerId": "701951435345",
"PrivateDnsName": "ip-10-0-0-252.ec2.internal",
"PrivateIpAddress": "10.0.0.252",
"PrivateIpAddresses": [
{
"Primary": true,
"PrivateDnsName": "ip-10-0-0-252.ec2.internal",
"PrivateIpAddress": "10.0.0.252"
}
],
"SourceDestCheck": true,
"Status": "in-use",
"SubnetId": "subnet-094f06a9e81c23778",
"VpcId": "vpc-01dcc1827af9ef5af",
"InterfaceType": "interface"
}
],
"RootDeviceName": "/dev/xvda",
"RootDeviceType": "ebs",
"SecurityGroups": [
{
"GroupName": "App-SG",
"GroupId": "sg-0ad65ec95b3c3e833"
:


root@kali: ~
File Actions Edit View Help
"RootDeviceType": "ebs",
"SecurityGroups": [
{
"GroupName": "App-SG",
"GroupId": "sg-0ad65ec95b3c3e833"
}
],
"SourceDestCheck": true,
"StateReason": {
"Code": "pending",
"Message": "pending"
},
"Tags": [
{
"Key": "Name",
"Value": "App Server"
}
],
"VirtualizationType": "hvm",
"CpuOptions": {
"CoreCount": 1,
"ThreadsPerCore": 1
},
"CapacityReservationSpecification": {
"CapacityReservationPreference": "open"
},
"MetadataOptions": {
"State": "pending",
"HttpTokens": "optional",
"HttpPutResponseHopLimit": 1,
"HttpEndpoint": "enabled",
"HttpProtocolIpv6": "disabled",
"InstanceMetadataTags": "disabled"
},
"EnclaveOptions": {
"Enabled": false
},
"PrivateDnsNameOptions": {
"HostnameType": "ip-name",
"EnableResourceNameDnsARecord": false,
"EnableResourceNameDnsAAAARecord": false
},
"MaintenanceOptions": {
"AutoRecovery": "default"
},
"CurrentInstanceBootMode": "legacy-bios"
:


root@kali: ~
File Actions Edit View Help
}
],
"SourceDestCheck": true,
"StateReason": {
"Code": "pending",
"Message": "pending"
},
"Tags": [
{
"Key": "Name",
"Value": "App Server"
}
],
"VirtualizationType": "hvm",
"CpuOptions": {
"CoreCount": 1,
"ThreadsPerCore": 1
},
"CapacityReservationSpecification": {
"CapacityReservationPreference": "open"
},
"MetadataOptions": {
"State": "pending",
"HttpTokens": "optional",
"HttpPutResponseHopLimit": 1,
"HttpEndpoint": "enabled",
"HttpProtocolIpv6": "disabled",
"InstanceMetadataTags": "disabled"
},
"EnclaveOptions": {
"Enabled": false
},
"PrivateDnsNameOptions": {
"HostnameType": "ip-name",
"EnableResourceNameDnsARecord": false,
"EnableResourceNameDnsAAAARecord": false
},
"MaintenanceOptions": {
"AutoRecovery": "default"
},
"CurrentInstanceBootMode": "legacy-bios"
}
],
"OwnerId": "701951435345",
"ReservationId": "r-0d9458c5de6c23470"
}
(END)

3. **Validate Setup:**
   - **Get the public DNS of the instance:**



Project 14: Automating Infrastructure Deployment with AWS CloudFormation

---

Task 1: Deploying a Networking Layer

1. **Download and inspect** the lab-network.yaml CloudFormation template, which defines the VPC, subnets, and networking components.
2. **Deploy the template** by creating a new stack in AWS CloudFormation:
   - **Stack Name**: lab-network
   - **Template Source**: Upload the lab-network.yaml file.
   - **Tags**: Add a tag with Key=application and Value=inventory.
3. **Monitor** the stack creation process and review the resources created, including the VPC and public subnet.
4. **Inspect the Outputs** tab for resource IDs and explore how values are exported for use in other stacks.

The Code

bash
Copy code

```
#!/bin/bash

# Create lab-network stack
echo "Creating lab-network
stack..." aws cloudformation
create-stack \
--stack-name lab-network \
--template-body file://lab-network.yaml \
--tags Key=application,Value=inventory
```

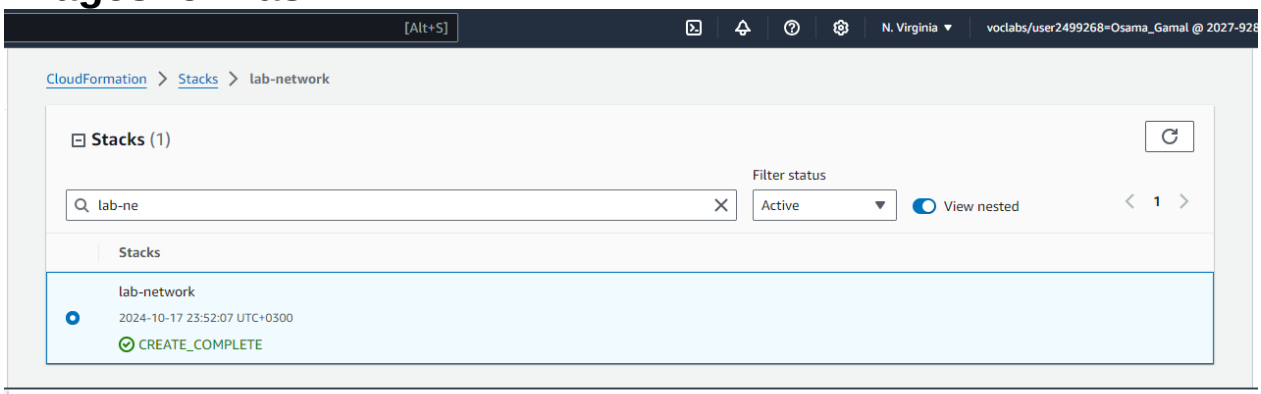
```
# Wait for lab-network stack creation to complete
echo "Waiting for lab-network stack creation to complete..."
aws cloudformation wait stack-create-complete --stack-name lab-network
```

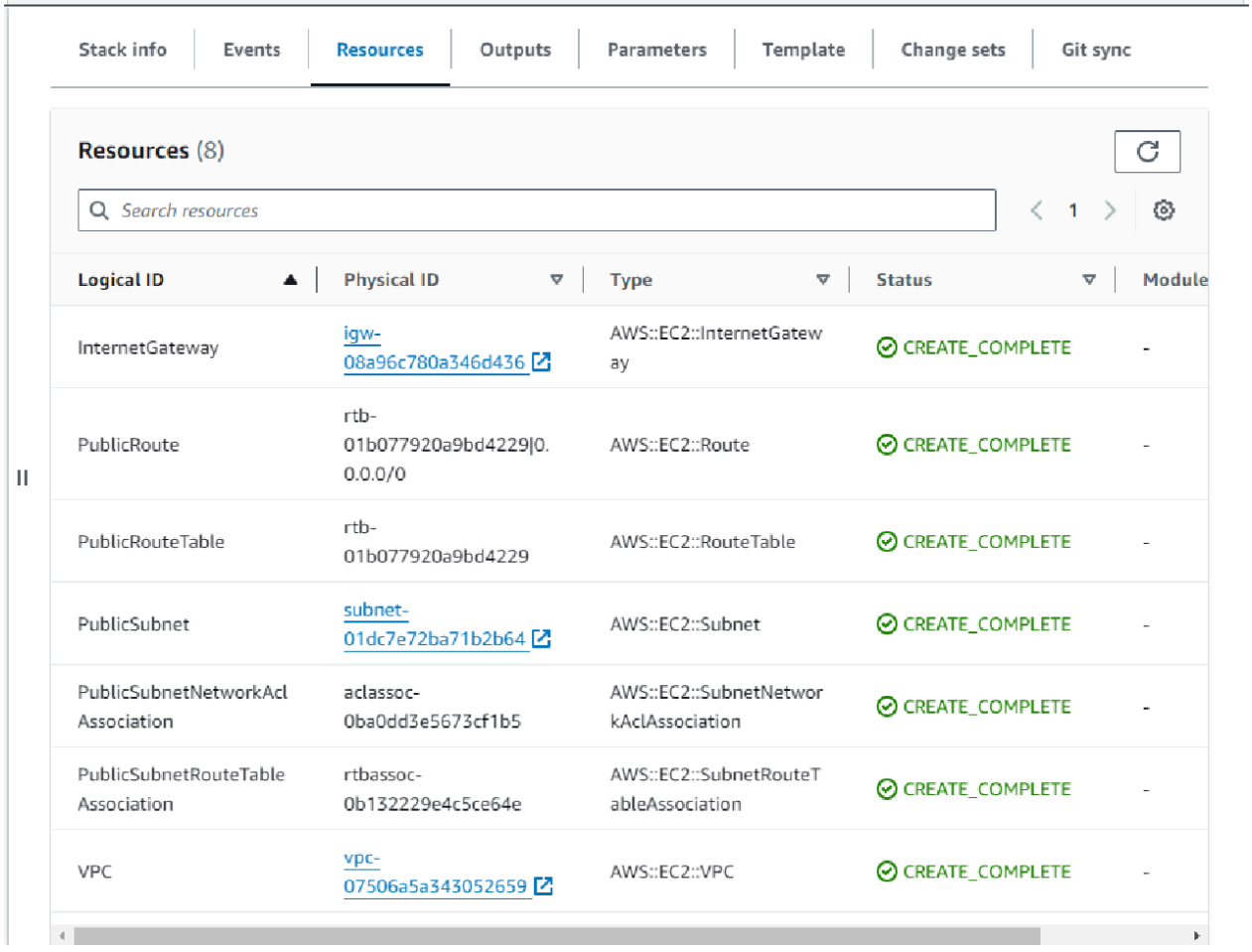
The Output

bash
Copy code

```
$ ./script.sh
Creating lab-network stack...
arn:aws:cloudformation:us-east-1:202792838471:stack/lab-network/abbed460- 8cc9-11ef-b978-0ee756e81a1d

Waiting for lab-network stack creation to complete... lab-network stack creation completed.
```

Images for Task 1:





Logical ID	Physical ID	Type	Status	Module
InternetGateway	igw-08a96c780a346d436	AWS::EC2::InternetGateway	CREATE_COMPLETE	-
PublicRoute	rtb-01b077920a9bd4229|0.0.0.0/0	AWS::EC2::Route	CREATE_COMPLETE	-
PublicRouteTable	rtb-01b077920a9bd4229	AWS::EC2::RouteTable	CREATE_COMPLETE	-
PublicSubnet	subnet-01dc7e72ba71b2b64	AWS::EC2::Subnet	CREATE_COMPLETE	-
PublicSubnetNetworkAclAssociation	aclassoc-0ba0dd3e5673cf1b5	AWS::EC2::SubnetNetworkAclAssociation	CREATE_COMPLETE	-
PublicSubnetRouteTableAssociation	rtbassoc-0b132229e4c5ce64e	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE	-
VPC	vpc-07506a5a343052659	AWS::EC2::VPC	CREATE_COMPLETE	-

Task 2: Deploying an Application Layer

1. **Download and inspect** the lab-application.yaml template, which sets up an EC2 instance and security group within the previously created VPC.

2. **Deploy the application layer** by creating a new stack:
    - **Stack Name**: lab-application
    - Ensure that the application stack references the lab-network stack to import VPC and subnet IDs.
3. **Verify the deployment** by accessing the Outputs tab, copying the URL, and testing the application in your browser.

The Code

bash
Copy code

```
#!/bin/bash

# Create lab-application stack
echo "Creating lab-application
stack..." aws cloudformation create-
stack \
--stack-name lab-application \
--template-body file://lab-application.yaml \
--parameters
ParameterKey=NetworkStackName,ParameterValue=lab-network \
--tags Key=application,Value=inventory

# Wait for lab-application stack creation to complete
echo "Waiting for lab-application stack creation to complete..."
aws cloudformation wait stack-create-complete --stack-name lab-
application echo "lab-application stack creation completed."

# Retrieve outputs for lab-application stack
echo "Retrieving outputs for lab-application stack..."
aws cloudformation describe-stacks --stack-name lab-
application --query 'Stacks[0].Outputs' --output table
```

The Output

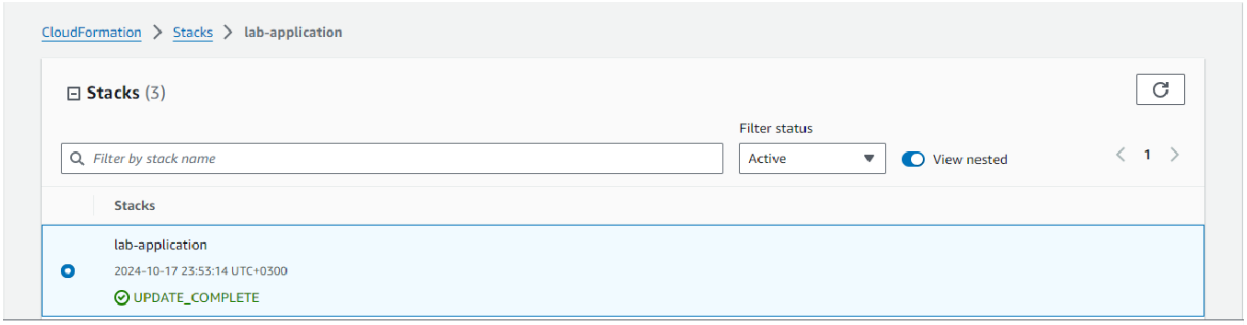
bash
Copy code

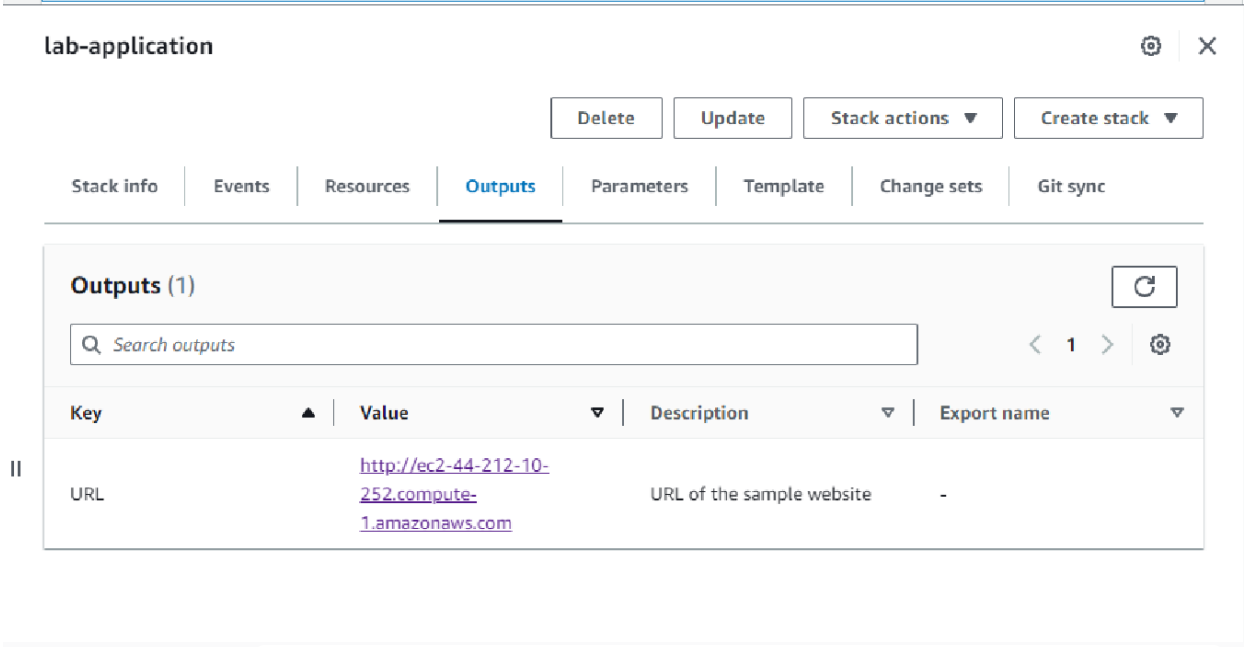
Creating lab-application stack...
arn:aws:cloudformation:us-east-1:202792838471:stack/lab-application/d3f5c830- 8cc9-11ef-94e1-0affe95ac3a5

Waiting for lab-application stack creation to complete... lab-application stack creation completed.
Retrieving outputs for lab-application stack...

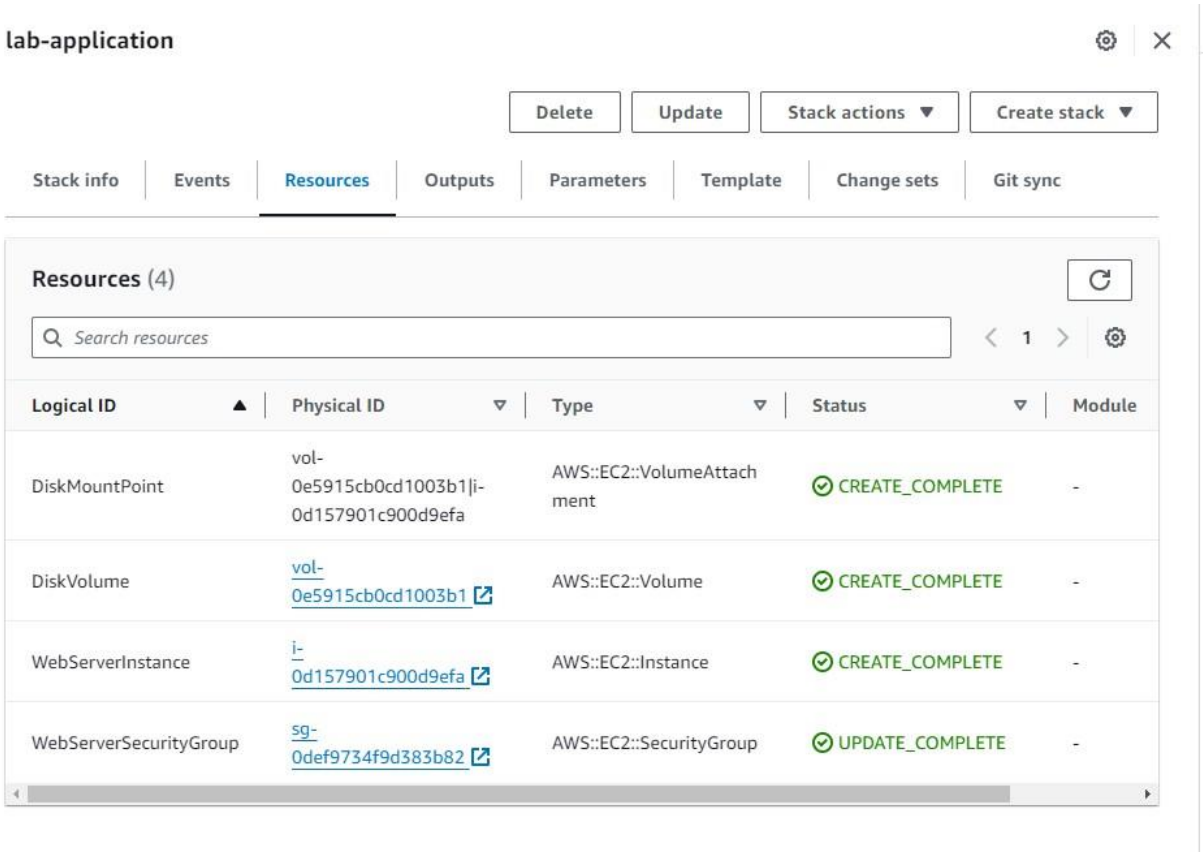
DescribeStacks	
Description	URL of the sample website
OutputKey	URL
OutputValue	http://ec2-44-212-10-252.compute-1.amazonaws.com

Images for Task 2:





Congratulations, you have successfully launched the AWS CloudFormation sample.



.

Task 3: Updating a Stack

1. **Download the updated** lab-application2.yaml template that adds HTTPS traffic permissions to the security group.
2. **Update the lab-application stack** using the new template to modify the security group without replacing it.
3. **Verify the changes** by inspecting the security group's inbound rules in the EC2 console.

The Code

bash
Copy code
#!/bin/bash

Create change set for updating the lab-application stack CHANGE_SET_NAME="lab-application-changeset-$(date +%s)"

echo "Creating change set for lab-application update..." aws cloudformation create-change-set \

```
--stack-name lab-application \
--template-body file://lab-application2.yaml \
--parameters
ParameterKey=NetworkStackName,ParameterValue=lab-network \
--tags Key=application,Value=inventory \
--change-set-name $CHANGE_SET_NAME \
--change-set-type UPDATE

# Wait for the change set creation to complete
echo "Waiting for the change set creation to
complete..." aws cloudformation wait change-
set-create-complete \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME
echo "Change set created: $CHANGE_SET_NAME"

# Display the details of the change set (resources that will be
updated) echo "Showing changes for the update..."
aws cloudformation describe-change-set \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME \
--query
'Changes[*].ResourceChange.{Action:Action,LogicalResourceId:Log
icalResourceId
,ResourceType:ResourceType,Replacement:Replacement}' \
--output table

# Confirm if the user wants to apply the change set
read -p "Do you want to execute the change set?
(yes/no): " choice if [ "$choice" == "yes" ]; then
# Execute the change set
echo "Executing the change set..."
aws cloudformation execute-change-set \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME

# Wait for lab-application stack update to complete
echo "Waiting for lab-application stack update to complete..."
aws cloudformation wait stack-update-complete --stack-name lab-
application echo "lab-application stack update completed."
else
echo "Change set not
executed." fi
```

The Output

bash
Copy code
Creating change set for lab-application update...
arn:aws:cloudformation:us-east-1:202792838471:changeSet/lab-application- changeset-1729198493/7ddf8425-2c94-4144-95fd-f599b7ab0406
arn:aws:cloudformation:us-east-1:202792838471:stack/lab-application/d3f5c830- 8cc9-11ef-94e1-0affe95ac3a5

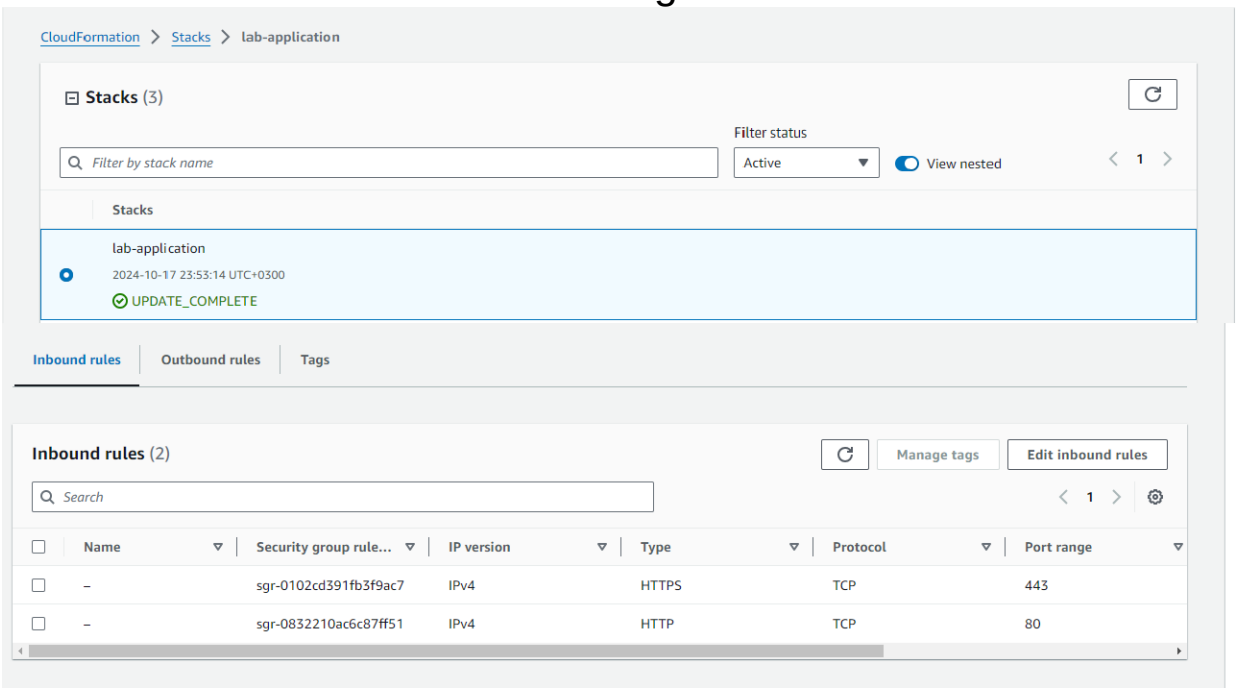
Waiting for the change set creation to complete... Change set created: lab-application-changeset-1729198493 Showing changes for the update...

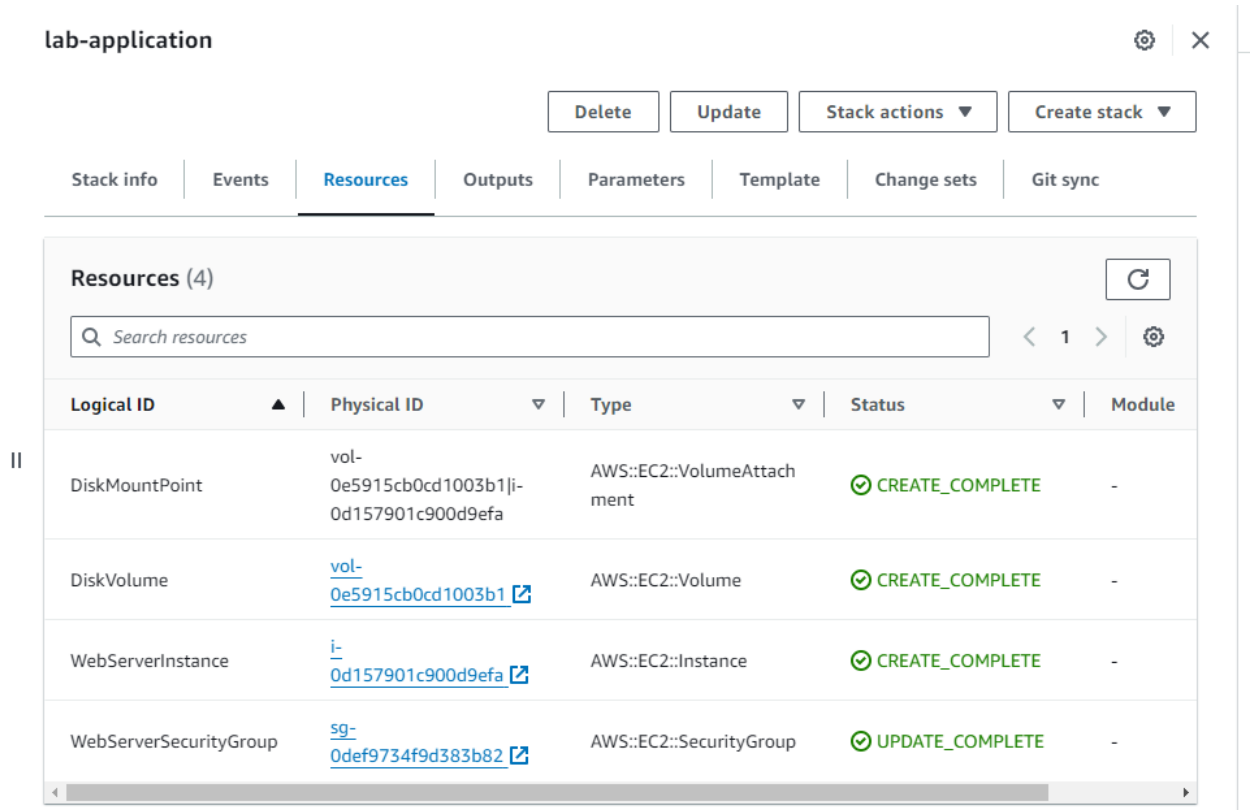
```
-----------------------------------------------------------------------------------------------
---
|                                    DescribeChangeSet
+----------+-----------------------------------+----------------+-------------------------------
--+
| Action |      LogicalResourceId| Replacement  |     ResourceType
|
+----------+-----------------------------------+----------------+-------------------------------
--+
|  Modify|  WebServerSecurityGroup  |  False  |
AWS::EC2::SecurityGroup
|
+----------+-----------------------------------+----------------+-------------------------------
--+
```

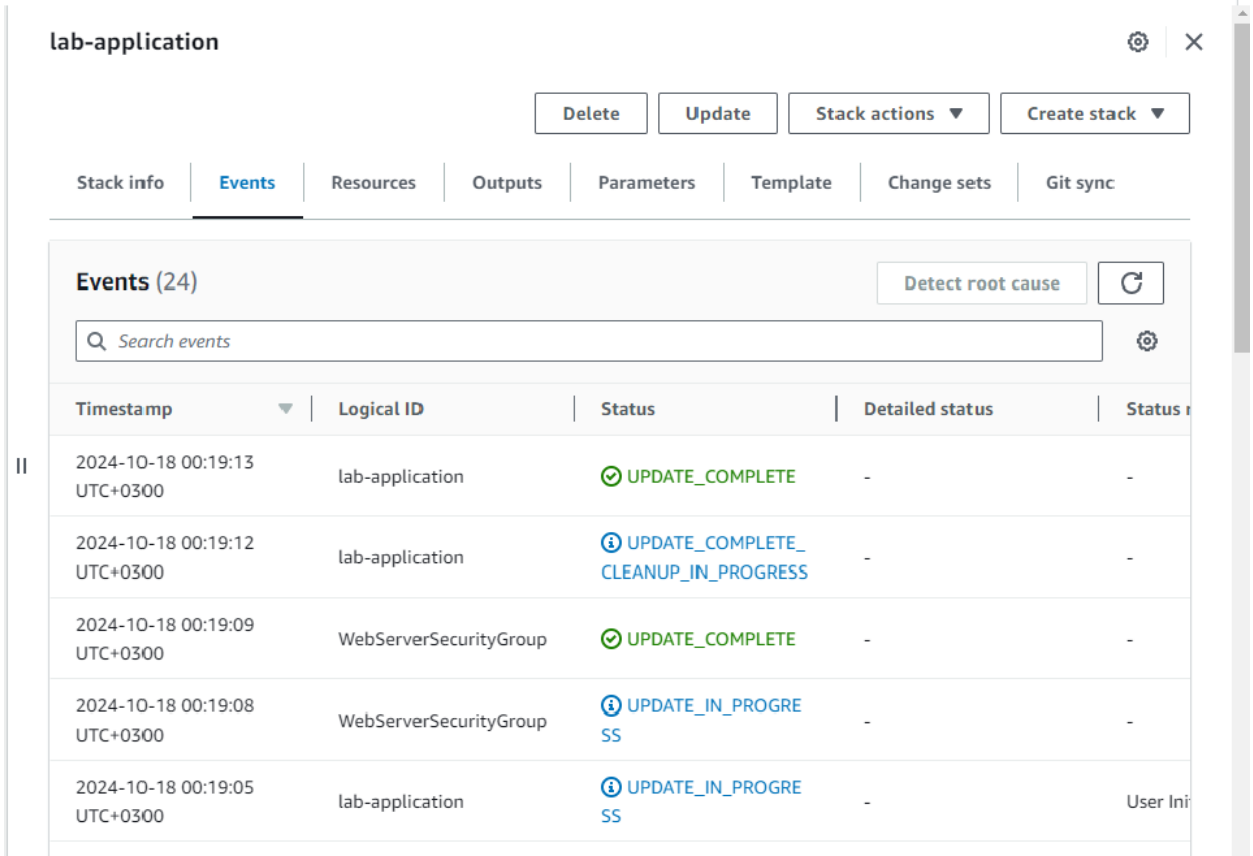
Do you want to execute the change set? (yes/no): yes Executing the change set... Waiting for lab-application stack update to complete... lab-application stack update completed.

Images for Task 3:

Include screenshots of the following for Task 3:



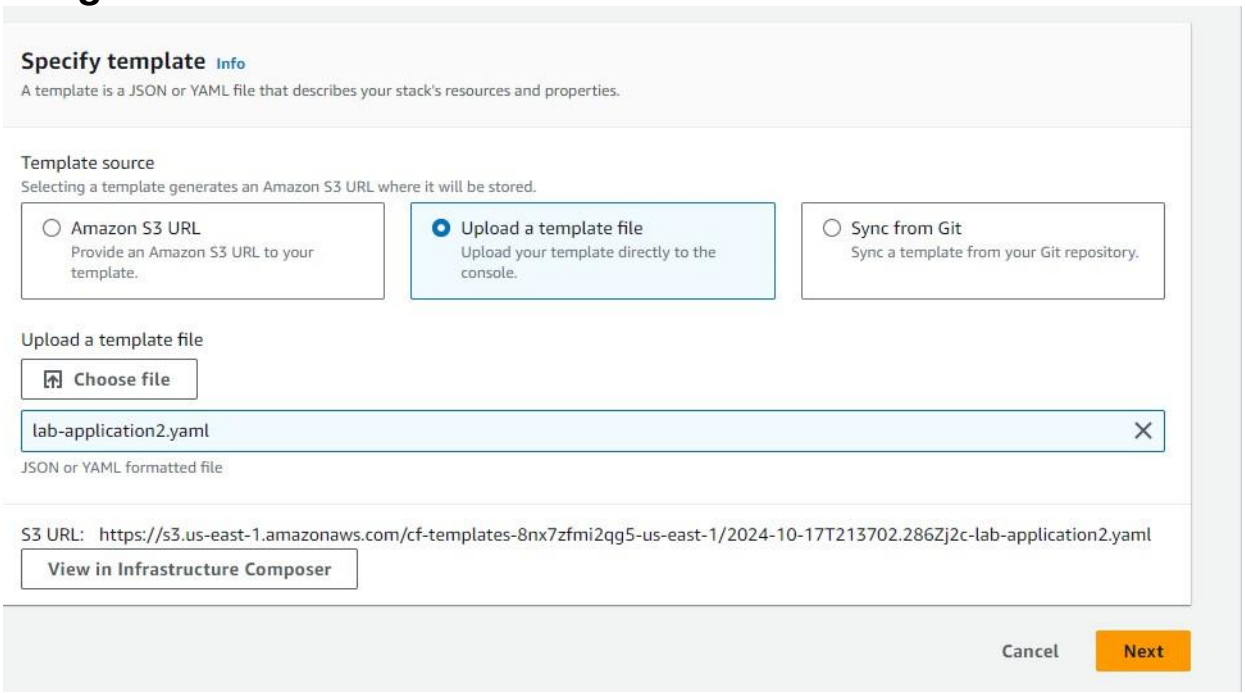

lab-application
Delete
Update
Stack actions
Create stack
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Git sync
Resources (4)
Search resources
1
Logical ID
Physical ID
Type
Status
Module
DiskMountPoint
vol-0e5915cb0cd1003b1|i-0d157901c900d9efa
AWS::EC2::VolumeAttachment
CREATE_COMPLETE
-
DiskVolume
vol-0e5915cb0cd1003b1
AWS::EC2::Volume
CREATE_COMPLETE
-
WebServerInstance
i-0d157901c900d9efa
AWS::EC2::Instance
CREATE_COMPLETE
-
WebServerSecurityGroup
sg-0def9734f9d383b82
AWS::EC2::SecurityGroup
UPDATE_COMPLETE
-

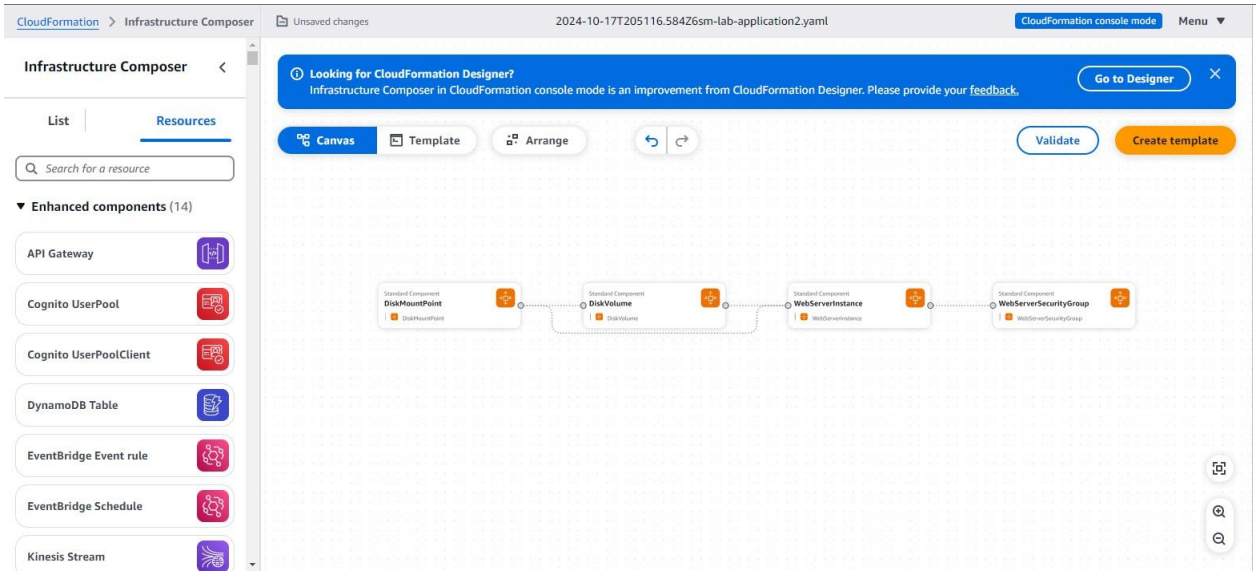

lab-application
Delete
Update
Stack actions
Create stack
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Git sync
Events (24)
Detect root cause
Search events
Timestamp
Logical ID
Status
Detailed status
2024-10-18 00:19:13 UTC+0300
lab-application
UPDATE_COMPLETE
-
-
2024-10-18 00:19:12 UTC+0300
lab-application
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS
-
-
2024-10-18 00:19:09 UTC+0300
WebServerSecurityGroup
UPDATE_COMPLETE
-
-
2024-10-18 00:19:08 UTC+0300
WebServerSecurityGroup
UPDATE_IN_PROGRESS
-
-
2024-10-18 00:19:05 UTC+0300
lab-application
UPDATE_IN_PROGRESS
-
User Ini

Task 4: Exploring Templates with AWS CloudFormation Designer

1. **Open the AWS CloudFormation Designer** tool to visualize and edit templates.
2. **Upload the lab-application2.yaml** template to explore its components and relationships.
3. **Experiment with adding new resources**, editing configurations, and connecting resources visually.

Images for Task 4:





Task 5: Deleting the Stack

1. **Delete the lab-application stack**, observing the deletion policy that creates a snapshot of the EBS volume before deletion.
2. **Verify the deletion process** in the Events tab and confirm that the EBS snapshot was created by checking the Snapshots section in the EC2 console.

The Code

bash
Copy code
#!/bin/bash

List resources that will be deleted from lab-application stack
echo "Listing resources that will be deleted with the lab-application stack..."
aws cloudformation list-stack-resources \
--stack-name lab-application \
--query

```
'StackResourceSummaries[*].{ResourceType:ResourceType,Logical
ResourceId:Logic
alResourceId,PhysicalResourceId:PhysicalResourceId}' \
--output table

# Confirm if the user wants to delete the lab-application stack
read -p "Do you want to delete the lab-application stack?
(yes/no): " delete_choice
if [ "$delete_choice" == "yes" ];
then # Delete lab-application
stack
echo "Deleting lab-application stack..."
```

```
aws cloudformation delete-stack --stack-name lab-application

# Wait for lab-application stack deletion to complete
echo "Waiting for lab-application stack deletion to complete..."
aws cloudformation wait stack-delete-complete --stack-name lab-
application echo "lab-application stack deleted successfully."
else
echo "Stack deletion
cancelled." fi
```

The Output

bash
Copy code

```
Listing resources that will be deleted with the lab-application stack...
-------------------------------------------------------------------------------------------------------------
-----------------------------------


|                                                ListStackResources
|
+---------------------------------+-------------------------------------------------------------------+-------
+---------------------------------
|       LogicalResourceId              |
        PhysicalResourceId             | ResourceType                 |
+---------------------------------+-------------------------------------------------------------------+-------
+---------------------------------
| DiskMountPoint       | vol-0f61f40b4888fd2f1|i-
031e8a3f8dd06be57  | AWS::EC2::VolumeAttachment |
| DiskVolume           | vol-0f61f40b4888fd2f1                     |
AWS::EC2::Volume       |
| WebServerInstance | i-031e8a3f8dd06be57                     |
AWS::EC2::Instance      |
| WebServerSecurityGroup| sg-0156ab497929174c6          |
AWS::EC2::SecurityGroup                                          |
+---------------------------------+-------------------------------------------------------------------+-------
+---------------------------------


Do you want to delete the lab-application stack? (yes/no):
yes Deleting lab-application stack...
Waiting for lab-application stack deletion to
complete... lab-application stack deleted
successfully.
```

Images for Task 5: Include screenshots of the following for Task 5: