

LAB – 5: Introduction to AWS IAM

Name:	Chaitanya Madhav R
SRN:	PES1UG20CS634
Section:	K

Deliverables:

1. user-1 added to the S3-Support Group.

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'User groups' selected under 'Access management'. The main content area shows the 'S3-Support' user group details. A green notification banner at the top states 'Users added to this group.' Below the group summary, the 'Users' tab is active, showing a table with one user: 'user-1'. The user's last activity is 'None' and it was added '5 minutes ago'. The console footer shows the date as 14-03-2023 and the time as 12:50.

User name	Groups	Last activity	Creation time
user-1	1	None	5 minutes ago

2. user-2 added to the EC2-Support Group.

The screenshot shows the AWS IAM console interface. A green notification banner at the top states "Users added to this group." The breadcrumb navigation indicates the path: IAM > User groups > EC2-Support. The main heading is "EC2-Support". Below it, a "Summary" section displays the following details:

Field	Value
User group name	EC2-Support
Creation time	March 14, 2023, 12:45 (UTC+05:30)
ARN	arn:aws:iam::773945764888:group/spi66/EC2-Support

Below the summary, there are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is active, showing "Users in this group (1)". A search bar is present. Below the search bar, a table lists the users in the group:

User name	Groups	Last activity	Creation time
user-2	1	None	5 minutes ago

The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The bottom of the screen shows a Windows taskbar with various application icons and system information.

3. user-3 added to the EC2-Support Group.

The screenshot shows the AWS IAM console interface. A green notification banner at the top states "Users added to this group." The breadcrumb navigation indicates the path: IAM > User groups > EC2-Admin. The main heading is "EC2-Admin". Below it, a "Summary" section displays the following details:

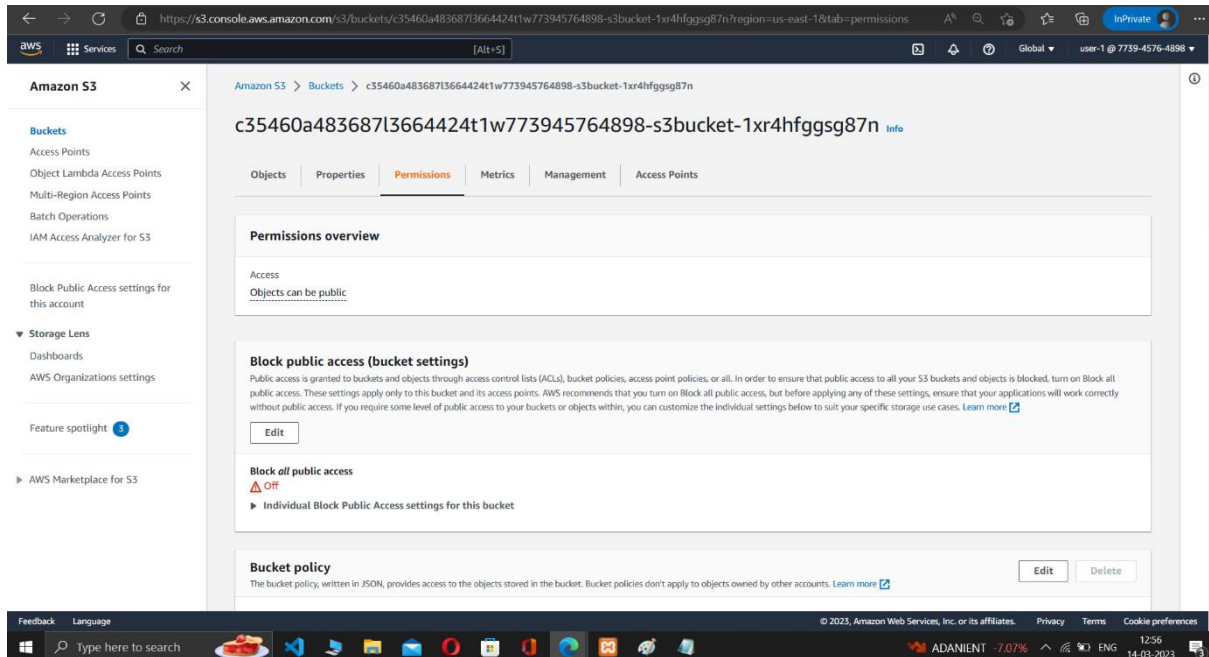
Field	Value
User group name	EC2-Admin
Creation time	March 14, 2023, 12:45 (UTC+05:30)
ARN	arn:aws:iam::773945764888:group/spi66/EC2-Admin

Below the summary, there are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is active, showing "Users in this group (1)". A search bar is present. Below the search bar, a table lists the users in the group:

User name	Groups	Last activity	Creation time
user-3	1	None	6 minutes ago

The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The bottom of the screen shows a Windows taskbar with various application icons and system information.

4. View S3 buckets with user-1 role



The screenshot shows the AWS S3 console interface. The left sidebar contains navigation links for Amazon S3 services, including Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, and AWS Marketplace for S3. The main content area displays the 'Permissions overview' for the bucket 'c35460a48368713664424t1w773945764898-s3bucket-1xr4hfggsg87n'. The 'Permissions overview' section includes a 'Block public access (bucket settings)' section with a 'Block all public access' toggle set to 'OFF' and an 'Individual Block Public Access settings for this bucket' link. Below this is a 'Bucket policy' section with an 'Edit' button. The bottom of the console shows the Windows taskbar with various application icons and the system clock.

Amazon S3 > Buckets > c35460a48368713664424t1w773945764898-s3bucket-1xr4hfggsg87n

c35460a48368713664424t1w773945764898-s3bucket-1xr4hfggsg87n

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
Objects can be public

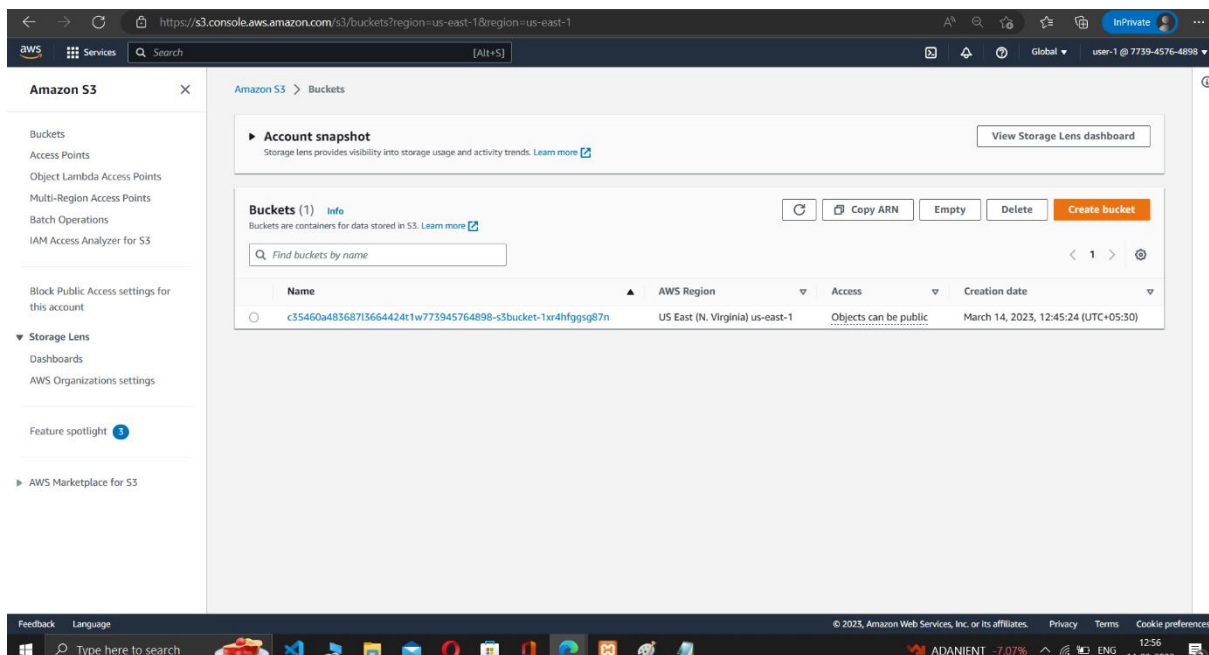
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings 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
OFF
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



The screenshot shows the AWS S3 console interface. The left sidebar contains navigation links for Amazon S3 services, including Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, and AWS Marketplace for S3. The main content area displays the 'Buckets (1)' section. It includes a search bar, a table of buckets, and a 'Create bucket' button. The table has columns for Name, AWS Region, Access, and Creation date. The bottom of the console shows the Windows taskbar with various application icons and the system clock.

Amazon S3 > Buckets

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

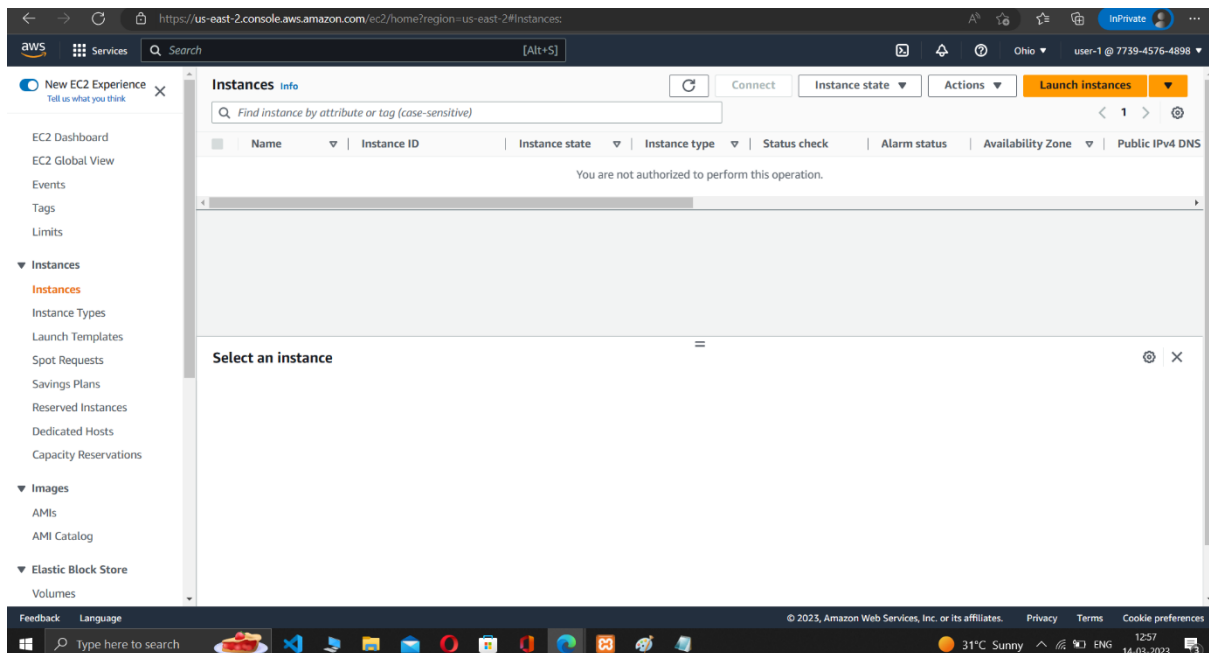
Buckets (1) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

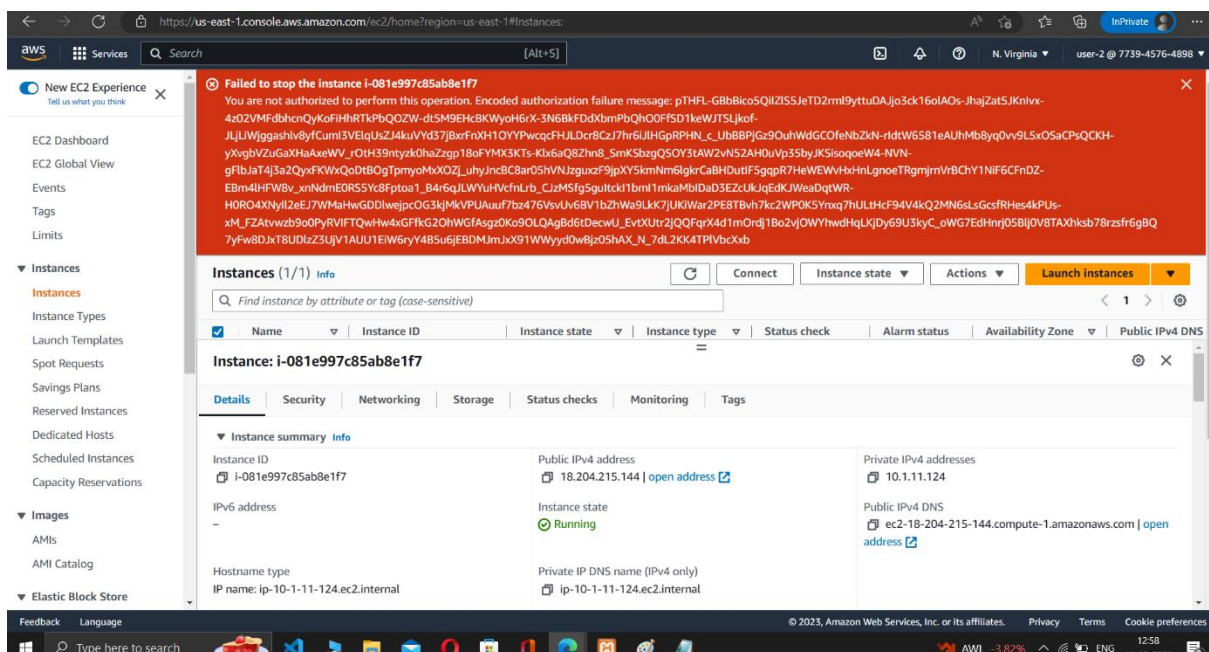
Name	AWS Region	Access	Creation date
c35460a48368713664424t1w773945764898-s3bucket-1xr4hfggsg87n	US East (N. Virginia) us-east-1	Objects can be public	March 14, 2023, 12:45:24 (UTC+05:30)

Create bucket

5. EC2 instance dashboard with user-1 role (Not authorized)



6. Failure message when instance stopped with user-2 role



7. Successful stoppage of E2 instance with user-3 role

The screenshot displays the AWS Management Console interface. At the top, a green banner indicates "Successfully stopped i-081e997c85ab8e1f7". The main content area shows the "Instances (1/1)" list with a single instance, i-081e997c85ab8e1f7, in the "Stopping" state. Below the list, the "Instance: i-081e997c85ab8e1f7" details are shown, including the "Instance summary" tab. The summary shows the instance is in the "Running" state, with a public IPv4 address of 18.204.215.144 and a private IP address of 10.1.11.124. The instance is running on the t2.micro instance type in the us-east-1a availability zone. The console also shows the "Launch instances" button and the "Connect" button. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The bottom of the console shows the Windows taskbar with the search bar and various application icons.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
-	i-081e997c85ab8e1f7	Stopping	t2.micro	2/2 checks passed	User: arn:aws:us-east-1a	ec2-18-204-215-	

Instance: i-081e997c85ab8e1f7

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID: i-081e997c85ab8e1f7

Public IPv4 address: 18.204.215.144 | open address

Private IPv4 addresses: 10.1.11.124

Instance state: Running

Public IPv4 DNS: ec2-18-204-215-144.compute-1.amazonaws.com | open address

Private IP DNS name (IPv4 only): ip-10-1-11-124.ec2.internal

IP name: ip-10-1-11-124.ec2.internal