

Name : Savani Ananth S  
Reg: 727721eucs137

Day 4

The screenshot displays the AWS Management Console interface, split into two panels. The top panel shows the 'Instances' page, and the bottom panel shows the 'Target groups' page.

**Top Panel: EC2 Instances**

A notification banner at the top states: "Successfully started i-0688cde7030bb40d2, i-0d7d61f42211c1204".

The 'Instances (2/7)' table lists the following instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
ec2instance1	i-0045a952b3d02fa3a	Terminated	t2.micro	-	No alarms	us-east-2a	-
ec2instance1	i-0688cde7030bb40d2	Running	t2.micro	-	No alarms	us-east-2a	ec2-18-191-234-
ec2instance2	i-0908084022fd4a3a4	Terminated	t2.micro	-	No alarms	us-east-2a	-
ec2instance1	i-0497642b4f82294a9	Terminated	t2.micro	-	No alarms	us-east-2a	-
ec2instance2	i-0d7d61f42211c1204	Running	t2.micro	-	No alarms	us-east-2b	ec2-3-128-254-2

The 'Monitoring' section shows four graphs: CPU utilization (%), Status check failed (any) (count), Status check failed (instance) (count), and Status check failed (system) (count). The CPU utilization graph shows a peak of 6.67%.

**Bottom Panel: EC2 Target Groups**

The 'Target groups (1)' table lists the following target group:

Name	ARN	Port	Protocol	Target type	Load balancer
ec2targets	arn:aws:elasticloadbalancing...	80	HTTP	Instance	ec2elb

The bottom panel also shows a '0 target groups selected' message.

Day 5

Name : Savani Ananth S  
Reg: 727721eucs137

The image shows two screenshots of the AWS Management Console. The top screenshot displays the 'Load balancers' page in the EC2 console for the us-east-2 region. It shows a single load balancer named 'ec2elb' with a state of 'Active'. The bottom screenshot shows the 'Security groups' page for the same region, specifically for the security group 'sg-03658f876439af967'. It displays details such as the security group name 'default', VPC ID 'vpc-0bda70f3ea0a82465', and inbound rules for HTTP on port 80.

**Load balancers (1)**  
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
ec2elb	ec2elb-1601512709.us-east-2.elb.amazonaws.com	Active	vpc-0bda70f3ea0a82465	3 Availability Zones	application	April 1, 2023 (UTC+05:30)

**0 load balancers selected**  
Select a load balancer above.

**sg-03658f876439af967 - default**

**Details**

Property	Value
Security group name	default
Security group ID	sg-03658f876439af967
Description	default VPC security group
VPC ID	vpc-0bda70f3ea0a82465
Owner	401782013484
Inbound rules count	1 Permission entry
Outbound rules count	1 Permission entry

**Inbound rules (1/1)**

IP version	Type	Protocol	Port range	Source	Description
-	HTTP	TCP	80	sg-03658f876439af967	-

Name : Savani Ananth S  
Reg: 727721eucs137

The screenshot displays the AWS Management Console interface. The top navigation bar shows the user is logged in as Savani Ananth S in the Singapore region. The left sidebar contains the navigation menu with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, 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, and Network & Security.

The main content area is divided into several sections:

- Resources:** A grid showing various Amazon EC2 resources in the Asia Pacific (Singapore) Region. Resources include Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. Most resources show an "API Error" status.
- Launch instance:** A section with a "Launch instance" button and a "Migrate a server" button. A note states: "Note: Your instances will launch in the Asia Pacific (Singapore) Region".
- Service health:** A section showing the status of the AWS service. It indicates that the service is "operating normally" in the Asia Pacific (Singapore) Region.
- Account attributes:** A section showing account settings and supported platforms. It includes links for EBS encryption, Zones, EC2 Serial Console, Default credit specification, and Console experiments.
- Explore AWS:** A section with a link to "10 Things You Can Do Today to Reduce AWS Costs".

The bottom section of the console shows the details of a specific EC2 instance, **i-079a814d92a3d06bc (day2server)**. The instance is in the "Running" state. The details are organized into tabs: Details, Security, Networking, Storage, Status checks, Monitoring, and Tags.

**Instance summary for i-079a814d92a3d06bc (day2server)**

- Instance ID: i-079a814d92a3d06bc (day2server)
- Public IPv4 address: 35.154.61.155 | [open address](#)
- Private IPv4 addresses: 172.31.46.147
- Public IPv4 DNS: ec2-35-154-61-155.ap-south-1.compute.amazonaws.com | [open address](#)
- Instance state: Running
- Private IP DNS name (IPv4 only): ip-172-31-46-147.ap-south-1.compute.internal
- Instance type: t2.micro
- VPC ID: vpc-08589d392401d95cb
- Subnet ID: subnet-0a9b179d38bcc9be8
- Auto-assigned IP address: 35.154.61.155 [Public IP]
- Hostname type: IP name: ip-172-31-46-147.ap-south-1.compute.internal
- Answer private resource DNS name: IPv4 (A)
- IAM Role: -
- IMDSv2: Optional

**Instance details**

- Platform: windows
- AMI ID: ami-06c2ec1ceac22e8d6
- Monitoring: disabled
- Platform details: Windows
- AMI name: Windows\_Server-2022-English-Full-Base-2023.04.12
- Termination protection: Disabled

Name : Savani Ananth S  
Reg: 727721eucs137

The image shows two screenshots of the AWS Management Console. The top screenshot displays the 'Storage' tab for an EC2 instance (t2.micro) in the ap-south-1 region. It shows details for the root device (sda1) and a list of block devices. The bottom screenshot shows the 'Upload succeeded' message in the S3 console, indicating that a file named 'index.html' (1.3 KB) has been successfully uploaded to the bucket 's3://hihello789/folder1/'.

**EC2 Instance Details (Storage Tab):**

- Answer private resource DNS name: IPv4 (A)
- Auto-assigned IP address: 15.207.86.159 [Public IP]
- IAM Role: -
- IMDSv2: Optional
- Instance type: t2.micro
- VPC ID: vpc-08589d392401d95cb
- Subnet ID: subnet-0a9b179d38bcc9be8
- Elastic IP addresses: -
- AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
- Auto Scaling Group name: -

**Root device details:**

- Root device name: /dev/sda1
- Root device type: EBS
- EBS optimization: disabled

**Block devices:**

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-07d2a5b0ec0757d73	/dev/sda1	35	Attaching	2023/04/17 15:08 GMT+5:30	No	-

**Recent root volume replacement tasks:**

Filter tasks
Replace root volume

**S3 Upload Status:**

Upload succeeded  
View details below.

The information below will no longer be available after you navigate away from this page.

**Summary**

Destination	Succeeded	Failed
s3://hihello789/folder1/	1 file, 1.3 KB (100.00%)	0 files, 0 B (0%)

**Files and folders (1 Total, 1.3 KB)**

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	1.3 KB	Succeeded	-

Name : Savani Ananth S  
Reg: 727721eucs137

The image displays two sequential screenshots of the AWS S3 console interface, showing the configuration of the 'hihello789' bucket.

**Top Screenshot: Permissions Overview**

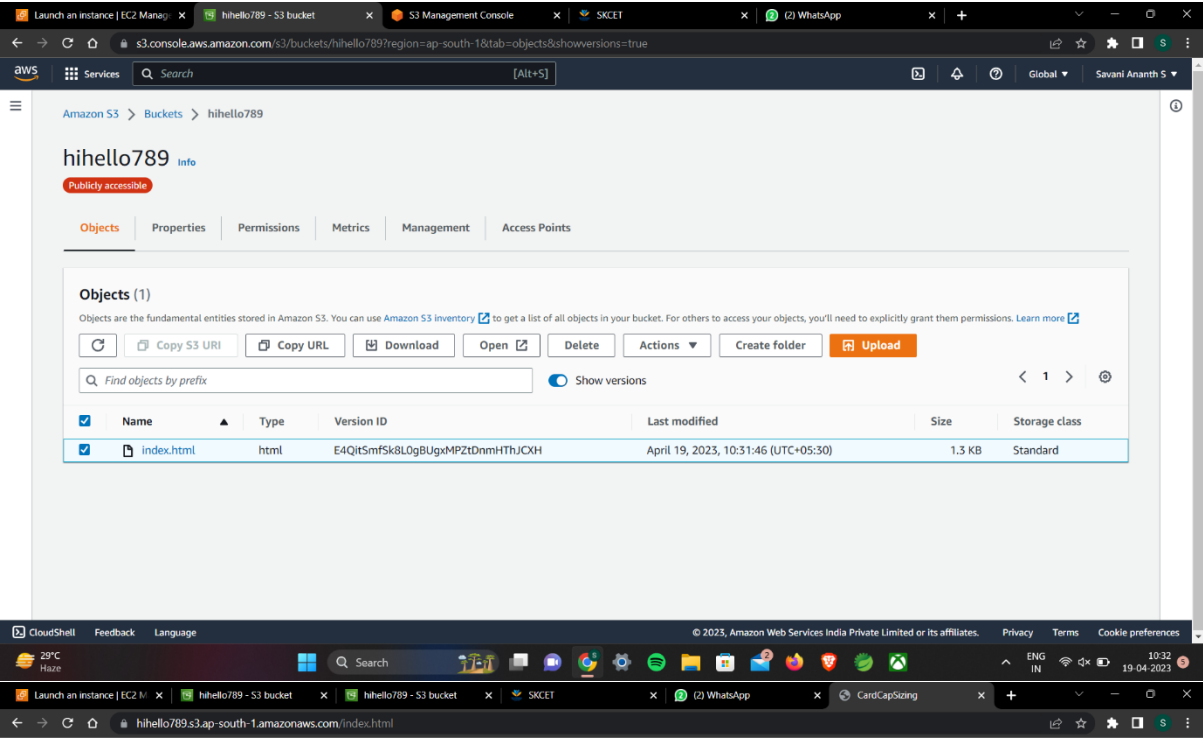
- Page Title:** Amazon S3 > Buckets > hihello789
- Navigation:** Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens (Dashboards, AWS Organizations settings), Feature spotlight, AWS Marketplace for S3.
- 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](#)
- Block all public access:** ☐ Off. Individual Block Public Access settings for this bucket.

**Bottom Screenshot: Bucket Policy**

- Page Title:** Amazon S3 > Buckets > hihello789
- Navigation:** Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens (Dashboards, AWS Organizations settings), Feature spotlight, AWS Marketplace for S3.
- 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](#)
- Policy JSON:**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::hihello789/*"
    }
  ]
}
```

Name : Savani Ananth S  
Reg: 727721eucs137



My Favourite Pokemon Character



Bulbasaur

Bulbasaur is a Grass/Poison type Pokémon introduced in Generation 1. It is known as the Seed Pokémon, Some powerful moves are Vine Whip and Razor Blade, it is one of the OG.

Height

0.7 m (2'04")

Weight

Unknown

Gender

Unknown

Category

Grass



Name : Savani Ananth S  
Reg: 727721eucs137

day 3

Amazon S3 > Buckets > hihello789 > Lifecycle configuration

## Lifecycle configuration [info](#)

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

**Lifecycle rules (1)**  
Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

[Refresh](#) [View details](#) [Edit](#) [Delete](#) [Actions](#) [Create lifecycle rule](#)

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
ggggg	Enabled	Filtered	Transition to Standard-IA	Transition to Standard-IA	-	-

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 31°C Haze Search 10:37 19-04-2023

Name : Savani Ananth S  
Reg: 727721eucs137

The image shows two screenshots of the AWS IAM console interface. The top screenshot displays the 'User groups' page with a green notification banner stating 'S3-Admins user group created.' and a 'View group' button. The bottom screenshot shows the 'S3-Admins' group details page, including a 'Summary' section with fields for 'User group name', 'Creation time', and 'ARN', and a 'Users' section showing one user, 'S3Admin1'.

**Top Screenshot: User groups page**

Notification: S3-Admins user group created. [View group]

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

User groups (1) info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
S3-Admins	Loading	Defined	Now

**Bottom Screenshot: S3-Admins group details**

Summary

User group name: S3-Admins

Creation time: April 19, 2023, 11:21 (UTC+05:30)

ARN: arn:aws:iam::666329062511:group/S3-Admins

Users | Permissions | Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

User name	Groups	Last activity	Creation time
S3Admin1	1	None	1 minute ago



Name : Savani Ananth S  
Reg: 727721eucs137

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Account settings. The main content area displays the 'S3-Admins' user group details. The 'Permissions' tab is selected, showing a list of permissions policies. The table lists two policies: 'AmazonS3FullAccess' (AWS managed) and 'topg' (Customer inline). The 'topg' policy is highlighted, and its details are shown below the table.

**S3-Admins**

**Summary**

User group name: S3-Admins  
Creation time: April 19, 2023, 11:21 (UTC+05:30)  
ARN: arn:aws:iam::666329062511:group/S3-Admins

**Permissions policies (2)**

Policy name	Type	Description
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via
topg	Customer inline	

**topg**

Copy Edit

day2

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu. The main content area displays the 's3fullaccess' role details. The 'Permissions' tab is selected, showing a list of permissions policies. The table lists one policy: 'AmazonS3FullAccess' (AWS managed). The 'AmazonS3FullAccess' policy is highlighted, and its details are shown below the table.

**s3fullaccess**

**Summary**

Creation date: April 19, 2023, 11:37 (UTC+05:30)  
ARN: arn:aws:iam::666329062511:role/s3fullaccess  
Instance profile ARN: arn:aws:iam::666329062511:instance-profile/s3fullaccess

**Permissions policies (1)**

Policy name	Type	Description
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management C...

Name : Savani Ananth S  
Reg: 727721eucs137

The screenshot displays the AWS IAM console interface. The top navigation bar shows the user is logged in as 'Savani Ananth S' in the 'us-east-1' region. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Credential report. The main content area shows the details for the user 'S3Admin1'. A green notification banner at the top states 'MFA device assigned'. Below this, the user's summary is shown, including their ARN, console access status, and creation date. The 'Permissions' tab is selected, showing three policies. A second screenshot below shows the 'Account settings' page, where the 'Password policy' is configured with requirements for minimum length, strength, and expiration. The 'Security Token Service (STS)' section is also visible.

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings

Credential report

Organization activity

Service control policies (SCPs)

**MFA device assigned**

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

IAM > Users > S3Admin1

**S3Admin1** [Delete]

**Summary**

ARN arn:aws:iam::666329062511:user/S3Admin1	Console access Enabled with MFA	Access key 1 Not enabled
Created April 19, 2023, 11:23 (UTC+05:30)	Last console sign-in Never	Access key 2 Not enabled

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

**Permissions policies (3)**

Permissions are defined by policies attached to the user directly or through groups.

[Refresh] [Remove] [Add permissions]

**Account settings** Info

**Password policy** Info

Configure the password requirements for the IAM users.

[Edit]

This AWS account uses the following custom password policy:

Password minimum length 8 characters	Other requirements • Never expire password
Password strength • Require at least one uppercase letter from the Latin alphabet (A-Z) • Require at least one lowercase letter from the Latin alphabet (a-z)	

**Security Token Service (STS)** Info

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

Session Tokens from the STS endpoints